ISRAEL JOURNAL OF MATHEMATICS, Vol. 70, No. 3, 1990

THE NILPOTENCY CLASS OF THE UNIT GROUP OF A MODULAR GROUP ALGEBRA II

BY

AVINOAM MANN AND ANER SHALEV†

Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel

ABSTRACT

Let G be a finite p-group, and let $U(G)$ be the group of units of the group algebra FG, where F is a field of characteristic p. It is shown that, if the commutative subgroup of G has order at least p^2, then the nilpotency class of $U(G)$ is at least $2p-1$.

Let G be a finite p-group, let K be the field of p elements, let $\Delta(G)$ be the augmentation ideal of the group algebra KG, and let $U(G) = 1 + \Delta(G)$ be the group of normalised units of KG. Then $U(G)$ is also a finite p-group. If G is not abelian, it is shown in [CP] that $U(G)$ involves the wreath product C_p wr C_p. It follows that the nilpotency class, cl $U(G)$, of $U(G)$ is at least p. It is known that cl $U(G)$ is exactly p if $|G'| = p$ [Ba], and R. Sandling conjectured that this is the only case [Sa]. In this paper we verify this conjecture, and indeed we prove

THEOREM A. *With the above notations, if* $|G'| > p$, *then* cl $U(G) \geqq 2p-1$.

The case $p = 2$ follows easily from a result of H. Laue (see below), so we are mostly interested in an odd p. In this case the second author has recently shown that, if G' is cyclic, then $U(G)$ involves C_p wr G', and hence deduced that cl $U(G) = |G'|$ under these circumstances (these results hold also for

† The authors are grateful to the Dipartimento di Matematica of the Universita di Trento, and to the Mathematical Institute of the University of Oxford, for their hospitality while this paper was being written. Then are also grateful to Robert Sandling, for communication of results, and problems, prior to publication.

Received January 16, 1990

$p = 2$, provided some extra conditions are satisfied) [Sh]. This implies that if G is a minimal counter example to Theorem A, then G' is elementary abelian of order p^2. Moreover, each proper section of G has a commutator subgroup of order p or 1. We first describe the structure of this type of p-groups. This then enables us to apply the methods of [Sh] to complete the proof. Indeed, in some cases these methods tell us more about the structure of $U(G)$.

THEOREM B. *Let G be a p-group of class two (p odd), with a non-cyclic commutator subgroup. Then $U(G)$ involves the wreath product* $C_p \operatorname{wr} (C_p \times C_p)$.

It would be interesting to know if the restrictions on p and on the class of G are really necessary. The previous results imply

COROLLARY C. *If G is a p-group of class two, and G' is elementary abelian of order p^2, then* $\operatorname{cl} U(G) = 2p - 1$.

The notation is mostly standard. We use $d(G)$ for the minimal number of generators of G, and G^p and $E(G)$ for the subgroups generated by all pth powers and by all elements of order p, respectively.

1. NC-critical groups

Let G be a p-group in which $|G'| > p$. Trying to prove Theorem A by induction, we may suppose that each proper section of G has a commutator subgroup of order 1 or p. Let N be a normal subgroup of G, contained in G', such that $|G' : N| = p^2$. Then G/N cannot be a proper section of G, and thus $N = 1$, and $|G'| = p^2$. If G' is cyclic, and $p > 2$, then [Sh] shows that $\operatorname{cl} U = p^2$. Since we are mostly interested in an odd p anyway, we will assume that G' is elementary abelian. If $p = 2$, we find it convenient to assume also that $\operatorname{cl} G = 2$.

DEFINITION. A p-group G is *NC-critical*, if G' is elementary abelian of order p^2, and each proper section of G is either abelian or has a derived subgroup of order p. If $p = 2$, we require also that G is of class two.

We are now going to describe the structure of such groups.

PROPOSITION 1. *Let G be an NC-critical p-group. Then*

(1) $G^p \subseteq Z(G) \subseteq \Phi(G)$, $|G : \Phi(G)| \leqq p^3$, *and either* $|\Phi(G) : G^p| \leqq p$, *or G has exponent p and order p^4 or p^5.*

(2) *All elements of order p in $Z(G)$ belong to G'.*

PROOF. If z is a central element of order p which does not lie in G', then $G/\langle z \rangle$ is a proper section of G whose commutator subgroup is isomorphic to G', which contradicts our assumptions. Similarly, if H is a maximal subgroup not containing $Z(G)$, then $G = HZ(G)$, so $G' = H'$, another contradiction.

If all elements of G have at most p conjugates, then $|G'| \leqq p$ [Kn]. Let x be an element with more than p conjugates. As all these conjugates belong to xG', there are exactly p^2 of them, and all elements of G' are commutators in x. If $[x, y]$ and $[x, z]$ generate G', and $H = \langle x, y, z \rangle$, then $H' = G'$, so $G = H$, $d(G) \leqq 3$, and $|G : \Phi(G)| \leqq p^3$.

Obviously, cl $G \leqq 3$. If cl $G = 2$, then G satisfies $[a^p, b] = [a, b]^p = 1$, and thus pth powers are central. Suppose cl $G = 3$. Then p is odd. The subgroup $\langle a, a^b \rangle = \langle a, [a, b] \rangle$ has class two, and so

$$(a^b)^p = (a[a, b])^p = a^p[a, b]^p[a, b, a]^{1/2p(p-1)} = a^p,$$

and again $G^p \subseteq Z(G)$.

Finally, if $G^p \neq 1$, it intersects G' non-trivially, by the first paragraph, and therefore $|\Phi(G) : G^p| < |G'|$, hence this index is not more than p. If G has exponent p, then $|\Phi(G)| = |G'| = p^2$, so $|G| \leqq p^5$.

We now discuss separately the groups of class two and three.

PROPOSITION 2. *Let G be an NC-critical group of class two. Then*

(1) *$Z(G) = \Phi(G)$ is a direct product of two non-identity cyclic subgroups, $G' = E(Z(G))$, and $|G : Z(G)| = p^3$.*

(2) *G contains an abelian maximal subgroup, which is unique.*

PROOF. The first equality follows from Proposition 1(1) and from $G' \subseteq Z(G)$. Since $|G : Z(G)| = p^2$ implies that $|G'| = p$, Proposition 1.1 implies also that $|G : Z(G)| = p^3$. Proposition 1(2) shows that $G' = E(Z(G))$, which implies the statement on the structure of $Z(G)$.

Let N be a normal subgroup of G of order p. Then $(G/N)' = p$, hence $|G/N : Z(G/N)| = p^{2k}$, for some k, and $k = 1$ is the only possibility. Thus there exists some element $z \notin Z(G)$, which is central (mod N). That means that z has exactly p conjugates, namely the elements of zN. Write $M = C_G(z)$. Then $|G : M| = p$. Since both $Z(G)$ and z are in $Z(M)$, we have $|M : Z(M)| \leqq p$, and thus M is an abelian subgroup of index p. Finally, if K is another abelian maximal subgroup, then $K \cap M \subseteq Z(G)$, contradicting $|G : Z(G)| = p^3$.

Proposition 3. *Let G be an NC-critical group of class two, and let M be its abelian maximal subgroup. Then $2 \leqq d(M) \leqq 4$. Moreover*

(1) *If $d(M) = 2$, then M is the direct product of two cyclic subgroups of order greater than p, say $M = \langle y \rangle \times \langle z \rangle$. If x is any element of $G - M$, then $[x, y] = u$, $[x, z] = v$, where u and v are independent generators of G'. If $p > 2$, we can choose x so that $x^p = 1$.*

(2) *If $d(M) = 4$, then either $\exp G = p$ and $|G| = p^5$, or there exist elements x, y, z, u, such that $G = \langle x, y, z \rangle$, $M = \langle x^p \rangle \times \langle y \rangle \times \langle z \rangle \times \langle u \rangle$, $[x, y] = u$, $[x, z] = x^{p^n}$, where x has order p^{n+1}.*

Proof. We know that $|M : Z(G)| = p^2$, and $d(Z(G)) = 2$, yielding the inequalities.

Suppose that $d(M) = 2$. Then $|G : \Phi(M)| = p^3 = |G : \Phi(G)|$, and so $\Phi(G) = \Phi(M) = M^p$. Then $G' \subseteq M^p$, and thus M^p is not cyclic, and M is the direct product of two cyclic subgroups of order greater than p. Let x be an element of $G - M$. Then, writing $M = \langle y \rangle \times \langle z \rangle$, we have

$$G = \langle x, y, z \rangle, \qquad G' = \langle [x, y], [x, z], [y, z] \rangle,$$

and here $[y, z] = 1$ and G' is generated by $[x, y]$ and $[x, z]$. Moreover, $x^p = b^p$, for some element $b \in M$, so if p is odd, then $(xb^{-1})^p = 1$, and we can replace x by xb^{-1}.

Now let $d(M) = 4$. Then M contains an elementary abelian subgroup E of order p^4, which is normal in G. Let x be any element outside M. Then $Z(G) = C_M(x)$, so $C_E(x) = E \cap Z(G) = G'$. It follows that $|[E, x]| = p^2$, and thus $|H'| = p^2$, where $H = \langle x, E \rangle$. The minimality of G shows that $G = H$. The structure of G is obtained now from the previous propositions.

Proposition 4. *Let G be an NC-critical group of class three. Then*

(1) *$Z(G)$ is cyclic, $Z(G) \neq \Phi(G)$, $d(G) = 2$, and either $G^p = Z(G)$, or $\exp G = p$. In the latter case, G has order p^4.*

(2) *G contains a unique abelian maximal subgroup, say M, and $d(M) = 2$ or 3.*

Proof. Since G' is not central, neither is $\Phi(G)$. If $\exp G > p$, then $G^p \subseteq Z(G)$ and $|\Phi(G) : G^p| = p$ show that $G^p = Z(G)$. Proposition 1(2) shows that $Z(G)$ has a unique subgroup of order p, hence it is cyclic.

Let $[x, y]$ be a non-central commutator. Suppose that $G \neq \langle x, y \rangle$. Then $H = \langle \Phi(G), x, y \rangle$ is a proper normal subgroup, so $H' \lhd G$, and $|H'| = p$. Then $H' \subseteq Z(G)$. But $H' = \langle [x, y] \rangle$, a contradiction. Thus $G = \langle x, y \rangle$, and

$d(G) = 2$. This shows that if $\exp G = p$, then $|G| = p^4$, because $\Phi(G) = G'$ in this case.

Denote $M = C_G(G')$. Then M is a maximal subgroup, containing $\Phi(G)$ as a central subgroup of index p, hence M is abelian, and it is the unique abelian maximal subgroup, because G has class three. Let x be any element outside M. Then $Z(G) = C_M(x)$, $G' = [M, x]$, so $|M : Z(G)| = p^2$. Since $Z(G)$ is cyclic, $d(M) \leqq 3$, while $d(M) > 1$, because M contains G'.

REMARK. We have just seen that G contains a cyclic subgroup of index p^3. The groups of this type are known [Ne]. Moreover, suppose that $\exp G > p$. Then Proposition 4 shows that G^p is a cyclic subgroup of index p^3 in G. Then $G^p = \langle x^p \rangle$, for some x, and $\langle x \rangle$ is even a cyclic subgroup of index p^2. Since our assumptions are so strong, we prefer to proceed without referring to the lists of groups with big cyclic subgroups.

PROPOSITION 5. *Let G and M be as in the previous proposition, and suppose that $d(M) = 2$. Assume also that $|G| \neq 3^4$. Then there exist elements x, y, z, and natural numbers i, n, such that $(i, p) = 1$, and*

$$G = \langle x, y \rangle, \quad M = \langle y \rangle \times \langle z \rangle, \quad x^p = z^p = y^{p^n} = 1,$$
$$[y, x] = z, \quad [z, x] = y^{ip^{n-1}}.$$

PROOF. The assumption $d(M) = 2$ rules out the possibility that $\exp G = p$. Let z be a non-central element of G'. Then z is not a pth power, so writing M as a direct product of two cyclic subgroups, one of them must have order p, and can be taken to be z. This yields the structure of M, if we let p^n be the order of y. Now $|G : M^p| = p^3 = |G : G^p|$, so $M^p = G^p$. If $p > 3$, then G is a regular p-group, and therefore $|E(G)| = |G : G^p| = p^3$. Thus there exists an element x of order p outside M. If $p = 3$, then G is not regular. But our assumption that the order of G is at least 3^5 shows that $\exp G > 3^2$, and therefore each section of exponent 3^2 is proper, and hence of class two. Then Theorem 1 of [Ma] shows that it is still true that $|E(G)| = 3^3$, and we can find x as before. The rest follows easily from the equality $G' = [M, x]$.

PROPOSITION 6. *Let G and M be as in Proposition 4, and let $d(M) = 3$. Assume also that $|G| \neq p^4$. Then there exist elements x, y, z and a natural number n, such that*

$$G = \langle x, y, z \rangle, \quad M = \langle x^p \rangle \times \langle y \rangle \times \langle z \rangle, \quad x^{p^n} = y^p = z^p = 1,$$
$$[y, x] = z, \quad [z, x] = x^{p^{n-1}}.$$

PROOF. The assumption on $|G|$ rules out the possibility that $\exp G = p$. Then G^p is cyclic, of index p^3 in G, and p^2 in M. Since $d(M) = 3$, G^p is a maximal cyclic subgroup of M, and thus $M = G^p \times \langle y \rangle \times \langle z \rangle$, where y and z have order p, and we may take z to be a non-central element of G'. Writing $G^p = \langle x^p \rangle$, the rest is standard.

REMARK. Propositions 1, 2, and 4, between them, show that $|G : Z(G)| = p^3$ in all cases. That fact almost, but not quite, has a converse, which we state for completeness, though it is not needed in the sequel, and its proof is left as an exercise.

PROPOSITION 7. *Let G be a p-group, in which $Z(G) \subseteq \Phi(G)$, and $|G : Z(G)| = p^3$. Then for each proper subgroup H of G we have $|H'| \leqq p$, while $|G'| \leqq p^3$ (equality is possible). Either $d(G) = 3$ and $\mathrm{cl}\, G = 2$, or $d(G) = 2$ and $\mathrm{cl}\, G = 3$.*

2. Proof of main results

In this section we apply some of the information derived in Section 1, in order to prove the main results. For a subset S of G, we denote by $\hat{S}$ the element of KG that is the sum of the elements of S.

PROOF OF THEOREM B. We are assuming, as we may, that G is an NC-critical group of class 2. We have to show that the wreath product $C_p \operatorname{wr}(C_p \times C_p)$ is involved in $U(G)$.

Let M be the (unique) maximal abelian subgroup of G, and let $x \in G - M$ (see Propositions 2 and 3). Then $C_p \times C_p = [x, G] = [x, M] \cong G/C_G(x) \cong M/C_M(x)$.

Two cases should be considered separately.

Case 1. $d(M) = 2$. Then, by Proposition 3(1), we may assume $x^p = 1$. Therefore $N_G(\langle x \rangle) = C_G(x)$, so that $G/N_G(\langle x \rangle) = G/C_G(x) \cong C_p \times C_p$. But, according to [Sh, Proposition D], if $\mathrm{cl}\, G = 2$ and H is any cyclic subgroup, then $C_p \operatorname{wr}(G/N_G(H))$ is involved in $U(G)$. Substituting $H = \langle x \rangle$ we get our conclusion.

Case 2. $d(M) > 2$. Then $|E(M)| \geqq p^3$ so that $E(M) \not\subseteq G'$. Let $a \in E(M) - G'$. Observe that, by Proposition 2(1), a is not central. Put $H = \langle a \rangle$. Let m_i $(0 \leqq i < p^2)$ be a set of representatives for $M/C_M(x)$, where $m_0 = 1$. Define $d = 1 + x\hat{H}$, $x_i = x^{m_i}$, $d_i = d^{m_i} = 1 + x_i\hat{H}$. Let $D = \langle d_i : i < p^2 \rangle$. This is a subgroup of $U(G)$, and we are going to show that it is elementary abelian with basis $\{d_i : i < p^2\}$.

First, observe that

$$d_i d_j = 1 + (x_i + x_j)\hat{H} + x_i\hat{H}x_j\hat{H} = 1 + (x_i + x_j)\hat{H} + x_i x_j \widehat{H^x}\hat{H}.$$

Now since x_i and x_j commute (as conjugate elements in a group of class 2), it follows that $d_i d_j = d_j d_i$. Put $u = [a, x]$. Since a is not central we must have $u \neq 1$ (otherwise $C_G(a) \supseteq \langle x, M \rangle = G$). Therefore $H^x \neq H$ so that $H^x \cap H = 1$ (recall that $|H| = p$). Thus $\hat{H}^x\hat{H} = \hat{B}$ where $B = \langle a^x, a \rangle = \langle a, u \rangle$. Note that $B \lhd G$, so B contains all the conjugates of H. This implies that, for all $0 \leqq i, j, k < p^2$,

$$x_i\hat{H}x_j\hat{H}x_k\hat{H} = x_i x_j x_k \widehat{H^{x^2}}\hat{H}^x\hat{H} = x_i x_j x_k \widehat{H^{x^2}}\hat{B} = 0.$$

We conclude that, given indices $0 \leqq i_1, i_2, \ldots, i_k < p^2$, we have

$$d_{i_1} d_{i_2} \cdots d_{i_k} = 1 + (x_{i_1} + \cdots + x_{i_k})\hat{H} + \Big(\sum_{s<t} x_{i_s} x_{i_t}\Big)\hat{B}.$$

In particular

$$d_i^p = 1 + p x_i \hat{H} + \binom{p}{2} x^2 \hat{B} = 1.$$

Therefore D is elementary abelian. We have to show that the d_i's form a basis for D. Since M acts transitively on the d_i's (by conjugation), it is sufficient to check that $\Pi\, d_i \neq 1$ (see [Sh, Lemma C1]).

Clearly, $\Pi_i\, d_i = 1 + (\Sigma_i\, x_i)\hat{H} + (\Sigma_{i<j}\, x_i x_j)\hat{B}$.

Now, since $\{x_i : 0 \leqq i < p^2) = xG'$ (the conjugacy class of x), we obtain $(\Sigma\, x_i)\hat{H} = x\hat{G}'\hat{H}$. Recall that, by the choice of a, $G' \cap H = 1$. Therefore $x\hat{G}'\hat{H} = x\widehat{G'H} \neq 0$. As for the next term, observe that

$$0 = x^2\widehat{G'}^2 = (x\widehat{G'})^2 = \Big(\sum_i x_i\Big)^2 = \sum_i x_i^2 + 2\sum_{i<j} x_i x_j = x^2\widehat{G'} + 2\sum_{i<j} x_i x_j.$$

It follows that $\Sigma\, x_i x_j = -\frac{1}{2}x^2\widehat{G'}$, so that $\Sigma\, x_i x_j \hat{B} = -\frac{1}{2}x^2\widehat{G'}\hat{B} = 0$ (since $G' \cap B = \langle u \rangle \neq 1$). We conclude that $\Pi_i\, d_i = 1 + x\widehat{G'H} \neq 1$, so that the d_i's are indeed a basis for D.

Next, consider the product $DM \subseteq U(G)$. Obviously $D \lhd DM$. The last calculation shows that $\Pi_i\, d_i \notin M$. Since M acts transitively on the d_i's, it follows from [Sh, Lemma C1] that $D \cap M = 1$. Therefore $DM = D \rtimes M$ is a semi-direct product. Finally, $C_M(x)$ is central in DM, and $DM/C_M(x) = D \times M/C_M(x) = C_p \operatorname{wr}(C_p \times C_p)$. This shows that $U(G)$ possesses a section isomorphic to $C_p \operatorname{wr}(C_p \times C_p)$, as required.

Before proving Theorem A, we collect a couple of results, which seem to be well known, but it is not easy to locate explicit proofs of them in the literature.

LEMMA 8. *Let G be a finite p-group, and consider KG as a Lie algebra (with the usual bracket operation). Then:*

(a) $\operatorname{cl} KG = p$ *if and only if* $|G'| = p$.

(b) *If* $\operatorname{cl} G = 2$, *then* $\operatorname{cl} KG \leqq t(G')$, *the nilpotency index of* $\Delta(G')$.

PROOF. (a) The 'if' part may be found in [Ba]. Now, assuming $|G'| > p$, pick an element x in G with more than p conjugates, and let y not commute with x. Consider the left normed Lie commutator of weight $p: c = (y^{1-p}x, y, \dots, y)$. Routine calculation shows that

$$c = x + x^{y} + x^{y^2} + \cdots + x^{y^{p-1}}.$$

Since these are not all the conjugates of x, c is not central. This means that $\operatorname{cl} KG > p$.

(b) Put $t = t(G')$. For $x_0, \dots, x_t$ in G, let c be the Lie commutator $(x_0, x_1, \dots, x_t)$. Since the group commutators $[g, h]$ are central, an easy induction yields

$$c = (1 - [x_1, x_0])(1 - [x_2, x_0x_1]) \cdots (1 - [x_t, x_0x_1 \cdots x_{t-1}])x_0x_1 \cdots x_t.$$

We conclude that $c \in \Delta(G')^t KG = 0$, as required.

PROOF OF THEOREM A. Consider first the case $p = 2$. According to a result of H. Laue [La], proved in a more general context, there is a simple connection between the second centres of $U(G)$ and the augmentation ideal $\Delta(G)$, viewed as a Lie algebra, namely $Z_2(U(G)) = 1 + Z_2(\Delta(G))$. This implies that $\operatorname{cl} U(G) = 2$ if and only if $\operatorname{cl} KG = 2$, where KG is also viewed as a Lie algebra. Lemma 8(a) completes the proof in this case.

Now let G be a p-group ($p > 2$) with $|G'| > p$. We want to show that $\operatorname{cl} U(G) \geqq 2p - 1$. We may assume that G is NC-critical. If $\operatorname{cl} G = 2$ we are done, by Theorem B, as $\operatorname{cl} C_p \operatorname{wr}(C_p \times C_p) = 2p - 1$. So suppose that $\operatorname{cl} G = 3$.

Let M be the maximal abelian subgroup of G (see Propositions 4 and 5) and let $x \in G - M$. Let u be a non-central element in G'. Then $[x, u] \neq 1$ (otherwise $C_G(u) = \langle x, M \rangle = G$, a contradiction). Set $v = [x, u]$. Then v is central, and $G' = \langle u, v \rangle$. Put $H = \langle u \rangle$, and consider the element $d = 1 + x\hat{H}$ in $U(G)$. For $0 \leqq i < p$ define $d_i = d^{x^i} = 1 + x\hat{H}_i$, where $H_i = H^{x^i}$. Observe that

$$x\hat{H}_i x\hat{H}_j = x^2\hat{H}_i^x\hat{H}_j = x^2\hat{H}_{i+1}\hat{H}_j = \begin{cases} x^2\hat{G}', & j \neq i + 1 \pmod{p}, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore $d_i d_j = 1 + x(\hat{H}_i + \hat{H}_j) + (1 - \delta_{i+1,j})x^2\hat{G}'$.

Since $\hat{H}_i\hat{G}' = 0$ it follows that

$$d_{i_1}\cdots d_{i_k} = 1 + x(\hat{H}_{i_1} + \cdots + \hat{H}_{i_k}) + \left[\binom{k}{2} - n\right]x^2\hat{G}',$$

where $n = |\{(s,t) : s < t,\, i_t = i_s + 1 \pmod p\}|$.

In particular

$$d_i^k = 1 + kx\hat{H}_i + \binom{k}{2}x^2\hat{G}',$$

therefore $d_i^p = 1$, and $d_i^{-1} = d_i^{p-1} = 1 - x\hat{H}_i + x^2\hat{G}'$. Now,

$$\begin{aligned}[d_i, d_j] &= d_i^{-1}d_j^{-1}d_i d_j\\ &= (1 - x\hat{H}_i + x^2\hat{G}')(1 - x\hat{H}_j + x^2\hat{G}')[1 + x(\hat{H}_i + \hat{H}_j) + (1 - \delta_{i+1,j})x^2\hat{G}']\\ &= [1 - x(\hat{H}_i + \hat{H}_j) + (3 - \delta_{i+1,j})x^2\hat{G}'][1 + x(\hat{H}_i + \hat{H}_j) + (1 - \delta_{i+1,j})x^2\hat{G}']\\ &= 1 - (x\hat{H}_i + x\hat{H}_j)^2 + (4 - 2\delta_{i+1,j})x^2\hat{G}'\\ &= 1 + (\delta_{j+1,i} - \delta_{i+1,j})x^2\hat{G}'.\end{aligned}$$

Put $c = 1 + x^2\hat{G}'$. Observe that c is central in $U(G)$, and satisfies $c^p = 1$, $c^{-1} = 1 - x^2\hat{G}'$. The last calculation shows that

$$[d_i, d_j] = c^{(\delta_{j+1,i} - \delta_{i+1,j})}.$$

It follows that, if $D = \langle d_0, \ldots, d_{p-1}\rangle$, then $D' = \langle c\rangle$ is of order p. Consider the group $E = \langle x, D\rangle \subseteq U(G)$. Obviously $D \lhd E$ and $\langle c\rangle \subseteq Z(E)$. Let $\bar{E} = E/\langle c\rangle$, $\bar{D} = D/\langle c\rangle$. Then $\bar{D}$ is elementary abelian, and $\bar{x}$ (the image of x in $\bar{E}$) acts on $\bar{d}_i$ by $\bar{d}_i^{\bar{x}} = \bar{d}_{i+1}$. This clearly implies

$$[\bar{d}, \underbrace{\bar{x}, \ldots, \bar{x}}_{p-1}] = \bar{d}\bar{d}^{\bar{x}}\bar{d}^{\bar{x}^2}\cdots\bar{d}^{\bar{x}^{p-1}} = \bar{d}_0\bar{d}_1\cdots\bar{d}_{p-1} = \overline{d_0 d_1\cdots d_{p-1}}.$$

It follows that $\overline{d_0\cdots d_{p-1}} \in \gamma_p(\bar{E})$, so that $q := d_0\cdots d_{p-1}c^n \in \gamma_p(E)$ (for some n). But

$$\begin{aligned}d_0\cdots d_{p-1} &= 1 + x(\hat{H}_0 + \cdots + \hat{H}_{p-1}) + \left[\binom{p}{2} - (p-1)\right]x^2\hat{G}'\\ &= 1 + x(\hat{H}_0 + \cdots + \hat{H}_{p-1}) + x^2\hat{G}',\end{aligned}$$

while $q = 1 + x(\hat{H}_0 + \cdots + \hat{H}_{p-1}) + mx^2\hat{G}'$, where $m = n + 1$.

Put $S = G' - \langle v \rangle$. Since S is a normal set in G, $\hat{S}$ is clearly central in KG. This implies that $(KG'\hat{S})^2 = KG \cdot \hat{S}^2 = 0$. Note that $\hat{H}_0 + \cdots + \hat{H}_{p-1} = \hat{S}$, so that $q = 1 + x\hat{S} + mx^2\hat{G}'$. We have just shown that $q \in \gamma_p(U(G))$. We will now produce an element g in G with the property that

$$[q, \underbrace{g, \ldots, g}_{p-1}] \neq 1.$$

This will show that $\gamma_{2p-1}(U(G)) \neq 1$, terminating the proof of the theorem. Since c is central in $U(G)$, it follows that

$$[q, \underbrace{g, \ldots, g}_{p-1}] = [qc^{-m}, \underbrace{g, \ldots, g}_{p-1}].$$

Therefore we may replace q by $r := qc^{-m} = 1 + x\hat{S}$.

Recall that $\langle u, v \rangle = G' = [x, M] = \{[x, g] : g \text{ in } M\}$. In particular, there exists an element g in M with $[x, g] = u$. Since $[u, g] = 1$ (as u, g are in M) we get $x^{g^i} = xu^i$ for all $0 \leqq i < p$. Consider the elements $r_i := r^{g^i} = 1 + xu^i\hat{S}$. Since the ideal $KG \cdot \hat{S}$ is nilpotent of index 2, the r_i's commute with each other. They clearly have order p. Therefore

$$[r, \underbrace{g, \ldots, g}_{k-1}] = rr^g \cdots r^{g^{p-1}} = r_0 r_1 \cdots r_{p-1} = 1 + (x + xu + \cdots + xu^{p-1})\hat{S}$$

$$= 1 + x\langle \hat{u} \rangle (G' - \langle \hat{v} \rangle) = 1 - x\langle \hat{u} \rangle \langle \hat{v} \rangle = 1 - x\hat{G}'.$$

This shows that

$$[r, \underbrace{g, \ldots, g}_{p-1}] \neq 1,$$

completing the proof of Theorem A.

PROOF OF COROLLARY C. Let G be a p-group of class 2, with $G' = C_p \times C_p$. By Theorem A we have cl $U(G) \geqq 2p - 1$. For the other inequality we apply [GL], to conclude that cl $U(G) \leqq$ cl KG. But, by Lemma 8(b), cl $KG \leqq t(G') = t(C_p \times C_p) = 2p - 1$ (see for example [MN] for the last equality).

References

[Ba] C. Baginski, *Groups of units of modular group algebras*, Proc. Am. Math. Soc. **101** (1987), 619–624.

[CP] D. B. Coleman and D. S. Passman, *Units in modular group rings*, Proc. Am. Math. Soc. **25** (1970), 510–512.

[GL] N. D. Gupta and F. Levin, *On the Lie ideals of a ring*, J. Algebra **81** (1983), 225–231.

[Kn] H. G. Knoche, *Uber den Frobeniusschen Klassenbegriff in nilpotenten Gruppen*, Math. Z. **55** (1951), 71–83.

[La] H. Laue, *On the associated Lie ring and the adjoint group of a radical ring*, Can. Math. Bull. **27** (1984), 215–222.

[Ma] A. Mann, *The power structure of p-groups I*, J. Algebra **42** (1976), 121–135.

[MN] K. Motose and Y. Ninomiya, *On the nilpotency index of the radical of a group algebra*, Hokkaido Math. J. **4** (1975), 261–264.

[Ne] L. I. Neikirk, *Groups of order p^n which contain cyclic subgroups of order p^{m-3}*, Trans. Am. Math. Soc. **6** (1905), 316–325.

[Sa] R. Sandling, *Presentations for unit groups of modular group algebras of groups of order* 2^4, to appear.

[Sh] A. Shalev, *The nilpotency class of the unit group of a modular group algebra I*, Isr. J. Math. **70** (1990), 257–266, this issue.