GROUPS OF UNITS
OF MODULAR GROUP ALGEBRAS

CZESŁAW BAGINSKI

(Communicated by Donald Passman)

Abstract. Let \( U(G) \) be the group of normalized units of the group algebra \( F[G] \) of a finite nonabelian \( p \)-group \( G \) over the field \( F = GF(p) \). The description is given of all \( p \)-groups, \( p > 2 \), for which \( U(G) \) does not contain subgroups isomorphic to the wreath product \( \mathbb{Z}_p \wr \mathbb{Z}_p \).

Let \( p \) be a prime, \( G \) be a finite nonabelian \( p \)-group, and \( F = GF(p) \). Referring to [1] the authors of the survey [5] wrote that the group \( U(G) \) of normalized units of a group algebra \( F[G] \) contains a subgroup isomorphic to the wreath product \( \mathbb{Z}_p \wr \mathbb{Z}_p \). In fact Coleman and Passman proved in [1] only that \( \mathbb{Z}_p \wr \mathbb{Z}_p \) is involved in \( U(G) \), that is it can be obtained as an epimorphic image of a subgroup of \( U(G) \). Moreover one can easily check that for the quaternion group \( Q \) all involutions of \( U(Q) \) lie in its center, i.e. \( U(Q) \) does not contain a subgroup isomorphic to \( \mathbb{Z}_2 \wr \mathbb{Z}_2 \). Obviously \( U(Q) \) is a 2-group. Hence Coleman-Passman's theorem cannot be sharpened, in general, to the form stated in [5]. It appears however that the stronger result holds quite frequently. In Theorem 1 we prove that \( U(G) \) contains a subgroup isomorphic to \( E_n \wr \mathbb{Z}_p \), where \( E_n \) is elementary abelian of order \( p^n \), if \( G \) contains noncentral elements of order \( p \) or \( |\Omega_1(G)| > p^3 \) or \( G' \neq \Omega_1(G) \). It allows us to give the complete description of all \( p \)-groups \( G \), \( p \) odd, for which \( \mathbb{Z}_p \wr \mathbb{Z}_p \) cannot be embedded in \( U(G) \) (Theorem 2). There are infinitely many nonisomorphic such groups and each is uniquely determined up to isomorphism by its group algebra.

We shall make use of the following notation. If \( G \) is a \( p \)-group then:\( \Omega_n(G) = \langle x: x^p = 1 \rangle \), \( Z(G) \) is the center of \( G \), \( C_G(x) = \{ g \in G : gx = xg \} \), \( G' = \gamma_2(G) \) is the commutator subgroup, \( \gamma_n(G) \) is the \( n \)th term of the lower central series of \( G \), and \( (x, y) = x^{-1}y^{-1}xy \). If \( R \) is a ring, then \( L_n(R) \), \( n \geq 2 \), is the ideal of \( R \) generated by all \( \text{Lie elements } [r_1, r_2, \ldots, r_n] \), where \( [r_1, r_2] = r_1r_2 - r_2r_1 \) and, inductively, \( [r_1, r_2, \ldots, r_n] = [[r_1, r_2, \ldots, r_{n-1}], r_n] \). The remaining notation follows [4].

We start with the following lemma.

**Lemma 1.** Let \( A \) be an elementary abelian subgroup of a finite \( p \)-group \( G \) and \( b \) an element of \( G \) of order \( p \) normalizing \( A \). If there are elements \( a_1, a_2, \ldots, a_n \) of \( A \) such
that the group \( \langle (ba_1)^p, (ba_2)^p, \ldots, (ba_n)^p \rangle \) has order \( p^n \) then \( B_n = \langle b, a_1, a_2, \ldots, a_n \rangle \) is isomorphic to \( E_n \setminus Z_p \).

**Proof.** It can be easily shown that the group \( E_n \setminus Z_p \) is isomorphic to the group \( W_n = \langle y, x_{ij}, i = 1, \ldots, n; \ j = 0, \ldots, p - 1 | y^p = x_{ij}^p = 1, \ x_{ij}x_{mn} = x_{mn}x_{ij}, \ y^{-1}x_{ij}y = x_{i,j+1}, \ \text{where} \ j + 1 \ \text{is taken modulo} \ p \rangle \). Since the correspondence \( y \rightarrow b, \ x_{ij} \rightarrow b^{-i}a_i b^j \) determines an epimorphism of \( W_n \) onto \( B_n \), it suffices to show that \( |W_n| = |B_n| = p^{n+1} \) or that \( |A_n| = p^{np} \), where \( A_n \) is a subgroup of \( B_n \) generated by all \( b^{-i}a_i b^j, i = 1, \ldots, n; \ j = 0, \ldots, p - 1 \). We proceed by induction on \( n \).

By III.10.5a of [3] \( B_n \) is not regular, so the case \( n = 1 \) follows immediately from III.10.2b of [3]. Now let \( C_n \) be a subgroup of \( A_n \) for \( n \geq 2 \) generated by all \( b^{-i}a_i b^j, i = 2, \ldots, n; \ j = 0, \ldots, p - 1 \). By the induction \( \langle b, C_n \rangle = E_{n-1} \setminus Z_p \) and so \( |C_n| = p^{(n-1)p} \). Since \( |Z(E_{n-1} \setminus Z_p)| = p^{n-1} \) and all \( (ba_i)^p \) centralize \( b \), the assumption gives \( Z(\langle b, C_n \rangle) = \langle (ba_2)^p, \ldots, (ba_n)^p \rangle \). Moreover \( Z(B_i) = \langle (ba_1)^p \rangle \). Each nontrivial normal subgroup of a finite \( p \)-group intersects nontrivially its center, so \( \langle (ba_1)^p \rangle \) is the smallest nontrivial normal subgroup of \( B_1 \). Now if \( A_1 \cap C_n \neq \{1\} \), then \( A_1 \cap C_n \) is a normal subgroup of \( B_1 \) and by the foregoing \( (ba_1)^p \in A_1 \cap C_n \). The element \( (ba_1)^p \) centralizes \( b \), so \( (ba_1)^p \in Z(\langle b, C_n \rangle) = \langle (ba_2)^p, \ldots, (ba_n)^p \rangle \) which contradicts the assumption of the lemma. Thus \( A_1 \cap C_n = \{1\} \) and \( |A_n| = |A_1| |C_n| = p^{np} \). It ends the proof.

**Theorem 1.** \( U(G) \) contains a subgroup isomorphic to \( E_{p-1} \setminus Z_p \) provided one of the following conditions holds:

(a) \( \Omega_1(G) \neq Z(G) \),
(b) \( |\Omega_1(G)| \geq p^3 \),
(c) \( G' \neq \Omega_1(G) \).

**Proof.** We consider separately the cases \( p = 2 \) and \( p > 2 \).

Case 1: \( p = 2 \). It is well known that the wreath product \( Z_2 \setminus Z_2 \) is isomorphic to the dihedral group of order 8. Hence \( U(G) \) contains a subgroup isomorphic to \( Z_2 \setminus Z_2 \) if and only if it contains two noncommuting involutions.

Let \( y \) be a noncentral involution of \( G \) and \( x \) an element of \( G \) noncommuting with \( y \). Let \( o(x) = 2^k, k \geq 2, \) and \( t = 1 + x(1 + x^{2^{k-1}}) \). Since \( t^2 = 1 \) we can assume that \( ty = yt \), that is \( y + xy + x^{2^{k-1}+1}y = y + yx + yx^{2^{k-1}+1} \). Thus \( yx = x^{2^{k-1}+1}y \) and \( (x, y) = x^{2^{k-1}} \). If \( k = 2 \), then \( xy \) is an involution noncommuting with \( y \). Thus let \( k > 2 \) and \( s = 1 + x(1 + x^{2^{k-2}})(1 + y) \). A straightforward computation shows that \( s^2 = 1 \) and \( sy \neq ys \).

Suppose now that \( |\Omega_1(G)| \geq 2^3 \) or \( |\Omega_1(G)| = 2^2 \) and \( G' \neq \Omega_1(G) \). By the foregoing we can assume that \( \Omega_1(G) \leq Z(G) \). Let \( x \) and \( y \) be noncommuting elements of \( G \). We can choose involutions \( v \) and \( w \) of \( \Omega_1(G) \), \( v \neq w \), such that \( (x, y) \in \langle v, w \rangle \).

Observe that elements \( a = 1 + x(1 + v) \) and \( b = 1 + y(1 + w) \) are involutions of \( U(G) \). Moreover \( ab \neq ba \). Indeed, if \( ab = ba \), then

\[
xy(1 + v + w + vw) = yx(1 + v + w + vw),
\]

that is \( (x, y) \in \{v, w, vw\} \) which contradicts the choice of \( v \) and \( w \).
Now let $G' \notin \Omega_1(G)$ and $|\Omega_1(G)| = 2$. By III.8.2 of [3] $G$ is a generalized quaternion group of order $\geq 2^4$. Let $x$ and $y$ be elements of $G$ such that $x^8 = 1$, $y^2 = x^4$, $y^{-1}xy = x^{-1}$. Then $1 + (1 + x^2)(x + y)$, $1 + (1 + x^2)(x + xy)$ are non-commuting involutions of $U(G)$. The computation is straightforward and we omit it.

**Case 2:** Let $y$ be a non-central element of $G$ of order $p$ and $x$ be an element of $G$ such that $z = (x, y) \in C_G(x) \cap C_G(y)$. The group $H = \langle y, z \rangle$ is clearly normalized by $x$ and, since $z^p = (x, y)^p = (x, y^p) = 1$, it is an elementary abelian group of order $p^2$. Let $A$ be the group generated by elements $a_{mn} = 1 + x^mz^n\hat{Y}$, $1 \leq m \leq p - 1, 0 \leq n \leq p - 1$, where $\hat{Y}$ denotes the sum of the elements of $Y = \langle y \rangle$. Observe that the group $A$ is elementary abelian. Indeed, if $i \neq j, 1 \leq i, j \leq p - 1$, then $\hat{Y}^x \hat{Y}^y = \hat{H}$ and hence $\hat{Y}^x \hat{Y}^y \hat{Y}^x = 0$ for all $i, j, k$. Thus

$$a_{mn}^p = (1 + x^mz^n\hat{Y})^p = 1 + (x^mz^n\hat{Y})$$

and

$$a_{mn}a_{jk} = 1 + (x^mz^n + x^jz^k)\hat{Y} + x^mz^kn\hat{H} = a_{jk}a_{mn}.$$  

Of course $A$ is normalized by $y$ and for all $k, 1 \leq k \leq p - 1$,

$$(ya_{k0})^p = (y + yx^k\hat{Y})^p = y^p + \sum_{i=0}^{p-1} y^{p-i}(x^k\hat{Y})y^i + \sum_{i+j=0}^{p-2} y^{p-2-i-j}(yx^k\hat{Y})y^i(yx^k\hat{Y})y^j = 1 + x^k\hat{H} \neq 1$$

because the second sum is equal to zero. So the group $B = \langle (ya_{10})^p, \ldots, (ya_{p-1,0})^p \rangle$ has order $p^{p-1}$ and by Lemma $1 \langle y, A \rangle$ contains a subgroup isomorphic to $E_{p-1} \setminus Z_p$.

Suppose now that $|\Omega_1(G)| \geq p^3$ and $\Omega_1(G) \leq Z(G)$. Let $x$ and $y$ be elements of $G$ such that $1 \neq (x, y) = z \in \Omega_1(G)$. Let $v$ and $w$ be elements of $\Omega_1(G)$ satisfying $|\langle v, w \rangle| = p^2$ and $z \notin \langle v, w \rangle$. Since $W = \langle w \rangle$ is a central subgroup of $G$, $F[G]\hat{W}$ is an ideal of $F[G]$ and hence $A = 1 + F[G]\hat{W}$ is a normal subgroup of $U(G)$. Since $(F[G]\hat{W})^2 = 0$, the group $A$ is elementary abelian. Now let $b = 1 + y(1 - v)$ and $a_k = 1 + x^k\hat{W}$, $1 \leq k \leq p - 1$. We have

$$(ba_k)^p = 1 + (y(1 - v) + x^k\hat{W} + yx^k(1 - v)\hat{W})^p$$

$$= 1 + \sum_{i=0}^{p-1} y^{p-1-ix^k}y^i(1 - v)^{p-1}\hat{W}$$

$$= 1 + y^{p-1}x^k(1 + z + \cdots + z^{p-1})(1 - v)^{p-1}\hat{W} \neq 1.$$  

Thus elements $(ba_k)^p, k = 1, \ldots, p - 1$, generate a subgroup of order $p^{p-1}$ and by Lemma $1 \langle b, A \rangle$ contains a subgroup isomorphic to $E_{p-1} \setminus Z_p$.

Suppose finally that $G' \notin \Omega_1(G)$. Assuming $\Omega_1(G) \leq Z(G)$ and $|\Omega_1(G)| = p^2$ we choose elements $x$ and $y$ of $G$ such that $z = (x, y) \in \Omega_1(G)$ and $z \in Z(G \mod \Omega_1(G))$. Let $W$ be a subgroup of $\Omega_1(G)$ of order $p$ and $v \in \Omega_1(G) - W$.

The same arguments as in the previous paragraph show that $A = 1 + F[G]\hat{W}$ is a
normal elementary abelian subgroup of $U(G)$. Let $b = 1 + y(1 - v)$ and $a_k = 1 + x^k \hat{W}$, $1 \leq k \leq p - 1$. Since
\[
x^k y^l = y^l x^k \equiv y^l x^k z^{ik} \mod \Omega_1(G)
\]
and $(1 - v)^{p-1}\hat{W} = \overline{\Omega_1(G)}$, a similar computation as above gives
\[
(b a_k)^p = 1 + y^{p-1} x^k (1 + z^k + \cdots + z^{(p-1)k}) \overline{\Omega_1(G)} \neq 1.
\]
So $\langle b, A \rangle$ contains a subgroup isomorphic to $E_{p-1} \setminus Z_p$. This completes the proof.

**Corollary 1.** If $p > 2$, then for every nonabelian $p$-group $G$, $U(G \times Z_p)$ contains a subgroup isomorphic to $E_{p-1} \setminus Z_p$.

**Corollary 2.** If $U(G)$ does not contain $Z_p \setminus Z_p$ for a nonabelian $p$-group $G$, then $1 \neq G' \leq \Omega_1(G)$ and $|\Omega_i(G)| \leq p^2$. In particular $G$ is nilpotent of class two.

**Lemma 2.** Let $|G'| = p$ and $H$ be an elementary abelian, central subgroup of $G$ of order $p^2$ containing $G'$. Then
(a) $U(G)$ is nilpotent of class $p$,
(b) $1 + \omega(F[H])F[G]$ is nilpotent of class $< p$.

**Proof.** (a) Let $G' = \langle z \rangle$. It is well known that $L_2(F[G]) = \omega(F[G'])F[G] = (1 - z)F[G]$. By easy induction $L_n(F[G]) \subseteq (1 - z)^n F[G]$. Hence $L_{p+1}(F[G]) = 0$. By Theorem A of [2] $\gamma_p(U(G)) \leq 1 + L_{p}(F[G])$ and so $\gamma_{p+1}(U(G)) = 1$, that is $U(G)$ is nilpotent of class at most $p$. On the other hand Coleman-Passman’s theorem of [1] implies that $U(G)$ contains a subgroup of class $p$. The result follows.

(b) Let $H = \langle t, z \rangle$, $G' = \langle z \rangle$, and $I = \omega(F[H])F[G]$. Since $I = (1 - z)F[G] + (1 - t)F[G]$, $L_p(I + F)$ is generated by all elements $[a_1, a_2, \ldots , a_p]$ with $a_i = (1 - t)b$ or $a_i = (1 - z)c$, $i = 1, \ldots , p$; $b, c \in F[G]$. If all $a_i$ are of the form $(1 - t)b$ then clearly $[a_1, a_2, \ldots , a_p] \in ((1 - t) F[G])^p = 0$. If $a_i = (1 - z)c$ for some $i$, then $a_i \in L_2(F[G])$, so $[a_1, a_2, \ldots , a_p] \in L_{p+1}(F[G]) = 0$. Thus by Theorem A of [2] $\gamma_p(1 + I) = 1$ which says that $1 + I$ is a group of class at most $p - 1$.

We shall say that a finite $p$-group $G$ is a $p_1$-group if $x^p = y^p$ implies $(xy^{-1})^p = 1$ for all $x, y \in G$. By III.10.6a of [3] all regular $p$-groups are $p_1$-groups. Let $\omega_1(F[G])$ be an ideal of $F[G]$ generated by all elements $a \in F[G]$ satisfying $a^p = 0$.

**Lemma 3.** If $G$ is a $p_1$-group and $x^p \in Z(G)$ for all $x \in G$, then $\omega_1(F[G]) = \omega(F[H])F[G]$, where $H = \Omega_1(G)$.

**Proof.** If $u = \sum r_g g \in F[G]$ then by 2.3.2 of [4] $u^p = \sum r_g g^p + v$, where $v$ belongs to the subspace $[F[G], F[G]]$ spanned by all Lie elements $[a, b], a, b \in F[G]$. Suppose $u^p = 0$. Since, by assumption and 2.3.1 of [4], no element of supp($\sum r_g g^p$) appears in $[F[G], F[G]]$ with nonzero coefficient, we have $\sum r_g g^p = 0$. For each $g$ of supp($u$) let $P_g$ denote the set $\{ h \in \text{supp}(u): h^p = g^p \}$. Since $G$ is a $p_1$-group, $h^p = g^p$ implies $h = gh_g$ for a suitable $h_g \in H$. Thus since sets $P_g$ form a partition of supp($u$), $\sum r_g g^p = 0$ implies $\sum r_h h^p = 0$. Hence $\sum_h r_h h^p = 0$. Therefore $\omega_1(F[G]) \subseteq \omega(F[H])F[G]$. The converse inclusion is obvious.
The following lemma can be easily derived from III.11.2 of [3].

**Lemma 4.** If $G$ is a metacyclic group of order $p^k$ with $|G'| = p > 2$, then there exist $m \geq 2$, $n \geq 1$ such that $m + n = k$ and $G$ is isomorphic to the group $\langle x, y : x^{p^m} = y^{p^n} = 1, y^{-1}xy = x^{p^{m-1} + 1} \rangle$.

**Theorem 2.** If $p > 2$ and $G$ is a nonabelian $p$-group, then $U(G)$ does not contain $Z_p \setminus Z_{p^2}$ if and only if $G$ is isomorphic to the group $\langle x, y : x^{p^m} = y^{p^n} = 1, y^{-1}xy = x^{p^{m-1} + 1} \rangle$, where $m, n \geq 2$.

**Proof.** Let us assume first that $Z_p \setminus Z_{p^2}$ is not contained in $U(G)$. Then by Corollary 2 $G$ is nilpotent of class two and, by III.10.2 of [3], regular. Since $|\Omega_1(G)| = p^2$, by III.10.7 and III.11.4 of [3], $G$ is metacyclic. Now applying Lemma 4 and the inclusion $G' \leq \Omega_1(G) \leq Z(G)$ (Corollary 2) we obtain the defining relations for $G$.

Now let $G$ be such as in the theorem. By the relations, $g^p \in Z(G)$ for all $g \in G$. Hence by Lemma 3 all elements of order $p$ of $U(G)$ lie in $1 + \omega_1(F[G])$. But $\omega_1(F[G]) = \omega(F[H])F[G]$, where $H = \langle x^{p^m}, y^{p^n} \rangle \leq Z(G)$, so by Lemma 2, $1 + \omega_1(F[G])$ is of class at most $p - 1$. Hence $1 + \omega_1(F[G])$ does not contain $Z_{p^2} \setminus Z_p$ and the result follows.

**Corollary.** If $G$ is a group described in Theorem 2, then $F[G] = F[H]$ implies $G \cong H$.

**Proof.** By Theorem 2 if $F[G] = F[H]$, then $H = \langle x, y : x^{p^r} = y^{p^s} = 1, y^{-1}xy = x^{p^{r-1} + 1} \rangle$, where $r, s \geq 2$. Since the groups $G/G'$, $Z(G)$, $H/H'$, $Z(H)$ are abelian of types $(p^{n-1}, p^m)$, $(p^{n-1}, p^{m-1})$, $(p^{r-1}, p^s)$, $(p^{r-1}, p^{s-1})$ respectively we have $n = r$ and $m = s$ by 14.7.2 of [4]. Thus $G \cong H$.

**Remark 1.** It can be easily seen that, if $G$ is isomorphic to the group $\langle x, y : x^{2^m} = y^{2^m} = 1, y^{-1}xy = x^{2^{m-1} + 1} \rangle$, where $m, n \geq 2$, then $G$ is a $p_1$-group and $g^2 \in Z(G)$ for all $g \in G$. Thus the arguments used in the proof of Theorem 2 show that $U(G)$ does not contain a subgroup isomorphic to $Z_2 \setminus Z_2$.

**Remark 2.** Let $Q = \langle x, y : x^2 = y^2, x^4 = 1, y^{-1}xy = x^{-1} \rangle$ be the quaternion group, $F = GF(2)$ and $I = (1 + x^2)f[Q]$. Since $h^{-1}(1 + x^2)gh = (1 + x^2)g$ for all $g, h \in Q$, we have $1 + I \leq Z(U(Q))$. We claim that all involutions of $U(Q)$ lie in $1 + I$. Indeed, the elements $x, y, t = 1 + x + y$ generate $U(Q)$ modulo $1 + I$ and no element of the set $S = \{ x, y, xy, t, xt, yt, xyt \}$ is an involution. Since $I^2 = 0$, all elements of $1 + I$ are of order $\leq 2$. Now the equality

$$U(Q) = (1 + I) \cup \bigcup_{s \in S} (1 + I)s$$

proves the claim. Observe that $Q$ is not a $p_1$-group.

**Remark 3.** Let $G$ be the direct product of $Q$ and $Z = \langle z : z^2 = 1 \rangle$. We show that all involutions of $U(Q)$ commute. Indeed, if $\varphi$ is a natural epimorphism of $F[G]$ onto $F[G/Z] = F[Q]$, then $\varphi^{-1}(I) = (1 + x^2)f[G] + (1 + z)f[G]$. By the previous example all involutions of $U(G)$ lie in $1 + \varphi^{-1}(I)$ and by Lemma 2 the group $1 + \varphi^{-1}(I)$ is abelian.
REFERENCES


INSTITUTE OF MATHEMATICS, UNIVERSITY OF WARSAW, BIAŁYSTOK DIVISION, AKADEMICKA 2, 15–267 BIAŁYSTOK, POLAND