Units of $p$-power order in principal $p$-blocks of $p$-constrained groups

Martin Hertweck

Universität Stuttgart, Fachbereich Mathematik, IGT, 70550 Stuttgart, Germany

Abstract

Let $G$ be a finite group having a normal $p$-subgroup $N$ that contains its centralizer $C_G(N)$, and let $R$ be a $p$-adic ring. It is shown that any finite $p$-group of units of augmentation one in $RG$ which normalizes $N$ is conjugate to a subgroup of $G$ by a unit of $RG$, and if it centralizes $N$ it is even contained in $N$.

Key words: principal block, torsion unit, permutation lattice, $p$-constrained group

1 Introduction

This paper grew out of an attempt to understand more fully part of a theorem due to Roggenkamp and Scott (see [10, Theorem 6], [16,17], [11, Theorem 19]) about conjugacy of certain finite $p$-subgroups in the group of units of a $p$-adic group ring. The theorem in question, by now called the F*-Theorem, is stated below together with references where a detailed account on its proof can be found (with the result from Section 2 of the present paper being relevant).

Some of the interesting aspects of the group of units of a group ring $SG$ of a finite group $G$ concern its finite subgroups, in particular when the coefficient ring $S$ is a $G$-adapted ring, i.e., an integral domain of characteristic zero in which no prime divisor of the order of $G$ is invertible. Below, a few well known results in this case are listed. Note that it suffices to consider only the group of units $V(SG)$ consisting of units of augmentation one. For $u \in V(SG)$, we say that $u$ is a trivial unit if $u \in G$, and the trace of $u$ is its 1-coefficient (with respect to the basis $G$). Let $S$ be a $G$-adapted ring. Then (see [15], [8] or [18]):

* Research supported by the Deutsche Forschungsgemeinschaft.

Email address: hertweck@mathematik.uni-stuttgart.de (Martin Hertweck).
(a) a non-trivial unit of $SG$ of finite order has trace zero;
(b) the order of a finite subgroup of $V(SG)$ divides the order of $G$;
(c) a central unit of finite order is a trivial unit.

Limiting attention only to finite $p$-subgroups in the group of units, one might ask whether comparable results hold with $S$ replaced by the ring $\mathbb{Z}_p$ of $p$-adic integers. However, (a) and (b) does not carry over, even not if $\mathbb{Z}_p G$ consists of a single block only (cf. [14, Section XIV]). Imposing additional conditions one might also ask how certain finite $p$-subgroups are embedded in $V(\mathbb{Z}_p G)$. If, for example, attention is directed to the principal block $B$ of $\mathbb{Z}_p G$, a Sylow $p$-subgroup $P$ of $G$ is identified with its projection on $B$, and $\alpha$ is an augmented automorphism of $B$, then the question whether $P$ is conjugate by a unit of $B$ to its image $P\alpha$, is part of Scott’s “defect group (conjugacy) question” (see [16, p. 267], [17]). For $p$-groups $G$, this question was answered in the affirmative by Roggenkamp and Scott [13].

Here, the following two theorems are proved. In both we assume that $G$ has a normal $p$-subgroup $N$ satisfying $C_G(N) \leq N$. By definition, this means that $G$ is $p$-constrained and $O_{p'}(G) = 1$ (see [6, VII, 13.3]).

Throughout the paper, $R$ denotes a $p$-adic ring, that is, the integral closure of the $p$-adic integers $\mathbb{Z}_p$ in a finite extension field of the $p$-adic field $\mathbb{Q}_p$. (Then $R$ is a complete discrete valuation ring.) Note that by our assumption on $G$, the group ring $RG$ will consist of a single (principal) block only (see [6, VII, 13.5]).

**Theorem A.** Suppose that $G$ has a normal $p$-subgroup $N$ that contains its centralizer $C_G(N)$. Then any finite $p$-group in $V(RG)$ which normalizes $N$ is conjugate to a subgroup of $G$ by a unit of $RG$.

**Theorem B.** Suppose that $G$ has a normal $p$-subgroup $N$ that contains its centralizer $C_G(N)$. Then any finite $p$-group in $V(RG)$ which centralizes $N$ is contained in $N$.

The proofs are somewhat complicated by the fact that we do not know in advance that $RG$ is free for the “multiplication action” of the finite $p$-group under consideration (taking this for granted, Theorem A should be part of the $F^*$-Theorem). Section 2 contains some preparatory results needed for the handling of the case $p = 2$. Theorems A and B are proved in Section 3. The bimodule arguments used there are inspired by [10, p. 231]. The proof depends heavily on the strong results of Weiss on $p$-permutation lattices (see [20,21], [12]). That these results can be applied rests upon the “Ward–Coleman Lemma.” Coleman’s contribution [1] is well known, but the first version of the lemma appears in an article of Ward [19] as a contribution to a seminar run by Richard Brauer at Harvard. See also [15, Proposition 1.14], [7, 2.6 Theorem]. Actually, for its proof it is only needed that $p$ is not invertible in the commutative ring $R$. 

2
**Ward–Coleman Lemma.** Let $H$ be a $p$-subgroup of the finite group $G$. Then $N_{V(RG)}(H) = N_G(H) \cdot C_{V(RG)}(H)$. □

A consequence of Theorem B deserves explicit mention.

**Corollary.** Suppose that $G$ has a normal $p$-subgroup $N$ that contains its centralizer $C_G(N)$. Then each central unit of (finite) $p$-power order in $V(RG)$ is a trivial unit, i.e. contained in $Z(G)$.

It is not known whether a corresponding result holds for the principal block of an arbitrary (non-solvable) group. Progress in this direction might lead to applications in finite group theory, through Robinson’s work [9] on odd analogues of Glauberman’s $Z^*$-Theorem.

Finally, we state the theorem of Roggenkamp and Scott.

**F*-Theorem.** Let $G$ be a finite group having a normal $p$-subgroup $N$ that contains its centralizer $C_G(N)$. If $\alpha$ is an automorphism of $RG$ stabilizing both the augmentation ideal $I_R(G)$ and the ideal $I_R(N)G$, then the groups $G$ and $G^\alpha$ are conjugate by a unit of $RG$.

The first step of the proof consists in showing that $N$ and $N^\alpha$ are conjugate by a unit of $RG$, so that $N = N^\alpha$ can be assumed (details of sketch proof in [10] are given in [4, Lemma 4.1]). Then the image $P^\alpha$ of a Sylow $p$-subgroup $P$ of $G$ normalizes $N$, and by Theorem A one can even assume that $P = P^\alpha$.

Now it can be shown that there exists an automorphism $\rho$ of $G$ such that the composition $\alpha \rho$ fixes the elements of $P$, which implies that $\alpha \rho$ is an inner automorphism of $RG$ (see [3] for a published account).

2 **(Mod 2) conjugacy for involutions**

The main result of this section is Proposition 5, which will be used in conjunction with Proposition 1 to prove in the next section Lemma 7 for $p = 2$, which then allows application of Weiss’ theorem on $p$-permutation lattices in the proof of Theorem A and B.

We continue to denote by $G$ a finite group and by $R$ a $p$-adic ring. For a subgroup $H$ of $G$, let $I_R(H)$ denote the augmentation ideal of $RH$, i.e. the $R$-span of the elements $h - 1$ ($h \in H$). If $H$ is a normal subgroup, $I_R(H)G$ is the kernel of the natural map $RG \to RG/H$. For any subset $T$ of $G$, let $R[T]$ denote the $R$-span of the elements of $T$.

The Ward–Coleman Lemma suggests a closer investigation of $C_{V(RG)}(N)$, for $G$ and $N$ as in Theorems A and B.
Proposition 1. Suppose that $G$ has a normal $p$-subgroup $N$ that contains its centralizer $C_G(N)$. Then the following holds.

(a) $C_{RG}(N) \subseteq R + I_R(N)G + pRG$.

(b) Assume that $p = 2$ and set $\bar{G} = G/\Omega_2(G)$. If a subset $T$ of $G$ is chosen such that $\bar{T}$ is the set of involutions in $\bar{G}$, then

$$C_{RG}(N) \subseteq R + I_R(\Omega_2(G))G + 4RG + 2R[T].$$

PROOF. For $g \in G$ define its “$N$-class sum” $\mathcal{C}_g^N$ to be the sum (in $RG$) of the distinct $g^x$, $x \in N$. Note that the $N$-class sums form an $R$-basis of $C_{RG}(N)$. Let $g \in G$. If $C_N(g) = N$, then $g \in C_G(N) \leq N$ and $\mathcal{C}_g^N = g$, and if $|N : C_N(g)| = p^a > 1$, then $\mathcal{C}_g^N \in p^a g + I_R(N)G$. Hence (a) holds.

Set $N^* = N/\Phi(N)$, the quotient of $N$ by its Frattini subgroup $\Phi(N)$. The group $G$ acts by conjugation on the elementary abelian group $N^*$. Since $N$ is not centralized by $p'$-elements of $G \setminus \{1\}$, the kernel $K$ of this operation is a $p$-group (see [5, III, 3.18]), whence contained in $\Omega_2(G)$. Now let $p = 2$ and suppose that $|N : C_N(g)| = 2$ for some $g \in G$. Then $|N^* : C_{N^*}(g)| \leq 2$, so $g^2 \in K \leq \Omega_2(G)$ and $\mathcal{C}_g^N \in R + I_R(\Omega_2(G))G + 2R[T]$, which completes the proof of (b). □

In particular, we are led to consider units $u$ of order $p$ in $RG/N$ which map to 1 in $(R/pR)(G/N)$. The following well known lemma (cf. [21, Lemma (53.3)]) shows that this is actually only a matter for $p = 2$.

Lemma 2. Let $p$ be an odd prime. Then the group of units in $1 + pRG$ has no $p$-torsion.

PROOF. Suppose that $u$ is a unit of order $p$ in $u \in 1 + pRG$ and write $u = 1 + p^a x$ with $a \in \mathbb{N}$ such that $x \in RG \setminus pRG$. Writing out the binomial expansion for $(1+p^a x)^p = 1$ and solving for $x$, we get $p \cdot p^a x = -\sum_{n=2}^{p} \binom{p}{n} p^n a x^n$. But the right-hand side has a factor $p \cdot p^{2a}$ since $p > 2$. This contradiction proves the lemma. □

The reader might wish to convince himself that the statement of the lemma does not hold for $p = 2$, even if $u$ is assumed to have augmentation one.

As usual, we let $[RG, RG]$ denote the additive commutator of $RG$, defined by

$$[RG, RG] = R \langle g^h - g \mid g, h \in G \rangle = \{xy - yx \mid x, y \in RG\}.$$
The following formulas are well known (see, for example, [18, Lemma (7.1)]). We write $K$ for the quotient field of $R$, let $a_1, \ldots, a_l \in RG$ and $n \in \mathbb{N}$.

\[ [KG, KG] \cap RG = [RG, RG] \quad (1.1) \]
\[ [RG, RG]^p \subseteq pRG + [RG, RG] \quad (1.2) \]
\[ (a_1 + \cdots + a_l)^n \equiv a_1^n + \cdots + a_l^n \mod pRG + [RG, RG] \quad (1.3) \]

Let $G_{\rho'}$ denote the set of $p'$-elements of $G$. It follows immediately from (1.2) and (1.3) that for large enough $n \in \mathbb{N}$ (it suffices that $p^n$ is the order of a Sylow $p$-subgroup of $G$) and any $x \in RG$,

\[ x^{p^n} \in pRG + [RG, RG] + R[G_{\rho'}]. \quad (1.4) \]

Fix some $c \in G$. We define

\[ [RG]^{1-c} = R\langle g - g^c \mid g \in G \rangle = \{ x - x^c \mid x \in RG \}. \]

Set $C = \langle c \rangle$. If $RG$ is considered as a $C$-module for the “conjugation action” $m \cdot c = c^{-1}mc$ ($m \in RG$), then $[RG]^{1-c}$ is the image of the map $RG \xrightarrow{(1-c)} RG$. Since $H^1(C, RG) = 0$ (see [13, (1.4.1) Proposition]), $[RG]^{1-c}$ is also the kernel of the map $RG \xrightarrow{\hat{C}} RG$ where $\hat{C}$ denotes the sum of the elements in $C$. In particular, it follows that

\[ [KG]^{1-c} \cap RG = [RG]^{1-c}. \quad (2) \]

We remark that $[RG]^{1-c}$ is invariant under left (and right) multiplication with $c$. Also, if $c^2 = 1$, then $([RG]^{1-c})^2 \subseteq 2RG + [RG]^{c-1}$ in analogy to (1.2) holds since $(g - g^c)(h - h^c) = gh + (gh)^c - g^ch - (g^ch)^c$ for all $g, h \in G$.

**Lemma 3.** Let $c \in G$ and $u \in V(RG)$ be 2-elements. Assume that $c^2 = u^2$ and $c^{-1}u = 1 + 2f$ for some $f \in RG$. Then

(a) $f + f^2 \in 2RG + [RG]^{1-c}$;
(b) $f + f^{2n} \in 2RG + [RG, RG]$ for all $n \in \mathbb{N}$;
(c) $f \in 2RG + [RG, RG] + R[G_{2'}].$

**Proof.** Squaring the equation $c^{-1}u = 1 + 2f$ yields $1 + 4(f + f^2) = (c^{-1}u)^2$, so $4(f + f^2)u^{-1}c = c^{-1}u - u^{-1}c$. Now $c^{-1}u = cu^{-1}$ since $c^2 = u^2$, and it follows that $4(f + f^2)u^{-1}c = cu^{-1} - (cu^{-1})^c \in [RG]^{1-c}$. By (2), and since $c^{-1}u \in 1 + 2RG$, (a) follows. Now (b) follows inductively from (1.2) and $f + f^{2n} = (f + f^2) + (f + f^{2n-1})^2 - 2f(f + f^{2n-1})$. Part (c) follows from (b) and (1.4). □
Let \( T_2 \) be the set of involutions in \( G \).

**Lemma 4.** If \( x \in R[T_2] \cap I_R(G) \) then \( x^2 \in (R[G \setminus T_2] \cap [RG, RG]) + 2RG \).

**PROOF.** Write \( x = \sum_{s \in T_2} r_s(s - 1) \) with \( r_s \in R \) for all \( s \in T_2 \). Then
\[
x^2 = \sum_{s \in T_2} r_s^2(s - 1)^2 + \sum_{\{s, t\} \subseteq T_2, s \neq t} r_s r_t((s - 1)(t - 1) + (t - 1)(s - 1)).
\]
Let \( s, t \in T_2 \). Then \( (s - 1)^2 = 2(1 - s) \in 2RG \) and
\[
(s - 1)(t - 1) + (t - 1)(s - 1)
= 2(1 - s - t + st) - st + ts
\in \begin{cases} 2RG & \text{if } [s, t] = 1, \\ 2RG + (R[G \setminus T_2] \cap [RG, RG]) & \text{otherwise.} \end{cases}
\]
This proves the lemma. \( \square \)

It is evident that up to now, letting \( R \) be a \( p \)-adic ring was unnecessarily restrictive, but finally we shall use results of Weiss on permutation modules to prove:

**Proposition 5.** Suppose that \( p = 2 \), so that \( R \) is a 2-adic ring, and let \( c \in G \) and \( u \in V(RG) \) be 2-elements with \( c^2 = u^2 \) and \( c^{-1}u = 1 + 2f \) for some \( f \in 2RG + R[T_2] + R \). Then \( c \) and \( u \) are conjugate in the units of \( RG \).

**PROOF.** By Lemma 3(c), \( f \in 2RG + [RG, RG] + R[G_p] \). Compared with \( f \in 2RG + R[T_2] + R \), it follows that \( f \in 2RG + (R[T_2] \cap [RG, RG]) + R \). Taking augmentation gives \( f \in 2RG + (R[G \setminus T_2] \cap [RG, RG]) \), so that by Lemma 4, \( f^2 \in 2RG + (R[G \setminus T_2] \cap [RG, RG]) \). By Lemma 3(a), \( f + f^2 \in 2RG + [RG]^{1-c} \). The last three equations show that
\[
f \in 2RG + [RG]^{1-c}. \tag{3}
\]
Let \( C \) be a cyclic group with generator \( x \) of order the maximum of the orders of \( c \) and \( u \). Consider \( RG \) as an \( RC \)-lattice, the action of \( x \) given by \( m \cdot x = c^{-1}mu \) for all \( m \in RG \). A 1-cocycle \( \beta : C \to RG \) is defined by \( \beta(x) = f = (c^{-1}u - 1)/2 \). Notice that \( c \) and \( u \) are conjugate in the units of \( RG \) if \( \beta \) is a 1-coboundary: For if \( \beta(x) = m - c^{-1}mu \) for some \( m \in RG \), then \( v = 1 + 2m \) is a unit in \( RG \) (see [2, (5.10)]) and \( u = c^v \). The exact sequence \( 0 \to RG \to RG \to \overline{RG} \to 0 \) has cohomology exact sequence
\[
\cdots \to H^1(C, RG) \xrightarrow{2} H^1(C, RG) \xrightarrow{-} H^1(C, \overline{RG}) \to \cdots
\]
By [21, Theorem (50.2)], $RG$ is a monomial lattice for $C$ over $R$, so that 2 annihilates $H^1(C, RG)$ by [21, Lemma (53.1)]. Hence the cohomology exact sequence implies that $H^1(C, RG) \to H^1(C, R\bar{G})$ is injective. By (3), the class of $\beta$ maps to zero under this map; hence $\beta$ is a 1-coboundary, and $c$ and $u$ are conjugate in the units of $RG$.

3 Proof of the theorems

From now on, $G$ will be a finite group which has a normal $p$-subgroup $N$ containing its centralizer $C_G(N)$. Still, $R$ is a $p$-adic ring. Let $Q$ be a finite $p$-subgroup of $V(RG)$ containing $N$ as a normal subgroup. We set $M = RG$ and consider $M$ as $R(G \times Q)$-module, the action given by $m \cdot r(g, x) = g^{-1}rmx$ for all $g \in G$, $x \in Q$, $r \in R$ and $m \in M$. We shall write, for example, $M_{G \times 1}$ for the restriction of $M$ to $G$ (acting from the left).

We will need the following indecomposability criterion which is proved in greater generality in [10, p. 231]. For convenience of the reader, the (short) proof is included.

**Lemma 6.** As $R(G \times N)$-module, $M$ is indecomposable.

**PROOF.** Any endomorphism of $M_{G \times 1}$ is given by right multiplication with some element of $RG$, so $\text{End}_{R(G \times N)}(M) \cong C_{RG}(N)$. The radical quotient $C_{RG}(N)/\text{rad}(C_{RG}(N))$ is isomorphic to $C_{kG}(N)/\text{rad}(C_{kG}(N))$ where $k$ denotes the residue class field of $R$ (see [2, (5.22)]), and the latter quotient is isomorphic to $k$ by Proposition 1(a) since $I_k(N)G$ is nilpotent (see [2, (5.26)]). Hence $\text{End}_{R(G \times N)}(M)$ is local, and $M$ is indecomposable (see [2, (6.10)]). □

By the Ward–Coleman Lemma, we may fix (and do) for each $x \in Q$ some $g_x \in G$ such that $g_x^{-1}x \in C_{V(RG)}(N)$. Set $U = \langle g_x \mid x \in Q \rangle \leq G$. Note that for all $x, y \in Q$ we have $(g_xg_y)^{-1}xy = (g_y^{-1}y)(g_x^{-1}x)^y \in C_{V(RG)}(N)$. Since $C_G(N) \leq N$, it follows that $x \mapsto g_xN$ defines a surjective homomorphism $Q \to UN/N$. We set $F = O_p(G)$ (the Fitting subgroup of $G$) and $\bar{G} = G/F$. We shall extend the bar convention when writing $\bar{m}$ for the image of $m$ in $RG$ under the natural map $RG \to R\bar{G}$.

**Lemma 7.** Let $x \in Q$. Then $\bar{x} \in \bar{g}_x + pR\bar{G}$. Further, if $g_x \in F$ then $\bar{x} = 1$. In other words, $x \mapsto \bar{g}_x$ defines an isomorphism $\bar{Q} \to \bar{U}$, and $\bar{Q}$ maps onto $\bar{U}$ under the natural map $R\bar{G} \to (R/pR)\bar{G}$.
**PROOF.** Let \( x \in Q \). Since \( x \) has augmentation one, \( \bar{x} \in g_x + pRG \) by Proposition 1(a). Now assume that \( g_x \in F \) and, by way of contradiction, that \( \bar{x} \) has order \( p \). Then \( p = 2 \) by Lemma 2, and by Proposition 1(b), \( \bar{x} = g_x^{-1} \bar{x} \in R + 4RG + 2R[T] \) where \( T \) is the set of involutions in \( G \). Hence we may apply Proposition 5 (to the group \( \tilde{G} \), with \( c = 1 \) and \( u = \bar{x} \)) to conclude that \( \bar{x} = 1 \), a contradiction. The lemma is proved. \( \square \)

The next lemma is the place where Weiss’ theorem obviously comes into play.

For a subgroup \( H \) of \( G \) we shall write \( \hat{H} \) for the sum of its elements in \( RG \).

**Lemma 8.** \( M_{P \times Q} \) is a permutation lattice for \( P \times Q \) over \( R \).

**PROOF.** First, we consider the module \( \hat{F} M_{1 \times Q} \) which is isomorphic to \( R \tilde{G} \) with \( Q \) acting by right multiplication via \( Q \rightarrow \tilde{Q} \). Write \( \tilde{G} \) as a disjoint union \( \tilde{G} = \bigcup_i \tilde{h}_i \tilde{U} \) with \( h_i \in G \), and set \( B = \bigcup_i \{ \tilde{h}_i \bar{x} \mid x \in Q \} \). By Lemma 7, \( B \) reduces modulo \( pRG \) to the canonical basis \( \tilde{G} \) of \( (R/pR)\tilde{G} \), and \( |B| = |	ilde{G}| \).

Thus \( B \) is an \( R \)-basis of \( R \tilde{G} \) by Nakayama’s Lemma. Since the elements of \( B \) are permuted under the action of \( Q \) it follows that \( \hat{F} M_{1 \times Q} \) is a permutation lattice.

Next, we shall show that \( \hat{P} M \) is a permutation lattice for \( 1 \times Q \) over \( R \). Set \( V = \hat{P} M_{1 \times Q} \). Write \( G \) as a disjoint union \( G = \bigcup_i P_k U \) with \( k_i \in G \) and set \( B = \bigcup_i \{ \hat{P}k_i x \mid x \in Q \} \). Write \( s \) for the sum of the elements of some system of coset representatives of \( F \) in \( P \), so that \( \hat{P} = \hat{F}s \).

The lemma thus follows from Weiss’ theorem [21, Theorem (50.1)]. \( \square \)

We are now in a position to prove Theorem B. We shall make use of the elementary theory of vertices and sources, the Krull-Schmidt Theorem and the Mackey decomposition. As a general reference we give [2].

**Theorem 9.** If \( c \) is a unit in \( V(RG) \) of finite \( p \)-power order and \([N, c] = 1\), then \( c \in N \).

**PROOF.** Set \( C = \langle c \rangle \), and consider \( M \) as \( R(G \times N \times C) \)-module, the action of \( G \times N \) being given as before, and \( m \cdot y = my \) for \( m \in M \), \( y \in C \).
Note that $C$ acts trivially on $\hat{N}M$. Indeed, $\hat{N}M$ is a permutation module for $C$ by Lemma 8 and $C$ acts trivially on $\hat{N}M/p\hat{N}M$ by Proposition 1(a).

By Lemma 8,

$$M_{P \times N \times C} \cong \bigoplus_{j=1}^{n} \uparrow_{U_j}^{P \times N \times C}$$

(4)

for some subgroups $U_j$ of $P \times N \times C$. The number of summands equals the $R$-rank of the fixed point module $M_{P \times 1 \times C}$, which coincides with $M_{P \times 1 \times 1}$ ($= \hat{P}R\hat{G}$). Hence $n = |G : P|$. Since the modules $M_{P \times 1 \times 1}$ and $M_{1 \times N \times 1}$ are both free, it follows from (4) and Mackey decomposition that $U_j \cap (P \times 1 \times 1) = 1$ and $U_j \cap (1 \times N \times 1) = 1$ for all $j$. In particular, $|U_j| \leq |N| \cdot |C|$ for all $j$, and comparing ranks in (4) gives $|U_j| = |N| \cdot |C|$ for all $j$. Restricting to $N \times N \times C$ in (4) gives

$$M_{N \times N \times C} \cong \bigoplus_{j=1}^{[G:P]} \bigoplus_{U_j \cap (N \times N \times C) \cap a} \uparrow_{U_j \cap (N \times N \times C)}^{N \times N \times C}.$$ 

The number of summands in this decomposition is the $R$-rank of $M_{N \times N \times C}$. Since $M_{N \times N \times C} = M_{N \times 1 \times 1}$ there are $[G : N]$ summands. It follows that $U_j \leq N \times N \times C$ for all $j$. Hence $U_j = \{(x, (x\alpha_j)z_j^{-1}, c) \mid x \in N, i \in \mathbb{Z}\}$ for some $z_j \in Z(N)$ and $\alpha_j \in Aut(N)$, and $\uparrow_{U_j}^{G \times N \times C}$ is isomorphic to $\uparrow_{U_j \cap (G \times N \times 1)}^{G \times N \times 1}$, that is, to $RG$, the action given by $m \cdot (g, x, 1) = g^{-1}m(x\alpha_j^{-1})$ for all $g \in G$, $x \in N$ and $m \in RG$. By Lemma 6, it follows that the modules $\uparrow_{U_j}^{G \times N \times C}$ are indecomposable. Since $M$ is relatively $P \times N \times C$-projective, $M$ is a direct summand of $M_{P \times N \times C} \uparrow_{G \times N \times C}$, and by (4)

$$M_{P \times N \times C} \uparrow_{G \times N \times C} \cong \bigoplus_{j=1}^{[G:P]} \uparrow_{U_j}^{G \times N \times C}.$$ 

By Lemma 6, $M$ is indecomposable, so it follows that $M \cong \uparrow_{U_j}^{G \times N \times C}$ for some $j$. Since $(G \times 1 \times 1) \cap U_j = 1$, this shows that there is $u \in M$ such that $Gu$ is an $R$-basis of $M$ and $u = u \cdot (1, z_j^{-1}, c) = uz_j^{-1}c$. It follows that $u$ is a unit in $RG$ and $c = z_j$. □

**Corollary 10.** If $x \in Q$ and $x \in 1 + I_R(N)G$ then $x \in N$.

**PROOF.** For such an $x$ we have $g_x \in N$ by Proposition 1(a), so $x \in N$ follows from Theorem 9, applied to $c = g_x^{-1}x \in C_Q(N)$. □

**Lemma 11.** $M_{1 \times Q}$ is a free $RQ$-module.

**PROOF.** By Lemma 8, $M_{1 \times Q}$ is a permutation lattice for $Q$ over $R$. By Corollary 10, the kernel of the natural map $Q \to V(RG/N)$ is $N$. By Proposi-
tion 1(a), an element $x$ in $Q$ acts on $\tilde{N}RG/p\tilde{N}RG$ by right multiplication with $g_x$. Since $N \leq Q$ and $RG/N$ is free for the multiplication action of $UN/N$—recall that $U = \{g_x \mid x \in Q\}$—it follows that $|Q| = |UN|$ and that each orbit of the action of $Q$ on a basis of $M_{i \times Q}$ the elements of which it permutes has length $|Q|$. □

Finally we prove Theorem A, again guided by the remarks from [10, p. 231].

**Theorem 12.** There is a unit $u$ of $RG$ with $Q \leq Pu$ and $N = Nu$.

**Proof.** By Lemma 8,

$$M_{P \times Q} \cong \bigoplus_{k=1}^{l} 1_{V_k}^{\uparrow P \times Q}$$

for some subgroups $V_k$ of $P \times Q$. Since the modules $M_{P \times 1}$ and $M_{1 \times Q}$ are both free (the latter by Lemma 11), it follows from Mackey decomposition that $V_k \cap (P \times 1) = 1$ and $V_k \cap (1 \times Q) = 1$ for all $k$. We shall show that the induced modules $1_{V_k}^{\uparrow G \times Q}$ are indecomposable. Mackey decomposition gives

$$M_{P \times N} \cong \bigoplus_{k=1}^{l} \bigoplus_{V_k \cap (P \times N)} 1_{V_k}^{\uparrow P \times N}.$$

If $g_1, \ldots, g_{[G:P]}$ is a system of right coset representatives of $P$ in $G$, then

$$M_{P \times N} \cong \bigoplus_{j=1}^{[G:P]} 1_{U_j}^{\uparrow P \times N}$$

where $U_j = \{(n, n^{g_j}) \mid n \in N\}$.

Let $1 \leq k \leq l$. From the above, it follows that there is $j = j(k)$ such that without lost of generality $V_k \cap (P \times N) = U_j$. In particular, $U_j \leq V_k$. Altogether, we see that there is a subgroup $Q_k$ of $Q$ containing $N$ so that $V_k = \{(x\beta_k, x) \mid x \in Q_k\}$ for some injective homomorphism $\beta_k : Q_k \rightarrow P$. Hence the induced module $1_{V_k}^{\uparrow G \times Q_k}$ is isomorphic to the $R(G \times Q_k)$-module $RG$, the operation given by $m \cdot (g, x) = g^{-1}m(x\beta_k)$ for all $g \in G$, $x \in Q_k$ and $m \in RG$, and so is indecomposable by Lemma 6 since $N\beta_k = N$. Repeated application of Green’s Indecomposability Theorem [2, (19.22)] now yields that $1_{V_k}^{\uparrow G \times Q}$ is indecomposable.

Since $M$ is relatively $P \times Q$-projective, $M$ is a direct summand of $M_{P \times Q}^{\uparrow G \times Q}$, and by (5)

$$M_{P \times Q}^{\uparrow G \times Q} \cong \bigoplus_{k=1}^{l} 1_{V_k}^{\uparrow G \times Q}.$$
By Lemma 6, $M$ is indecomposable. Hence $M \cong 1\bigg|_{V_k}^{G \times Q}$ for some $k$. Comparing ranks shows that $Q_k = Q$. Since $V_k \cap (G \times 1) = 1$, this means that there is $u \in M$ such that $Gu$ is an $R$-basis of $M$, i.e., $u$ is a unit in $RG$, and $u = u \cdot (x\beta_k, x) = (x^{-1}\beta_k)ux$ for all $x \in Q$. In other words, $Q \leq P^u$ and $N = N^u$. □

References

[1] D. B. Coleman, On the modular group ring of a $p$-group, Proc. Amer. Math. Soc. 15 (1964) 511–514.

[2] C. W. Curtis, I. Reiner, Methods of representation theory. Vol. I, John Wiley & Sons Inc., New York, 1981, With applications to finite groups and orders, A Wiley-Interscience Publication.

[3] M. Hertweck, Automorphisms of principal blocks stabilizing Sylow subgroups, Arch. Math. (Basel) 82 (3) (2004) 193–199.

[4] M. Hertweck, W. Kimmerle, On principal blocks of $p$-constrained groups, Proc. London Math. Soc. (3) 84 (1) (2002) 179–193.

[5] B. Huppert, Endliche Gruppen. I, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.

[6] B. Huppert, N. Blackburn, Finite groups. II, Vol. 242 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 1982, AMD, 44.

[7] S. Jackowski, Z. Marciniak, Group automorphisms inducing the identity map on cohomology, J. Pure Appl. Algebra 44 (1-3) (1987) 241–250.

[8] G. Karpilovsky, Unit groups of group rings, Vol. 47 of Pitman Monographs and Surveys in Pure and Applied Mathematics, Longman Scientific & Technical, Harlow, 1989.

[9] G. R. Robinson, The $Z_p^*$-theorem and units in blocks, J. Algebra 134 (2) (1990) 353–355.

[10] K. W. Roggenkamp, Some new progress on the isomorphism problem for integral group rings, in: Ring theory (Granada, 1986), Vol. 1328 of Lecture Notes in Math., Springer, Berlin, 1988, pp. 227–236.

[11] K. W. Roggenkamp, The isomorphism problem for integral group rings of finite groups, in: Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, pp. 369–380.

[12] K. W. Roggenkamp, Subgroup rigidity of $p$-adic group rings (Weiss arguments revisited), J. London Math. Soc. (2) 46 (3) (1992) 432–448.
[13] K. Roggenkamp, L. Scott, Isomorphisms of $p$-adic group rings, Ann. of Math. (2) 126 (3) (1987) 593–647.

[14] K. W. Roggenkamp, Group rings: units and the isomorphism problem, in: Group rings and class groups, Vol. 18 of DMV Sem., Birkhäuser, Basel, 1992, pp. 1–152, with contributions by W. Kimmerle and A. Zimmermann.

[15] A. I. Saksonov, Group rings of finite groups. I, Publ. Math. Debrecen 18 (1971) 187–209 (1972).

[16] L. L. Scott, Recent progress on the isomorphism problem, in: The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), Vol. 47 of Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, RI, 1987, pp. 259–273.

[17] L. L. Scott, Defect groups and the isomorphism problem, Astérisque (181-182) (1990) 257–262.

[18] S. K. Sehgal, Units in integral group rings, Vol. 69 of Pitman Monographs and Surveys in Pure and Applied Mathematics, Longman Scientific & Technical, Harlow, 1993, with an appendix by Al Weiss.

[19] H. N. Ward, Some results on the group algebra of a group over a prime field, in: Seminar in Group Theory, Harvard University, 1960-61, pp. 13–19, mimeographed notes.

[20] A. Weiss, Rigidity of $p$-adic $p$-torsion, Ann. of Math. (2) 127 (2) (1988) 317–332.

[21] A. Weiss, Rigidity of $\pi$-adic $p$-torsion, appendix in Sehgal [18], pp. 309–329.