# ON OLIVER'S $p$-GROUP CONJECTURE: II

DAVID J. GREEN, LÁSZLÓ HÉTHELYI, AND NADIA MAZZA

Abstract. Let $p$ be an odd prime and $S$ a finite $p$-group. B. Oliver's conjecture arises from an open problem in the theory of $p$-local finite groups. It is the claim that a certain characteristic subgroup $\mathfrak{X}(S)$ of $S$ always contains the Thompson subgroup. In previous work the first two authors and M. Lilienthal recast Oliver's conjecture as a statement about the representation theory of the factor group $S/\mathfrak{X}(S)$. We now verify the conjecture for a wide variety of groups $S/\mathfrak{X}(S)$.

## 1. Introduction

Let $p$ be an odd prime and $S$ a finite $p$-group. An open question in the theory of $p$-local finite groups asks whether there is a unique centric linking system associated to every fusion system (see the survey article [4] by Broto, Levi and Oliver). Bob Oliver derived in [13] a purely group-theoretic conjecture which would imply existence and uniqueness of the linking system, at least at odd primes. He constructed a characteristic subgroup $\mathfrak{X}(S)$, and conjectured that it always contains the Thompson subgroup $J(S)$ generated by the elementary abelian subgroups of greatest rank. The first two authors and M. Lilienthal studied Oliver's conjecture in [8] and recast it as a question about the quotient group $G = S/\mathfrak{X}(S)$.

In this paper we shall use methods from the area of finite group theory known as Thompson factorization (see §32 in Aschbacher's book [2]) to study the properties of certain faithful $\mathbb{F}_pG$-modules which arise in this reformulation of Oliver's conjecture. This allows us to prove the conjecture for a wide variety of quotient groups $G$. Our main result is as follows:

**Theorem 1.1.** *Suppose that $p$ is an odd prime and $S$ is a $p$-group such that $S/\mathfrak{X}(S)$ satisfies any of the following conditions*

(1) *its (nilpotence) class is at most four;*
(2) *it is metabelian;*
(3) *it is of maximal class;*

*Date*: 24 January 2009.

2000 *Mathematics Subject Classification.* Primary 20D15.

*Key words and phrases.* $p$-group; offending subgroup; quadratic offender; Timmesfeld replacement theorem; $p$-local finite group.

Héthelyi supported by the Hungarian Scientific Research Fund OTKA, grant T049 841.

(4) *its p-rank is at most p.*

*Then Oliver's conjecture $J(S) \leq \mathfrak{X}(S)$ holds for $S$.*

*Remark.* Alperin showed that every regular 3-group is metabelian [1]. So Oliver's conjecture also holds if $S/\mathfrak{X}(S)$ is a regular 3-group.

*Remark.* Every $p$-group $G$ does indeed occur as such a quotient $G = S/\mathfrak{X}(S)$, by Lemma 2.3 of [8]. A computation using GAP [6] shows that the iterated wreath product group $G = C_3 \wr C_3 \wr C_3$ satisfies none of the above conditions. This group has order $3^{13}$ and class 9, so it is neither class $\leq 4$ or maximal class. The derived subgroup has class 3, so it is not metabelian. And the "double diagonal" subgroup shows that the rank is at least 9.

Theorem 1.1 follows by translating the following two module-theoretic results back into the original language of Oliver's conjecture. The notions of "quadratic element" and "$F$-module" are recalled in §2 and §4, respectively.

**Theorem 1.2.** *Suppose that $G$ is a $p$-group and $V$ is a faithful $\mathbb{F}_pG$-module such that $\Omega_1(Z(G))$ has no quadratic elements. If $G$ satisfies either of the following conditions*

(1) *$G$ has class at most four;*
(2) *$G$ is metabelian;*

*then $V$ cannot be an $F$-module.*

Notice that the assumption that there are no quadratic elements in $\Omega_1(Z(G))$ implies that the prime $p$ has to be odd. Recall now that the rank of an elementary abelian $p$-group is its dimension as $\mathbb{F}_p$-vector space, and that the $p$-rank of a finite group is the maximum of the ranks of its elementary abelian $p$-subgroups.

**Theorem 1.3.** *Suppose that $p$ is an odd prime, that $G$ is a $p$-group, and that $V$ is a faithful $\mathbb{F}_pG$-module such that every non-identity element of $\Omega_1(Z(G))$ acts with minimal polynomial $X^p - 1$. If $G$ satisfies either of the following conditions*

(1) *$G$ is of maximal class;*
(2) *the $p$-rank of $G$ is at most $p$;*

*then $V$ cannot be an $F$-module.*

A key step in the proof of Theorem 1.2 is the following result. We recall the term "offender" in §4 below.

**Theorem 1.4.** *Let $G$ be a $p$-group and $V$ a faithful $\mathbb{F}_pG$-module such that there are no quadratic elements in $\Omega_1(Z(G))$.*

(1) *If $A$ is an abelian normal subgroup of $G$, then $A$ does not contain any offender.*
(2) *Suppose that $E$ is an offender. Then $[G', E] \neq 1$.*

*Proof of Theorem 1.1.* The condition in Theorem 1.3 on the minimal polynomial of each non-identity element of $\Omega_1(Z(G))$ is condition (PS) of [8]. Since $p > 2$, this condition implies that there are no quadratic elements in $\Omega_1(Z(G))$. Now combine our Theorems 1.2 and 1.3 with Theorem 1.2 of [8]. $\square$

*Proof of Theorem 1.2.* Theorem 5.2 deals with the case of class at most four, and Theorem 6.2 treats the metabelian case. $\square$

*Proof of Theorem 1.3.* Theorem 8.1 handles the case $p$-rank$(G) \leq p$. Lemma 7.1 shows that groups of maximal class have $p$-rank at most $p$. $\square$

For sake of completeness, we remind the reader that the Oliver subgroup $\mathfrak{X}(S)$ is the largest normal subgroup of $S$ that has a $Q$-series; that is, there are an integer $n \geq 1$ and a series $1 = Q_0 \leq Q_1 \leq \cdots \leq Q_n = \mathfrak{X}(S)$ of normal subgroups $Q_i$ of $S$ and such that $[\Omega_1(C_S(Q_{i-1})), Q_i; p-1] = 1$, for all $1 \leq i \leq n$.

*Structure of the paper* In §2 we comment on a few commutator relations in a semidirect product and introduce some handy notation for these. In the short §3 we recall a lemma of Meierfrankenfeld and Stellmacher. We prove Theorem 1.4 in §4, after recalling Timmesfeld's replacement theorem. In §5 we derive a result (Lemma 5.1) about offenders and central series and apply this to the case of class at most four. We treat the metabelian case in §6, and show in §7 that every group of maximal class has $p$-rank at most $p$. Finally, §8 is concerned with the case of a finite $p$-group of $p$-rank at most $p$ of Theorem 1.3.

## 2. Two notational conventions

Throughout the paper, $G$ denotes a finite $p$-group, for an odd prime $p$. We adopt the usual notation and conventions from the group theory literature (see for example [5]). In addition, if $V$ is a *right* $\mathbb{F}_pG$-module, we also view $V$ as an elementary abelian $p$-group, written additively, and form the semidirect product $\Gamma := G \ltimes V$, with $V$ the normal subgroup. The group multiplication in $\Gamma$ is

$$(g, v)(h, w) = (gh, v * h + w)\,,$$

where we use $*$ to denote the module action of $\mathbb{F}_pG$ on $V$.

Our second convention regards the commutators. For any $a, b \in G$, we set

$$[a, b] := a^{-1}b^{-1}ab \quad \text{and} \quad [a_1, a_2, \ldots, a_{n+1}] = [[a_1, \ldots, a_n], a_{n+1}]\ .$$

Inductively, we define $[a, b; 1] = [a, b]$ and $[a, b; n] = [[a, b; n-1], b]$, for all $n \geq 2$. In particular, $g \in G$ identifies with $(g, 0) \in \Gamma$ and $v \in V$ with $(1, v) \in \Gamma$. Hence, the commutator $[v, g]$ can be written as

$$\begin{aligned}[(1, v), (g, 0)] &= (1, -v)(g^{-1}, 0)(1, v)(g, 0) \\ &= (1, -v)(1, v * g) = (1, v * g - v) = (1, v * (g-1))\,.\end{aligned}$$

That is,

$$[v, g] = v * (g - 1)\,. \tag{1}$$

In particular, $[v, g^p] = v * (g^p - 1) = v * (g - 1)^p = [v, g; p]$, and so

$$[v, g^p] = [v, g; p] \,. \tag{2}$$

By identifying $G$ and $V$ with the corresponding subgroups of $\Gamma$, one obtains

$$C_V(H) = \{v \in V \mid \forall h \in H \ v * h = v\} = V^H$$

for a subgroup $H \leq G$, and

$$C_G(V) = \{g \in G \mid \forall v \in V \ v * g = v\} \trianglelefteq G \,.$$

Note that the $\mathbb{F}_pG$-module $V$ is faithful if and only if $C_G(V) = 1$. In this paper we will only be interested in faithful modules.

*Definition.* Let $G$ be a $p$-group and $V$ a faithful $\mathbb{F}_pG$-module. A non identity element $g \in G$ is called *quadratic on* $V$ if $[V, g, g] = 0$. If there is no confusion for $V$, we simply say that $g$ is *quadratic*. Since $[V, g^p] = [V, g; p]$, faithfulness implies that quadratic elements must have order $p$.

## 3. A lemma of Meierfrankenfeld and Stellmacher

*Definition* ([12] 2.3). Let $G$ be a finite group and $V$ a faithful $\mathbb{F}_pG$-module. For a subgroup $H \leq G$ one sets

$$j_H(V) := \frac{|H| \, |C_V(H)|}{|V|} \in \mathbb{Q} \,.$$

Note that $j_1(V) = 1$.

**Lemma 3.1** (Lemma 2.6 of [12]). *Let $A$ be an abelian group and $V$ a faithful $\mathbb{F}_pA$-module. Let $H, K$ be two subgroups of $A$. Then*

$$j_{HK}(V) j_{H \cap K}(V) \geq j_H(V) j_K(V) \,,$$

*with equality if and only if $C_V(H \cap K) = C_V(H) + C_V(K)$.*

*Proof.* Since $\langle H, K\rangle = HK$, we have an equality $C_V(HK) = C_V(H) \cap C_V(K)$. In addition, $C_V(H \cap K) \supseteq C_V(H) + C_V(K)$. Therefore,

$$\begin{aligned} j_{HK}(V) j_{H\cap K}(V) &= \tfrac{|HK||C_V(HK)||H\cap K||C_V(H\cap K)|}{|V|^2} \geq \\ &\geq \tfrac{|HK||H\cap K||C_V(H)||C_V(K)|}{|V|^2} = j_H(V) j_K(V) \,, \end{aligned}$$

because $|HK| \, |H \cap K| = |H| \, |K|$. ∎

## 4. Offenders and abelian normal subgroups

*Notation.* Let $G$ be a finite group and $p$ a fixed prime number. We denote by $\mathscr{E}(G)$ the poset of non-trivial elementary abelian $p$-subgroups of $G$.

*Definition* ([7] 26.5). Let $G$ be a finite group and $V$ a faithful $\mathbb{F}_pG$-module. A subgroup $E \in \mathscr{E}(G)$ is an *offender of* $G$ *on* $V$ if $j_E(V) \geq 1$. If there is no confusion on $G$ and $V$, we simply say that $E$ is an *offender*. If $V$ has an offender, then $V$ is called an *$F$-module*. An offender $E$ is *quadratic on* $V$ (or simply *quadratic*) if $[V, E, E] = 0$. Define

$$\mathscr{P}(G, V) := \{E \leq G \mid E \in \mathscr{E}(G) \text{ and } j_E(V) \geq j_F(V) \ \forall\, 1 \leq F \leq E\}\,.$$

Consequently every $E \in \mathscr{P}(G, V)$ is an offender, and every minimal[1] offender lies in $\mathscr{P}(G, V)$.

Note that $V$ is an $F$-module if and only if $\mathscr{P}(G, V)$ is nonempty. The subgroups in $\mathscr{P}(G, V)$ are sometimes called *best offenders*.

We shall assume that the reader is familiar with Chermak's treatment [5] of Timmesfeld's replacement theorem [14].

**Lemma 4.1.** *Let $V$ be a faithful $\mathbb{F}_pG$-module and $E \in \mathscr{P}(G, V)$. Then there is a quadratic offender $F \in \mathscr{P}(G, V)$ which satisfies $j_F(V) = j_E(V)$ and $F \leq E$.*

*Proof.* This is Timmesfeld's replacement theorem ([5, Theorem 2]), applied with $F = C_E([V, E])$. The construction of $F$ implies $[V, F, F] = 0$. □

*Remark.* Note that Timmesfeld's replacement theorem also gives the decomposition $C_V(F) = [V, E] + C_V(E)$ .

**Lemma 4.2.** *Let $G$ be a $p$-group and $V$ a faithful $\mathbb{F}_pG$-module such that there are no quadratic elements in $\Omega_1(Z(G))$. Then $E \cap Z(G) = 1$ for every quadratic offender $E$. In particular, a quadratic offender does not contain any non-trivial normal subgroup of $G$.*

*Proof.* Let $E$ be a quadratic offender. We have $E \cap Z(G) = E \cap \Omega_1(Z(G))$. Now, every non-trivial element of $E$ is quadratic, whereas no element of $\Omega_1(Z(G))$ is. Hence, $E \cap Z(G) = 1$. The last statement follows from the fact that every non-trivial normal subgroup meets $Z(G)$. □

We are now ready to show Theorem 1.4.

*Proof of Theorem 1.4.* We first show the implication (1) $\Rightarrow$ (2). Let $E$ be an offender. Then $Z(G'E)$ is an abelian normal subgroup of $G$, since $G'E \trianglelefteq G$. By part (1), this means that $E \nleq Z(G'E)$. Since $E$ is abelian, this can only happen if $[G', E] \neq 1$.

For part (1), suppose that $A$ does contain an offender $E$. Note that $E$ lies in the elementary abelian subgroup $C := \Omega_1(A)$. Of course, $V$ is faithful as an $\mathbb{F}_pC$-module. Set

$$j_0 := \max\{j_E(V) \mid E \in \mathscr{E}(C)\}$$

[1] That is, a minimal element of the set of offenders, partially ordered by inclusion.

Choose $E \in \mathscr{E}(C)$ with $j_E(V) = j_0$. Note that every such $E$ lies in $\mathscr{P}(G, V)$. By Lemma 4.1 we may assume that $E$ is quadratic. Among the quadratic offenders in $A$ (and hence in $C$) with $j_E(V) = j_0$, let us pick $E$ of minimal order. We claim that $E$ is a T.I. subgroup of $G$, that is $E \cap E^g = 1$, for all $g \in G - N_G(E)$. Note that since $C$ is normal in $G$, then all the $G$-conjugates of $E$ lie in $C$. Observe also that $E$ lies in $\mathscr{M}(C, V)$, in the terminology of [5, Lemma 1], since $C$ is elementary abelian and we chose $j_E(V)$ maximal. So every $G$-conjugate of $E$ lies in $\mathscr{M}(C, V)$. By Lemma 1 of [5], the intersection of any family of conjugates of $E$ lies in $\mathscr{M}(C, V)$, and hence, the minimality assumption on the order of $E$ forces any such intersection to be trivial, whenever it is a proper subgroup of $E$. So $E$ is a T.I. subgroup of $G$, as claimed.

Now $E \ntrianglelefteq G$ by Lemma 4.2. Hence 1 is an intersection of conjugates of $E$. This implies that $j_0 = j_1(V) = 1$. Let $F$ be a $G$-conjugate of $E$, with $F \neq E$, and hence $F \cap E = 1$, since $E$ is a T.I. subgroup of $G$. Moreover, we have equalities $j_E(V) = j_F(V) = j_1(V) = 1$, and also $j_{EF}(V) \leq j_0 = 1$, as $EF \leq C$ is elementary abelian. So from Lemma 3.1 we deduce that $j_{EF}(V) = 1$ and that $V = C_V(1) = C_V(E) + C_V(F)$. So Lemma 4.3 shows that $[V, E] \subseteq C_V(H)$, where $H \leq A$ is the normal closure of $E$ in $G$. The same argument shows that $[V, F] \subseteq C_V(H)$ for every conjugate $F$ of $E$. We therefore deduce that

$$[V, H] \subseteq C_V(H)\,. \tag{3}$$

Now, $H \in \mathscr{E}(C)$, since $E \in \mathscr{E}(C)$ and $C$ is a normal elementary abelian subgroup of $G$. So $H$ is itself a quadratic offender, by Eqn. (3). But $H$ is also normal in $G$, so $H$ contradicts Lemma 4.2. □

**Lemma 4.3.** *Let $A$ be an abelian subgroup of a $p$-group $G$ such that $[A, B] = 1$ for every $G$-conjugate $B$ of $A$. Let $V$ be an $\mathbb{F}_pG$-module such that $[V, A, A] = 0$ and $V = C_V(A) + C_V(B)$ for every conjugate $B \neq A$ of $A$. Then $[V, A] \leq C_V(H)$, where $H$ is the normal closure of $A$ in $G$.*

*Proof.* It suffices to show that $[V, A] \leq C_V(B)$ for every $G$-conjugate $B$ of $A$, since $C_V(H)$ is the intersection of all the $C_V(B)$. For $B = A$, we have $[V, A, A] = 0$, by assumption. For $B \neq A$, let $v \in V$, $a \in A$ and $b \in B$. By hypothesis, there is a decomposition $v = u + w$ with $u \in C_V(A)$ and $w \in C_V(B)$. Thus,

$$[v, a, b] = [u, a, b] + [w, a, b] = [w, a, b] = w * (a - 1)(b - 1) = w * (b - 1)(a - 1)\,,$$

and so $[v, a, b] = [w, b, a] = 0$, as was left to be shown. □

## 5. Central series

Recall the following terminology. Given a finite group $G$, the ascending central series is defined inductively by $Z_0(G) = 1$ and $Z_{r+1}(G)$ is the normal subgroup of $G$ containing $Z_r(G)$ and such that $Z_{r+1}(G)/Z_r(G) = Z(G/Z_r(G))$, for all $r \geq 1$. The descending central series is given by $K_1(G) = G$ and inductively $K_{r+1}(G) = [K_r(G), G]$, for all $r \geq 1$. The class $n$ of $G$ is the smallest number such that $Z_n(G) = G$. This is also the smallest number such that $K_{n+1}(G) = 1$. Note that if the class is $n$, then

$$K_{n+1-r}(G) \leq Z_r(G) \quad (0 \leq r \leq n). \tag{4}$$

Further details are given in [9, III.1], or also [2, (8.7)], where $K_r(G)$ is denoted by $L_r(G)$. From the Three Subgroups Lemma ([2, (8.7)]), we have

$$[K_r(G), K_s(G)] \leq K_{r+s}(G)\,. \tag{5}$$

We shall make repeated use of the following lemma from [8]:

> [8]**, Lemma 4.1.** Suppose that $p$ is an odd prime, that $G \neq 1$ is a finite $p$-group, and that $V$ is a faithful $\mathbb{F}_pG$-module. Suppose that $A, B \in G$ are such that $C := [A, B]$ is a non-trivial element of $C_G(A, B)$. If $C$ is non-quadratic, then so are $A$ and $B$.

**Lemma 5.1.** *Let $G$ be a $p$-group of class $n$, let $V$ be a faithful $\mathbb{F}_pG$-module, and suppose that $E$ is a quadratic offender. If $2r \geq n$ and $K_{r+1}(G)$ contains no quadratic elements, then*

$$[K_r(G), E] = 1\,.$$

*In particular if $n \geq 4$ and there are no quadratic elements in $\Omega_1(Z(G))$, then*

$$[K_{n-2}(G), E] = 1\,.$$

*Remark.* The last part has no meaning for $n \leq 2$, and the example discussed in [8, §5] shows that it is false for $n = 3$.

*Proof.* We prove the first part by induction, starting with $r = n$ and working downwards. We have $[K_n(G), E] \leq K_{n+1}(G) = 1$, by Equation (5), and so the claim holds for $r = n$. Now, let $\frac{n}{2} \leq r < n$ and suppose that $[K_{r+1}(G), E] = 1$. If $[K_r(G), E] \neq 1$, then there are $a \in K_r(G)$ and $e \in E$ with $c := [a, e] \neq 1$. Since $c \in K_{r+1}(G)$, we have $[c, a] \in [K_{r+1}(G), K_r(G)] \leq K_{2r+1}(G) \leq K_{n+1}(G) = 1$. Moreover, $[c, e] = 1$ since $c \in K_{r+1}(G)$ and the inductive hypothesis states that $[K_{r+1}(G), E] = 1$. In other words, we have $1 \neq c = [a, e]$ with $e$ quadratic and $[c, a] = [c, e] = 1$. But then, [8, Lemma 4.1] says that $c$ is quadratic, which contradicts the assumption that no quadratic element lies in $K_{r+1}(G)$.

For the second part, if $n \geq 4$, we have $2r \geq n$ for $r = n-2$. So, it is enough to show that $K_{n-1}(G)$ contains no quadratic element. As recalled above, there is an inclusion $K_{n-1}(G) \leq Z_2(G)$. By [8, Lemma 4.1], since $\Omega_1(Z(G))$ does not contain any quadratic elements, there are no quadratic elements in $Z_2(G)$ either. □

**Theorem 5.2.** *Suppose that $G$ is a $p$-group and $V$ is a faithful $\mathbb{F}_pG$-module such that $\Omega_1(Z(G))$ has no quadratic elements. If $G$ has class at most four then $V$ cannot be an $F$-module.*

*Proof.* Recall that $V$ is an $F$-module if and only if $\mathscr{P}(G, V)$ is not empty. By definition of $\mathscr{P}(G, V)$, every offender contains an element of $\mathscr{P}(G, V)$, and by

Timmesfeld's replacement theorem (Lemma 4.1), every offender contains a quadratic offender which lies in $\mathscr{P}(G, V)$. It therefore suffices to prove that there are no quadratic offenders. Let $E \in \mathscr{E}(G)$. From part (2) of Theorem 1.4, we have $[G', E] \neq 1$ if $E$ is a quadratic offender.

If $G$ has class three or less, then $[G', E] \leq Z(G)$. Since $\Omega_1(Z(G))$ contains no quadratic elements, neither does the setwise commutator $[G', E]$. Thus, [8, Lemma 4.1] shows that $E$ is not a quadratic offender.

Now assume the class is four. In this case we have $G' = K_2(G) = K_{4-2}(G)$ and so $[G', E] = 1$ by Lemma 5.1. So, $E$ is not a quadratic offender. □

## 6. Metabelian groups

Recall that a group is metabelian if and only if its derived subgroup is abelian. In this section we will need the following well-known result:

**Lemma 6.1.** *Suppose that $G$ is a finite group and that $A$ is an abelian normal subgroup such that $G/A$ is cyclic, generated by the coset $xA$ of $x \in G$. Then $G' = \{[a, x] \mid a \in A\}$.*

*Proof.* This is Lemma 4.6 of Isaacs' book [10], or more precisely the equality $\theta(A) = G'$ in the proof. It is also Aufgabe 2 a) on p. 259 of Huppert's book [9]. □

**Theorem 6.2.** *Suppose that $G$ is a $p$-group and $V$ is a faithful $\mathbb{F}_pG$-module such that $\Omega_1(Z(G))$ has no quadratic elements. If the derived subgroup $G'$ is abelian, then $V$ cannot be an $F$-module.*

*Proof.* As noted in the proof of Theorem 5.2, if $V$ is an $F$-module then there is a quadratic offender $E$. From Part (2) of Theorem 1.4, we then have $[G', E] \neq 1$. So, there is an $a \in E$ with $[G', a] \neq 1$. The subgroup $K := G'\langle a \rangle$ of $G$ is a non-abelian normal subgroup of $G$. In particular, $K' \cap \Omega_1(Z(G)) > 1$. Let $c \in K' \cap \Omega_1(Z(G))$ be a non-identity element. By Lemma 6.1 there is an element $b \in G'$ with $c = [b, a]$. So $c$ must be quadratic by [8, Lemma 4.1], since $a$ is quadratic and $c$ is central. But that cannot be, for $c$ lies in $\Omega_1(Z(G))$ and is therefore non-quadratic by assumption. □

**Corollary 6.3.** *Suppose that $G$ is a $p$-group and $V$ is a faithful $\mathbb{F}_pG$-module such that $\Omega_1(Z(G))$ has no quadratic elements. Suppose that $G$ has an abelian normal subgroup $A \trianglelefteq G$ such that $G/A$ is abelian too. Then $V$ cannot be an $F$-module.*

*Proof.* As $G/A$ is abelian, we have $G' \leq A$ and hence $G'$ is abelian. □

## 7. Maximal class

**Lemma 7.1.** *Let $G$ be a finite $p$-group of maximal class. Then the $p$-rank of $G$ is at most $p$. Moreover, if $p$ is odd, only the wreath product $C_p \wr C_p$ has $p$-rank $p$.*

*Remark.* This fact does not appear to be generally known. However, we believe that it is remarked in passing by Berkovich [3].

Let us also point out that the definition of $p$-groups of maximal class may vary. Indeed, in [9], Huppert allows abelian groups of order $p^2$ to be of maximal class, whereas in [11] Leedham-Green and McKay stipulate that groups of maximal class have order at least $p^4$. We follow Huppert's conventions.

*Proof.* Let $G$ be a finite $p$-group of order $p^n$ and maximal class $n-1$. First we consider the small cases with $n \leq p+1$. An abelian group of order $p^2$ has $p$-rank at most two. A nonabelian group of order 8 can have 2-rank at most two. If $p$ is odd and $G$ is nonabelian with an elementary abelian subgroup of rank $p$, then its order must be at least $p^{p+1}$. So to finish off the cases with $n \leq p+1$, we just need to consider the case where $p$ is odd, $n = p+1$ and $G$ contains an elementary abelian subgroup $V$ of rank $p$. As $G$ is not abelian, the $p$-rank of $G$ is $p$. As $V$ has index $p$ in $G$, it is normal and the factor group $G/V$ has order $p$. Since $G$ has class $p$, the group $G/V$ acts on $V$ as one $(p \times p)$-Jordan block with eigenvalue 1. Let $a \in G \setminus V$. Then, $a$ acts on $V$ with minimal polynomial $(x-1)^p$ and $G = \langle V, a\rangle$. Note that $a^p \in V$ lies in the one-dimensional eigenspace, i.e. the center $Z(G)$ of $G$. So replacing $a$ by $ab$ for a suitably chosen element $b$ of the set-theoretic difference $V \setminus [V, a]$, we may assume that $a^p = 1$. Hence the extension splits, and $G$ is isomorphic to the wreath product $C_p \wr C_p$.

From now on we assume that $|G| = p^n$ with $n \geq p+2$, and we appeal to the following results of [9, III]. By 14.16 Satz, we have that $G_1 = C_G(K_2(G)/K_4(G))$ is regular, and that $|G_1 \colon \mho_1(G_1)| = p^{p-1}$, and so, by 10.7 Satz, $|\Omega_1(G)| = p^{p-1}$. Thus, if $G$ contains an elementary abelian subgroup $V$ of rank $p$, then $V$ contains some $g \in G \setminus G_1$. It is hence enough to show that no element of order $p$ in $G \setminus G_1$ has a centralizer of $p$-rank greater than $p-1$. By 14.6 Hauptsatz b), $G$ is not exceptional, as $n \geq p+2$. Recall that by 14.5 Definition, exceptional groups arise for $n \geq 5$, whence this result is relevant only for $n \geq p+2$ and for $p$ odd. Now, we apply 14.13 Hilfsatz b), which states that if $g \in G \setminus G_1$, then $|C_G(g)| = p^2$. Consequently, $G$ has at most rank $p-1$. $\square$

## 8. Rank $p$

**Theorem 8.1.** *Suppose that $p$ is odd, that $G$ is a $p$-group, and that $V$ is a faithful $\mathbb{F}_pG$-module such that every non-identity element of $\Omega_1(Z(G))$ acts with minimal polynomial $X^p-1$. If the $p$-rank of $G$ is at most $p$, then $V$ cannot be an $F$-module.*

Recall that the condition that every element of $\Omega_1(Z(G))$ acts with minimal polynomial $X^p - 1$ is condition (PS) of [8].

*Proof.* Suppose that $V$ is an $F$-module. By Lemma 4.1, $\mathscr{P}(G, V)$ contains a quadratic offender $E$. Since $E \cap Z(G) = 1$ and $G$ has rank $p$, the rank of $E$ can be at most $p-1$. So by Lemma 8.2 below, the rank of $E$ is exactly $p-1$. Moreover, the normal closure $F$ of $E$ in $N_G(N_G(E))$ is elementary abelian of rank $p$, since it is strictly larger than $E$. Pick $h \in N_G(N_G(E)) \setminus N_G(E)$. Then $E^h \neq E$, so $F = \langle E, E^h \rangle$. Moreover $E \cap E^h$ must have size at least $p^{p-2}$ and is therefore nontrivial. Pick $1 \neq c \in E^h \cap E$. By Lemma 8.2 Eqn. (6), this means that $C_V(E) = C_V(c) = C_V(E^h)$ and therefore $C_V(F) = C_V(E)$. So given that $j_E(V) = 1$, the definition of $j_F$ means that $j_F(V) = p$. But this contradicts Timmesfeld's replacement theorem (Lemma 4.1), as there is no quadratic offender $H$ with $j_H(V) = p$. □

**Lemma 8.2.** *Suppose that $p$ is odd, that $G$ is a $p$-group, and that $V$ is a faithful $\mathbb{F}_pG$-module such that every non-identity element of $\Omega_1(Z(G))$ acts with minimal polynomial $X^p - 1$.*

(1) *If $E \in \mathscr{E}(G)$ is an offender, then its rank is at least $p-1$.*
(2) *If $E \in \mathscr{E}(G)$ is a rank $p-1$ offender, then $E$ is a quadratic offender and lies in $\mathscr{P}(G,V)$. Moreover, $j_E(V) = 1$; we have*
$$C_V(g) = C_V(E) \quad \text{for every } 1 \neq g \in E; \tag{6}$$
*and the normal closure $F$ of $E$ in $N_G(N_G(E))$ is elementary abelian with $F > E$.*

*Proof.* Every offender contains an element of $\mathscr{P}(G,V)$, which in turn contains a quadratic offender. So minimal elements of the poset of offenders are quadratic and lie in $\mathscr{P}(G,V)$. So it is enough to consider the case of a quadratic offender $E$.

For all $g \in E$ the subspace $C_V(g)$ of $V$ is $Z(G)$-invariant: if $z \in Z(G)$ and $v \in C_V(g)$ then
$$[v * z, g] = v * z * (g-1) = v * (g-1) * z = 0\,.$$
Now choose a non-identity element $g \in E$, and let $i$ be the smallest integer such that $[V, Z(G); i] \subseteq C_V(g)$. We claim that $[V, Z(G); i] \subseteq C_V(g^h)$ for every $h \in G$. To see this, note that $[V, Z(G); i]$ is an invariant subspace of $V$, and therefore $[V, Z(G); i] * h^{-1} = [V, Z(G); i]$. Hence
$$[[V, Z(G); i], g^h] = [V, Z(G); i] * h^{-1} * (g-1) * h = [V, Z(G); i] * (g-1) * h = 0\,.$$
This means that $[V, Z(G); i] \subseteq C_V(H)$, where $H$ is the normal closure of $\langle g \rangle$ in $G$. So $H \cap \Omega_1(Z(G)) \neq 1$, and for any $z \in H \cap \Omega_1(Z(G))$ we have that $[V, z; i+1] = 0$. The minimal polynomial assumption on $\Omega_1(Z(G))$ therefore implies that $i+1 \geq p$: and so the definition of $i$ means that $|V : C_V(g)| \geq p^{p-1}$. As $C_V(E) \subseteq C_V(g)$, it follows that $|V : C_V(E)| \geq p^{p-1}$. But $|E| = j_E(V)\,|V : C_V(E)|$, and $j_E(V) \geq 1$ since $E$ is an offender. This proves the first part.

Second part: If $E$ is a rank $p-1$ offender, then it is minimal in the poset of offenders, therefore quadratic and a member of $\mathscr{P}(G,V)$. The proof of the first part shows Eqn. (6). It also shows that $j_E(V) = 1$ and that $|V : C_V(E)| = p^{p-1}$.

Set $N = N_G(E)$. Observe that $N_G(N) > N$, since $E \ntrianglelefteq G$ by Lemma 4.2. This shows that $F > E$. Pick $g, h \in N_G(N)$ with $Ng \neq Nh$. Then $E^g, E^h \leq N$; and as $N_G(E^g) = N_G(E)^g = N$, we see that $E^g, E^h$ normalize each other. If they always centralize each other, then $F$ is indeed elementary abelian, since it is generated by all such $E^g$. So suppose $a \in E^g$, $b \in E^h$ have nontrivial commutator $c = [a, b]$. As $E^g, E^h$ normalize each other, we have $c \in E^g \cap E^h$. Since $E^g, E^h$ are rank $p-1$ offenders, it follows by Eqn. (6) that $C_V(a) = C_V(c) = C_V(b)$. So $[a, b] = 1$ by Lemma 8.3 below, a contradiction. □

**Lemma 8.3.** *Let $G$ be a $p$-group and $V$ is a faithful $\mathbb{F}_pG$-module. Suppose that $a, b \in G$ satisfy either of the following conditions:*

(1) *$a, b$ are quadratic, and $C_V(a) = C_V(b)$; or*
(2) *$[V, a] \subseteq C_V(b)$ and $[V, b] \subseteq C_V(a)$.*

*Then $[a, b] = 1$.*

*Proof.* Recall that $[V, a] \subseteq C_V(a)$, for any quadratic element $a \in G$. So $[V, a] \subseteq C_V(b)$ and $[V, b] \subseteq C_V(a)$ do hold if $a, b$ are quadratic and have the same centralizer in $V$. That is, the first case is a consequence of the second one.

In the second case we have $[V, a, b] = [V, b, a] = 0$, using additive notation in the $\mathbb{F}_pG$-module $V$. Hence, a routine computation yields $[V, [a, b]] = 0$. Since $V$ is faithful, we deduce that $[a, b] = 1$, as claimed. □

## References


[1] J. L. Alperin. On a special class of regular $p$-groups. *Trans. Amer. Math. Soc.*, 106:77–99, 1963.

[2] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[3] Y. Berkovich. On subgroups and epimorphic images of finite $p$-groups. *J. Algebra*, 248(2):472–553, 2002.

[4] C. Broto, R. Levi, and B. Oliver. The theory of $p$-local groups: a survey. In P. Goerss and S. Priddy, editors, *Homotopy theory: relations with algebraic geometry, group cohomology, and algebraic $K$-theory*, volume 346 of *Contemp. Math.*, pages 51–84. Amer. Math. Soc., Providence, RI, 2004.

[5] A. Chermak. Quadratic action and the $\mathscr{P}(G, V)$-theorem in arbitrary characteristic. *J. Group Theory*, 2(1):1–13, 1999.

[6] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.10*, 2007. (`http://www.gap-system.org`).

[7] D. Gorenstein, R. Lyons, and R. Solomon. *The classification of the finite simple groups. Number 2*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1996.

[8] D. J. Green, L. Héthelyi, and M. Lilienthal. On Oliver's $p$-group conjecture. *Algebra Number Theory*, 2(8):969–977, 2008. arXiv:0804.2763v2 [math.GR].

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

[10] I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[11] C. R. Leedham-Green and S. McKay. *The structure of groups of prime power order*, volume 27 of *London Mathematical Society Monographs. New Series*. Oxford University Press, Oxford, 2002. Oxford Science Publications.

[12] U. Meierfrankenfeld and B. Stellmacher. The other $\mathscr{P}(G,V)$-theorem. *Rend. Sem. Mat. Univ. Padova*, 115:41–50, 2006.

[13] B. Oliver. Equivalences of classifying spaces completed at odd primes. *Math. Proc. Cambridge Philos. Soc.*, 137(2):321–347, 2004.

[14] F. Timmesfeld. A remark on Thompson's replacement theorem and a consequence. *Arch. Math. (Basel)*, 38(6):491–495, 1982.

Department of Mathematics, Friedrich-Schiller-Universität Jena, 07737 Jena, Germany

*E-mail address*: `David.Green@uni-jena.de`

Department of Algebra, Budapest University of Technology and Economics, Budapest, Hungary

Department of Mathematics and Statistics, Fylde College, Lancaster University, Lancaster LA1 4YF, United Kingdom