# Conjugacy classes and characters of finite $p$-groups

László Héthelyi
Department of Algebra
Budapest University of Technology and Economics
H-1521 Budapest Műegyetem Rkp. 3-9
Hungary
hethelyi@math.bme.hu

Burkhard Külshammer
Mathematisches Institut
Friedrich-Schiller-Universität
07743 Jena
Germany
kuelshammer@uni-jena.de

Benjamin Sambale
Mathematisches Institut
Friedrich-Schiller-Universität
07743 Jena
Germany
benjamin.sambale@uni-jena.de

November 30, 2009

**Abstract**

Let $K$ be a conjugacy class of a finite $p$-group $G$ where $p$ is a prime, and let $K^{-1}$ denote the conjugacy class of $G$ consisting of the inverses of the elements in $K$. We observe that, in several cases, the number of elements in the product $KK^{-1}$ is congruent to 1 modulo $p-1$, and we pose the question in which generality this congruence is valid. We also consider related properties of the class multiplication constants of $G$. Furthermore, let $\chi$ be an irreducible character of $G$, and let $\overline{\chi}$ denote the complex conjugate of $\chi$. We show that, in several cases, the number of irreducible constituents of the product $\chi\overline{\chi}$ is congruent to 1 modulo $p-1$, and we pose the question in which generality this congruence is valid.

## 1 Introduction

This paper is motivated by results of Adan-Bante [1], [2]. Let $G$ be a finite $p$-group where $p$ is a prime, and let $K \in \mathrm{Cl}(G)$ where $\mathrm{Cl}(G)$ denotes the set of conjugacy classes of $G$. Then

$$K^{-1} := \{a^{-1} : a \in K\} \in \mathrm{Cl}(G),$$

and the product $KK^{-1} = \{ab^{-1} : a, b \in K\}$ is a union of conjugacy classes of $G$. We denote the number of conjugacy classes of $G$ contained in $KK^{-1}$ by $\eta(K)$. In [2], Adan-Bante proved that

$$\eta(K) \geq n(p-1)+1 \text{ whenever } |K| = p^n.$$

Moreover, she showed that this bound is sharp. Our own interest started with the observation that, in many cases, we have

$$\eta(K) \equiv 1 \pmod{p-1}. \tag{P1}$$

Of course, the length $|K|$ of $K$ is a power of $p$; in particular, $|K| \equiv 1 \pmod{p-1}$. Thus $\eta(K) \equiv |KK^{-1}| \pmod{p-1}$, so that (P1) is equivalent to

$$|KK^{-1}| \equiv 1 \pmod{p-1}. \tag{P2}$$

At present, we do not have a single example where these congruences are violated. In this paper, we approach the problem via the class multiplication constants of $G$. Thus, in the following, we denote by $\mathbb{Z}G$ the integral group ring of $G$ and, for a subset $X$ of $G$, we set $X^+ := \sum_{x \in X} x \in \mathbb{Z}G$. Then the class sums $K^+$ ($K \in \mathrm{Cl}(G)$) form a $\mathbb{Z}$-basis of the center $\mathrm{Z}(\mathbb{Z}G)$ of $\mathbb{Z}G$. For $K, L, M \in \mathrm{Cl}(G)$ and $z \in M$, the nonnegative integer

$$c_{KLM} := |\{(x, y) \in K \times L : xy = z\}|$$

is called a class multiplication constant; it is independent of the choice of $z$. Moreover we have

$$K^+L^+ = \sum_{M \in \mathrm{Cl}(G)} c_{KLM} M^+, \tag{$\star$}$$

and $c_{KLM} \neq 0$ if and only if $M \subseteq KL$. The map

$$\epsilon : \mathbb{Z}G \to \mathbb{Z}, \ \sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g,$$

is a homomorphism of rings called the augmentation map of $\mathbb{Z}G$. Applying $\epsilon$ to the equation ($\star$) we obtain

$$1 \equiv |K||L| = \sum_{M \in \mathrm{Cl}(G)} c_{KLM}|M| \equiv \sum_{M \in \mathrm{Cl}(G)} c_{KLM} \pmod{p-1}.$$

Suppose that the following condition is satisfied:

$$c_{KK^{-1}L} \equiv 1 \pmod{p-1} \text{ for all } L \in \mathrm{Cl}(G) \text{ such that } L \subseteq KK^{-1}. \tag{P3}$$

Then

$$\eta(K) = \sum_{\substack{L \in \mathrm{Cl}(G) \\ L \subseteq KK^{-1}}} 1 \equiv \sum_{\substack{L \in \mathrm{Cl}(G) \\ L \subseteq KK^{-1}}} c_{KK^{-1}L} = \sum_{L \in \mathrm{Cl}(G)} c_{KK^{-1}L} \equiv 1 \pmod{p-1}.$$

This shows that (P3) implies (P1) and (P2). We will prove that, in several "small" cases, $c_{KK^{-1}L}$ is in fact a power of $p$, for all $K, L \in \mathrm{Cl}(G)$ such that $L \subseteq KK^{-1}$, a property which is slightly stronger than (P3). However, we will also give an example of a group of order $3^7$ where (P3) does not hold.

The questions above can also be dualized: Let $\chi \in \mathrm{Irr}(G)$ where $\mathrm{Irr}(G)$ denotes the set of irreducible characters of $G$. Then $\overline{\chi}$, the complex conjugate of $\chi$, is again an irreducible character of $G$, and the product $\chi\overline{\chi}$ is a character of $G$. In [1], Adan-Bante proved that

$$|\operatorname{Irr}(\chi\overline{\chi})| \geq 2n(p-1) + 1 \text{ whenever } \chi(1) = p^n;$$

here $\mathrm{Irr}(\xi)$ denotes the set of irreducible constituents of a character $\xi$ of $G$. Adan-Bante also showed that her bound is sharp. Our own interest started with the observation that, in many cases, we have

$$|\operatorname{Irr}(\chi\overline{\chi})| \equiv 1 \pmod{p-1}. \tag{Q1}$$

At present, we do not have a single example where this congruence is violated. In the following, we write

$$(\chi|\psi)_G := \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi}(g),$$

for complex characters $\chi, \psi$ of $G$. Then, for $\psi \in \mathrm{Irr}(G)$, $(\chi|\psi)_G$ is the multiplicity of $\psi$ as an irreducible constituent of $\chi$; in particular, we have

$$\chi(1) = \sum_{\psi \in \mathrm{Irr}(G)} (\chi|\psi)_G \psi(1). \tag{$\star\star$}$$

Suppose now that $\chi \in \mathrm{Irr}(G)$. Then $\chi(1)$ is a power of $p$; in particular, we have $\chi(1) \equiv 1 \pmod{p-1}$. Thus $(\star\star)$ implies that

$$1 \equiv \chi(1)^2 = (\chi\overline{\chi})(1) \equiv \sum_{\psi \in \mathrm{Irr}(\chi\overline{\chi})} (\chi\overline{\chi}|\psi)_G \pmod{p-1}.$$

Thus suppose that the following holds, for every $\chi \in \mathrm{Irr}(G)$ and every $\psi \in \mathrm{Irr}(\chi\overline{\chi})$:

$$(\chi\overline{\chi}|\psi)_G \equiv 1 \pmod{p-1}. \tag{Q2}$$

Then $1 \equiv \sum_{\psi \in \mathrm{Irr}(\chi\overline{\chi})} 1 = |\mathrm{Irr}(\chi\overline{\chi})| \pmod{p-1}$, so that (Q2) implies (Q1). We will prove that, in several "small" cases, $(\chi\overline{\chi}|\psi)_G$ is in fact a power of $p$, for all $\chi \in \mathrm{Irr}(G)$ and all $\psi \in \mathrm{Irr}(\chi\overline{\chi})$, a property slightly stronger than (Q2). However, we will also give an example of a group of order $3^7$ where (Q2) does not hold.

It is perhaps of interest to point out some connections of this paper to other results in the literature. J. G. Thompson has conjectured that every nonabelian finite simple group $G$ contains a conjugacy class $K$ such that $KK = G$. It is easy to see that then $K = K^{-1}$, so that also $KK^{-1} = G$, and $\eta(K) = |\mathrm{Cl}(G)|$. Thompson's conjecture is a strengtheninig of a conjecture by Ore which claims that every element in a nonabelian finite simple group can be written as a commutator. Also, there have been considerable efforts in recent years to determine the so-called covering number

$$\mathrm{cn}(G) = \max_{K \in \mathrm{Cl}(G)} \{n \in \mathbb{N} : K^n = G \neq K^{n-1}\}$$

of a finite simple group $G$ (see [3] and [15], for example). So one can view our results and questions on conjugacy classes as variants of these problems.

Of course, our results on class multiplication constants contribute to the general theory of integral group rings and their centers (see [12], for example).

Every finite group $G$ acts on itself by conjugation, and the character of the corresponding permutation module is $\sum_{\chi \in \mathrm{Irr}(G)} \chi\overline{\chi}$. Thus, looking at the Wedderburn decomposition

$$\mathbb{C}G = \bigoplus_{\chi \in \mathrm{Irr}(G)} A_\chi$$

of the group algebra $\mathbb{C}G$, the character $\chi\overline{\chi}$ of $G$ comes from the conjugation action of $G$ on the minimal ideal $A_\chi$ of $\mathbb{C}G$, for $\chi \in \mathrm{Irr}(G)$.

We also note that our results on characters are related to the theory of S-characters (see p. 161 in [4], for example). A character $\theta$ of a finite group $G$ is called an S-character if $(\theta|1_G)_G = 1$ and $\theta(g) \geq 0$ for every $g \in G$. Important examples are provided by characters of the form $\chi\overline{\chi}$ where $\chi \in \mathrm{Irr}(G)$, and by characters of the form $(1_H)^G$ where $H \leq G$.

H. Blau [5] has pointed out that some of our questions can also be formulated in the framework of integral table algebras (see [6], for example). However, we do not pursue this direction here.

Some of the results in this paper are taken from the Diplomarbeit [13] of the third author written under the direction of the second author.

Most of our notation will be standard. We write $H \leq G$ if $H$ is a subgroup of $G$, and $H \trianglelefteq G$ if $H$ is a normal subgroup of $G$. For $a, b \in G$, the element $[a,b] := aba^{-1}b^{-1}$ is called a commutator. For subsets $A, B$ of $G$, we set $[A,B] := \langle [a,b] : a \in A,\ b \in B \rangle$ where $\langle X \rangle$ denotes the subgroup of $G$ generated by $X \subseteq G$. Then $G' := [G,G]$ is the commutator subgroup of $G$. We denote the derived series of $G$ by

$$G = G^{(0)} \geq G^{(1)} = G' \geq G^{(2)} \geq \ldots,$$

the lower central series of $G$ by

$$G = K_1(G) \geq K_2(G) = G' \geq K_3(G) \geq \ldots,$$

and the upper central series of $G$ by

$$1 = Z_0(G) \leq Z_1(G) = \mathrm{Z}(G) \leq Z_2(G) \leq \ldots.$$

The nilpotency class of $G$ will be denoted by $\mathrm{cl}(G)$. We write $a =_G b$ if $a, b$ are conjugate elements of $G$. We denote the set of maximal subgroups of $G$ by $\mathrm{Max}(G)$, and the set of maximal abelian normal subgroups of $G$ by $\mathrm{SCN}(G)$ (cf. [8]). Recall that $\mathrm{C}_G(A) = A$ for $A \in \mathrm{SCN}(G)$. Also, we denote the set of integers by $\mathbb{Z}$, the set of positive integers by $\mathbb{N}$ and the set of nonnegative integers by $\mathbb{N}_0$. For $i \in \mathbb{N}_0$, we set

$$\Omega_i(G) := \langle g \in G : g^{p^i} = 1 \rangle \text{ and } \mho_i(G) := \langle g^{p^i} : g \in G \rangle.$$

Moreover, we denote the Frattini subgroup of $G$ by $\Phi(G)$. We set

$$\widehat{G} := \{\chi \in \mathrm{Irr}(G) : \chi(1) = 1\}.$$

Then $\widehat{G}$ is a group under multiplication, and $\widehat{G} \cong G/G'$. The trivial character $1_G$ is the identity element of $\widehat{G}$. For $\chi \in \mathrm{Irr}(G)$, we set

$$\mathrm{Z}(\chi) := \{g \in G : |\chi(g)| = \chi(1)\}.$$

Then $\ker(\chi) \trianglelefteq \mathrm{Z}(\chi) \trianglelefteq G$. For $H \leq G$ and a character $\xi$ of $G$, we denote its restriction to $H$ by $\xi_H$. Also, for a character $\phi$ of $H$, we denote its induction to $G$ by $\phi^G$. Moreover, we write $\rho_G$ for the regular character of $G$. If $N$ is a normal subgroup of $G$ and $\psi$ is a character of $G/N$, we will often identify $\psi$ with its inflation to $G$. Also, for $\nu \in \mathrm{Irr}(N)$, we denote its inertia group in $G$ by $\mathrm{I}_G(\nu)$.

## 2 Class multiplication constants

In the following, we fix a prime number $p$ and a finite $p$-group $G$. We start by proving some general elementary facts on the class multiplication constants $c_{KLM}$, for $K, L, M \in \mathrm{Cl}(G)$. These results will be used throughout the paper.

**Lemma 2.1.** *Let $x \in K \in \mathrm{Cl}(G)$, let $L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$ (so that $L \cap xK^{-1} \neq \emptyset$), and let $t \in L \cap xK^{-1}$. Then the following hold:*

*(i)* $c_{KK^{-1}L} \leq |K| \leq |KK^{-1}|$;

*(ii)* $c_{KK^{-1}L} = |K| \;\Leftrightarrow\; L \subseteq xK^{-1}$;

*(iii)* $L \subseteq \mathrm{Z}(G) \;\Rightarrow\; c_{KK^{-1}L} = |K|$;

*(iv)* $|K| = |KK^{-1}| \;\Rightarrow\; c_{KK^{-1}L} = |K|$;

*(v)* $c_{KK^{-1}L} \geq |\,\mathrm{C}_G(t) : \mathrm{C}_G(t) \cap \mathrm{C}_G(x)| \geq \frac{|K|}{|L|}$;

*(vi)* $|KK^{-1} \cap \mathrm{Z}(G)| \leq \eta(K) \leq |K|$;

*(vii)* $\eta(K) = |K| \;\Rightarrow\; c_{KK^{-1}L} = \frac{|K|}{|L|}$;

*(viii)* $|\,\mathrm{C}_G(x) : \mathrm{C}_G(x) \cap \mathrm{C}_G(t)| \leq |L \cap xK^{-1}| \leq |L|$;

*(ix)* $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(t) \trianglelefteq G \;\Rightarrow\; c_{KK^{-1}L} = |L \cap xK^{-1}| \frac{|K|}{|L|}$.

*Proof.* Since $L \subseteq KK^{-1}$, there are $g, h \in G$ such that $gxg^{-1} \cdot hx^{-1}h^{-1} \in L$. Then $x \cdot g^{-1}hx^{-1}h^{-1}g \in L \cap xK^{-1}$, so that indeed $L \cap xK^{-1} \neq \emptyset$.

(i) The inequality $|K| \leq |KK^{-1}|$ is trivial. Moreover, for $a \in K$, there is at most one $b \in K^{-1}$ such that $ab = t$. Thus

$$c_{KK^{-1}L} = |\{(a, b) \in K \times K^{-1} : ab = t\}| \leq |K|.$$

(ii) Suppose first that $c_{KK^{-1}L} = |K|$, and let $g \in G$. Then, by the proof of (i), there exists $h \in G$ such that $t = gxg^{-1} \cdot hx^{-1}h^{-1}$. Thus $g^{-1}tg = x \cdot g^{-1}hx^{-1}h^{-1}g \in xK^{-1}$. This shows that $L \subseteq xK^{-1}$.

Now suppose conversely that $L \subseteq xK^{-1}$, and let $g \in G$. Then there is $h \in G$ such that $gtg^{-1} = xhx^{-1}h^{-1}$. Thus $t = g^{-1}xg \cdot g^{-1}hx^{-1}h^{-1}g$, and the proof of (i) implies that $c_{KK^{-1}L} = |K|$.

(iii) If $L \subseteq \mathrm{Z}(G)$ then $L = \{t\} \subseteq xK^{-1}$, and the result follows from (ii).

(iv) Suppose that $|KK^{-1}| = |K| = |xK^{-1}|$. Since $xK^{-1} \subseteq KK^{-1}$ this implies that $L \subseteq KK^{-1} = xK^{-1}$. Thus (iv) follows from (ii).

(v) Since $\mathrm{C}_G(t)$ acts by conjugaction on the set $\{(a,b) \in K \times K^{-1} : ab = t\}$ and since $c := |\mathrm{C}_G(t) : \mathrm{C}_G(t) \cap \mathrm{C}_G(x)|$ is the length of the orbit $(x, x^{-1}t)$, we have

$$c_{KK^{-1}L} \geq c \geq \frac{|\mathrm{C}_G(t)|}{|\mathrm{C}_G(x)|} = \frac{|K|}{|L|}.$$

(vi) The inequality $|KK^{-1} \cap \mathrm{Z}(G)| \leq \eta(K)$ is trivial. Since every element in $KK^{-1}$ is conjugate to an element in $xK^{-1}$, we get $\eta(K) \leq |K|$.

(vii) Suppose that $\eta(K) = |K|$. Then the proof of (vi) shows that any two elements of $xK^{-1}$ are contained in distinct conjugacy classes of $G$. So there is a unique $y \in K^{-1}$ such that $xy \in L$. Since this holds for every $x \in K$, the conclusion follows.

(viii) The inequality $|L \cap xK^{-1}| \leq |L|$ is trivial. Moreover, $\mathrm{C}_G(x)$ acts on $L \cap xK^{-1}$ via conjugation, and $|\mathrm{C}_G(x) : \mathrm{C}_G(x) \cap \mathrm{C}_G(t)|$ is the length of the orbit of $t$ under this action.

(ix) Suppose that $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(t) \trianglelefteq G$, and let $n := |L \cap xK^{-1}|$. We write $L \cap xK^{-1} = \{a_1 t a_1^{-1}, \ldots, a_n t a_n^{-1}\}$ and $a_i t a_i^{-1} = x k_i x^{-1} k_i^{-1}$ for $i = 1, \ldots, n$.

Let $g, h \in G$ be such that $t = gxg^{-1} \cdot hx^{-1}h^{-1}$. Then $g^{-1}tg = x \cdot g^{-1}hx^{-1}h^{-1}g \in L \cap xK^{-1}$. Thus $g^{-1}tg = a_j t a_j^{-1}$ for some $j \in \{1, \ldots, n\}$ and $ga_j \in C_G(t)$, i. e. $g \in \mathrm{C}_G(t)a_j^{-1} = a_j^{-1}\,\mathrm{C}_G(t)$.

Conversely, let $g \in \mathrm{C}_G(t)a_j^{-1}$ for some $j \in \{1, \ldots, n\}$. Then $c := ga_j \in \mathrm{C}_G(t)$. Setting $h := ca_j^{-1}k_j$ we have

$$gxg^{-1} \cdot hx^{-1}h^{-1} = ca_j^{-1}xa_jc^{-1}ca_j^{-1}k_jx^{-1}k_j^{-1}a_jc^{-1} = ca_j^{-1}a_jta_j^{-1}a_jc^{-1} = ctc^{-1} = t.$$

This shows:

$$c_{KK^{-1}L} = |\{gxg^{-1} : g \in \bigcup_{i=1}^{n} a_i^{-1}\,\mathrm{C}_G(t)\}|.$$

Let $i, j \in \{1, \ldots, n\}$ and $c, d \in \mathrm{C}_G(t)$ be such that $a_i^{-1}cxc^{-1}a_i = a_j^{-1}dxd^{-1}a_j$. Then $c^{-1}a_ia_j^{-1}d \in \mathrm{C}_G(x) \subseteq \mathrm{C}_G(t)$ and $a_ia_j^{-1} \in \mathrm{C}_G(t)$. Thus $i = j$ and $cxc^{-1} = dxd^{-1}$. This implies that $c^{-1}d \in \mathrm{C}_G(x)$, and we have shown:

$$c_{KK^{-1}L} = n|\,\mathrm{C}_G(t) : \mathrm{C}_G(x)| = n\frac{|K|}{|L|}. \qquad \square$$

Now we investigate the connection between the class multiplication constants of $G$ and of $G/N$, for $N \trianglelefteq G$. These results will allow us to use induction on $|G|$.

**Lemma 2.2.** *Let $K, L \in \mathrm{Cl}(G)$, and let $N \trianglelefteq G$. Then $\overline{K} := \{aN : a \in K\}$ and $\overline{L} := \{bN : b \in L\}$ are conjugacy classes of $\overline{G} := G/N$. If $KLN = KL$ then $|KL| = |\overline{KL}| \cdot |N| \equiv |\overline{KL}| \pmod{p-1}$.*

*Proof.* Let $a_1, \ldots, a_r \in G$ be such that $KL$ is the disjoint union of $a_1N, \ldots, a_rN$. Then

$$|KL| = r|N| = |\overline{KL}||N| \equiv |\overline{KL}| \pmod{p-1}. \qquad \square$$

The following result will be useful in order to construct suitable normal subgroups $N$ of $G$.

**Lemma 2.3.** *If $z \in \mathrm{Z}(G)$ and $K \in \mathrm{Cl}(G)$ then $zK \in \mathrm{Cl}(G)$. In this way $\mathrm{Z}(G)$ acts on $\mathrm{Cl}(G)$. For $K \in \mathrm{Cl}(G)$, the stabilizer of $K$ in $\mathrm{Z}(G)$ is $Z := KK^{-1} \cap \mathrm{Z}(G)$.*

*Proof.* The first two statements are obvious. Let $z \in \mathrm{Z}(G)$, $K \in \mathrm{Cl}(G)$ and $a \in K$. Then the following holds:

$$zK = K \iff za \in K \iff z \in Ka^{-1} \iff z \in KK^{-1},$$

and the result follows. $\square$

Our next result is a variant of Lemma 2.2.

**Lemma 2.4.** *Let $K, L, M \in \mathrm{Cl}(G)$, and let $N \trianglelefteq G$. We denote the images of $K, L, M$ in $\overline{G} := G/N$ by $\overline{K}, \overline{L}, \overline{M}$, respectively. If $MN = M$ then the class multiplication constants $c_{KLM}$ and $c_{\overline{KLM}}$ differ by a factor which is a power of $p$. In particular, we have:*

*(i)* $c_{KLM} = 0 \Leftrightarrow c_{\overline{KLM}} = 0$;
*(ii)* $c_{KLM} \equiv 1 \pmod{p-1} \Leftrightarrow c_{\overline{KLM}} \equiv 1 \pmod{p-1}$.

*Proof.* The canonical epimorphism $G \to \overline{G}$ induces a ring homomorphism $\nu : \mathbb{Z}G \to \mathbb{Z}\overline{G}$. Applying $\nu$ to the equation $(\star)$ we obtain

$$\frac{|K| \cdot |L|}{|\overline{K}| \cdot |\overline{L}|} \overline{K}^+ \overline{L}^+ = \sum_{C \in \mathrm{Cl}(G)} c_{KLC} \frac{|C|}{|\overline{C}|} \overline{C}^+.$$

The hypothesis $MN = M$ implies that $M$ is the only conjugacy class of $G$ which maps onto $\overline{M}$. Thus $|K| \cdot |L| \cdot |\overline{M}| \cdot c_{\overline{KLM}} = |\overline{K}| \cdot |\overline{L}| \cdot |M| \cdot c_{KLM}$, and the result follows. □

The following elementary fact will be applied in connection with Lemma 2.1.

**Lemma 2.5.** *Let $g, h \in G$ and $i, j \in \mathbb{Z}$ be such that $i \not\equiv j \pmod{p}$ and $[h, g^i] =_G [h, g^j]$. Then $g \in \mathrm{C}_G(h)$.*

*Proof.* Let $G$ be a counterexample of minimal order. Since $\overline{G} := G/\mathrm{Z}(G)$, $\overline{g} := g\,\mathrm{Z}(G)$ and $\overline{h} := h\,\mathrm{Z}(G)$ also satisfy the hypothesis of the lemma, minimality ensures that $\overline{g} \in \mathrm{C}_G(\overline{h})$. Thus $[h, g^i] \in \mathrm{Z}(G)$, and our hypothesis implies that $[h, g^i] = [h, g^j]$. Hence $g^{i-j} \in \mathrm{C}_G(h)$, and the result follows. □

# 3 Elementary results on conjugacy classes

Let $G$ be a finite $p$-group where $p$ is a prime. In this section we are going to present some elementary positive results concerning (P1), (P2) and (P3). We begin with the trivial remark that these conditions are always satisfied for $p = 2$. It is also easy to show that (P1) and (P2) are satisfied for $p = 3$:

**Proposition 3.1.** *Let $p > 2$ and $K \in \mathrm{Cl}(G)$. Then $|KK^{-1}|$ and $\eta(K)$ are odd.*

*Proof.* Let $x \in KK^{-1}$, and write $x = a \cdot ga^{-1}g^{-1}$ where $a \in K$ and $g \in G$. Then $x^{-1} = gag^{-1} \cdot a^{-1} \in KK^{-1}$. Moreover, $x \neq x^{-1}$ unless $x = 1$. Thus the elements in $KK^{-1} \setminus \{1\}$ come in pairs of the form $(x, x^{-1})$. Hence $|KK^{-1}|$ is odd. The result follows since $\eta(K) \equiv |KK^{-1}| \pmod{p-1}$. □

Our next goal is to show that (P1), (P2) and (P3) are satisfied for finite $p$-groups of nilpotency class 2. We start with a slightly more general result.

**Proposition 3.2.** *Let $H \leq G$, and let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1} \subseteq \mathrm{C}_G(H)$ and $G = H\,\mathrm{C}_G(x)$ for some $x \in K$. Then $|KK^{-1}| = |K|$ and $c_{KK^{-1}L} = |K|$; in particular,* (P3)*,* (P2) *and* (P1) *hold.*

*Proof.* The hypothesis $G = H\,\mathrm{C}_G(x)$ implies that $K = \{hxh^{-1} : h \in H\}$. Thus the hypothesis $KK^{-1} \subseteq \mathrm{C}_G(H)$ forces

$$KK^{-1} = \{h_1 x h_1^{-1} \cdot h_2 x^{-1} h_2^{-1} : h_1, h_2 \in H\} = \{x \cdot h_1^{-1} h_2 x^{-1} h_2^{-1} h_1 : h_1, h_2 \in H\} = xK^{-1}.$$

Hence the result follows from Lemma 2.1(iv). □

Our first application of Proposition 3.2 is to finite $p$-groups of nilpotency class 2.

**Corollary 3.3.** *Let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$. If $\mathrm{cl}(G) \leq 2$ then $|KK^{-1}| = |K|$ and $c_{KK^{-1}L} = |K|$; in particular,* (P3)*,* (P2) *and* (P1) *hold.*

*Proof.* Since $\mathrm{cl}(G) \leq 2$, we have $KK^{-1} = \{a \cdot ga^{-1}g^{-1} : a \in K, g \in G\} \subseteq G' \subseteq \mathrm{Z}(G) = \mathrm{C}_G(G)$. Thus we can apply Proposition 3.2 with $H := G$. □

Our next result is another application of Proposition 3.2.

**Corollary 3.4.** *Let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$, and let $A \trianglelefteq G$ be abelian such that $G' \subseteq A$ and $G = A\,\mathrm{C}_G(x)$ for some $x \in K$. Then $|KK^{-1}| = |K|$ and $c_{KK^{-1}L} = |K|$; in particular,* (P3), (P2) *and* (P1) *hold.*

*Proof.* As in the proof of Corollary 3.3, we have $KK^{-1} \subseteq G' \subseteq A = \mathrm{Z}(A) \subseteq \mathrm{C}_G(A)$. Thus we can apply Proposition 3.2 with $H := A$. □

Much of the following result comes from a paper by Adan-Bante [2].

**Proposition 3.5.** *Let $|G| = p^n$ for some $n \geq 2$, and let $K, L \in \mathrm{Cl}(G)$ be such that $|K| \in \{1, p, p^{n-2}\}$ and $L \subseteq KK^{-1}$. Then $c_{KK^{-1}L} \in \{1, |K|\}$; in particular,* (P3), (P2) *and* (P1) *hold.*

*Proof.* The case $|K| = 1$ is trivial. Suppose that $|K| = p$. Then, by Lemma 4.1 in [2], we have $\eta(K) = p = |K|$. Thus the result follows from Lemma 2.1(vii) in this case.

Finally, suppose that $|K| = p^{n-2}$. If $x \in K$ then

$$p^{n-2} = |K| \leq |KK^{-1}| = |\{a \cdot ga^{-1}g^{-1} : a \in K, g \in G\}| \leq |G'| \leq p^{n-2}.$$

Thus $|KK^{-1}| = |K|$, and the result follows from Lemma 2.1(iv). □

We note that a $p$-group of order $p^n$ with a conjugacy class of length $p^{n-2}$ has maximal class, by Satz III.14.23 in [9]. The following result is a consequence of Corollary 3.4 and Proposition 3.5.

**Corollary 3.6.** *Let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$, and let $A \in \mathrm{Max}(G)$ be abelian. Then $|K| \leq p$ or $|KK^{-1}| = |K|$, and $c_{KK^{-1}L} \in \{1, |K|\}$; in particular,* (P3), (P2) *and* (P1) *hold.*

*Proof.* Let $x \in K$. If $x \in A$ then $A \leq \mathrm{C}_G(x)$ and therefore $|K| \leq p$. In this case the result follows from Proposition 3.5. Thus we may assume that $x \notin A$. In this case Corollary 3.4 implies the result. □

The following result will also be useful.

**Lemma 3.7.** *Let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$, and let $K \subseteq N \trianglelefteq G$ where $|N| = p|K|$. Then $KK^{-1} = [G, N]$ and $|KK^{-1}| = |K|$. Thus $c_{KK^{-1}L} = |K|$, and* (P3), (P2) *and* (P1) *hold.*

*Proof.* Let $x \in K$. Then

$$KK^{-1} = \{gxg^{-1} \cdot hx^{-1}h^{-1} : g, h \in G\} = \{g[x, g^{-1}h]g^{-1} : g, h \in G\} \subseteq [N, G] < N.$$

Thus $|N| = p|K| \leq p|KK^{-1}| \leq p|[G, N]| \leq |N|$, and we conclude that $|K| = |KK^{-1}|$ and $KK^{-1} = [G, N]$. The result follows as before. □

Now we can deal with the groups of order $p^n$, for $n = 0, 1, \ldots, 5$.

**Proposition 3.8.** *Let $|G| = p^n$ where $n \leq 5$, and let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$. Then $c_{KK^{-1}L}$ is a power of $p$; in particular,* (P3), (P2) *and* (P1) *hold.*

*Proof.* By Proposition 3.5 and Lemma 2.1(iv), we may assume that $p^2 = |K| < |KK^{-1}|$ and $|G| = p^5$. Since $KK^{-1} \subseteq G'$ this implies that $|G'| = p^3$ and $G' = \Phi(G)$. Moreover, Lemma 3.7 shows that $K \nsubseteq G'$. Let $x \in K$, so that $M := G'\langle x\rangle \in \mathrm{Max}(G)$.

If $|L| = 1$ then $L \subseteq \mathrm{Z}(G)$, and the result follows from Lemma 2.1(iii). If $|L| = p^2$ then $LL^{-1} = K_3(G)$ by Lemma 3.7 since $L \subseteq KK^{-1} \subseteq G'$. Thus $N := LL^{-1} \cap \mathrm{Z}(G) \neq 1$, and $NL = L$ by Lemma 2.3. Hence the result follows from Lemma 2.4.

It remains to deal with the case $|L| = p$. Let $t \in L \cap xK^{-1}$. Then $t = xgx^{-1}g^{-1}$ for some $g \in G$, and $|\,\mathrm{C}_G(t)| = p^4$.

Suppose first that $g \in M$. Thus $t \in M'$ and $L \subseteq M'$. Since $|M'| \leq p^2$, Lemma 3.7 implies that $LL^{-1} = [G, M']$; in particular, $N := LL^{-1} \cap \mathrm{Z}(G) \neq 1$. Since $NL = L$ by Lemma 2.3, the result follows in this case from Lemma 2.4.

Thus we may assume that $g \notin M$, so that $G = M\langle g\rangle = G'\langle x, g\rangle = \Phi(G)\langle x, g\rangle = \langle x, g\rangle$. Since $[x, g] = t \in \mathrm{Z}(\mathrm{C}_G(t))$ we conclude that $G/\mathrm{Z}(\mathrm{C}_G(t))$ is abelian. Thus $G' \subseteq \mathrm{Z}(\mathrm{C}_G(t))$ and $|\mathrm{C}_G(t)/\mathrm{Z}(\mathrm{C}_G(t))| \leq p$. Hence $\mathrm{C}_G(t)$ is abelian, and the result follows from Corollary 3.6. □

Our next result generalizes Corollary 3.3. It will be used in Section 4.

**Lemma 3.9.** *Let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$, and let $n \in \mathbb{N}_0$ be such that $KK^{-1} \cap Z_n(G) = 1$ and $KK^{-1} \subseteq Z_{n+1}(G)$. Then $\eta(K) = |K|$, and $c_{KK^{-1}L}$ is a power of $p$; in particular,* (P3), (P2) *and* (P1) *hold.*

*Proof.* Let $x \in K$, and let $g, h \in G$ be such that $[x, g] =_G [x, h]$. We set $\overline{G} := G/Z_n(G)$, $\overline{x} := xZ_n(G)$, etc. Then $[\overline{x}, \overline{g}] =_{\overline{G}} [\overline{x}, \overline{h}]$. But $[\overline{x}, \overline{g}] \in \overline{KK}^{-1} \subseteq Z_{n+1}(G)/Z_n(G) = \mathrm{Z}(\overline{G})$, so that $[\overline{x}, \overline{g}] = [\overline{x}, \overline{h}]$. Thus $\overline{g}^{-1}\overline{h} \in \mathrm{C}_{\overline{G}}(\overline{x})$ and $[x, g^{-1}h] \in KK^{-1} \cap Z_n(G) = 1$. Therefore $g^{-1}h \in \mathrm{C}_G(x)$ and $[x, g] = [x, h]$.

This shows that the elements in $xK^{-1}$ lie in distinct conjugacy classes of $G$. Thus $\eta(K) \geq |xK^{-1}| = |K|$. Lemma 2.1(vi) implies that $\eta(K) = |K|$, and the result follows from Lemma 2.1(vii). □

# 4 Conjugacy classes of groups of order $p^6$

In this section we will extend Proposition 3.8 to groups of order $p^6$ where $p$ is a prime. In the following, let $G$ be a finite $p$-group. Our first lemma is well-known, so we omit the proof.

**Lemma 4.1.** *The Sylow $p$-subgroups of $\mathrm{GL}(3, p)$ are nonabelian of order $p^3$.*

Next we consider $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$.

**Lemma 4.2.** *Let $G = \langle a\rangle \times \langle b\rangle$ where $|\langle a\rangle| = p^2$ and $|\langle b\rangle| = p$. Then $\mathrm{Aut}(G)$ has order $p^3(p-1)^2$ and a unique Sylow $p$-subgroup $P$. Moreover, $P' \neq 1$.*

*Proof.* Every $\alpha \in \mathrm{Aut}(G)$ is uniquely determined by $\alpha(a)$ and $\alpha(b)$, and we may write

$$\alpha(a) = a^i b^j,\ \alpha(b) = a^{kp} b^l$$

with uniquely determined $i \in \{0, \ldots, p^2 - 1\}$, $j, k, l \in \{0, \ldots, p-1\}$ such that $l \neq 0$ and $p \nmid i$. Conversely, every 4-tuple $(i, j, k, l)$ of this form determines an automorphism $\alpha$ of $G$. This shows that $|\mathrm{Aut}(G)| = p^3(p-1)^2$.

Restriction induces a homomorphism $\rho : \mathrm{Aut}(G) \to \mathrm{Aut}(\Phi(G))$. Since $\Phi(G) = \langle a^p\rangle$, $\rho$ is surjective. Thus $|\ker(\rho)| = p^3(p-1)$. By Sylow's Theorem, $\ker(\rho)$ has a unique Sylow $p$-subgroup $P$. Then $P$ is the only Sylow $p$-subgroup of $\mathrm{Aut}(G)$.

Let $\alpha, \beta \in \mathrm{Aut}(G)$ be defined by $\alpha(a) = a^{1+p}b$, $\alpha(b) = b$, $\beta(a) = a$ and $\beta(b) = a^p b$. Then $\alpha^p = 1 = \beta^p$, so that $\alpha, \beta \in P$. Since $\alpha\beta \neq \beta\alpha$ we conclude that $P' \neq 1$. □

Our next result gives useful information concerning the structure of groups of order $p^6$.

**Lemma 4.3.** *Suppose that $|G| = p^6$ and $|G'| = p^3$. Then $G'$ is abelian, but $G' \notin \mathrm{SCN}(G)$.*

*Proof.* Satz III.7.11 in [9] implies that $G'$ is abelian. Assume that $G' \in \mathrm{SCN}(G)$. Then the abelian group $G/G' = G/\mathrm{C}_G(G')$ of order $p^3$ embeds into $\mathrm{Aut}(G')$. Thus $G'$ cannot be cyclic. By Lemma 4.1, $G'$ cannot be elementary abelian. In the remaining case, Lemma 4.2 leads to a contradiction. □

Next we prove (P3) for groups of order $p^6$ in special situations.

**Lemma 4.4.** *Let $|G| = p^6$, and suppose that $G'' \neq 1$. Moreover, let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$. Then $c_{KK^{-1}L}$ is a power of $p$.*

*Proof.* Lemma 4.3 implies that $|G'| = p^4$. Satz III.7.8(b) in [9] shows that $\mathrm{Z}(G')$ is noncyclic. Thus $\mathrm{Z}(G')$ and $G'/\mathrm{Z}(G')$ are both elementary abelian of order $p^2$. Also, Hilfssatz III.7.10 in [9] shows that $|G''| = p$. In particular $G'' \subseteq \mathrm{Z}(G)$.

By Lemma 2.1(iv), we may assume that $|K| < |KK^{-1}| \leq |G'| = p^4$. Thus, by Proposition 3.5, we may assume that $|K| \in \{p^2, p^3\}$, and $|L| \leq p^3$. If $|L| = 1$ then $c_{KK^{-1}L} = |K|$ by Lemma 2.1(iii). So we may assume that $|L| > 1$. Then, by Lemma 2.3, $Z := LL^{-1} \cap \mathrm{Z}(G) \trianglelefteq G$ and $ZL = L$. Thus, by Lemma 2.4 and Proposition 3.8, it suffices to show that $Z \neq 1$. Let $t \in L$. If $|L| = p$ then $|\,\mathrm{C}_G(t)| = p^5$ and $G' \subseteq \mathrm{C}_G(t)$. Thus $t \in \mathrm{Z}(G')$ and $LL^{-1} = [G, \mathrm{Z}(G')]$, by Lemma 3.7. Hence $Z \neq 1$ in this case.

Suppose that $|L| = p^2$. If $G' = \mathrm{C}_G(t)$ then $t \in \mathrm{Z}(G')$ and $L \subseteq \mathrm{Z}(G')$; however, this is impossible since $|\,\mathrm{Z}(G')| = p^2$. Thus $G' \neq \mathrm{C}_G(t)$ and $1 \neq \{[t, y] : y \in G'\} \subseteq LL^{-1} \cap G'' \subseteq LL^{-1} \cap \mathrm{Z}(G) = Z$. Hence we are done in this case. Finally, suppose that $|L| = p^3$. Then Lemma 3.7 implies that $LL^{-1} = K_3(G)$. Hence $Z \neq 1$ also in this case. □

Thus it remains to deal with the case $G'' = 1$.

**Lemma 4.5.** *Let $|G| = p^6$, let $K, L \in \mathrm{Cl}(G)$ be such that $|K| = p^2$ and $L \subseteq KK^{-1}$, and let $x \in K$. Suppose that $|KK^{-1} \cap \mathrm{Z}(G)| = p$ and $\mathrm{C}_G(x) \trianglelefteq G$. Then $c_{KK^{-1}L}$ is a power of $p$; in particular,* (P3), (P2) *and* (P1) *hold.*

*Proof.* Let $g \in G$ be such that $1 \neq [x, g] \in KK^{-1} \cap \mathrm{Z}(G)$. Then $[x, g^i] = [x, g]^i \in KK^{-1} \cap \mathrm{Z}(G)$ for $i \in \mathbb{Z}$. The case $g^p \notin \mathrm{C}_G(x)$ leads to the contradiction $|KK^{-1} \cap \mathrm{Z}(G)| = p^2$. Thus $g^p \in \mathrm{C}_G(x)$ and $|\,\mathrm{C}_G(x)\langle g\rangle| = p^5$. Let $h \in G$ be such that $G = \mathrm{C}_G(x)\langle g, h\rangle$. Then

$$xK^{-1} = \{[x, h^i g^j] : i, j = 0, \ldots, p-1\}.$$

Let $t \in L \cap xK^{-1}$, and write $t = [x, h^i g^j]$ with $i, j \in \{0, \ldots, p-1\}$. Since $\mathrm{C}_G(x) \trianglelefteq G$, we have $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(t) \trianglelefteq G$. Thus, by Lemma 2.1(ix), it suffices to prove that $|L \cap xK^{-1}| \in \{1, p\}$. We may therefore assume that $|L \cap xK^{-1}| \neq 1$. Then $i \neq 0$; for otherwise $t = [x, g^j] \in \mathrm{Z}(G)$ and therefore $|L \cap xK^{-1}| \leq |L| = 1$. We can now replace $h$ by $h^i g^j$ and therefore assume that $i = 1$ and $j = 0$.

Let $t \neq u \in L \cap xK^{-1}$, and write $u = [x, h^k g^l]$ with $k, l \in \{0, \ldots, p-1\}$. Then $k \neq 0$ since otherwise $u = [x, g^l] \in \mathrm{Z}(G)$ and $|L| = 1$. Since $[x, g] \in \mathrm{Z}(G)$, we get

$$u = [x, h^k g^l] = [x, h^k]h^k[x, g^l]h^{-k} = [x, h^k][x, g]^l.$$

We set $\overline{G} := G/\mathrm{Z}(G)$, $\overline{x} := x\,\mathrm{Z}(G)$, etc. Then $t =_G u$ implies that $[\overline{x}, \overline{h}] = \overline{t} =_{\overline{G}} \overline{u} = [\overline{x}, \overline{h}^k]$.

Assume that $k \neq 1$. Then Lemma 2.5 implies that $\overline{h} \in \mathrm{C}_{\overline{G}}(\overline{x})$. Hence $\overline{t} = 1$ and $t \in \mathrm{Z}(G)$, a contradiction.

Thus we must have $k = 1$. Then $l \neq 0$. Let $y \in G$ be such that

$$yty^{-1} = u = [x, hg^l] = [x, h][x, g]^l = t[x, g]^l.$$

Then, for $m = 0, \ldots, p-1$, we obtain

$$y^m t y^{-m} = t[x, g]^{lm} = [x, h][x, g]^{lm} = [x, hg^{lm}] \in L \cap xK^{-1}.$$

This shows that $L \cap xK^{-1} = \{[x, hg^n] : n = 0, \ldots, p-1\}$, so that $|L \cap xK^{-1}| = p$, which remained to be proved. □

**Lemma 4.6.** *Let $|G| = p^6$, and let $x \in K \in \mathrm{Cl}(G)$ be such that $|K| = p^2$, $|KK^{-1}| \leq p^3$ and $\mathrm{C}_G(x) \trianglelefteq G$. Suppose that the following conditions are satisfied:*

*(i)* $KK^{-1} \cap \mathrm{Z}(G) = 1$ *and* $KK^{-1} \subseteq Z_3(G)$;

*(ii)* $1 \neq y \in KK^{-1} \cap Z_2(G) \;\Rightarrow\; |\,\mathrm{C}_G(y)| = p^5$.

*Then $c_{KK^{-1}L}$ is a power of $p$, for all $L \in \mathrm{Cl}(G)$ such that $L \subseteq KK^{-1}$.*

*Proof.* Since $x \in \mathrm{Z}(\mathrm{C}_G(x)) \trianglelefteq G$, we have $K \subseteq \mathrm{Z}(\mathrm{C}_G(x))$ and $\langle K\rangle \leq \mathrm{Z}(\mathrm{C}_G(x))$. Thus $p^2 = |K| < |\langle K\rangle| \leq |\mathrm{Z}(\mathrm{C}_G(x))|$, so that $|\mathrm{C}_G(x)/\mathrm{Z}(\mathrm{C}_G(x))| \leq p$, and $\mathrm{C}_G(x)$ is abelian.

Let $L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$, and let $t \in L \cap xK^{-1}$. Then $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(\langle K\rangle) \subseteq \mathrm{C}_G(t) \trianglelefteq G$. Thus, by Lemma 2.1(ix), it suffices to show that $|L \cap xK^{-1}|$ is a power of $p$.

If $KK^{-1} \subseteq Z_2(G)$ then the result follows from Lemma 3.9 with $n := 1$, and if $KK^{-1} \cap Z_2(G) = 1$ then the result follows from Lemma 3.9 with $n := 2$. Thus we may assume that

$$1 \neq KK^{-1} \cap Z_2(G) \neq KK^{-1}.$$

Hence there exists $g \in G$ such that $1 \neq [x, g] \in KK^{-1} \cap Z_2(G)$. For $i \in \mathbb{N}$, we then have

$$[x, g^i] = ([x, g]g)^i g^{-i} \equiv [x, g]^i \pmod{\mathrm{Z}(G)}.$$

Thus $[x, g^i] \in Z_2(G)$.

Assume that $g^p \notin \mathrm{C}_G(x)$. Then $xK^{-1} = \{[x, g^i] : i = 0, \ldots, p^2 - 1\} \subseteq Z_2(G)$ and therefore $KK^{-1} \subseteq Z_2(G)$, a contradiction.

Hence $g^p \in \mathrm{C}_G(x)$ and $|\mathrm{C}_G(x)\langle g\rangle| = p^5$. Let $h \in G$ be such that $G = \mathrm{C}_G(x)\langle g, h\rangle$. Then

$$xK^{-1} = \{[x, h^i g^j] : i, j = 0, \ldots, p - 1\}.$$

Assume that $[x, h] \in Z_2(G)$. Then $[x, h^i g^j] = [x, h^i]h^i[x, g^j]h^{-i} \equiv [x, h]^i[x, g]^j \pmod{\mathrm{Z}(G)}$, so that $[x, h^i g^j] \in Z_2(G)$ for $i, j \in \mathbb{N}$. Thus $xK^{-1} \subseteq Z_2(G)$ and $KK^{-1} \subseteq Z_2(G)$, a contradiction.

Thus $[x, h] \notin Z_2(G)$. Since we can replace $h$ by $h^i g^j$ whenever $p \nmid i$ we obtain:

$$xK^{-1} \cap Z_2(G) = \{[x, g^j] : j = 0, \ldots, p - 1\}.$$

By Lemma 2.5, the elements $[x, g^j]$ $(j = 0, \ldots, p - 1)$ are contained in $p$ distinct conjugacy classes of $G$. If $L$ is one these conjugacy classes then certainly $|L \cap xK^{-1}| = 1$. Thus it remains to deal with the conjugacy classes of $G$ contained in $KK^{-1} \setminus Z_2(G)$.

Suppose that $i, j, k, l \in \{0, \ldots, p - 1\}$ are such that $i \neq 0 \neq k$ and $[x, h^i g^j] =_G [x, h^k g^l]$. Setting $\overline{G} := G/Z_2(G)$, $\overline{x} := xZ_2(G)$, etc. we get $[\overline{x}, \overline{h}^i\overline{g}^j] =_{\overline{G}} [\overline{x}, \overline{h}^k\overline{g}^l]$. But $[\overline{x}, \overline{h}^i\overline{g}^j] = [\overline{x}, \overline{h}^i]\overline{h}^i[\overline{x}, \overline{g}^j]\overline{h}^{-i} = [\overline{x}, \overline{h}^i]$ and similarly $[\overline{x}, \overline{h}^k\overline{g}^l] = [\overline{x}, \overline{h}^k]$.

Assume that $i \neq k$. Then $\overline{h} \in \mathrm{C}_{\overline{G}}(\overline{x})$ by Lemma 2.5. Thus $[x, h] \in Z_2(G)$, a contradiction.

This means that $i = k$. We have thus shown that $|L \cap xK^{-1}| \leq p$ for every $L \in \mathrm{Cl}(G)$ with $L \subseteq KK^{-1} \setminus Z_2(G)$. We distinguish two cases:

**Case 1:** $g \in \mathrm{C}_G([x, g])$, i. e. $\mathrm{C}_G([x, g]) = \mathrm{C}_G(x)\langle g\rangle$.
Again, we distinguish between two cases:

**Case 1.1:** There are $i, j \in \{0, \ldots, p - 1\}$ with $i \neq 0$ such that the conjugacy class of $[x, h^i g^j]$ has length $p$. We will show that $|L \cap xK^{-1}| = 1$ for every $L \in \mathrm{Cl}(G)$ with $L \subseteq KK^{-1}$ in this case.

Since we can replace $h$ by $h^i g^j$ we may assume that $i = 1$ and $j = 0$. Let $s \in G$ be such that $\mathrm{C}_G([x, h]) = \mathrm{C}_G(x)\langle s\rangle$.

Assume that $s \in \mathrm{C}_G([x, g])$. Then $g \in \mathrm{C}_G([x, g]) = \mathrm{C}_G(x)\langle s\rangle = \mathrm{C}_G([x, h])$. Since $\mathrm{C}_G(x)$ and $G/\mathrm{C}_G(x)$ are abelian we conclude:

$$\begin{aligned} h[x, g]h^{-1} &= hxh^{-1}hgx^{-1}g^{-1}h^{-1} = (hxh^{-1})(ghx^{-1}h^{-1}g^{-1}) = (ghx^{-1}h^{-1}g^{-1})(hxh^{-1}) \\ &= ghx^{-1}h^{-1}g^{-1}[x, h]^{-1}x = ghx^{-1}h^{-1}[x, h]^{-1}g^{-1}x = (gx^{-1}g^{-1})x = x(gx^{-1}g^{-1}) = [x, g]. \end{aligned}$$

Thus $h \in \mathrm{C}_G([x, g])$, so that $[x, g] \in \mathrm{Z}(G)$, a contradiction.

Hence we must have $s \notin \mathrm{C}_G([x, g])$.

Next assume that there are $k, l \in \{0, \ldots, p-1\}$ such that $k \neq l$ and $[x, hg^k] =_G [x, hg^l]$. Then there exist $y \in G$ and $z \in \mathrm{Z}(G)$ such that

$$y[x,h]y^{-1}yh[x,g^k]h^{-1}y^{-1} = y[x,hg^k]y^{-1} = [x,hg^l] = [x,h]h[x,g^l]h^{-1}$$

and

$$y[x,h]y^{-1}[x,g]^k = [x,h][x,g]^l z.$$

Thus $y[x,h]y^{-1} = [x,h][x,g]^{l-k}z$. Since $s \in \mathrm{C}_G([x,h]) = \mathrm{C}_G(y[x,h]y^{-1})$ we obtain the contradiction $s \in \mathrm{C}_G([x,g])$.

This shows that the elements $[x, hg^k]$ $(k = 0, \ldots, p-1)$ lie in $p$ distinct conjugacy classes of $G$. Moreover, for $i = 1, \ldots, p-1$, we have $[x, h^i] = [x,h]h[x,h^{i-1}]h^{-1}$. Since $\mathrm{C}_G([x,h]) \trianglelefteq G$ we obtain by induction that $\mathrm{C}_G([x,h]) = \mathrm{C}_G([x,h^i])$. So we can conclude, analogously, that, for fixed $i$, the elements $[x, h^i g^k]$ $(k = 0, \ldots, p-1)$ are contained in $p$ distinct conjugacy classes of $G$. Thus, in this case, we indeed have $|L \cap xK^{-1}| = 1$ for every $L \in \mathrm{Cl}(G)$ such that $L \subseteq KK^{-1}$.

**Case 1.2:** All conjugacy classes of $G$ contained in $KK^{-1} \setminus Z_2(G)$ have length $p^2$.
Since $|KK^{-1} \setminus Z_2(G)| < p^3$ there are at most $p-1$ such conjugacy classes. Thus, for $i \in \{1, \ldots, p-1\}$, the elements $[x, h^i g^k]$ $(k = 0, \ldots, p-1)$ are all in the same conjugacy class of $G$. Thus, in this case, we have $|L \cap xK^{-1}| = p$ for each such conjugacy class $L$, which remained to be proved.

**Case 2:** $g \notin \mathrm{C}_G([x,g])$.
In this case we may assume, choosing $h$ appropriately, that $\mathrm{C}_G([x,g]) = \mathrm{C}_G(x)\langle h \rangle$. Then a computation, similar to the one in Case 1.1, shows that $g[x,h]g^{-1} = \ldots = [x,h]$. Thus $g \in \mathrm{C}_G([x,h])$.

Assume that there are $k, l \in \{0, \ldots, p-1\}$ such that $k \neq l$ and $[x, hg^k] =_G [x, hg^l]$. Let $y \in G$ be such that $y[x, hg^k]y^{-1} = [x, hg^l]$. But $y[x, hg^k]y^{-1} = y[x,h]y^{-1}yh[x,g^k]h^{-1}y^{-1}$ and $[x, hg^l] = [x,h]h[x,g^l]h^{-1}$. Thus there is $z \in \mathrm{Z}(G)$ such that

$$y[x,h]y^{-1}[x,g]^k = [x,h][x,g]^l z.$$

Hence $y[x,h]y^{-1} = [x,h][x,g]^{l-k}z$. Since $g \in \mathrm{C}_G([x,h]) = \mathrm{C}_G(y[x,h]y^{-1})$ this leads to the contradiction $g \in \mathrm{C}_G([x,g])$.

This shows that the elements $[x, hg^k]$ $(k = 0, \ldots, p-1)$ are contained in $p$ distinct conjugacy classes of $G$. Since we can replace $h$ by $h^i$, for each $i \in \{1, \ldots, p-1\}$, we also obtain that, for each $i$, the elements $[x, h^i g^k]$ $(k = 0, \ldots, p-1)$ are contained in $p$ distinct conjugacy classes of $G$. Thus, in this case, we also have $|L \cap xK^{-1}| = 1$ for every $L \in \mathrm{Cl}(G)$ such that $L \subseteq KK^{-1}$. This finishes the proof of Lemma 4.6. □

Now we deal with the case $|G'| = p^3$.

**Lemma 4.7.** *Let $|G| = p^6$, and suppose that $|G'| \leq p^3$. Moreover, let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$. Then $c_{KK^{-1}L}$ is a power of $p$.*

*Proof.* By Lemma 2.1(iv), we may assume that $|K| < |KK^{-1}| \leq |G'| \leq p^3$, so that $|K| \leq p^2$. Thus, by Proposition 3.5, we may assume that $|K| = p^2$ and $|G'| = p^3$. By Lemma 4.3, $G'$ is abelian, and there exists $A \in \mathrm{SCN}(G)$ such that $G' < A$. Then Corollary 3.6 implies that $|A| = p^4$. Let $x \in K$, so that $|\mathrm{C}_G(x)| = p^4$. Then Corollary 3.4 implies that $A\,\mathrm{C}_G(x) < G$, and Lemma 3.7 implies that $x \notin G'$. Since $KK^{-1} \subseteq G'$, we must have $|L| \leq p^2$. We distinguish two cases:

**Case 1:** $G' \not\subseteq \mathrm{C}_G(x)$.
Then $x \notin A$, and $p^4 = |A| < |A\langle x \rangle| \leq |A\,\mathrm{C}_G(x)| \leq p^5$. Thus $M := A\langle x \rangle = A\,\mathrm{C}_G(x) \in \mathrm{Max}(G)$, and $|\mathrm{C}_A(x)| = |A \cap \mathrm{C}_G(x)| = p^3$. Setting $H := \{[x,a] : a \in A\}$, we have $|H| = |A : \mathrm{C}_A(x)| = p$ and $H \subseteq KK^{-1} \subseteq G' \subseteq A$. It is easy to see that $H \leq G$. Then $H \trianglelefteq M$ since $xHx^{-1} = H$. But $M/H$ is abelian, so $M' \subseteq H \subseteq M'$. Thus $H = M' \trianglelefteq G$, and $H \subseteq \mathrm{Z}(G)$.

By Lemma 2.1(iii), we may assume that $|L| > 1$. Suppose that $|L| = p^2$. Since $L \subseteq KK^{-1} \subseteq G'$ Lemma 3.7 implies that $LL^{-1} = K_3(G)$. Thus $Z := LL^{-1} \cap \mathrm{Z}(G) \neq 1$, and $ZL = L$ by Lemma 2.3. Hence by Lemma 2.4 and Proposition 3.8, $c_{KK^{-1}L}$ is a power of $p$.

It remains to deal with the case $|L| = p$. Let $t \in L \cap xK^{-1}$, so that $|\mathrm{C}_G(t)| = p^5$, and write $t = [x,g]$ for some $g \in G$.

Assume that $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(t)$. Since $A \subseteq \mathrm{C}_G(G') \subseteq \mathrm{C}_G(t)$ we get $M = A\,\mathrm{C}_G(x) = \mathrm{C}_G(t)$. Then $g \notin M$, for otherwise $t \in M' = H \subseteq \mathrm{Z}(G)$. Thus $G = M\langle g \rangle = \mathrm{C}_G(t)\langle g \rangle$. Since $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(t) = \mathrm{C}_G(xgx^{-1}g^{-1})$ we get $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(gx^{-1}g^{-1}) =$

$g\,\mathrm{C}_G(x^{-1})g^{-1} = g\,\mathrm{C}_G(x)g^{-1}$ and $g \in \mathrm{N}_G(\mathrm{C}_G(x))$. Since $|\,\mathrm{C}_G(t) : \mathrm{C}_G(x)| = p$ we also have $\mathrm{C}_G(t) \subseteq \mathrm{N}_G(\mathrm{C}_G(x))$. We conclude that $G = \mathrm{C}_G(t)\langle g\rangle \subseteq \mathrm{N}_G(\mathrm{C}_G(x))$, i. e. $\mathrm{C}_G(x) \trianglelefteq G$ and $G' \subseteq \mathrm{C}_G(x)$, a contradiction.

Thus we must have $\mathrm{C}_G(x) \nsubseteq \mathrm{C}_G(t)$, so that $G = \mathrm{C}_G(t)\,\mathrm{C}_G(x)$ and $|\,\mathrm{C}_G(t) \cap \mathrm{C}_G(x)| = p^3$. Hence $|\,\mathrm{C}_G(t) : \mathrm{C}_G(t) \cap \mathrm{C}_G(x)| = p^2$. So $c_{KK^{-1}L} = p^2$ by Lemma 2.1(i), (v). The result follows in this case.

**Case 2:** $G' \subseteq \mathrm{C}_G(x)$.
Then $\mathrm{C}_G(x) = G'\langle x\rangle$ is abelian and normal in $G$. If $|KK^{-1} \cap \mathrm{Z}(G)| = p^2$ then Lemma 2.1(vi), (vii) imply the result, and if $|KK^{-1} \cap \mathrm{Z}(G)| = p$ then Lemma 4.5 implies the result.

Thus we are left with the case $|KK^{-1} \cap \mathrm{Z}(G)| = 1$. Since $|G'| = p^3$ we have $\mathrm{cl}(G) \leq 4$. Hence $KK^{-1} \subseteq G' \subseteq Z_3(G)$. If $KK^{-1} \subseteq Z_2(G)$ or $|KK^{-1} \cap Z_2(G)| = 1$ then the result follows from Lemma 3.9. Thus we may assume that $1 \neq KK^{-1} \cap Z_2(G) \neq KK^{-1}$. Hence $|G' \cap Z_2(G)| \in \{p, p^2\}$. Since $G/\,\mathrm{C}_G(G' \cap Z_2(G))$ is isomorphic to a $p$-subgroup of $\mathrm{Aut}(G' \cap Z_2(G))$ we conclude that $|G/\,\mathrm{C}_G(G' \cap Z_2(G))| \leq p$. In particular, $|\,\mathrm{C}_G(y)| = p^5$ whenever $1 \neq y \in KK^{-1} \cap Z_2(G) \subseteq G' \cap Z_2(G)$. The result now follows from Lemma 4.6. □

It remains to deal with the case where $G'$ is abelian of order $p^4$. We distinguish the cases $|K| \neq p^3$ and $|K| = p^3$.

**Lemma 4.8.** *Let $|G| = p^6$, and suppose that $|G'| = p^4$ and $G'' = 1$. Moreover, let $K, L \in \mathrm{Cl}(G)$ be such that $|K| \neq p^3$ and $L \subseteq KK^{-1}$. Then $c_{KK^{-1}L}$ is a power of $p$.*

*Proof.* By Proposition 3.5 and Lemma 2.1(iv), we may assume that $p^2 = |K| < |KK^{-1}|$. Also, we may assume that $|KK^{-1} \cap \mathrm{Z}(G)| < |K|$, by Lemma 2.1(vi), (vii). Thus $|KK^{-1} \cap \mathrm{Z}(G)| \in \{1, p\}$ by Lemma 2.3. Let $x \in K$, let $t \in L \cap xK^{-1}$, and let $g \in G$ be such that $t = [x, g]$. Since $G' \subseteq \mathrm{C}_G(t)$ we must have $|L| \leq p^2$. Corollary 3.6 implies that $G' = \Phi(G) \in \mathrm{SCN}(G)$. We distinguish two cases:

**Case 1:** $x \notin G'$.
Then $M := G'\langle x\rangle = G'\,\mathrm{C}_G(x) \in \mathrm{Max}(G)$ by Corollary 3.4, and $H := \{[x, y] : y \in G'\} \subseteq KK^{-1} \subseteq G'$. It is easy to see that $H \leq G$, and $|H| = |G' : \mathrm{C}_{G'}(x)| = p$. Since $xHx^{-1} = H$ we have $H \trianglelefteq M$. But $M/H$ is abelian, so that $M' \subseteq H \subseteq M'$, and we see that $H = M' \trianglelefteq G$. Thus $H \subseteq KK^{-1} \cap \mathrm{Z}(G)$. Since $|H| = p \geq |KK^{-1} \cap \mathrm{Z}(G)|$ we conclude that $H = KK^{-1} \cap \mathrm{Z}(G)$. In particular, $KK^{-1}$ contains exactly $p$ conjugacy classes of $G$ of length 1. If $L$ is one of these then the result follows from Lemma 2.1(iii).

Assume that $|L| = p$, so that $|\,\mathrm{C}_G(t)| = p^5$. We must have $g \notin M$; for otherwise $t \in M' = H \subseteq \mathrm{Z}(G)$. Thus $G = M\langle g\rangle = G'\langle x, g\rangle = \Phi(G)\langle x, g\rangle = \langle x, g\rangle$. Since $[x, g] = t \in \mathrm{Z}(\mathrm{C}_G(t))$ we conclude that $G/\,\mathrm{Z}(\mathrm{C}_G(t))$ is abelian. Hence $G' \subseteq \mathrm{Z}(\mathrm{C}_G(t))$. Since $|G'| = p^4$ this implies that $\mathrm{C}_G(t)$ is abelian, and we have a contradiction to Corollary 3.6.

This means that $KK^{-1}$ does not contain conjugacy classes of $G$ of length $p$. Let $l$ denote the number of conjugacy classes of $G$ of length $p^2$ contained in $KK^{-1}$. Then Theorem A in [2] implies that $p + l = \eta(K) \geq 2(p-1) + 1 = 2p - 1$, so that $l \geq p - 1$. Suppose now that $|L| = p^2$. Then $\mathrm{C}_G(t) = G'$ since $t \in G'$. Moreover, Lemma 2.1(v) implies that $c_{KK^{-1}L} \geq |G' : \mathrm{C}_{G'}(x)| = p$. The augmentation map $\epsilon$ gives

$$\begin{aligned} p^4 = |K| \cdot |K^{-1}| &= \epsilon(K^+)\epsilon((K^{-1})^+) = \epsilon(K^+(K^{-1})^+) \\ &= \sum_{J \in \mathrm{Cl}(G)} c_{KK^{-1}J}|J| \geq |KK^{-1} \cap \mathrm{Z}(G)| \cdot |K| + lp^3 \geq p^4. \end{aligned}$$

Hence $l = p - 1$ and $c_{KK^{-1}L} = p$, and the result follows in this case.

**Case 2:** $x \in G'$.
Then $G' = \mathrm{C}_G(x)$ and $KK^{-1} = \{axa^{-1} \cdot bx^{-1}b^{-1} : a, b \in G\} = \{a[x, a^{-1}b]a^{-1} : a, b \in G\} \subseteq K_3(G) < G'$. Hence $p^4 = |G'| > |K_3(G)| \geq |KK^{-1}| > p^2$, so that $|K_3(G)| = p^3$. If $|KK^{-1} \cap \mathrm{Z}(G)| = p$ then the result follows from Lemma 4.5. Thus we may assume that $KK^{-1} \cap \mathrm{Z}(G) = 1$. If $\mathrm{cl}(G) \leq 4$ then $KK^{-1} \subseteq K_3(G) \subseteq Z_2(G)$. In this case the result follows from Lemma 3.9. Hence we may assume that $G$ has maximal class. Then $KK^{-1} \subseteq K_3(G) = Z_3(G)$, and $|\,\mathrm{Z}(G)| = p$. If $1 \neq y \in KK^{-1} \cap Z_2(G)$ then $hyh^{-1} \in y\,\mathrm{Z}(G)$ for $h \in G$, so $|\,\mathrm{C}_G(y)| = p^5$. Now the result follows from Lemma 4.6. □

Now it remains to handle the case where $|K| = p^3$ and $G'$ is abelian of order $p^4$.

**Theorem 4.9.** *Let $|G| = p^6$, and let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$. Then $c_{KK^{-1}L}$ is a power of $p$.*

*Proof.* By the preceding results, we may assume that $|G'| = p^4$, $G'' = 1$ and $|K| = p^3$. By Lemma 2.1(iv), we may assume that $|KK^{-1}| > p^3$. Let $x \in K$, let $t \in L \cap xK^{-1}$, and let $g \in G$ be such that $t = [x, g] \in G'$. Then $G' \subseteq \mathrm{C}_G(t)$, so that $|L| \leq p^2$. Corollary 3.6 implies that $G' = \Phi(G) \in \mathrm{SCN}(G)$. Moreover, Lemma 3.7 implies that $x \notin G'$. Thus $M := G'\langle x\rangle = G'\,\mathrm{C}_G(x) \in \mathrm{Max}(G)$ by Corollary 3.4. Furthermore, $H := \{[x, y] : y \in G'\} \subseteq KK^{-1} \subseteq G'$ and $|H| = |G' : \mathrm{C}_{G'}(x)| = p^2$. As before, we have $H \leq G$. Also, $H \trianglelefteq M$ since $xHx^{-1} = H$. Since $M/H$ is abelian, we get $M' \subseteq H \subseteq M'$, so that $H = M' \trianglelefteq G$ and $1 \neq H \cap \mathrm{Z}(G) \subseteq KK^{-1} \cap \mathrm{Z}(G)$. Let $y \in KK^{-1} \cap \mathrm{Z}(G)$. Then there is $h \in G$ such that $y = [x, h]$.

Assume that $h \notin M$. Then $G = M\langle h\rangle = G'\langle x, h\rangle = \Phi(G)\langle x, h\rangle = \langle x, h\rangle$. Since $[x, h] = y \in \mathrm{Z}(G)$ this implies that $G/\mathrm{Z}(G)$ is abelian. Thus $\mathrm{cl}(G) \leq 2$ which contradicts Corollary 3.3.

Hence $h \in M$ and $y \in M' \cap \mathrm{Z}(G) = H \cap \mathrm{Z}(G)$. This shows that $H \cap \mathrm{Z}(G) = KK^{-1} \cap \mathrm{Z}(G)$. We distinguish two cases:

**Case 1:** $|KK^{-1} \cap \mathrm{Z}(G)| = p^2$.
In this case we have $KK^{-1} \cap \mathrm{Z}(G) = H$, and $KK^{-1}$ contains exactly $p^2$ conjugacy classes of $G$ of length 1. By Lemma 2.1(iii), we may assume that $|L| > 1$. Then $g \notin M$; for otherwise $t \in M' = H \subseteq \mathrm{Z}(G)$. Thus $G = M\langle g\rangle = G'\langle x, g\rangle = \Phi(G)\langle x, g\rangle = \langle x, g\rangle$.

Assume that $|L| = p$, so that $|\,\mathrm{C}_G(t)| = p^5$. Then $[x, g] = t \in \mathrm{Z}(\mathrm{C}_G(t)) \trianglelefteq G$, so we conclude that $G/\mathrm{Z}(\mathrm{C}_G(t))$ is abelian. Hence $G' \subseteq \mathrm{Z}(\mathrm{C}_G(t))$. Since $|G'| = p^4$ this means that $\mathrm{C}_G(t)$ is abelian. However, this contradicts Corollary 3.6.

This shows that $KK^{-1}$ does not contain conjugacy classes of $G$ of length $p$. Suppose that $|L| = p^2$. Since $t \in G'$ we conclude that $\mathrm{C}_G(t) = G'$. We determine $|L \cap xK^{-1}|$. Note that $\mathrm{C}_G(x) \trianglelefteq M$ since $M' = H \subseteq \mathrm{Z}(G) \subseteq \mathrm{C}_G(x)$. Also, we have $x \notin G' = \mathrm{C}_G(t) = \mathrm{C}_G([x, g])$, so we conclude that $\mathrm{C}_G(x) \neq \mathrm{C}_G(gxg^{-1})$ and $\mathrm{C}_G(x) \cap \mathrm{C}_G(gxg^{-1}) = \mathrm{Z}(G)$. Furthermore, $\mathrm{C}_G(x)\,\mathrm{C}_G(gxg^{-1}) \in \mathrm{Max}(M)$. Let $a \in \mathrm{C}_G(x)$ be such that $\mathrm{C}_G(x)\,\mathrm{C}_G(gxg^{-1}) = \mathrm{C}_G(gxg^{-1})\langle a\rangle$, and let $b \in G'$ be such that $M = \mathrm{C}_G(x)\,\mathrm{C}_G(gxg^{-1})\langle b\rangle$. Since $G = M\langle g\rangle$ we conclude that

$$K = \{g^i b^j a^k (gxg^{-1}) a^{-k} b^{-j} g^{-i} : i, j, k = 0, \ldots, p-1\}.$$

Note that $[x, a^k g] = a^k [x, g] a^{-k} = a^k t a^{-k} \in L \cap xK^{-1}$ for $k = 0, \ldots, p-1$. Suppose now that also $[x, b^j a^k g] \in L$ for some $j, k \in \{0, \ldots, p-1\}$ such that $j \neq 0$. Since we may replace $b$ by $b^j$ we may assume that $j = 1$. Note that $c := ba^k b^{-1} \in b\,\mathrm{C}_G(x) b^{-1} = \mathrm{C}_G(x)$. Since $[x, ba^k g] = [x, cbg] = c[x, bg]c^{-1}$ we then also have $[x, bg] \in L$. Let $y \in G$ be such that

$$yty^{-1} = [x, bg] = [x, b][x, g] = [x, b]t.$$

Since $[x, b] \in H \subseteq \mathrm{Z}(G)$ we conclude that

$$y^l t y^{-l} = y^{l-1}[x, b] t y^{1-l} = [x, b] y^{l-1} t y^{1-l} = \ldots = [x, b]^l t = [x, b^l][x, g] = [x, b^l g],$$

for $l = 0, \ldots, p-1$. Thus $[x, a^m b^l g] = a^m [x, b^l g] a^{-m} = a^m y^l t y^{-l} a^{-m} \in L$ for $l, m = 0, \ldots, p-1$. Since $\mathrm{C}_G(gxg^{-1}) \trianglelefteq M$ these are precisely the elements $[x, b^l a^m g]$ $(l, m = 0, \ldots, p-1)$. Hence $L = \{[x, b^l a^m g] : l, m = 0, \ldots, p-1\}$.

Assume that $[x, g^i b^j a^k g] \in L$ for some $i, j, k \in \{0, \ldots, p-1\}$ such that $i \neq 0$. Note that $y := g^i b^j a^k g^{-i} \in M$, and $[x, g^i b^j a^k g] = [x, yg^{i+1}]$. Thus there is $z \in G$ such that

$$ztz^{-1} = [x, yg^{i+1}] = [x, y]y[x, g^{i+1}]y^{-1} \equiv y[x, g^{i+1}]y^{-1} \pmod{\mathrm{Z}(G)}$$

since $[x, y] \in M' = H \subseteq \mathrm{Z}(G)$. We set $\overline{G} := G/\mathrm{Z}(G)$, $\overline{g} := g\,\mathrm{Z}(G)$, etc. Then $[\overline{x}, \overline{g}] =_{\overline{G}} [\overline{x}, \overline{g}^{i+1}]$. Thus Lemma 2.5 implies that $\overline{g} \in \mathrm{C}_{\overline{G}}(\overline{x})$. This leads to the contradiction $t = [x, g] \in \mathrm{Z}(G)$.

This shows that $[x, g^i b^j a^k g] \notin L$ for all $i, j, k \in \{0, \ldots, p-1\}$ such that $i \neq 0$. So we have proved that $|L \cap xK^{-1}| \in \{p, p^2\}$ in this case. However, we cannot apply Lemma 2.1(ix) here since $\mathrm{C}_G(x) \not\subseteq G' = \mathrm{C}_G(t)$. But Lemma 2.1(v) implies that $c_{KK^{-1}L} \geq |G' : \mathrm{C}_{G'}(x)| = p^2$. If $|L \cap xK^{-1}| = p^2$ then $L \subseteq xK^{-1}$, and the result follows from Lemma 2.1(ii).

Thus we may assume that $|L \cap xK^{-1}| = p$. Let $h_1, h_2 \in G$ be such that $t = h_1 x h_1^{-1} \cdot h_2 x^{-1} h_2^{-1}$. Then there is $i \in \{0, \ldots, p-1\}$ such that $h_1^{-1} t h_1 = x h_1^{-1} h_2 x^{-1} h_2^{-1} h_1 = a^i t a^{-i}$. Thus $h_1 a^i \in \mathrm{C}_G(t) = G'$ and $h_1 \in M$. Since $|M : \mathrm{C}_G(x)| = p^2$ this implies that $c_{KK^{-1}L} \leq p^2$. Hence $c_{KK^{-1}L} = p^2$, and the result follows in this case.

**Case 2:** $|KK^{-1} \cap \mathrm{Z}(G)| = p$.
In this case $KK^{-1}$ contains exactly $p$ conjugacy classes of $G$ of length 1. If $L$ is one of these then we have

$c_{KK^{-1}L} = |K|$ by Lemma 2.1(iii). Thus we may assume that $|L| > 1$. Let us consider next the case $|L| = p$, i. e. $|\mathrm{C}_G(t)| = p^5$.

Assume that $g \notin M$. Then $G = M\langle g\rangle = G'\langle x, g\rangle = \Phi(G)\langle x, g\rangle = \langle x, g\rangle$ and $[x, g] = t \in \mathrm{Z}(\mathrm{C}_G(t))$. Thus $G/\mathrm{Z}(\mathrm{C}_G(t))$ is abelian and $G' \subseteq \mathrm{Z}(\mathrm{C}_G(t))$. Since $|G'| = p^4$ this means that $\mathrm{C}_G(t)$ is abelian. However, this contradicts Corollary 3.6.

Thus $g \in M$ and $t = [x, g] \in M' = H$. Then $L \subseteq H \subseteq xK^{-1}$, and Lemma 2.1(ii) implies that $c_{KK^{-1}L} = |K|$. It is clear that $H$ contains exactly $p - 1$ conjugacy classes of $G$ of length $p$.

It remains to consider the case $|L| = p^2$. Then $g \notin M$; for otherwise $t = [x, g] \in M' = H$ and $L \subseteq H$, which is impossible. Thus $G = M\langle g\rangle$ and $\mathrm{C}_G(t) = G'$ since $t \in G'$. It is easy to see that

$$B := \{h \in G' : [x, h] \in \mathrm{Z}(G)\} \leq G'.$$

Moreover, $|B \cap \mathrm{C}_G(x)| = |G' \cap \mathrm{C}_G(x)| = p^2$ and $|B| = p^3$. We claim that $B \trianglelefteq G$.

Indeed, if $y \in B$ and $z \in G$ then

$$\begin{aligned}[x, zyz^{-1}] &= [x, z]z[x, yz^{-1}]z^{-1} = [x, z]z[x, y]y[x, z^{-1}]y^{-1}z^{-1} = [x, z][x, y]z[x, z^{-1}]z^{-1}\\ &= [x, z]z[x, z^{-1}]z^{-1}[x, y] = [x, y] \in \mathrm{Z}(G),\end{aligned}$$

so $zyz^{-1} \in B$.

In particular, we have $B\,\mathrm{C}_G(gxg^{-1}) \in \mathrm{Max}(M)$.

Assume that $\mathrm{C}_G(x) \subseteq B\,\mathrm{C}_G(gxg^{-1})$. Then $B\,\mathrm{C}_G(gxg^{-1}) = B\,\mathrm{C}_G(x)$ and $g \in \mathrm{N}_G(B\,\mathrm{C}_G(x))$. Since also $M \subseteq \mathrm{N}_G(B\,\mathrm{C}_G(x))$ we conclude that $B\,\mathrm{C}_G(x) \trianglelefteq G$. Thus $G' = B\,\mathrm{C}_G(x)$ and $x \in G'$, a contradiction.

Hence $\mathrm{C}_G(x) \nsubseteq B\,\mathrm{C}_G(gxg^{-1})$ and $M = \mathrm{C}_G(x)B\,\mathrm{C}_G(gxg^{-1})$. Let $B\,\mathrm{C}_G(gxg^{-1}) = \langle b\rangle\,\mathrm{C}_G(gxg^{-1})$ with $b \in B$, and let $a \in \mathrm{C}_G(x)$ be such that $M = \langle a\rangle B\,\mathrm{C}_G(gxg^{-1})$. Then

$$K := \{g^i a^j b^k (gxg^{-1}) b^{-k} a^{-j} g^{-i} : i, j, k = 0, \ldots, p - 1\}.$$

Note that $[x, a^j g] = a^j[x, g]a^{-j} = a^j t a^{-j} \in L$ for $j = 0, \ldots, p - 1$.

Assume that $[x, g^i a^j b^k g] \in L$ for some $i, j, k \in \{0, \ldots, p - 1\}$ such that $i \neq 0$. Then $y := g^i a^j b^k g^{-i} \in M$. Let $z \in G$ be such that

$$ztz^{-1} = [x, g^i a^j b^k g] = [x, yg^{i+1}] = [x, y]y[x, g^{i+1}]y^{-1}.$$

Since $[x, y] \in M' = H$ this implies that $z[x, g]z^{-1} = ztz^{-1} \equiv y[x, g^{i+1}]y^{-1} \pmod H$. We set $\overline{G} := G/H$, $\overline{g} := gH$, etc. Then $[\overline{x}, \overline{g}] =_{\overline{G}} [\overline{x}, \overline{g}^{i+1}]$. Thus Lemma 2.5 implies that $\overline{g} \in \mathrm{C}_{\overline{G}}(\overline{x})$ and $t = [x, g] \in H$. So we have the contradiction $L \subseteq H$.

This shows that $[x, g^i a^j b^k g] \notin L$ for all $i, j, k \in \{0, \ldots, p - 1\}$ such that $i \neq 0$. Let us consider the case where $[x, a^j b^k g] \in L$ for some $j, k \in \{0, \ldots, p - 1\}$ such that $k \neq 0$. Since we may replace $b$ by $b^k$ we may assume that $k = 1$. Then also $[x, bg] \in L$. Let $y \in G$ be such that

$$yty^{-1} = [x, bg] = [x, b]b[x, g]b^{-1} = [x, b]t.$$

Since $[x, b] \in \mathrm{Z}(G)$ we conclude that, for $l = 0, \ldots, p - 1$, we have

$$y^l t y^{-l} = [x, b]y^{l-1}ty^{1-l} = \ldots = [x, b]^l t = [x, b^l g].$$

Thus $L = \{[x, a^m b^l g] : l, m = 0, \ldots, p - 1\} \subseteq xK^{-1}$ in this case, and Lemma 2.1(ii) implies $c_{KK^{-1}L} = |K|$.

It remains to consider the case

$$L \cap xK^{-1} = \{[x, a^j g] : j = 0, \ldots, p - 1\}.$$

Lemma 2.1(v) implies that $c_{KK^{-1}L} \geq |G' : \mathrm{C}_{G'}(x)| = p^2$. On the other hand, let $h_1, h_2 \in G$ be such that $t = h_1 x h_1^{-1} \cdot h_2 x^{-1} h_2^{-1}$. Then $h_1^{-1} t h_1 = x \cdot h_1^{-1} h_2 x^{-1} h_2^{-1} h_1 \in L \cap xK^{-1}$, so $h_1^{-1} t h_1 = a^j t a^{-j}$ for some $j \in \{0, \ldots, p - 1\}$. Thus $h_1 a^j \in \mathrm{C}_G(t) = G'$ and $h_1 \in M$. Since $|M : \mathrm{C}_G(x)| = p^2$ we get $c_{KK^{-1}L} \leq p^2$ in this case, so that $c_{KK^{-1}L} = p^2$. The theorem is now proved in all cases. □

It can be shown that (P3) does not hold, in general, for groups of order $p^7$. Indeed, the following GAP code gives a group $G$ of order $3^7$ with conjugacy classes $K$ of length $3^3$ and $L$ of length 3 such that $c_{KK^{-1}L} = 18 \not\equiv 1 \pmod 2$:

```
G:=PcGroupCode(32162330624780229618657386444736,3^7);
CC:=ConjugacyClasses(G);
K:=CC[24];
L:=CC[6];
x:=Representative(L);
product:=function(x,y) return x*y^-1; end;
Size(Filtered(ListX(K,K,product),y->y=x)); # = c_{KK^{-1}L}
```

Although (P3) certainly holds for finite 2-groups, it is not true, in general, that the relevant class multiplication constants $c_{KK^{-1}L}$ are always powers of 2. Indeed, the group `SmallGroup(2^8,503)` of order $2^8$ in the "Small Group Library" gives a counterexample.

# 5 Conjugacy classes of metacyclic $p$-groups

The purpose of this section is to show that (P3) holds for metacyclic $p$-groups. We start with an elementary observation.

**Lemma 5.1.** *Let $G$ be a metacyclic $p$-group where $p$ is an odd prime. More precisely, let $G = AB$ where $A = \langle a\rangle \trianglelefteq G$ and $B = \langle b\rangle \leq G$. Then*

$$G' = \{[a^i, b] : i \in \mathbb{Z}\} = \{[a, b^i] : i \in \mathbb{Z}\}$$

*and $|A : \mathrm{C}_A(B)| = |B : C_B(A)|$.*

*Proof.* Since $G/A$ is cyclic, we have $N := \{[a^i, b] : i \in \mathbb{Z}\} \subseteq G' \subseteq A$. Thus $[a^i, b] = [a, b]^i$ for $i \in \mathbb{Z}$, so that $N = \langle [a, b]\rangle \leq A$. Since $N$ is characteristic in $A$, we have $N \trianglelefteq G$. But $G/N$ is abelian, so $G' \subseteq N \subseteq G'$, i. e. $G' = N$.

We know that $M := \{[a, b^i] : i \in \mathbb{Z}\} \subseteq G' = N$ and that $|M| = |B : \mathrm{C}_B(A)| = p^s$ for some $s \in \mathbb{N}_0$. Let $|A| = p^n$ where $n \in \mathbb{N}$, so that $|\operatorname{Aut}(A)| = p^{n-1}(p-1)$. Since $p$ is odd, $\operatorname{Aut}(A)$ is cyclic, and its Sylow $p$-subgroup $P$ is generated by the automorphism $\alpha$ of $A$ satisfying $\alpha(a) = a^{1+p}$. Every subgroup of $P$ has the form $\langle \alpha^{p^t}\rangle$ for some $t \in \{0, \ldots, n-1\}$. Replacing $b$ by a suitable power we may assume that

$$bab^{-1} = \alpha^{p^t}(a) = a^{(1+p)^{p^t}} \text{ for some } t \in \{0, \ldots, n-1\}.$$

Since $|B : \mathrm{C}_B(A)| = p^s$ we have

$$a = b^{p^s} a b^{-p^s} = a^{(1+p)^{p^{s+t}}}.$$

Thus $(1+p)^{p^{s+t}} \equiv 1 \pmod{p^n}$. This implies that $s + t \geq n - 1$. On the other hand, we have $(1+p)^{p^t} \equiv 1 \pmod{p^{t+1}}$, so we can write $(1+p)^{p^t} = 1 + kp^{t+1}$ with $k \in \mathbb{Z}$. Then

$$ba^{p^s}b^{-1} = a^{p^s(1+p)^{p^t}} = a^{p^s(1+kp^{t+1})} = a^{p^s + kp^{s+t+1}} = a^{p^s}.$$

Thus $|G'| = |N| = |A : \mathrm{C}_A(B)| \leq p^s = |M|$ and therefore $M = G'$. Hence $|A : \mathrm{C}_A(B)| = |B : C_B(A)|$. □

The dihedral group of order 16 shows that the hypothesis $p \neq 2$ is necessary.

**Proposition 5.2.** *Let $G$ be a metacyclic $p$-group where $p$ is an odd prime. Moreover, let $K, L \in \mathrm{Cl}(G)$ be such that $L \subseteq KK^{-1}$. Then $c_{KK^{-1}L} = |K|$; in particular,* (P3), (P2) *and* (P1) *are satisfied.*

*Proof.* Let $A = \langle a \rangle$ and $B = \langle b \rangle$ as in Lemma 5.1. Moreover, let $x \in K$, and let $s, t \in \mathbb{Z}$ be such that $x = b^s a^t$. Then the elements in $K$ have the form

$$\begin{aligned} a^i b^j x b^{-j} a^{-i} &= x(a^{-t} b^{-s} a^i b^j b^s a^t b^{-j} a^{-i}) = x(a^{-t} \cdot b^{-s} a^i b^s \cdot b^j a^t b^{-j} \cdot a^{-i}) \\ &= x(a^{-t} \cdot b^j a^t b^{-j} \cdot b^{-s} a^i b^s \cdot a^{-i}) = x[a^{-t}, b^j][b^{-s}, a^i] \end{aligned}$$

with $i, j \in \mathbb{Z}$. Since $U := \langle a^t \rangle B$ and $V := A\langle b^s \rangle$ are also metacyclic, we have

$$U' = \{[a^{-t}, b^j] : j \in \mathbb{Z}\} \text{ and } V' = \{[a^i, b^{-s}] : i \in \mathbb{Z}\},$$

by Lemma 5.1. Since $U' \leq A$ and $V' \leq A$, we have $U' \trianglelefteq G$ and $V' \trianglelefteq G$, so that $N := U'V' \trianglelefteq G$. Thus $K = xN$ and $KK^{-1} = Nxx^{-1}N = N$. This implies that $|KK^{-1}| = |N| = |K|$, and the result follows from Lemma 2.1(iv). □

Also in this case the dihedral group of order 16 shows that the hypothesis $p \neq 2$ is necessary.

# 6 Elementary abelian normal subgroups with cyclic quotients

In this section we fix a prime number $p > 2$ and a finite $p$-group $G$ containing an elementary abelian normal subgroup $A$ such that $G/A$ is cyclic. We are going to prove that (P1) and (P2) hold for $G$. We start with the following elementary observation.

**Lemma 6.1.** *In the situation above, let $g \in G$ be such that $G = A\langle g \rangle$, and suppose that $g^p = 1$. Moreover, let $a \in A$ and $i, j \in \mathbb{Z}$ be such that $[a, g^i] =_G [a, g^j]$. Then $[a, g^i] = [a, g^j]$.*

*Proof.* Assume that $[a, g^i] \neq [a, g^j]$. Then $g^i \neq g^j$, so that $i \not\equiv j \pmod{p}$. But now Lemma 2.5 gives a contradiction. □

Next we extend the result above.

**Lemma 6.2.** *In the situation above, let $g \in G$ be such that $G = A\langle g \rangle$. Moreover, let $a \in A$ and $i, j \in \mathbb{Z}$ be such that $[a, g^i] =_G [a, g^j]$. Then $[a, g^i] = [a, g^j]$.*

*Proof.* It is clear that we can replace $G$ by the semidirect product of $A$ and $\langle g \rangle$. In other words, we may assume that $A \cap \langle g \rangle = 1$. With this additional condition, let $G$ be a minimal counterexample. Then $\langle g \rangle$ acts faithfully on $A$. Moreover, we have $G = \langle a, g \rangle$ and $A = \langle g^k a g^{-k} : k \in \mathbb{Z} \rangle$. Moreover, we can write $[a, g^j] = g^s [a, g^i] g^{-s}$ with $s \in \mathbb{Z}$. Let $Z$ be a minimal normal subgroup of $G$, so that $Z \subseteq A$. Then $\overline{G} := G/Z$, $\overline{A} := A/Z$, $\overline{g} := gZ$ and $\overline{a} := aZ$ also satisfy the hypothesis of Lemma 6.2. Thus $[\overline{a}, \overline{g}^i] = [\overline{a}, \overline{g}^j]$ by minimality, and $\overline{g}^{i-j} \in \mathrm{C}_{\overline{G}}(\overline{a})$. Thus $\overline{g}^{i-j} \in \mathrm{Z}(\overline{G})$ since $\overline{G} = \langle \overline{a}, \overline{g} \rangle$. Also, $[a, g^{i-j}] \in Z \subseteq \mathrm{Z}(G)$ implies that $[a, (g^{i-j})^p] = [a, g^{i-j}]^p = 1$, so $g^{(i-j)p} \in \mathrm{C}_G(a)$. Thus $g^{(i-j)p} \in \mathrm{Z}(G)$ since $G = \langle a, g \rangle$. Since $\langle g \rangle$ acts faithfully on $A$ we conclude that $g^{(i-j)p} = 1$. Let $p^m := |\langle g \rangle|$. Then $m \geq 2$ by Lemma 6.1, and $i \equiv j \pmod{p^{m-1}}$; in particular, $\langle g^i \rangle = \langle g^j \rangle$. If $G$ contains distinct minimal normal subgroups $Z_1, Z_2$ then the argument above shows that $[a, g^{i-j}] \in Z_1 \cap Z_2 = 1$, so $g^{i-j} \in \mathrm{C}_G(a)$ and $[a, g^i] = [a, g^j]$. Thus the result is proved in this case. Hence we may assume that $Z$ is the only minimal normal subgroup of $G$. We distinguish between two cases:

**Case 1:** $i \equiv 0 \pmod{p}$.
Then $j \equiv i \equiv 0 \pmod{p}$. If $s \equiv 0 \pmod{p}$ as well then $H := A\langle g^p \rangle$ also satisfies the hypothesis of Lemma 6.2. By minimality, this implies that $[a, g^i] = [a, g^j]$. Thus we may assume that $s \not\equiv 0 \pmod{p}$. Then we can replace $g$ by $g^s$ and assume that $[a, g^j] = g[a, g^i]g^{-1}$. Thus $\overline{g}$ centralizes $[\overline{a}, \overline{g}^i]$. Hence $g$ normalizes $\langle [a, g^i], Z \rangle$ and centralizes both $Z$ and $\langle [a, g^i], Z \rangle / Z$. Therefore $g^p$ centralizes $\langle [a, g^i], Z \rangle$; in particular, $g^i$ centralizes $[a, g^i]$. Since $\langle g^i \rangle = \langle g^j \rangle$ there is $k \in \mathbb{Z}$ such that $g^j = (g^i)^k$. Then $g[a, g^i]g^{-1} = [a, g^{ik}] = [a, g^i]^k$, so $g$ normalizes $\langle [a, g^i] \rangle$. Thus $\langle [a, g^i] \rangle \trianglelefteq G$, so $\langle [a, g^i] \rangle \subseteq Z \subseteq \mathrm{Z}(G)$, and $[a, g^j] = g[a, g^i]g^{-1} = [a, g^i]$.

**Case 2:** $i \not\equiv 0 \pmod{p}$.
In this case we may replace $g$ by $g^i$ and assume that $i = 1$. The map $f : A \to A$, $b \mapsto [b, g]$, is a homomorphism;

in particular, $f(A) = \{[b,g] : b \in A\} \leq A$. Moreover, $f(A) \trianglelefteq G$ and $G/f(A)$ is abelian. Thus $G' \leq f(A) \leq G'$, so that

$$G' = f(A) = \langle f(g^k a g^{-k}) : k \in \mathbb{Z}\rangle = \langle [g^k a g^{-k}, g] : k \in \mathbb{Z}\rangle.$$

We know that $[\overline{a},\overline{g}] \in \mathrm{C}_{\overline{G}}(\overline{g}^s)$. Thus $[\overline{g}^k \overline{a} \overline{g}^{-k}, \overline{g}] = \overline{g}^k [\overline{a},\overline{g}] \overline{g}^{-k} \in \mathrm{C}_{\overline{G}}(\overline{g}^s)$ for $k \in \mathbb{Z}$. We conclude that $\overline{G}' \subseteq \mathrm{C}_{\overline{G}}(\overline{g}^s)$ and set $H := G'\langle g^s\rangle$. Then $\overline{H} := HZ/Z$ is an abelian normal subgroup of $\overline{G}$. Thus $H' \subseteq Z \subseteq \mathrm{Z}(G)$. Since $p$ is odd, $H$ is a regular $p$-group. Hence $(xy)^p = x^p y^p$ for $x, y \in H$, by Satz III.10.8 in [9]. In particular, we have $\mho_1(H) = \langle g^{sp}\rangle$. Since $Z \nsubseteq \mho_1(H) \trianglelefteq G$ we must have $1 = \mho_1(H) = \langle g^{sp}\rangle$. Thus $g^s \in \langle g^{p^{m-1}}\rangle = \langle g^{i-j}\rangle \in \mathrm{C}_G(\overline{A})$. Hence we can write $g^s a g^{-s} = az$ with $z \in Z$. We conclude:

$$[a, g^j] = g^s [a,g] g^{-s} = [g^s a g^{-s}, g] = [az, g] = [a,g],$$

and the proof is complete. □

**Lemma 6.3.** *In the situation above, let $K, L \in \mathrm{Cl}(G)$ be such that $K \subseteq A$ and $L \subseteq KK^{-1}$. Then $c_{KK^{-1}L} = \frac{|K|}{|L|}$; in particular,* (P3)*,* (P2) *and* (P1) *hold.*

*Proof.* Let $x \in K$. Then Lemma 6.2 shows that

$$\eta(K) \geq |\{[x, g^i] : i \in \mathbb{Z}\}| = |G : \mathrm{C}_G(x)| = |K|.$$

Thus Lemma 2.1(vi) implies that $\eta(K) = |K|$, and $c_{KK^{-1}L} = \frac{|K|}{|L|}$ by Lemma 2.1(vii). □

**Proposition 6.4.** *Let $G$ be a finite $p$-group where $p$ is an odd prime, and let $A$ be an elementary abelian normal subgroup of $G$ such that $G/A$ is cyclic. Then $|KK^{-1}| \equiv 1 \pmod{p-1}$ for $K \in \mathrm{Cl}(G)$.*

*Proof.* Let $g \in G$ be such that $G = A\langle g\rangle$, and let $x = ag^s \in K$ where $a \in A$ and $s \in \mathbb{Z}$. Then $KK^{-1}$ consists of the conjugates of the elements

$$\begin{aligned}[ag^s, bg^i] &= ag^s bg^i g^{-s} a^{-1} g^{-i} b^{-1} = a \cdot g^s b g^{-s} \cdot g^i a^{-1} g^{-i} \cdot b^{-1} \\ &= ag^i a^{-1} g^{-i} \cdot g^s b g^{-s} b^{-1} = [a, g^i][g^s, b]\end{aligned}$$

($b \in A, i \in \mathbb{Z}$). The map $f : A \to A$, $b \mapsto [g^s, b]$, is a homomorphism; in particular,

$$N := f(A) = \{[g^s, b] : b \in A\} \leq A.$$

Clearly, $N \trianglelefteq G$. The equation above shows that $\{[ag^s, bg^i] : b \in A, i \in \mathbb{Z}\}$ is a union of complete cosets of $N$ in $G$. Thus $KK^{-1}$ is a union of complete cosets of $N$ in $G$. Hence Lemma 2.2 implies that $|KK^{-1}| \equiv |\overline{K}\,\overline{K}^{-1}| \pmod{p-1}$ where $\overline{K} \in \mathrm{Cl}(\overline{G})$ denotes the image of $K$ in $\overline{G} := G/N$. Therefore it suffices to show that $|\overline{K}\,\overline{K}^{-1}| \equiv 1 \pmod{p-1}$. Note that $\overline{G}$ also satisfies the hypothesis of the proposition. So we may replace $G$ by $\overline{G}$. Then $g^s$ centralizes $A$, so $g^s \in \mathrm{Z}(G)$. Hence $K = Lg^s$ where $L$ is the conjugacy class of $a$ in $G$, and $KK^{-1} = LL^{-1}$. Thus we may also replace $K$ by $L$. But then the result follows from Lemma 6.3. □

# 7 Elementary results on characters

In the following, let $p$ be a prime, and let $G$ be a finite $p$-group. Our first result is analogous to Lemma 2.3.

**Lemma 7.1.** *Let $\chi \in \mathrm{Irr}(G)$. Then $\Lambda := \mathrm{Irr}(\chi\overline{\chi}) \cap \widehat{G}$ is a subgroup of $\widehat{G}$. Furthermore, $\Lambda$ acts on $\mathrm{Irr}(G)$ by multiplication, and we have $(\chi\overline{\chi}|\lambda\psi)_G = (\chi\overline{\chi}|\psi)_G$ for $\lambda \in \Lambda$ and $\psi \in \mathrm{Irr}(G)$.*

*Proof.* If $\lambda \in \widehat{G}$ then $\chi\lambda \in \mathrm{Irr}(G)$, and $(\chi\overline{\chi}|\lambda)_G = (\chi|\chi\lambda)_G \in \{0,1\}$. Moreover, we have $(\chi\overline{\chi}|\lambda)_G \neq 0$ if and only if $\chi\lambda = \chi$. Thus $\Lambda$ is the stabilizer of $\chi$ in $\widehat{G}$, under the action of $\widehat{G}$ on $\mathrm{Irr}(G)$ by multiplication. In particular, $\Lambda$ is a subgroup of $\widehat{G}$. If $\lambda \in \Lambda$ and $\psi \in \mathrm{Irr}(G)$ then

$$(\chi\overline{\chi}|\lambda\psi)_G = (\chi|\chi\lambda\psi)_G = (\chi|\chi\psi)_G = (\chi\overline{\chi}|\psi)_G.$$

□

It is clear that (Q1) and (Q2) hold for $p = 2$. It is also easy to see that (Q1) holds whenever $p = 3$:

**Lemma 7.2.** *Suppose that $p \neq 2$. Then $|\operatorname{Irr}(\chi\overline{\chi})|$ is odd for $\chi \in \operatorname{Irr}(G)$; in particular,* (Q1) *holds for $p = 3$.*

*Proof.* For $\psi \in \operatorname{Irr}(G)$, we have

$$(\chi\overline{\chi}|\psi)_G = \overline{(\chi\overline{\chi}|\psi)_G} = (\overline{\chi\overline{\chi}}|\overline{\psi})_G = (\chi\overline{\chi}|\overline{\psi})_G.$$

Since the trivial character of $G$ is the only real-valued irreducible character of $G$ the elements in $\operatorname{Irr}(\chi\overline{\chi}) \setminus \{1_G\}$ come in pairs of the form $(\psi, \overline{\psi})$. The result follows since certainly $1_G \in \operatorname{Irr}(\chi\overline{\chi})$. □

Our next result is an easy observation.

**Lemma 7.3.** *Let $\chi, \psi \in \operatorname{Irr}(G)$. Then $(\chi\overline{\chi}|\psi)_G \leq \psi(1)$.*

*Proof.* Since $(\chi\overline{\chi}|\psi)_G = (\chi|\chi\psi)_G$ is the multiplicity of $\chi$ in $\chi\psi$ we have $\chi(1)\psi(1) \geq (\chi\overline{\chi}|\psi)_G\chi(1)$, and the result follows. □

The next result comes from the paper [1] by Adan-Bante.

**Lemma 7.4.** *Let $\chi \in \operatorname{Irr}(G)$ be such that $\chi(1) \in \{1, p\}$. Then $(\chi\overline{\chi}|\psi)_G = 1$ for $\psi \in \operatorname{Irr}(\chi\overline{\chi})$.*

*Proof.* The case $\chi(1) = 1$ is trivial, and the case $\chi(1) = p$ is a consequence of Lemma 5.1 in [1]. □

As an application of Lemma 7.4, we obtain:

**Corollary 7.5.** *Suppose that $G$ contains an abelian subgroup $A$ of index $p$. Then $(\chi\overline{\chi}|\psi)_G = 1$ for $\psi \in \operatorname{Irr}(\chi\overline{\chi})$.*

*Proof.* This follows from Lemma 7.4 since $\chi(1) \leq |G : A| = p$ by Problem 2.9 in [11]. □

We now turn our attention to irreducible characters of "large" degree.

**Lemma 7.6.** *Let $\chi \in \operatorname{Irr}(G)$ be such that $\chi(1)^2 = |G : \operatorname{Z}(\chi)|$. Then $(\chi\overline{\chi}|\psi)_G = \psi(1)$ is a power of $p$, for $\psi \in \operatorname{Irr}(\chi\overline{\chi})$. Thus* (Q2) *holds, in particular, if $|G| = p^{2n+1}$ and $\chi(1) = p^n$ for some $n \in \mathbb{N}$.*

*Proof.* By Corollary 2.30 in [11], $\chi$ vanishes on $G \setminus \operatorname{Z}(\chi)$. Moreover, by Lemma 2.27 in [11], there is $\zeta \in \operatorname{Irr}(\operatorname{Z}(\chi))$ such that $\zeta(1) = 1$ and $\chi_{\operatorname{Z}(\chi)} = \chi(1)\zeta$. Thus $\chi\overline{\chi}$ is the regular character of $G/\operatorname{Z}(\chi)$, viewed as a character of $G$. Hence

$$\chi\overline{\chi} = \sum_{\phi \in \operatorname{Irr}(G/\operatorname{Z}(\chi))} \phi(1)\phi,$$

and $(\chi\overline{\chi}|\psi)_G = \psi(1)$ for $\psi \in \operatorname{Irr}(\chi\overline{\chi}) = \operatorname{Irr}(G/\operatorname{Z}(\chi))$. Suppose that $|G| = p^{2n+1}$ and $\chi(1) = p^n$ for some $n \in \mathbb{N}$. Since

$$p^{2n} = \chi(1)^2 \leq |G : \operatorname{Z}(\chi)| \leq |G : \operatorname{Z}(G)| \leq p^{2n}$$

we conclude that $|\operatorname{Z}(G)| = p$ and $\chi(1)^2 = |G : \operatorname{Z}(\chi)|$. Then the result follows from the first part of the proof. □

The preceding results allow to deal with the groups of order $p^n$, for $n = 0, 1, \ldots, 5$.

**Proposition 7.7.** *Suppose that $|G| \leq p^5$. Then $(\chi\overline{\chi}|\psi)_G$ is a power of $p$, for $\chi \in \operatorname{Irr}(G)$ and $\psi \in \operatorname{Irr}(\chi\overline{\chi})$.*

*Proof.* Since $\chi(1)^2 \leq |G : \operatorname{Z}(\chi)| \leq |G : \operatorname{Z}(G)| \leq p^4$, we must have $\chi(1) \leq p^2$. If $\chi(1) = p^2$ then $|G : \operatorname{Z}(G)| = p^4$, and therefore $|G| = p^5$. Hence the result follows from Lemma 7.6 in this case. On the other hand, if $\chi(1) < p^2$ then Lemma 7.4 implies the result. □

We will deal with the groups of order $p^6$ in the next section. Another consequence of Lemma 7.6 is the following result:

**Proposition 7.8.** *Let $\chi \in \operatorname{Irr}(G)$ be such that $G' \subseteq \operatorname{Z}(\chi)$. Then $(\chi\overline{\chi}|\psi)_G = \psi(1)$ for $\psi \in \operatorname{Irr}(\chi\overline{\chi})$. In particular,* (Q2) *holds for finite $p$-groups of nilpotency class* 2.

*Proof.* Theorem 2.31 in [11] implies that $\chi(1)^2 = |G : \operatorname{Z}(\chi)|$. Thus the result follows from Lemma 7.6. □

# 8 Characters of groups of order $p^6$

In this section we show that (Q1) and (Q2) hold for groups of order $p^6$ where $p$ is a prime.

**Proposition 8.1.** *Let $p$ be a prime, let $G$ be a group of order $p^6$, and let $\chi \in \mathrm{Irr}(G)$. Then $(\chi\overline{\chi}|\psi)_G$ is a power of $p$, for $\psi \in \mathrm{Irr}(\chi\overline{\chi})$; in particular,* (Q1) *and* (Q2) *hold.*

*Proof.* By Proposition 7.8, we may assume that $\mathrm{cl}(G) > 2$. By Proposition 7.7, we may assume that $\chi$ is faithful. By Lemma 7.4, we may also assume that $\chi(1) = p^2$. Let $A \in \mathrm{SCN}(G)$. Then $|A| \geq p^3$ since $G/A = G/\mathrm{C}_G(A)$ is isomorphic to a $p$-subgroup of $\mathrm{Aut}(A)$. On the other hand, $p^2 = \chi(1) \leq |G : A|$ by Problem 2.9 in [11]. Thus $|A| \in \{p^3, p^4\}$, and we distinguish the corresponding cases.

**Case 1:** $|A| = p^4$.
Let $\lambda \in \mathrm{Irr}(\chi_A)$. Then $\lambda(1) = 1$ and $0 \neq (\chi_A|\lambda)_A = (\chi|\lambda^G)_G$, by Frobenius reciprocity. Since $\chi(1) = p^2 = \lambda^G(1)$ we conclude that $\lambda^G = \chi \in \mathrm{Irr}(G)$. Hence $\mathrm{I}_G(\lambda) = A$ by Theorem 17.4 in [10]. Let $\Lambda$ denote the orbit of $\lambda$, in the action of $G$ on $\mathrm{Irr}(A)$ by conjugation, and let $\Lambda^+$ denote the sum of the elements in $\Lambda$. Then $\chi_A = \Lambda^+$, and $\psi_A = p^e\Psi^+$ where $\Psi$ is another $G$-orbit on $\mathrm{Irr}(A)$, and $e \in \mathbb{N}_0$. Since

$$\chi\overline{\chi} = \chi\overline{\lambda}^G = (\chi_A\overline{\lambda})^G = (\Lambda^+\overline{\lambda})^G$$

we obtain, by Frobenius reciprocity:

$$\begin{aligned}(\chi\overline{\chi}|\psi)_G &= ((\Lambda^+\overline{\lambda})^G|\psi)_G = (\Lambda^+\overline{\lambda}|\psi_A)_A = p^e(\Lambda^+\overline{\lambda}|\Psi^+)_A = p^e|\{\lambda' \in \Lambda : \lambda'\overline{\lambda} \in \Psi\}| \\ &= \frac{p^e}{|\Lambda|}|\{(\lambda_1, \lambda_2) \in \Lambda^2 : \lambda_1\overline{\lambda_2} \in \Psi\}| = p^e\frac{|\Psi|}{|\Lambda|}c_{\Lambda\Lambda^{-1}\Psi}\end{aligned}$$

where $c_{\Lambda\Lambda^{-1}\Psi}$ denotes a class multiplication constant of the semidirect product $\widehat{A} \rtimes (G/A)$. Thus Theorem 4.9 implies that $c_{\Lambda\Lambda^{-1}\Psi}$ is a power of $p$, and we are done in this case.

**Case 2:** $|A| = p^3$.
By Case 1, we may assume that there is no $B \in \mathrm{SCN}(G)$ such that $|B| = p^4$. We are going to show that $G$ has maximal class, and that $G$ is an exceptional group, in the sense of Definition III.14.5 of [9].

Assume first that $G'$ is abelian. Then we may assume that $G' \subseteq A$. Thus $G/A = G/\mathrm{C}_G(A)$ is isomorphic to an abelian $p$-subgroup of $\mathrm{Aut}(A)$. Since $|G/A| = p^3$, $A$ cannot be cyclic. By Lemma 4.1, $A$ cannot be elementary abelian, and by Lemma 4.2, $A$ cannot be isomorphic to $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Thus we have a contradiction in this case.

Hence $G'$ is nonabelian. Then Hilfssatz III.7.10 in [9] implies:

$$|G'| \geq p^4,\ |\mathrm{Z}(G')| \geq p^2,\ |G'/G''| \geq p^3.$$

This means that $|G'| = p^4$, $|G''| = p$, $G' = \Phi(G)$ and $|\mathrm{Z}(G')| = p^2$. We claim that $A \subseteq G' = \Phi(G)$.

Indeed, otherwise $|G/A\Phi(G)| \leq p$, and $G = \langle g\rangle A\Phi(G) = \langle g\rangle A$ for some $g \in G$. But then $G/A$ is cyclic, and $G' \subseteq A$. Since $G'$ is nonabelian we have a contradiction.

We conclude that $\mathrm{Z}(G) \subseteq \mathrm{C}_G(A) = A \subseteq G'$. We claim that even $Z_2(G) \subseteq G' = \Phi(G)$.

Indeed, otherwise $|G/Z_2(G)\Phi(G)| \leq p$, and $G = \langle g\rangle Z_2(G)\Phi(G) = \langle g\rangle Z_2(G)$ for some $g \in G$. Then $G/\mathrm{Z}(G)$ is abelian, so that $\mathrm{cl}(G) \leq 2$, a contradiction.

Hauptsatz III.2.11 in [9] implies that $[Z_2(G), G'] = 1$, so that $Z_2(G) \subseteq \mathrm{Z}(G')$. Since $p^2 = |\mathrm{Z}(G')| \geq |Z_2(G)| \geq p^2$ we conclude that $Z_2(G) = \mathrm{Z}(G')$ has order $p^2$. Hence $|\mathrm{Z}(G)| = p$. Since $|G/\Phi(G)| = p^2$, Hilfssatz III.1.11 in [9] implies that $K_2(G)/K_3(G)$ is cyclic. Furthermore, Satz III.2.13 in [9] shows that $\exp(K_2(G)/K_3(G))$ divides $\exp(G/K_2(G)) = p$. Thus $|K_2(G)/K_3(G)| = p$ and $|K_3(G)| = p^3$; in particular, $K_3(G) \nsubseteq Z_2(G)$. Hence $K_4(G) = [K_3(G), G] \nsubseteq Z(G)$ and $K_5(G) = [K_4(G), G] \neq 1$. We conclude that $G$ must have maximal class. We claim that $G$ is an exceptional group, in the sense of Definition III.14.5 of [9].

Otherwise Hauptsatz III.14.7 in [9] implies that $[K_2(G), K_3(G)] \subseteq K_6(G) = 1$, i. e. $K_3(G) \subseteq \mathrm{Z}(G')$. This is a contradiction since $|K_3(G)| = p^3$ and $|\mathrm{Z}(G')| = p^2$.

Now Aufgabe 35 in Chapter III of [9] shows that $A = K_3(G)$ is the only maximal abelian normal subgroup of $G$.

Next we turn our attention to the character theory of $G$. Recall that we are considering a faithful $\chi \in \mathrm{Irr}(G)$ of degree $p^2$. Let $\lambda \in \mathrm{Irr}(\chi_A)$ and $T := \mathrm{I}_G(\lambda)$.

Assume that $G' \subseteq T$. Since $|G' : A| = p$, $\lambda$ has exactly $p$ extensions to $G'$, and $\lambda^{G'}$ is the sum of these extensions. Since $0 \neq (\chi_A|\lambda)_A = (\chi_{G'}|\lambda^{G'})_{G'}$ there exists an extension $\mu$ of $\lambda$ to $G'$ such that $0 \neq (\chi_{G'}|\mu) = (\chi|\mu^G)$. Since $\chi(1) = p^2 = \mu^G(1)$ this implies that $\chi = \mu^G$. Since $G'' \subseteq \ker(\mu)$ we are led to the contradiction $1 < G'' \leq \ker(\mu^G) = \ker(\chi) = 1$.

Thus we must have $G' \not\subseteq T$; in particular, $|G : T| \geq p^2$. By Clifford Theory, $\chi = \mu^G$ for a unique $\mu \in \mathrm{Irr}(T|\lambda)$. Hence $|G : T| = p^2$, and $\mu(1) = 1$. Since $|T| = p^4 = |G'|$ and $T \cap G' = A$ we conclude that $|TG'| = p^5$. Hence $TG'$ is the only maximal subgroup of $G$ containing $T$; in particular, we have $TG' = \mathrm{N}_G(T) =: W$. Since $A = \mathrm{C}_G(A)$, $T$ is nonabelian, i. e. $1 \neq T' \subseteq \ker(\mu)$. Since $\mu^G = \chi$ is faithful, $T'$ does not contain any nontrivial normal subgroup of $G$; in particular, we have $T' \not\trianglelefteq G$ and $T' \cap \mathrm{Z}(G) = 1$. On the other hand, we have $T' \trianglelefteq \mathrm{N}_G(T) = W$, so $T' \cap \mathrm{Z}(W) \neq 1$, and $\mathrm{Z}(G) \neq \mathrm{Z}(W) \trianglelefteq G$. Thus $Z_2(G) \leq \mathrm{Z}(W)$ and $W \subseteq \mathrm{C}_G(Z_2(G))$. Since $|G : \mathrm{C}_G(Z_2(G))| = p$ we conclude that $W = \mathrm{C}_G(Z_2(G))$. Since $1 \neq T' \leq W' \trianglelefteq G$ and $T' \not\trianglelefteq G$ we have $T' < W'$; in particular, $|W'| \geq p^2$.

Let $W \neq M \in \mathrm{Max}(G)$. Then $TM = G$ and $T \cap M = A$. The Mackey formula shows that

$$\chi_M = (\mu^G)_M = (\mu_A)^M = \lambda^M \in \mathrm{Irr}(M);$$

for $\mathrm{I}_M(\lambda) = T \cap M = A$. Thus $p^4 = \chi_M(1)^2 \leq |M : \mathrm{Z}(M)| \leq p^4$. Hence $\mathrm{Z}(M) = \mathrm{Z}(G)$, and $\chi_M(1)^2 = |M : \mathrm{Z}(M)|$. So Corollary 2.30 in [11] implies that $\chi_M(g) = 0$ for all $g \in M \setminus \mathrm{Z}(M)$. This yields that $\chi_M\overline{\chi_M}$ is the regular character $\rho_{M/\mathrm{Z}(M)}$ of $M/\mathrm{Z}(M)$, viewed as a character of $M$.

Suppose first that $|M'| = p$, i. e. $M' = \mathrm{Z}(G) = \mathrm{Z}(M)$. Then $\chi_M\overline{\chi_M} = \sum_{\alpha \in \mathrm{Irr}(M/\mathrm{Z}(M))} \alpha$. If $\psi(1) = 1$ then $(\chi\overline{\chi}|\psi)_G \leq \psi(1) = 1$ by Lemma 7.9, so that $(\chi\overline{\chi}|\psi) = 1$, and we are done. If $\psi(1) \neq 1$ then $\psi = \alpha^G$ for some $\alpha \in \mathrm{Irr}(M/\mathrm{Z}(M)) \subseteq \mathrm{Irr}(M)$, and

$$(\chi\overline{\chi}|\psi)_G = (\chi\overline{\chi}|\alpha^G)_G = (\chi_M\overline{\chi_M}|\alpha)_M = 1,$$

and the result follows in this case.

Thus we may assume that $|M'| \geq p^2$ for all $M \in \mathrm{Max}(G)$. This means that $G/\mathrm{Z}(G)$ does not have an abelian maximal subgroup. Hence Theorem 12.11 in [11] shows that $G/\mathrm{Z}(G)$ has an irreducible character of degree $p^2$. This character vanishes outside of $Z_2(G)/Z(G)$. Algebraic conjugation gives precisely $p - 1$ irreducible characters of $G/\mathrm{Z}(G)$ of degree $p^2$. Also, $G/\mathrm{Z}(G)$ has precisely $p^2$ irreducible characters of degree 1. The remaining irreducible characters of $G/\mathrm{Z}(G)$ must have degree $p$. Since

$$p^2 \cdot 1 + (p^2 - 1) \cdot p^2 + (p - 1) \cdot p^4 = p^5,$$

$G/\mathrm{Z}(G)$ has precisely $p^2 - 1$ irreducible characters of degree $p$. Similarly, $G/Z_2(G)$ has precisely $p^2$ irreducible characters of degree 1. All other irreducible characters of $G/Z_2(G)$ must have degree $p$. Since $p^4 = p^2 \cdot 1 + (p^2 - 1) \cdot p^2$, $G/Z_2(G)$ has precisely $p^2 - 1$ irreducible characters of degree $p$. This implies that all irreducible characters of $G/\mathrm{Z}(G)$ of degree $p$ have $Z_2(G)/\mathrm{Z}(G)$ in their kernel. We now analyze the multiplicity of any $\beta \in \mathrm{Irr}(G/\mathrm{Z}(G)) \subseteq \mathrm{Irr}(G)$ in $\chi\overline{\chi}$.

Suppose first that $\beta(1) = p^2$. Let $W \neq M \in \mathrm{Max}(G)$. Then $\beta = \phi^G$ for some $\phi \in \mathrm{Irr}(M/\mathrm{Z}(G))$, and $\phi(1) = p$. Then

$$(\chi\overline{\chi}|\beta)_G = (\chi\overline{\chi}|\phi^G)_G = (\chi_M\overline{\chi_M}|\phi)_M = (\rho_{M/\mathrm{Z}(M)}|\phi)_M = \phi(1) = p.$$

This shows that every irreducible character of $G/\mathrm{Z}(G)$ of degree $p^2$ occurs with multiplicity $p$ in $\chi\overline{\chi}$.

Suppose next that $\beta(1) = p$. We consider $\beta$ as an irreducible character of $\widetilde{G} := G/Z_2(G)$. There are two possibilities:

Suppose first that $\beta$ is not faithful, considered as a character of $\widetilde{G}$. Then $\mathrm{Z}(\widetilde{G}) \subseteq \ker(\beta)$. Let $W \neq M \in \mathrm{Max}(G)$, so that $\widetilde{M} := M/Z_2(G) \in \mathrm{Max}(\widetilde{G})$, and $|\widetilde{M}| = p^3$. Then $\widetilde{M}' \subseteq \mathrm{Z}(\widetilde{G}) \subseteq \ker(\beta)$, and $\beta = \alpha^G$ for some $\alpha \in \mathrm{Irr}(\widetilde{M}) \subseteq \mathrm{Irr}(M)$. We conclude that

$$(\chi\overline{\chi}|\beta)_G = (\chi\overline{\chi}|\alpha^G)_G = (\chi_M\overline{\chi_M}|\alpha)_M = (\rho_{M/\mathrm{Z}(M)}|\alpha)_M = \alpha(1) = 1.$$

Now suppose that $\beta$ is a faithful character of $\widetilde{G}$. Since $\widetilde{G}$ is an M-group, there are $\widetilde{L} = L/Z_2(G) \in \mathrm{Max}(\widetilde{G})$ and $\omega \in \mathrm{Irr}(\widetilde{L})$ such that $\beta = \omega^{\widetilde{G}}$. Since $\widetilde{L}' \subseteq \ker(\omega)$ and $\widetilde{L}' \trianglelefteq \widetilde{G}$ we have $\widetilde{L}' \subseteq \ker(\omega^{\widetilde{G}}) = \ker(\beta) = 1$, i. e. $\widetilde{L}$ is abelian. In particular, $\widetilde{L}$ does not have maximal class.

Note that $\widetilde{G}$ is a $p$-group of maximal class, but not an exceptional group, by Hauptsatz III.14.6 in [9]. Thus, by Satz III.14.22 in [9], $\widetilde{G}_1 := \mathrm{C}_{\widetilde{G}}(K_2(\widetilde{G})/K_4(\widetilde{G}))$ is the only maximal subgroup of $\widetilde{G}$ which does not have maximal class; in particular, $\widetilde{L} = \widetilde{G}_1$, and $L = G_1 \neq \mathrm{C}_G(Z_2(G)) = W$ since $G$ is an exceptional group. Thus, as we showed above, $\chi_L \in \mathrm{Irr}(L)$ and $\chi_L\overline{\chi_L} = \rho_{L/\mathrm{Z}(L)}$. Moreover,

$$(\chi\overline{\chi}|\beta)_G = (\chi\overline{\chi}|\omega^G)_G = (\chi_L\overline{\chi_L}|\omega)_L = (\rho_{L/\mathrm{Z}(L)}|\omega)_L = 1.$$

We have thus shown that each of the $p^2 - 1$ irreducible characters of $G/\mathrm{Z}(G)$ of degree $p$ occurs in $\chi\overline{\chi}$ with multiplicity 1.

It remains to consider the irreducible characters of $G/\mathrm{Z}(G)$ of degree 1. Again, let $W \neq M \in \mathrm{Max}(G)$. Then $G$ acts by conjugation on the nontrivial elementary abelian $p$-group $\mathrm{Irr}(M/\Phi(M))$. Thus $G$ has at least $p$ fixed points on $\mathrm{Irr}(M/\Phi(M))$. If $\omega$ is one of these, then $\omega^G$ is the sum of the $p$ extensions of $\omega$ to $G$. We get $1 = (\chi_M\overline{\chi_M}|\omega)_M = (\chi\overline{\chi}|\omega^G)_G$. In this way we obtain (at least) $p$ irreducible constituents of $\chi\overline{\chi}$ of degree 1. However, since

$$p + (p^2 - 1) \cdot p + (p - 1) \cdot p \cdot p^2 = p^4$$

we have already accounted for all irreducible constituents of $\chi\overline{\chi}$, and the result is proved. □

The result above does not extend to groups of order $p^7$. In fact, there is a group of order $3^7$ with two irreducible characters $\chi, \psi$ such that $(\chi\overline{\chi}|\psi)_G = 2$, as the example following Theorem 4.9 shows. This can be checked easily using GAP [7].

# 9 Characters of metacyclic $p$-groups

In this section we prove (Q1) and (Q2) for metacyclic $p$-groups.

**Proposition 9.1.** *Let $G$ be a metacyclic $p$-group where $p$ is an odd prime, and let $\chi \in \mathrm{Irr}(G)$. Then $\chi\overline{\chi}$ is the regular character of $G/\mathrm{Z}(\chi)$, viewed as a character of $G$. Thus $(\chi\overline{\chi}|\psi)_G = \psi(1)$ for $\psi \in \mathrm{Irr}(\chi\overline{\chi})$; in particular, (Q1) and (Q2) are satisfied.*

*Proof.* Let $A = \langle a \rangle \trianglelefteq G$ and $B = \langle b \rangle \leq G$ such that $G = AB$. Then $C := \mathrm{C}_G(A) \trianglelefteq G$. Moreover, $C$ is abelian since $A \subseteq \mathrm{Z}(C)$ and $C/A$ is cyclic. By Lemma 5.1, we have $G' = \{[a, b^i] : i \in \mathbb{Z}\}$, so

$$|G'| = |\{b^i a b^{-i} : i \in \mathbb{Z}\}| = |\{gag^{-1} : g \in G\}| = |G : \mathrm{C}_G(a)| = |G : C|.$$

Also, Lemma 12.12 in [11] implies that $|C| = |G'| \cdot |\mathrm{Z}(G)|$. Thus

$$|G : \mathrm{Z}(G)| = |G : C| \cdot |C : \mathrm{Z}(G)| = |G'|^2.$$

Now let $\chi \in \mathrm{Irr}(G)$. We may assume that $\chi$ is faithful. Let $\lambda \in \mathrm{Irr}(\chi_A)$, and let $T := \mathrm{I}_G(\lambda)$. Then $A \leq C \leq T \trianglelefteq G$, and $T/A$ is cyclic. Thus $\chi = \mu^G$ where $\mu \in \widehat{T}$ is an extension of $\lambda$. Now $T' \subseteq \ker(\mu)$ and $T' \trianglelefteq G$, so $T' \subseteq \ker(\mu^G) = \ker(\chi) = 1$. Hence $T$ is abelian, so that $T \leq \mathrm{C}_G(A) = C$. We conclude that $T = C$ and $\chi(1) = |G : T| = |G : C| = |G'|$; in particular, $\chi(1)^2 = |G'|^2 = |G : \mathrm{Z}(G)| = |G : \mathrm{Z}(\chi)|$. Now Corollary 2.30 in [11] implies that $\chi$ vanishes on $G \setminus \mathrm{Z}(\chi)$. Moreover, $(\chi\overline{\chi})(z) = \chi(1)^2 = |G : \mathrm{Z}(\chi)|$ for $z \in \mathrm{Z}(\chi)$. Thus $\chi\overline{\chi}$ is indeed the regular character of $G/\mathrm{Z}(\chi)$. The result follows. □


### Acknowledgments

The authors are grateful to J. Schmidt [14] for providing GAP files containing the groups of order $3^7$ and $5^7$. Also, the first named author was supported by an OTKA grant (National Scientific Research Grant No. T049841).

## References


[1] E. Adan-Bante, *Products of characters and finite p-groups. II*, Arch. Math. (Basel) **82** (2004), 289–297.

[2] E. Adan-Bante, *Conjugacy classes and finite p-groups*, Arch. Math. (Basel) **85** (2005), 297–303.

[3] Z. Arad and M. Herzog (ed.), Products of conjugacy classes in groups, LNM 1112, Springer-Verlag, Berlin 1985

[4] Y.G. Berkovich and E.M. Zhmud', *Characters of finite groups, Part 2*, American Mathematical Society, Providence RI 1999

[5] H. I. Blau, Private communication

[6] H. I. Blau, Bangteng Xu, Z. Arad, E. Fisman, V. Milolavsky and M. Muzychuk, *Homogeneous integral table algebras of degree three: a trilogy*, Mem. Amer. Math. Soc. **144** (2000)

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

[8] D. Gorenstein, *Finite groups*, Harper & Row Publishers, New York 1968.

[9] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin 1967.

[10] B. Huppert, *Character theory of finite groups*, Walter de Gruyter & Co., Berlin 1998.

[11] I. M. Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006.

[12] C. Polcino Milies and S. Sehgal, *An introduction to group rings*, Kluwer Academic Publishers, Dordrecht 2002

[13] B. Sambale, *Konjugationsklassen und Charaktere in endlichen p-Gruppen*, Diplomarbeit, Jena 2008.

[14] J. Schmidt, Private communication.

[15] A. Shalev, *Commutators, words, conjugacy classes and character methods*, Turkish J. Math. **31** (2007), 131-148