Squares of real conjugacy classes in finite groups.

Antonio Beltrán

Departamento de Matemáticas,

Universidad Jaume I, 12071 Castellón, Spain

e-mail: abeltran@mat.uji.es

María José Felipe

Instituto Universitario de Matemática Pura y Aplicada,

Universidad Politécnica de Valencia, 46022 Valencia, Spain

e-mail: mfelipe@mat.upv.es

Carmen Melchor

Departamento de Matemáticas,

Universidad Jaume I, 12071 Castellón, Spain

e-mail: cmelchor@uji.es

Abstract

We prove that if a finite group G contains a conjugacy class K whose square is of the form $1 \cup D$, where D is a conjugacy class of G, then $\langle K \rangle$ is a solvable proper normal subgroup of G and we completely determine its structure. We also obtain the structure of those groups in which the assumption above is true for all conjugacy classes and when every conjugacy class satisfies that its square is the union of all central conjugacy classes except at most one.

1 Introduction

In 1985, Arad and Herzog conjectured that in a non-abelian simple group, the product of two non-trivial conjugacy classes can never be a single conjugacy class. This conjecture is still open but many results have appeared in the literature concerning products of conjugacy classes in finite groups and the normal

structure. For instance, Arad and Fisman proved that if the product of two conjugacy classes of a group G is exactly the union of these two classes, then G is not a non-abelian simple group. More recently, Navarro and Guralnick have proved in [6] that when a conjugacy class $K = x^G$ of an element x in a finite group G satisfies that K^2 is again a conjugacy class then $K = x[x, G]$, and what is more relevant, they prove that $[x, G]$ is a solvable (normal) subgroup of G by means of the Classification of the Finite Simple Groups (CFSG). Furthermore, in this case, it turns out $\langle K \rangle = \langle x \rangle [x, G]$ is solvable too. So, the fact that the square of a conjugacy class is a conjugacy class implies the existence of certain solvable normal subgroup in G, which is consistent with Arad and Herzog's conjecture.

Suppose now that K is a non-trivial real conjugacy class of G, that is, a conjugacy class satisfying that $K^{-1} = K$. It trivially follows that K^2 can never be a conjugacy class unless K consists exactly of a central involution of G. However, as K^2 is always a G-invariant set, we can write $K^2 = 1 \cup A$, where A is union of conjugacy classes of G. In this note, we study the extrem case in which A is a single conjugacy class, and we wonder whether one may obtain somewhat information concerning solvavility inside the group G. The answer is affirmative: K generates a solvable (normal) subgroup and we determine its structure. Notice that every class satisfying the property of the following theorem needs to be a real class. In fact, this is not a very unsual situation in finite groups.

Theorem A. *Let $K = x^G$ be a conjugacy class of a finite group G and suppose that $K^2 = 1 \cup D$, where D is a conjugacy class of G. Then $\langle D \rangle = [x, G]$ is either cyclic or p-group for some prime p, and so $\langle K \rangle = \langle x \rangle [x, G]$ is solvable. More precisely,*

1. *Suppose that $|K| = 2$.*

    1.1. If $o(x) = 2$, then $\langle K \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \cong \langle D \rangle \subseteq \mathbf{Z}(G)$.

    1.2. If $o(x) = n > 2$, then $\langle K \rangle \cong \mathbb{Z}_n$ and $\langle D \rangle$ is cyclic.

2. *Suppose that $|K| \geq 3$.*

    2.1. If $o(x) = 2$ then either $\langle K \rangle$ and $\langle D \rangle$ are 2-elementary abelian groups or $\langle D \rangle$ is a p-group and $|K| = p^r$ with p an odd prime and r a positive integer.

    2.2. If $o(x) > 2$, then $\langle D \rangle$ is a p-elementary abelian group for some odd prime p. Furthermore, either $o(x) = p$ or $o(x) = 2p$.

    In every case, $|\langle K \rangle / \langle D \rangle| \leq 2$.

Observe that in case 2 of Theorem A we determine the order of the elements of K that may be either 2, p or $2p$ with p and odd prime.

All cases of Theorem A are feasible and we provide examples of each one. Our techniques for proving Theorem A are quite elementary although we make use of Glauberman's Z* theorem [5] and a result of Berkovich and Kazarin in [2]. Both results require techniques from modular representation theory, so our results are based on it too. Other two main ingredients of the proof of Theorem A are Burnside's classification of finite 2-groups having exactly one involution and the classification of groups of order 16. We remark that we do not use the Classification of Finite Simple Groups.

As an application of Theorem A we obtain the following corollaries. The first one is related to groups having every conjugacy class satisfying the hypothesis of Theorem A and its proof is a trivial consequence. The second concerns those groups in which there exists a conjugacy class whose square is union of conjugacy classes all central except at most one.

Corollary B. *Let G be a finite group such that every non-central conjugacy class K satisfies that $K^2 = 1 \cup D$, where D is a conjugacy class of G. Then $G/\mathbf{F}(G)$ is an elementary abelian 2-group.*

Corollary C. *Let K be a conjugacy class of a finite group G such that K^2 is union of conjugacy classes all of them central except at most one. Then $\langle K \rangle$ is solvable.*

Suppose now that every conjugacy class K of a group G satisfies that K^2 is a conjugacy class too. It is trivial that every real element must lie in $\mathbf{Z}(G)$ and must have order 2. In [3], Chillag and Mann described the groups in which every real element is a central element. Particularly, in Remark 5.5. of [3], the authors also assert, with omitted proof, that a group satisfying these properties is really nilpotent. We include here an extension of this result which will be needed in order to obtain the structure of those groups in which all conjugacy classes satisfy the hypothesis of Corollary C. Notice that these groups are solvable by Theorem A and we prove that they are close to nilpotent groups.

Corollary D. *Let π be a set of primes. Suppose that K^2 is a conjugacy class for all conjugacy class K of π-elements of G. Then $G/\mathbf{O}_{\pi'}(G)$ is nilpotent. In particular, if $\pi = \pi(G)$, then G is nilpotent.*

Corollary E. *Let G be a finite group such that every conjugacy class K satisfies that K^2 is union of conjugacy classes all of them central except at most one. Let $M/\mathbf{F}(G) = \mathbf{O}_2(G/\mathbf{F}(G))$. Then G/M is nilpotent and, consequently, G is solvable with Fitting length at most 3.*

2 Preliminary results

We begin by stating the Z^* theorem version appearing in [7].

Theorem 2.1 (see Theorem 2 of [5]) *Suppose that $P \in \mathrm{Syl}_2(G)$ and $j \in P$ such that $j^2 = 1 \neq j$ and $P \cap \{j^g | g \in G\} = \{j\}$. Then $\mathbf{O}_{2'}(G)\langle j \rangle \trianglelefteq G$.*

The following elementary properties will be frequently used in the proofs.

Lemma 2.2 *Let K be a real conjugacy class of a group G. Then*

a) *$\langle K \rangle / \langle K^2 \rangle$ is trivial or cyclic of order 2.*

b) *If $K^2 = 1 \cup K$, then $\langle K \rangle$ is a minimal normal subgroup of G and it is p-elementary abelian for some prime p.*

Proof. We write $N = \langle K^2 \rangle$ and we consider the factor group $\langle K \rangle / N$ which is generated by elements xN with $x \in K$. But, if $x, y \in K$ we know that $xy^{-1} \in K^2 \subseteq N$, so $xN = yN$, and consequently $\langle K \rangle / N$ is generated by just one element, say xN, with $x \in K$, and $(xN)^2 = N$. Thus, a) is proved. Statement b) trivially follows because K^2 is a subgroup and all non-trivial elements of K^2 are conjugate, so all of them have the same order. $\square$

As we have already indicated, we also use the following result of Berkovich and Kazarin of [2], which is based on the well-known Kazarin's Theorem (see for instance [7]), which asserts that any conjugacy class with prime-power size generates a solvable normal subgroup of G.

Lemma 2.3 (see Lemma 3 of [2]) *Let $x \in G$. If $|x^G|$ is a power of $q \in \pi(G)$, then $(\langle x \rangle^G)'$ is a q-subgroup. In particular, $\langle x \rangle^G / \mathbf{O}_q(\langle x \rangle^G)$ is an abelian $\pi(o(x))$-group.*

Finally, the following result to which we referred at the beginning of the Introduction, will also be used in the proof of Theorem C.

Theorem 2.4 (see Theorem A of [6]) *Let G be a finite group, let $x \in G$, and let $K = x^G$ be the conjugacy class of x in G. Then the following are equivalent:*

a) *K^2 is a conjugacy class of G.*

b) *$K = x[x, G]$ and $\mathbf{C}_G(x) = \mathbf{C}_G(x^2)$.*

In this case, $[x, G]$ is solvable. Furthermore, if x has order a power of a prime p, then $[x, G]$ has a normal p-complement.

The original result of [6] includes one more assertion related to Character Theory but we do not use it in this paper. Furthermore, the proof of the equivalence between a) and b) in the above theorem, although is omitted, can be

easily obtained without using characters. The last assertion of Theorem 2.4 needs the Classification of Finite Simple Groups. We are not going to use it to prove Theorem A, but we do it for proving Corollary C.

We will also use the following lemma for our puposes which is a known result of Burnside whose proof can be found in Section 1.2. of [8].

Lemma 2.5 (see Theorem 1.2.6 of [8]) A non-cyclic 2-group P has only one involution if and only if P is a generalized quaternion group.

3   Proofs

Recall that the conjugacy classes K and D of the statement of Theorem A are real classes.

We start by proving the equalities concerning commutators that appear in Theorem A.

Lemma 3.1 Let $K = x^G$ be a conjugacy class of a finite group G and suppose that $K^2 = 1 \cup D$, where D is a conjugacy class of G. Then $\langle D \rangle = [x, G]$ and $\langle K \rangle = \langle x \rangle [x, G]$.

Proof. If $K = \{x_1, \ldots, x_n\}$ we trivially have $K^2 = x_1 K \cup \cdots \cup x_n K$. Let $y \in x_i K$ so, since K is real, $y = x_i g^{-1} x_i^{-1} g \in [x_i^{-1}, G] = [\langle x_i^{-1} \rangle, G] = [\langle x_i \rangle, G] = [x_i, G]$ for some $g \in G$. Furthermore, if $i \neq j$, then $x_j = x_i^h$ for some $h \in G$. Thus, $[x_j, G] = [x_i^h, G] = [x_i, G]^h = [x_i, G]$. Consequently, $K^2 \subseteq [x, G]$ and $\langle D \rangle \subseteq [x, G]$. On the other hand, if $[x, t]$ is a generator of $[x, G]$, then $[x, t] \in K^2$ so $[x, G] \subseteq \langle K^2 \rangle = \langle D \rangle$ and hence, $\langle D \rangle = [x, G]$. The equality $\langle K \rangle = \langle x \rangle [x, G]$ is standard, since the normal closure $\langle x \rangle^G$ of a subgroup $\langle x \rangle$ is equal to $\langle x \rangle [x, G]$. $\square$

Proof Theorem A. The proof is divided into two cases: when $|K| = 2$ and when $|K| \geq 3$.

Case 1: Suppose that $|K| = 2$.

Case 1.1. Let $K = \{x, x^g\}$ with $g \in G$. If $o(x) = 2$, then $K^2 = 1 \cup \{xx^g, x^g x\}$ but observe that since $\mathbf{C}_G(x) \trianglelefteq G$, we have $\mathbf{C}_G(x) = \mathbf{C}_G(x^g)$, so $xx^g = x^g x$. Thus, $K^2 = 1 \cup \{xx^g\}$, so $xx^g \in \mathbf{Z}(G)$ and $\langle D \rangle = \langle xx^g \rangle \subseteq \mathbf{Z}(G)$. Furthermore, $\langle K \rangle = \langle x, x^g \rangle = \langle x \rangle \times \langle x^g \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $|\langle K \rangle / \langle D \rangle| = 2$. So, 1.1 is proved.

Case 1.2. If $o(x) = n > 2$, then $K = \{x, x^{-1}\}$ and as a consequence, $\langle K \rangle = \langle x \rangle \trianglelefteq G$, which is cyclic of order n and $\langle D \rangle = \langle x^2 \rangle$. If n is odd, then $\langle D \rangle = \langle x \rangle = \langle D \rangle$. If n is even, then $|\langle K \rangle / \langle D \rangle| = 2$. Therefore, 1.2 is proved.

Case 2: Suppose that $|K| \geq 3$.

Case 2.1. Suppose that $o(x) = 2$ and let $t \in D$. We distinguish two cases depending on the order of t. Suppose that $o(t) = 2$. We set $K = \{x_1, \cdots, x_s\}$ and we have $K^2 = 1 \cup \{x_i x_j | i \neq j\}$. Since $o(x_i x_j) = 2$ for every $1 \leqslant i, j \leqslant s$ and $i \neq j$ we obtain that $1 = x_i^2 x_j^2 = x_i x_i x_j x_j = x_i x_j x_i x_j$ so x_i and x_j commute. Consequently, $\langle K \rangle = \langle x_1, \ldots, x_s \rangle$ is generated by two pairwise commuting elements of order 2, so $\langle K \rangle$ is 2-elementary abelian and we obtain the first assertion of 2.1.

Suppose now that $o(t) > 2$. Observe that any two distinct elements of K do not commute. Otherwise, the order of t would be necessarily 2. As a consequence, each $x_i \in K$ acts via conjugation on K in such a way that it fixes only the element x_i and permutes in pairs the elements of $K \setminus \{x_i\}$. As a result, $|K|$ is odd. This implies that $x \in \mathbf{Z}(P)$ for some $P \in \mathrm{Syl}_2(G)$. Therefore, $P \cap K = \{x\}$ and we have $\mathbf{O}_{2'}(G)\langle x \rangle \trianglelefteq G$ by Theorem 2.1.

By applying Frattini's argument it follows that $G = \mathbf{N}_G(\langle x \rangle)\mathbf{O}_{2'}(G)$. But observe that $\mathbf{N}_G(\langle x \rangle) = \mathbf{C}_G(x)$ because $o(x) = 2$. Thus, $G = \mathbf{C}_G(x)\mathbf{O}_{2'}(G)$. As a result,

$$K^2 = \{x^{-1}x^g | x \in K, g \in G\} = \{[x, g] | x \in K, g \in \mathbf{O}_{2'}(G)\} \subseteq \mathbf{O}_{2'}(G).$$

Then $D \subseteq \mathbf{O}_{2'}(G)$ and in particular, $|\langle D \rangle|$ is odd.

Now, we prove that $|K|$ is a power of an odd prime. Since $x \notin \mathbf{Z}(G)$, we can take an odd prime p dividing $|\mathbf{O}_{2'}(G) : \mathbf{C}_{\mathbf{O}_{2'}(G)}(x)|$. Since $\mathbf{O}_{2'}(G)$ has odd order, then the number of Sylow p-subgroups of $\mathbf{O}_{2'}(G)$ is also odd, and hence x, which acts on this set of subgroups, must fix one of them for the prime p. Let $P \in \mathrm{Syl}_p(\mathbf{O}_{2'}(G))$ such that $P^x = P$. Thus, we have $[x, P] \subseteq P$. Now, if $[x, P] = 1$ this contradicts that p divides the index $|\mathbf{O}_{2'}(G) : \mathbf{C}_{\mathbf{O}_{2'}(G)}(x)|$ so $[x, g]$ is a non-trivial p-element for some $g \in P$. Therefore, $[x, g] = xx^g \in K^2$ is a p-element in D, so all elements of D are p-elements. Consequently, the prime p is unique. Moreover,

$$p^m = |\mathbf{O}_{2'}(G) : \mathbf{C}_{\mathbf{O}_{2'}(G)}(x)| = |\mathbf{C}_G(x)\mathbf{O}_{2'}(G) : \mathbf{C}_G(x)| = |G : \mathbf{C}_G(x)| = |K|$$

for some $m \geq 1$. By applying Lemma 2.3 we get

$$\langle K \rangle' \subseteq \mathbf{O}_p(\langle K \rangle) \subseteq \mathbf{O}_{2'}(\langle K \rangle) = \langle D \rangle \subseteq \langle K \rangle$$

and that $\langle K \rangle / \mathbf{O}_p(\langle K \rangle)$ is an abelian 2-group. Therefore, $\langle D \rangle = \mathbf{O}_{2'}(\langle K \rangle) = \mathbf{O}_p(\langle K \rangle)$ is a p-group. As a consequence, by Lemma 2.2.(i), $\langle K \rangle / \langle D \rangle$ is cyclic of order 2 because it is non-trivial. Hence, the second assertion of case 2.1 follows.

Case 2.2. Suppose that $o(x) > 2$. We prove first that $|D| = |K|$. We know that $|K| \leqslant |K^2| = 1 + |D|$ and $D = (x^2)^G$. Observe that $|D|$ divides $|K|$ because $\mathbf{C}_G(x) \subseteq \mathbf{C}_G(x^2)$. Thus, either $|D| = |K|$ or $|D| \leqslant |K|/2$. But, if $|D| \leqslant |K|/2$,

the first inequality implies that $|K| \leq 1 + |K|/2$, so $|K| \leq 2$, a contradiction. Consequently, $|K| = |D|$ as wanted. Furthermore, notice that $xK \cup x^{-1}K \subseteq K^2$ and we claim that $xK \neq x^{-1}K$. Indeed, if we suppose that $xK = x^{-1}K$, then $x^2K = K$. Hence for all $g \in G$, it follows that $(x^g)^2K = (x^2K)^g = K^g = K$, which means that $DK = K$. As a result, $\langle D \rangle K = K$. This implies that $|\langle D \rangle|$ divides $|K|$, but this is a contradiction because $|D| = |K|$ and $|D| < |\langle D \rangle|$.

Hence, $xK \neq x^{-1}K$ with $xK \cup x^{-1}K \subseteq K^2$. Since $|K^2| = |K| + 1$ and $|K| = |xK| = |x^{-1}K|$, there exists only just one element $z \in xK \setminus x^{-1}K$. Moreover, it is easy to prove that z^{-1} is the only element contained in $x^{-1}K \setminus xK$. So, K^2 can be decomposed as follows:

$$K^2 = xK \cup x^{-1}K = (xK \cap x^{-1}K) \cup \{z\} \cup \{z^{-1}\}.$$

Since $(xK)(x^{-1}K) = K^2$ and $K^4 = (1 \cup D)(1 \cup D) = K^2 \cup D^2$, we deduce that

$$K^4 = K^2 \cup \{z^2\} \cup \{z^{-2}\} = 1 \cup D \cup \{z^2\} \cup \{z^{-2}\}.$$

Let us see that $K^4 = D^2$. We know that D^2 is a G-invariant set, so we can write $D^2 = 1 \cup A_1 \cup \cdots \cup A_r$ with A_i a conjugacy class for $1 \leq i \leq r$. On the other hand, since $xK \subseteq K^2 = 1 \cup D$ then $xK = 1 \cup D'$ with $D' \subseteq D$ and similarly $x^{-1}K = 1 \cup D''$ with $D'' \subseteq D$. Thus, $D'D'' \subseteq K^2 \cap D^2$ and $|D'D''| \geq |D'| = |K| - 1 \geq 2$. We conclude that there exists $1 \neq g \in K^2 \cap D^2$. As a result, $g \in D$. Also, we have that $g \in A_i$ for some $1 \leq i \leq r$. Consequently, $D = A_i$ and hence $D \subseteq D^2$. Accordingly, $K^4 = 1 \cup D \cup D^2 = D^2$, as wanted. Therefore,

$$D^2 = 1 \cup D \cup \{z^2\} \cup \{z^{-2}\}.$$

We distinguish two subcases depending on whether $z^2 \in K^2$, subcase $a)$, or $z^2 \notin K^2$, subcase $b)$.

a) If $z^2 \in K^2$, we have either $z^2 = 1$ or $z^2 \in D$ (and $z^{-2} \in D$). In both cases, it follows $D^2 = K^2 = 1 \cup D$ and then $\langle D \rangle$ is a p-elementary abelian group for some prime p by applying Lemma 2.2(b). Furthermore, $\langle D \rangle = \langle K^2 \rangle$, so $|\langle K \rangle / \langle D \rangle| \leq 2$ by Lemma 2.2(a). Observe that $(x^2)^G = D$, so $o(x)$ divides $2p$ and hence, either $o(x) = p$ or $o(x) = 2p$. It $o(x) = p > 2$, then $\langle x \rangle = \langle x^2 \rangle$ and $\langle K \rangle = \langle D \rangle$ is p-elementary abelian.

Let us see that if $o(x) = 2p$, then p is odd. If $p = 2$, then $o(x) = 4$ and we know that $2^a = |\langle D \rangle| = 1 + |D|$ for some $a > 1$. Thus, $|D| = 2^a - 1 = |K|$ is odd and, since $\langle K \rangle / \langle D \rangle$ is trivial or cyclic of order 2 by Lemma 2.2(a), we have that $\langle K \rangle$ is a 2-group, so $\langle K \rangle \subseteq \mathbf{C}_G(x)$ and, in particular, $xx^g = x^gx$ for every $g \in G$. Since $xx^g \in D^2$, either $xx^g \in D$ or $xx^g = 1$. If $xx^g \neq 1$, then $o(xx^g) = 2$ and $1 = (xx^g)^2 = x^2(x^g)^2$ and $(x^2)^g = x^2$. In the other case, if $xx^g = 1$, then $x^g = x^{-1} = x^3$ and $(x^2)^g = (x^g)^2 = x^3x^3 = x^2$. Thus, in both cases $x^2 \in \mathbf{Z}(G)$, which means that $1 = |D| = |K|$, a contradiction. We obtain, as a consequence, the assertion of 2.2, as wanted.

b) Suppose that $z^2 \notin K^2$, what is equivalent to claim that either $\{z^2\}$ and $\{z^{-2}\}$ are central classes or $\{z^2, z^{-2}\}$ is a single conjugacy class of cardinality 2. The rest of the proof consists in getting a contradiction by following a series of steps.

Step 1: $\langle D \rangle / \langle z^2 \rangle$ is a 2-elementary abelian group. Moreover, $\langle D \rangle$ is nilpotent of class at most 2. Therefore, we write $\langle D \rangle = P \times H$ with $P \in \mathrm{Syl}_2(\langle D \rangle)$ and H a 2-complement of $\langle D \rangle$ with $H \subseteq \langle z^2 \rangle \subseteq \mathbf{Z}(\langle D \rangle)$.

By the hypotheses of b), it follows that $\langle z^2 \rangle \trianglelefteq G$. We denote $\overline{G} = G/\langle z^2 \rangle$ and consider $\overline{D}$. We have $\overline{D}^2 = \overline{D^2} = \overline{1} \cup \overline{D}$. So, by Lemma 2.2(ii), $\langle \overline{D} \rangle$ is a p-elementary abelian group for some prime p. Observe that if $d \in D$, then $d = z^g$ for some $g \in G$ and $d^2 = (z^g)^2 = (z^2)^g \in \{z^2, z^{-2}\}$. Thus, $\overline{d}^2 = \overline{d^2} = 1$ and $p = 2$. Furthermore, $z \in \mathbf{C}_G(z^2) \trianglelefteq G$ and $D \subseteq \mathbf{C}_G(z^2)$. This means that $\langle z^2 \rangle \subseteq \mathbf{Z}(\langle D \rangle)$, and $\langle D \rangle / \mathbf{Z}(\langle D \rangle)$ is abelian, and $\langle D \rangle$ is nilpotent of class at most 2. Thus, the decomposition for $\langle D \rangle$ of the statement holds.

Step 2: We can assume that $o(z^2)$ is even.

If $z^2 \in \mathbf{Z}(G)$, since $z \in D$ and D is real, we have that z^2 and z^{-2} are also conjugate and hence $z^2 = z^{-2}$. Thus, $o(z^2) = 2$. Consequently, we can assume that $\{z^2, z^{-2}\}$ is a conjugacy class for the rest of this step. Suppose that $o(z^2) = k$ is odd and we will get a contradiction. We know that $o(z) = 2k$, so we can write $z = z^k z^2$ where z^k and z^2 are the $2'$-part and the 2-part of z, respectively. Moreover, there exists $g \in G$ such that $(z^2)^g = z^{-2}$. We know that $zz^g \in D^2 = 1 \cup D \cup \{z^2, z^{-2}\}$. Furthermore, $zz^g = z^k z^2 (z^k)^g z^{-2} = z^k (z^k)^g \in P$ by taking into account that $P \trianglelefteq G$, so zz^g is a 2-element. As a consequence, zz^g can only be equal to 1, z^2 or z^{-2} because the elements of D have odd order. Now, if $zz^g = 1$, then $z^{-1} = z^g = (z^k)^g (z^2)^g = (z^k)^g z^{-2}$ what means that $z = (z^k)^g$, a contradiction. If zz^g is equal to either z^2 or z^{-2} we can easily compute that $o(z) = 4$, again a contradiction. Thus, $o(z^2)$ is even, as wanted.

Step 3: $\langle D \rangle = \langle z^2 \rangle \cup D\langle z^2 \rangle$ and $\langle D \rangle$ has just one element of order 2 that is the involution of $\langle z^2 \rangle$.

Since $D \subseteq D^2$, it is easy to prove by induction on k that for every $k \geqslant 2$, $D^{k-1} \subseteq D^k \subseteq 1 \cup D \cup \langle z^2 \rangle \cup D\langle z^2 \rangle$. We can deduce that there exists $l \in \mathbb{N}$, depending on the order of z, such that $\langle D \rangle = D^l \subseteq 1 \cup D \cup \langle z^2 \rangle \cup D\langle z^2 \rangle \subseteq \langle D \rangle$. We conclude that

$$\langle D \rangle = 1 \cup D \cup \langle z^2 \rangle \cup D\langle z^2 \rangle = \langle z^2 \rangle \cup D\langle z^2 \rangle$$

Accordingly, it is enough to conside that there exists an element $dz^{2i} \in Dz^{2i}$ with $d \in D$ such that $o(dz^{2i}) = 2$. Thus, $(dz^{2i})^2 = d^2 z^{4i} = 1$ and notice that $d^2 = (z^g)^2 = (z^2)^g \in \{z^2, z^{-2}\}$ for some $g \in G$. Consequently, either $z^{4i+2} = z^{2(2i+1)} = 1$ or $z^{4i-2} = z^{2(2i-1)} = 1$. In both cases, $o(z^2)$ would be odd, which contradicts Step 2. As a result, the unique element of order 2 in $\langle D \rangle$ is the involution of $\langle z^2 \rangle$.

Step 4: Final contradiction.

By Step 3 and Lemma 2.5, we have that P is cyclic or generalized quaternion. We will get a contradiction in both cases. Assume first that P is cyclic. Since $\langle D \rangle / \langle z^2 \rangle \cong P/P \cap \langle z^2 \rangle$ is 2-elementary abelian by Step 1 and P is cyclic, either $\langle \overline{D} \rangle \cong \mathbb{Z}_2$ or $\langle \overline{D} \rangle$ is trivial. Furthermore, $\langle z \rangle \neq \langle z^2 \rangle$. Otherwise, $\mathbf{C}_G(z) = \mathbf{C}_G(z^2)$ and $|z^G| = |D| = |K|$ is either 1 or 2, which contradicts the fact that $|K| \geq 3$. Thus, $\langle z^2 \rangle < \langle z \rangle \leq \langle D \rangle$ and $\langle D \rangle = \langle z \rangle$. As the elements of D have ever order, this equality implies that they are odd powers of z and, as a consequence, the elements of D^2 are even powers of z. This contradicts that $D \subseteq D^2$, as wanted.

Consequently, we can assume that P is generalized quaternion. We denote $\widetilde{G} = G/H$ and we have $\langle \widetilde{D} \rangle = \widetilde{\langle D \rangle} \cong P$. Notice that $\mathbf{Z}(P) = \mathbf{Z}(\langle \widetilde{D} \rangle) = \mathbf{Z}(\langle D \rangle / H) = \mathbf{Z}(\langle D \rangle)/H$, because $\langle D \rangle = P \times H$, and $\langle \widetilde{D} \rangle / \mathbf{Z}(\langle \widetilde{D} \rangle)$ is dihedral. Also, $\langle \widetilde{D} \rangle / \mathbf{Z}(\langle \widetilde{D} \rangle) \cong \langle D \rangle / \mathbf{Z}(\langle D \rangle)$ is 2-elementary abelian by Step 1. By joining both facts, we conclude that $\langle \widetilde{D} \rangle / \langle \mathbf{Z}(\widetilde{D}) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore, $\langle \widetilde{D} \rangle \cong Q_8$ and $\langle D \rangle \cong Q_8 \times H$. Notice that, $\langle \widetilde{z}^2 \rangle \subseteq \mathbf{Z}(\langle \widetilde{D} \rangle)$ which has order 2 because it is the center of a generalized quaterion group. This forces that the order of $\langle \widetilde{z}^2 \rangle$ is either 1 or 2. If $\langle \widetilde{z}^2 \rangle$ is trivial, from Step 3, we have

$$\langle \widetilde{D} \rangle = \langle \widetilde{z}^2 \rangle \cup \widetilde{D} \langle \widetilde{z}^2 \rangle = \widetilde{1} \cup \widetilde{D}$$

and by Lemma 2.2, $\langle \widetilde{D} \rangle$ is elementary abelian, a contradiction. Thus, we assume that $o(\widetilde{z}^2) = 2$ and from Step 3, we have

$$\langle \widetilde{D} \rangle = \langle \widetilde{z}^2 \rangle \cup \widetilde{D} \langle \widetilde{z}^2 \rangle = \widetilde{1} \cup \widetilde{D} \cup \widetilde{D} \widetilde{z}^2 \cup \{\widetilde{z}^2\}$$

We distinguish two cases. If $\widetilde{D} \neq \widetilde{D} \widetilde{z}^2$, then $2^3 = 2 + 2|\widetilde{D}| = 2(1 + |\widetilde{D}|)$, what means that $|\widetilde{D}|$ is odd and, since $\widetilde{D}$ is real, this forces that $o(\widetilde{z}) = 2$, a contradiciton. Therefore, $\widetilde{D} = \widetilde{D} \widetilde{z}^2$ and $8 = |\langle \widetilde{D} \rangle| = 2 + |\widetilde{D}|$, so $|\widetilde{D}| = 6$. Now, we prove that $|\widetilde{K}| = |\widetilde{D}|$. Moreover, we have that $\widetilde{K}^2 = \widetilde{1} \cup \widetilde{D}$. Since $o(\widetilde{z}^2) = 2$ and $\widetilde{x}^2$ and $\widetilde{z}$ are $\widetilde{G}$-conjugate, we know that $o(\widetilde{x}) > 2$. So, $\widetilde{D} = (\widetilde{x}^2)^{\widetilde{G}}$ and, since $\mathbf{C}_{\widetilde{G}}(\widetilde{x}) \subseteq \mathbf{C}_{\widetilde{G}}(\widetilde{x}^2) \subseteq \widetilde{G}$, we conclude that $|\widetilde{D}|$ divides $|\widetilde{K}|$. Since $6 = |\widetilde{D}| \leq |\widetilde{K}| \leq |\widetilde{K}^2| = 1 + |\widetilde{D}|$, we get $|\widetilde{D}| = |\widetilde{K}|$.

9

On the other hand, taking into account that $\widetilde{K}$ is a real class, by Lemma 2.2(i) we know that $\langle \widetilde{K} \rangle / \langle \widetilde{K}^2 \rangle = \langle \widetilde{K} \rangle / \langle \widetilde{D} \rangle$ is trivial or cyclic of order 2. In the former case, that is, if $\langle \widetilde{K} \rangle = \langle \widetilde{D} \rangle = \widetilde{1} \cup \{\widetilde{z}^2\} \cup \widetilde{D}$, let us see that this leads to a contradiction. We know that $\widetilde{1} \neq \widetilde{x} \in \langle \widetilde{K} \rangle$. If $\widetilde{x} = \widetilde{z}^2$, then $o(\widetilde{x}) = 2$ so $x^2 \in H$ which implies that $z \in H$ and $o(z^2)$ is odd, a contradiction. So $\widetilde{x} \in \widetilde{D}$ and we can write $x = dh$ with $d \in D$ and $h \in H \subseteq \langle z^2 \rangle \subseteq \mathbf{Z}(\langle D \rangle)$. Then $x^2 = d^2 h^2 \in \langle z^2 \rangle$ and we conclude that $z = (x^2)^g \in \langle z^2 \rangle$ and $\langle z \rangle = \langle z^2 \rangle$ so $\mathbf{C}_G(z) = \mathbf{C}_G(z^2) \subseteq G$ and $|D| = |z^G| = |(z^2)^G| = 2$, which contradicts that $|K| \geqslant 3$. We can assume that $\langle \widetilde{K} \rangle / \langle \widetilde{D} \rangle \cong \mathbb{Z}_2$. Therefore, $\langle \widetilde{K} \rangle$ is a 2-group of order 16, which has a normal subgroup isomorphic to Q_8, and moreover, $\langle \widetilde{K} \rangle$ possesses at least 6 elements of order 8 (the elements of K). However, the only groups of order 16 having a normal subgroup isomorphic to Q_8 are: SD_{16} the semidihedral group; Q_{16}, the generalized quaternion group; the central product of D_8 and $\mathbb{Z}_4$; and the direct product $Q_8 \times \mathbb{Z}_2$. The latter two groups have no elements of order 8 and the former two groups have exactly 4 elements of order 8. In all cases, we get a contradiction. $\square$

Examples. Let us show several examples illustrating every case of Theorem A. In some cases, we use the SmallGroups library of GAP [4]. The m-th group of order n in the SmallGroups library is identified by $n\#m$.

Case 1.1. We take the dihedral group

$$D_8 = \langle a, \ b \mid a^4 = b^2 = 1, \ b^{-1}ab = a^{-1} \rangle$$

and we consider the conjugacy class $K = \{b, a^2 b\}$ so we have that $K^2 = 1 \cup D$ where D is the conjugacy class of the element $\{a^2\}$.

Case 1.2. We consider the dihedral group of order $2n$ for every $n \geq 3$

$$D_{2n} = \langle x, \ y \mid x^n = y^2 = 1, \ y^{-1}xy = x^{-1} \rangle$$

and we consider $K = x^G$. Then $K^2 = 1 \cup D$ where $D = (x^2)^G$. Remark that if n is odd we have $\langle D \rangle = \langle K \rangle$ whereas if it is not it follows $|\langle K \rangle / \langle D \rangle| = 2$.

Case 2.1. Let $N = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ and consider the natural action of S_r on N, that is, $G = NS_r$ is the wreath product of N and S_r. In this case, $K = \{x_1, \cdots, x_r\}$ is a conjugacy class of G such that $K^2 = 1 \cup D$ where $D = \{x_i x_j | i \neq j\}$ is a conjugacy class, because S_r acts transitively on D, and $o(x_i x_j) = 2$ for every $i \neq j$ and $|K| = r$. This is an example of case 2.1 of Theorem A in which $\langle D \rangle$ is 2-elementary abelian and $|\langle K \rangle / \langle D \rangle| = 2$.

The alternating group A_4 with the conjugacy class K of elements of order 2 is another example of this case but with $\langle K \rangle = \langle D \rangle$.

Let $G = 216\#8(\cong ((\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3) \rtimes Q_8)$ which is generated by two elements x, y of order 4 and an element z of order 3. The conjugacy class $K = (x^2)^G$ satisfies that $K^2 = 1 \cup D$ where $D = z^G$. Moreover, $o(x^2) = 2$, $o(z) = 3$, $|K| = 9$ and $|D| = 24$. This is an example of case 2.1 in which $\langle D \rangle$ is a non-abelian 3-group of order 27.

Case 2.2. Let $\langle a \rangle \cong \mathbb{Z}_5$ and let $\langle b \rangle \cong \mathbb{Z}_8$ acting on $\langle a \rangle$ in the following way: $a^b = a^2$. Let G be the associated semidirect product $G = \langle a \rangle \rtimes \langle b \rangle$ and take $K = (b^4 a)^G$. We have $K^2 = 1 \cup D$ where $D = a^G$, $o(b^4 a) = 10$, $o(a) = 5$, $|K| = 4$ and $|D| = 4$. This shows case 2.2 of Theorem A with $\langle D \rangle \cong \mathbb{Z}_5$ and $\langle K \rangle \cong \mathbb{Z}_{10}$.

We get another example if we take $G = 72\#41(\cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes Q_8)$. In this case, $K = s^G$, with s being an element of order 3, satisfies that $K^2 = 1 \cup K$ with $|K| = 8$. Furthermore, $\langle K \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Observe that in both examples of this case we have $|K| = |D|$ as it us showed in the proof of Theorem A.

Proof of Corollary B. For every element $x \in G$, we know that $(x^G)^2 = 1 \cup D$ for some conjugacy class D. Then $x^2 \in \langle D \rangle$ and $\langle D \rangle$ is nilpotent by Theorem A. Thus, $x^2 \in \mathbf{F}(G)$ for every $x \in G$. Consequently, $G/\mathbf{F}(G)$ is 2-elementary abelian group. $\square$

Proof of Corollary C. Under the hypothesis it can occur that K^2 is a conjugacy class and by applying Theorem 2.4. we have that $\langle K \rangle$ is solvable. Otherwise, it happens that either $K^2 = A_1 \cup A_2 \cup \cdots A_n$ or $K^2 = A_1 \cup A_2 \cup \cdots A_n \cup D$ with A_i a central classs for every i and D a non-central class. We consider $\overline{G} = G/\mathbf{Z}(G)$ and it follows that either $\overline{K}^2 = \overline{1}$ or $\overline{K}^2 = \overline{1} \cup \overline{D}$. In the former case, $\langle \overline{K} \rangle$ is cyclic of order 2 and as a consequence, $\langle K \rangle$ is solvable. In the second case, by applying Theorem A, $\langle \overline{K} \rangle = \langle K \rangle \mathbf{Z}(G)/\mathbf{Z}(G)$ is solvable and consequently $\langle K \rangle$ is solvable too.$\square$

Proof of Corollary D. Taking into account that if $N \trianglelefteq G$ and $\overline{x} \in \overline{G} = G/N$ π'-element, we can consider that x is π'-element we can easily prove that the hypotheses are inherited by factor groups and we work by induction on the order of G. If $\mathbf{O}_{\pi'}(G) \neq 1$ it easily follows by induction that $\overline{G} = G/\mathbf{O}_{\pi'}(G)$ is nilpotent. So we can assume that $\mathbf{O}_{\pi'}(G) = 1$ and let us see that G is nilpotent. Let $p \in \pi$ and $P \in \mathrm{Syl}_p(G)$. Then there exists $1 \neq x_p \in \mathbf{Z}(P)$, what means that $P \subseteq \mathbf{C}_G(x_p)$. The hypotheses imply that $(x_p^G)^2$ is a conjugacy class and by Theorem 2.4 we have that $|x_p^G| = |[x_p, G]|$ is p'-number.

Let $K_{p'}/[x_p, G] = \mathbf{O}_{\pi'}(G/[x_p, G]))$ which is a p'-group. Since $[x_p, G]$ is p'-group, then $K_{p'}$ is a p'-group too. Furthermore, $K_{p'} \trianglelefteq G$ thus, $K_{p'} \subseteq \mathbf{O}_{p'}(G)$.

By induction, we have that

$$G/[x_p, G]/\mathbf{O}_{\pi'}(G/[x_p, G]) \cong G/K_{p'}$$

is nilpotent. Now, we consider the natural monomorphism

$$\phi : G \longrightarrow G/K_{p'_1} \times \cdots \times G/K_{p'_s}$$

where $\pi = \{p_1, \cdots, p_s\}$. Since $\bigcap_{i=1}^s K_{p'_i} \subseteq \bigcap_{i=1}^s \mathbf{O}_{p'_i}(G) = \mathbf{O}_{\pi'}(G) = 1$, we deduce that G is nilpotent. $\square$

Proof of Corollary E. The hypotheses are inherited by taking factor groups. Let us see that we can assume $\mathbf{Z}(G) = 1$. Indeed, if we consider $\overline{G} = G/\mathbf{Z}(G)$ we have

$$\mathbf{O}_2(\overline{G}/\mathbf{F}(\overline{G})) = \mathbf{O}_2(\overline{G}/\overline{\mathbf{F}(G)}) \cong$$
$$\mathbf{O}_2(G/\mathbf{F}(G)) = M/\mathbf{F}(G) \cong \overline{M}/\overline{\mathbf{F}(G)}.$$

If $\mathbf{Z}(G) > 1$, arguing by induction on the order of G, we have that

$$\overline{G}/\overline{M} \cong G/M$$

is nilpotent and then the theorem is proved. Thus, we can assume $\mathbf{Z}(G) = 1$, as wanted.

Let $\widehat{G} = G/\mathbf{F}(G)$ and suppose that for every non-trivial $2'$-element $\widehat{x}$ of $\widehat{G}$ we have that $(\widehat{x}^{\widehat{G}})^2$ is a conjugacy class of $\widehat{G}$. We can certainly assume that x is a $2'$-element of G such that $x \notin \mathbf{F}(G)$ and that $(x^G)^2$ is a conjugacy class. We apply Theorem D with $\pi = \{2\}'$ to obtain that $\widehat{G}/\mathbf{O}_2(\widehat{G})$ is nilpotent, which implies that G/M is nilpotent, and the proof is finished.

Therefore, we can assume that there exists a $2'$-element x in G with $x \notin \mathbf{F}(G)$ such that $(x^G)^2$ is not a class. However, $(x^G)^2$ is union of conjugacy classes, all of them central except at most one. As $\mathbf{Z}(G) = 1$, we have $(x^G)^2 = 1 \cup D$, where D is a non-central class of G. By Theorem A we have $x^2 \in \langle D \rangle \subseteq \mathbf{F}(G)$ and, since $\langle x \rangle = \langle x^2 \rangle$, we get a contradiction. $\square$

Acknowledgements

References

[1] Z. Arad and E. Fisman, An analogy between products of two conjugacy classes and products of two irreducible characters. Proc. Edinb. Math. Soc., (30) (1987), 7-22.

[2] Y. Berkovich and L. Kazarin, Indices of elements and normal structure of finite groups. J. Algebra, (283) (2005), 564-583.

[3] Z. Chillag and A. Mann, Nearly odd-order and nearly real finite group. Comm. in Algebra, 26(7) (1998), 2041-2064.

[4] The GAP Group, GAP - Groups, Algorithms and Programming, Vers. 4.7.7; 2015. (http://www.gap-system.org)

[5] G. Glauberman, Central elements in core-free groups. J. Algebra, (4) (1966), 403-420.

[6] R. Guralnick and G. Navarro, Squaring a conjugacy class and cosets of normal subgroups. Proc. Am. Math. Soc., **144**(5) (2016), 1939-1945.

[7] B. Huppert Character Theory of Finite Groups. Walter de Gruyter. Berlín. New York, (1998).

[8] G. O. Michler, Theory of finite simple groups. New Mathematical Monographs, 8. Cambridge University Press, Cambridge, (2006).