Multiplying a conjugacy class by its inverse in a finite group

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

Suppose that G is a finite group and K is a non-trivial conjugacy class of G such that $KK^{-1} = 1 \cup D \cup D^{-1}$ with D a conjugacy class of G. We prove that G is not a non-abelian simple group and we give arithmetical conditions on the class sizes determining the solvability and the structure of $\langle K \rangle$ and $\langle D \rangle$.

Keywords. Finite groups, conjugacy classes, product of conjugacy classes, irreducible characters.
Mathematics Subject Classification (2010): 20E45, 20D15, 20C20.

1 Introduction

There are many studies about the structure of a finite group focused on the product of its conjugacy classes. Perhaps, the most relevant problem was posed by Z. Arad and M. Herzog ([4]) who conjectured that if S is a non-abelian simple group and A and B are non-trivial conjugacy classes of S, then AB (defined as the set $\{ab \,|\, a \in A, b \in B\}$) cannot be a single conjugacy class of S. This

conjecture still remains open although some specific cases have been solved. For instance, in [15], the conjecture is verified for several families of finite simple groups of Lie type. On the other hand, Arad and E. Fisman proved in [3] that if C and D are non-trivial conjugacy classes of a finite group G such that either $CD = C \cup D$ or $CD = C^{-1} \cup D$, then G is not a simple group. However, no solvability information of the subgroups $\langle C \rangle$ or $\langle D \rangle$ was given. Recently, G. Navarro and R.M. Guralnick ([9]) have proved that when a conjugacy class K of a finite group G satisfies that K^2 is a conjugacy class, then $\langle K \rangle$ is a solvable (normal) subgroup of G by appealing to the Classification of the Finite Simple Groups (CFSG). This is, of course, consistent with Arad and Hergoz's conjecture.

In general, for any G-invariant subset X of G, we denote by $\eta(X)$ the number of distinct conjugacy classes appearing in X. Let K be a conjugacy class of a finite group G. When we multiply K by its inverse class, K^{-1}, then KK^{-1} is a G-invariant set. We will prove that if $\eta(KK^{-1}) = 2$, then G is not simple. The fact that $\eta(KK^{-1}) = 3$ does not imply that $\langle K \rangle$ or $\langle KK^{-1} \rangle$ is solvable. In fact, $\langle KK^{-1} \rangle$ may be even simple. For instance, if $G = S_n$ for any $n \geq 5$ and K is the conjugacy class of transpositions, then $\eta(KK^{-1}) = 3$ and $\langle KK^{-1} \rangle = A_n$. In this paper we study the particular case in which $KK^{-1} = 1 \cup D \cup D^{-1}$ with D a conjugacy class of G, and we demonstrate that G cannot be simple by means of the CFSG and a character theoretical property characterizing such condition for conjugacy classes.

Theorem A. *Let K be a non-trivial conjugacy class of a finite group G and suppose that $KK^{-1} = 1 \cup D \cup D^{-1}$, where D is a conjugacy class of G. Then G is not a non-abelian simple group. In particular, this theorem holds if $KK^{-1} = 1 \cup D$.*

We remark that $KK^{-1} = 1 \cup D$ forces that D is real, but it does not necessarily imply that K is a real class too (see section 5). Moreover, under the assumption of Theorem A, if K is real, then we see (Lemma 3.1) that D is real too, and thus, $K^2 = 1 \cup D$. In this case, the structure and solvability of $\langle K \rangle$ is obtained in [5], without employing the CFSG.

In order to prove Theorem A, we use the following characterization in terms of characters of the property appearing in such theorem. We denote by $\mathrm{Irr}(G)$ the set of all irreducible complex characters of G.

Theorem B. *Let G be a group and $x, d \in G$. Let $K = x^G$ and $D = d^G$. The following are equivalent:*

a) $KK^{-1} = 1 \cup D \cup D^{-1}$

b) For every $\chi \in \mathrm{Irr}(G)$

$$|K||\chi(x)|^2 = \chi(1)^2 + \frac{(|K|-1)}{2}\chi(1)(\chi(d) + \chi(d^{-1})).$$

In particular, if $D = D^{-1}$, then $KK^{-1} = 1 \cup D$ if and only if for every $\chi \in \mathrm{Irr}(G)$

$$|K||\chi(x)|^2 = \chi(1)^2 + (|K| - 1)\chi(1)\chi(d).$$

Under the hypotheses of the particular case of Theorem A the group G need not be solvable. The typical non-solvable situation in this case is a group of type $Z.S.2$, where $|Z| = 3$, Z is in the center of $Z.S$, and in addition, S is a non-solvable group acted by an automorphism of order 2, such that the non-trivial elements of Z are conjugate by this automorphism.

If K is the conjugacy class in Theorem A such that $KK^{-1} = 1 \cup D \cup D^{-1}$, then we conjecture that the subgroup $\langle K \rangle$ is solvable. Unfortunately, we have only been able to prove this solvability in some specific cases.

Theorem C. *Let K be a conjugacy class of a finite group G and suppose that $KK^{-1} = 1 \cup D$, where D is a conjugacy class of G. Then $|D|$ divides $|K|(|K| - 1)$ and $\langle K \rangle / \langle D \rangle$ is cyclic. In addition,*

1. *If $|D| = |K| - 1$, then $\langle K \rangle$ is metabelian. More precisely, $\langle D \rangle$ is p-elementary abelian for some prime p.*
2. *If $|D| = |K|$, then $\langle K \rangle$ is solvable with derived length at most 3.*
3. *If $|D| = |K|(|K| - 1)$, then $\langle K \rangle$ is abelian.*

We will provide examples showing that each case is feasible as well as an example in which $|D|$ is a divisor of $|K|(|K| - 1)$ distinct from those appearing in Theorem C and satisfying $dl(\langle K \rangle) = 3$. Although in these examples $\langle K \rangle$ is solvable, the general proof remains open as we have said before.

In [13], G. Malle classified the groups G with $G/\mathbf{Z}(G)$ almost-simple satisfying that there exist $\chi, \psi \in \mathrm{Irr}(G)$ such that $\chi\overline{\chi} = 1 + \psi$. A possible problem could be to classify the groups of this type satisfying the conjugacy class condition, but we are not attempting that.

2 Preliminary results and proof of Theorem B

We begin this section by presenting several results appeared in the literature that we need in order to prove Theorem A. The next theorem will be useful in the interest of discarding the alternating groups A_n with $n > 5$ in Theorem A.

Theorem 2.1 (Theorem A of [2]) *Let S_n be the symmetric group of n-letters, $n > 5$, and $\alpha, \beta \in S_n \setminus 1$. Then $\eta(\alpha^{S_n}\beta^{S_n}) \geq 2$, and if $\eta(\alpha^{S_n}\beta^{S_n}) = 2$ then either α or β is a fixed point free permutation. Assume that α is fixed point free. Then one of the following holds*

1. *n is even, α is the product of $n/2$ disjoint transpositions and β is either a transposition or a 3-cycle.*

2. *n is a multiple of 3, α is the product of $n/3$ disjoint 3-cycles and β is a transposition.*

The following result due to R.M. Guralnick and G.R. Robinson is an extension for odd primes of Glauberman's Z*-Theorem [8].

Theorem 2.2 (Theorem D of [10]) *Let G be a finite group. If $x \in G$ has order p and $[x, g]$ is a p'-element for every $g \in G$, then x is central modulo $\mathbf{O}_{p'}(G)$.*

We give a variation of such theorem for p-elements (not necessarily of order p) by adding an hypothesis to the class size of the p-element. We use the following property (based on the CFSG) so as to obtain our variation, which is also a key result to prove Theorem 2.2.

Theorem 2.3 (Theorem 4.1 of [10]) *Let G be a finite group. If $x \in G$ has order p and is not central modulo $\mathbf{O}_{p'}(G)$, then x commutes with some conjugate $x^g \neq x$, for some $g \in G$.*

Our extension of Theorem 2.2 is the following.

Theorem 2.4. *Let G be a finite group. Let $x \in G$ be a p-element such that $|x^G|$ is a p'-number and that $[x, g]$ is a p'-element for every $g \in G$. Then x is central modulo $\mathbf{O}_{p'}(G)$.*

Proof. Let $o(x) = p^r$. By Theorem 2.2, we can assume that $r > 1$. We write $y = x^{p^{r-1}}$, so $o(y) = p$. We will argue by induction on $|G|$.

We claim that there is no $g \in G$ such that $y \neq y^g \in \mathbf{C}_G(x)$. Suppose that there exists $g \in G$ such that y^g centralizes x and $y \neq y^g$. Since $|x^G|$ is a p'-number, we can choose $P \in \mathrm{Syl}_p(G)$ such that $P \subseteq \mathbf{C}_G(x) \subseteq \mathbf{C}_G(y)$, so there exists $n \in \mathbf{C}_G(y)$ such that $y^{gn} \in P \subseteq \mathbf{C}_G(x)$. In addition, $y^{-1} \in \mathbf{C}_G(x)$, so $[y, gn] \in \mathbf{C}_G(x)$, that is, $[gn, y, x] = 1$. Moreover, $[y, x, gn] = 1$, so by the Three Subgroups Lemma, we get $[x, gn, y] = 1$. Then $x^{-1}x^{gn} = [x, gn] \in \mathbf{C}_G(y)$. As a result, $x^{gn} \in \mathbf{C}_G(y)$. Analogously, there is $n' \in \mathbf{C}_G(y)$ such that $x^{gnn'} \in \mathbf{C}_G(x)$ and hence, $x^{-1}x^{gnn'}$ is a p-element. By applying the hypothesis, $x = x^{gnn'}$, which implies that $gnn' \in \mathbf{C}_G(x) \subseteq \mathbf{C}_G(y)$. In particular, $g \in \mathbf{C}_G(y)$, a contradiction. As a consequence, there is no $g \in G$ such that $y \neq y^g \in \mathbf{C}_G(x)$ as claimed. As $|x^G|$ is a p'-number, it follows that there is no $g \in G$ such that $y \neq y^g \in \mathbf{C}_G(y)$. So $y\mathbf{O}_{p'}(G) \in \mathbf{Z}(G/\mathbf{O}_{p'}(G))$ by Lemma 2.3.

We distinguish two cases depending on whether $\mathbf{O}_{p'}(G) \neq 1$ or $\mathbf{O}_{p'}(G) = 1$. Assume first that $\mathbf{O}_{p'}(G) = 1$, and hence $y \in \mathbf{Z}(G)_p \neq 1$. Let $\overline{G} = G/\mathbf{Z}(G)_p$.

We have that $1 \neq \overline{x}$ is a p-element, $|\overline{x}^{\overline{G}}|$ is a p'-number and $[\overline{x}, \overline{g}] = \overline{[x,g]}$ is p'-element for every $\overline{g} \in \overline{G}$. By the inductive hypothesis, $\overline{x}\mathbf{O}_{p'}(\overline{G}) \in \mathbf{Z}(\overline{G}/\mathbf{O}_{p'}(\overline{G}))$. But observe that $\mathbf{O}_{p'}(\overline{G}) = 1$, so $\overline{x} \in \mathbf{Z}(\overline{G})$. This means that $[x,g] \in \mathbf{Z}(G)_p$ for every $g \in G$. By hypothesis, $[x,g]$ is also a p'-element, so $[x,g] = 1$ for every $g \in G$. This shows that $x \in \mathbf{Z}(G)$ and the theorem is proved.

Suppose now that $\mathbf{O}_{p'}(G) \neq 1$ and let $\overline{G} = G/\mathbf{O}_{p'}(G)$. Again $1 \neq \overline{x}$ is a p-element, $|\overline{x}^{\overline{G}}|$ is a p'-number and $[\overline{x}, \overline{g}] = \overline{[x,g]}$ is a p'-element for every $g \in G$. Notice that $\mathbf{O}_{p'}(\overline{G}) = 1$. By induction, $\overline{x} \in \mathbf{Z}(\overline{G})$, or equivalently $[x,g] \in \mathbf{O}_{p'}(G)$ for every $g \in G$, so the proof is finished. □

We state two very well-known Burnside's results.

Lemma 2.5 (Theorem 1.2.6 of [14]) *A non-cyclic 2-group P has only one involution if and only if P is a generalized quaternion group.*

Lemma 2.6 (Lemma 15.1 of [11]) *Let $\chi \in \mathrm{Irr}(G)$ and K a conjugacy class of an element $g \in G$. Suppose that $(|K|, \chi(1)) = 1$. Then either $g \in \mathbf{Z}(\chi)$, that is $|\chi(g)| = \chi(1)$, or $\chi(g) = 0$.*

For our purposes we need some properties related to the product of class sums in the complex group algebra $\mathbb{C}[G]$ of a finite group G. Let $K_1, \ldots, K_n$ be the conjugacy classes of G and let denote by $\widehat{K_i}$ the class sum of the elements of K_i in $\mathbb{C}[G]$. If S is a G-invariant subset of G, then

$$\widehat{S} = \sum_{g \in S} g = \sum_{i=1}^{n} n_i \widehat{K_i}$$

denotes the sum of all elements in S and we denote by $n_i = (\widehat{S}, \widehat{K_i}) = (\widehat{K_i}, \widehat{S})$ the multiplicity of $\widehat{K_i}$ in $\widehat{S}$, which is of course a non-negative integer. For more details, we refer the reader to Chapter 3 of [11].

Proof of Theorem B. Suppose that $KK^{-1} = 1 \cup D \cup D^{-1}$. Observe that if D_1, D_2 and D_3 are conjugacy classes of a finite group G, then it is easy to prove that $(\widehat{D_1}\widehat{D_2}, \widehat{D_3}) = (\widehat{D_1^{-1}}\widehat{D_2^{-1}}, \widehat{D_3^{-1}})$ (see for instance the proof of Theorem A of [3]), so

$$(\widehat{K}\widehat{K^{-1}}, \widehat{D}) = (\widehat{K^{-1}}\widehat{K}, \widehat{D^{-1}}) = (\widehat{K}\widehat{K^{-1}}, \widehat{D^{-1}}).$$

Thus, $\widehat{K}\widehat{K^{-1}} = |K|\widehat{1} + m\widehat{D} + m\widehat{D^{-1}}$ where m is a positive integer. Therefore,

$$|K|^2 = |K| + 2m|D|. \tag{1}$$

By applying Theorem 3.9 of [11],

$$\frac{|K|^2|\chi(x)|^2}{\chi(1)^2} = |K| + \frac{m|D|\chi(d)}{\chi(1)} + \frac{m|D|\chi(d^{-1})}{\chi(1)}$$

for each $\chi \in \mathrm{Irr}(G)$. Taking into account Eq.(1) and rearranging the equality we get the stated formula in b).

Conversely, suppose that b) is true. Let C_i be the conjugacy classes of G with $1 \leq i \leq n$. By exercise 3.9 of [12], for any pair of conjugacy class sums $\widehat{C}_m$ and $\widehat{C}_n$ with representatives c_m and c_n we have

$$\widehat{C}_m\widehat{C}_n = \sum_k \alpha_k \widehat{C}_k$$

where

$$\alpha_k = \frac{|C_m||C_n|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(c_m)\chi(c_n)\overline{\chi(c_k)}}{\chi(1)}$$

and c_k is a representative of C_k. In particular,

$$\widehat{K}\widehat{K^{-1}} = \sum_k \alpha_k \widehat{C}_k \quad \text{with} \quad \alpha_k = \frac{|K|^2}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(x)|^2\chi(c_k^{-1})}{\chi(1)}. \tag{2}$$

If we pour out $|\chi(x)|^2$ from b) we obtain

$$|\chi(x)|^2 = \frac{(|K|-1)\chi(1)(\chi(d)+\chi(d^{-1})) + 2\chi(1)^2}{2|K|}, \tag{3}$$

and by replacing Eq.(3) in Eq.(2) and making easy calculations, it follows that

$$\alpha_k = \frac{|K|^2}{|G|}\Big(\sum_{\chi \in \mathrm{Irr}(G)} \frac{(|K|-1)(\chi(d)+\chi(d^{-1}))\chi(c_k^{-1})}{2|K|} + \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(1)\chi(c_k^{-1})}{|K|}\Big).$$

Consequently, by using the second orthogonality relation, if $D \neq D^{-1}$, we deduce

$$\alpha_k = \begin{cases} |K| & \text{if } C_k = 1 \\ \frac{|K|(|K|-1)}{2|D|} & \text{if } C_k = D \text{ or } D^{-1} \\ 0 & \text{in other case} \end{cases}$$

This means that

$$\widehat{K}\widehat{K^{-1}} = |K|\widehat{1} + \frac{|K|(|K|-1)}{2|D|}\widehat{D} + \frac{|K|(|K|-1)}{2|D|}\widehat{D^{-1}}$$

and in particular, $KK^{-1} = 1 \cup D \cup D^{-1}$, so a) is proved.□

The following elementary property concerning commutators is basic for proving Theorem C.

Lemma 2.8. *Let G be a finite group and let $K = x^G$, $D = d^G$ where x and d are elements of G and $KK^{-1} = 1 \cup D$. Then, $\langle D \rangle = [x, G]$ and $\langle K \rangle = \langle x \rangle [x, G]$.*

Proof. If $K = \{x_1, \ldots, x_n\}$, then $K^{-1}K = x_1^{-1}K \cup \cdots \cup x_n^{-1}K$. If $y \in x_i^{-1}K$, then $y = x_i^{-1}x_i^g \in [x_i, G]$ for some $g \in G$. 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, $KK^{-1} \subseteq [x, G]$ and $\langle D \rangle \subseteq [x, G]$. On the other hand, since any element $[x, t]$ lies in KK^{-1} for all $t \in G$, then $[x, G] \subseteq \langle KK^{-1} \rangle = \langle D \rangle$ and hence, $\langle D \rangle = [x, G]$. The equality $\langle K \rangle = \langle x \rangle [x, G]$ is standard, so the lemma is proved.

3 Proof of Theorem A

Before proving Theorem A, we analyze a particular case under the assumption $KK^{-1} = 1 \cup D \cup D^{-1}$ appearing in Theorem A. If, in addition, we assume that $K = K^{-1}$, we prove in Lemma 3.1 that $D = D^{-1}$, that is, $K^2 = 1 \cup D$, and there is no need to use the CFSG to show the non-simplicity of G. In fact, $\langle K \rangle$ is solvable and its structure is completely determined by the authors in Theorem A of [5].

Lemma 3.1. *Let K and D be conjugacy classes of a finite group G such that $KK^{-1} = 1 \cup D \cup D^{-1}$. If K is real, then D is real.*

Proof. Assume that $K = K^{-1}$ and let $x \in K$. If $o(x) = 2$ we can assume that any two different elements of K do not commute, because otherwise the elements of D (and of D^{-1}) would have order 2 and D would trivially be a real class. If $|K| = 2$, say for instance $K = \{x, x^g\}$, then $KK^{-1} = 1 \cup \{xx^g, x^g x\}$. Notice that $\{xx^g, x^g x\}$ cannot be decomposed into two central classes. In fact, if xx^g and $x^g x$ are central elements, then x and x^g would commute. Therefore, $|K| \geq 3$ and we write $K = \{x_1, \ldots, x_n\}$ with $n \geq 3$. If $x_i, x_j \in K$ are distinct, we have $x_i^{x_j} = x_l \in K$ for some positive integer l. Furthermore, $x_i \neq x_l$, otherwise x_i and x_j would commute. Thus, $x_l^{x_j} = (x_i^{x_j})^{x_j} = x_i$ and $(x_i x_l)^{x_j} = x_l x_i = (x_i x_l)^{-1}$. Since $x_i x_l \in D$ or $x_i x_l \in D^{-1}$, we conclude that D is real too.

Suppose now that $o(x) > 2$. We can clearly assume that $x^2 \in D$ (analogous if $x^2 \in D^{-1}$). Moreover, since there exists $g \in G$ such that $x^g = x^{-1}$, we have $(x^2)^g = (x^g)^2 = (x^{-1})^2 = x^{-2}$. Now, if $x^2 = x^{-2}$, then $o(x^2) = 2$ and D is real and if $x^2 \neq x^{-2}$, then x^2, $x^{-2} \in D$ and D is real.□

Proof of Theorem A. Let $x, d \in G$ such that $K = x^G$, $D = d^G$ and $KK^{-1} = 1 \cup D \cup D^{-1}$. We suppose that G is simple and we will look for a contradiction. We distinguish three parts appealing to the CFSG. We show that for any alternating group, simple group of Lie type or sporadic group there is no conjugacy class satisfying the hypotheses of the theorem.

Case 1. Suppose that $G = A_n$ with $n \geq 5$.

It is easy to check that A_5 does not satisfy the property of the statement for any non-trivial conjugacy class K. Suppose that $n > 5$. Note that x and x^{-1} are permutations of the same type. We distinguish two cases: $x^{S_n} = x^{A_n}$ or $x^{S_n} \neq x^{A_n}$. If $x^{S_n} = x^{A_n}$, it follows that $x^{S_n}(x^{-1})^{S_n} = 1 \cup D^{S_n} \cup (D^{-1})^{S_n} = 1 \cup D^{S_n}$ and hence $\eta(x^{S_n}(x^{-1})^{S_n}) = 2$. By applying Theorem 2.1, we get a contradiction because x and x^{-1} should be permutations of different type and this case is finish. We remark that if $x^{S_n} \neq x^{A_n}$ the result can be obtained by applying an unpublished result for alternating groups by Adan-Bante which is similar to Theorem 2.1. Nevertheless, we provide an alternative proof by employing Theorem B.

Suppose then that $x^{S_n} \neq x^{A_n} = K$. It is well-known that in this case x is a permutation that is product of disjoint cycles whose lengths are odd and different to each other (including cycles of length 1). Let us see that $|K| > (n-1)^2$ for every $n \geq 6$. We know that if $C = x^{S_n}$, then

$$|C| = \frac{n!}{\prod_{j=1}^{n}(j)^{a_j} a_j!},$$

where a_j is the multiplicity of the cycle of length j for each j. In particular, for K we obtain

$$|K| = |C|/2$$

where $a_j = 0$ if j is even, a_j is either 0 or 1 if j is odd, and $\sum_{j=1}^{n} j a_j = n$. The fact that $|K| > (n-1)^2$ for every $n \geq 6$ can be easily proved by arguing by induction on n.

Now, let χ be the natural permutation character of A_n and $\psi := \chi - 1 \in \mathrm{Irr}(G)$ with $\psi(1) = n-1$ (see for instance Corollary 5.17 of [12]). In particular, for the permutation x we have either $\chi(x) = 0$ or $\chi(x) = 1$ and $\psi(x) = -1$ or $\psi(x) = 0$. Assume first that $\chi(x) = 0$. By replacing ψ in the equation of Theorem B we deduce

$$\psi(d) = \frac{|K| - (n-1)^2}{(|K|-1)(n-1)},$$

which certainly is an integer less than 1. Consequently, $\psi(d)$ may only take the values -1 or 0. In the first case we deduce $|K| = n-1$ and in the second case $|K| = (n-1)^2$, contradicting the above property in both cases. Assume finally that $\chi(x) = 1$. Again by using Theorem B we obtain

$$(n-1)^2 + (|K|-1)(n-1)(\chi(d)-1) = 0.$$

If $\chi(d) > 0$, then the left side of the equality is bigger than 0, a contradiction, and if $\chi(d) = 0$, it follows that $|K| = n$, a contradiction too.

Case 2. Suppose that G is a finite simple group of Lie type.

If G is a finite simple group of Lie type in characteristic p, we can always take the Steinberg character $\psi \in \mathrm{Irr}(G)$ which satisfies $\psi(t) = \pm|\mathbf{C}_G(t)|_p$ for every p-regular element $t \in G$ and $\psi(t) = 0$ for every p-singular element $t \in G$. Furthermore, $\psi(1) = |G|_p$ (see for instance Chapter 6 of [6]). Assume that there exists a non-trivial pair of elements $x, d \in G$ such that the assertion b) of Theorem B holds and we will work to get a contradiction.

Case 2.1. Suppose that x is p-regular. We know that $\psi(x) = \pm|\mathbf{C}_G(x)|_p \neq 0$. By the equivalence of Theorem B we have

$$|K||\mathbf{C}_G(x)|_p^2 - |G|_p^2 = \frac{|K|-1}{2}|G|_p(\psi(d) + \psi(d^{-1})). \tag{4}$$

If $\psi(d) = \psi(d^{-1}) = 0$, then $|K| = |K|_p^2$ and this contradicts p^a-Burnside's Lemma (see for instance Theorem 15.2 of [11]). Thus, $\psi(d) = \psi(d^{-1}) = \pm|\mathbf{C}_G(d)|_p$ and by replacing in Eq.(4) we obtain

$$(|K|_{p'} - |K|_p)|\mathbf{C}_G(x)|_p = (|K| - 1)(\pm|\mathbf{C}_G(d)|_p).$$

If p divides $|K|$, it follows that $|K|_{p'} - |K|_p = |K| - 1$, which implies $|K| = |K|_{p'}$ and $|K|_p = 1$, a contradiction. Consequently, p does not divide $|K|$ and since $\psi(1) = |G|_p$ we conclude by Lemma 2.6 that either $\psi(x) = 0$ or $1 \neq x \in \mathbf{Z}(\psi)$. Both possibilities yield to a contradiction.

Case 2.2. Suppose that x is p-singular. We know that $\psi(x) = 0$ and $\psi(1) = |G|_p$. By the assertion b) of Theorem B,

$$\psi(d) + \psi(d^{-1}) = \frac{-2|G|_p}{(|K|-1)} < 0.$$

This means that d is a p-regular element and we necessarily have

$$\psi(d) = \psi(d^{-1}) = -|\mathbf{C}_G(d)|_p.$$

As a consequence, by the two equalities above, $|K| = |D|_p + 1$. Thus, p does not divide $|K|$.

Now we prove that x is a p-element. We consider the decomposition $x = x_p x_{p'}$. Notice that $\mathbf{C}_G(x) = \mathbf{C}_G(x_p) \cap \mathbf{C}_G(x_{p'}) \subseteq \mathbf{C}_G(x_{p'})$, which shows that $|x_{p'}^G|$ divides $|K|$, and then p does not divide $|x_{p'}^G|$ either. By applying Lemma 2.6 again, we obtain either $\psi(x_{p'}) = 0$, which leads to a contradiction because $x_{p'}$ is p-regular, or $x_{p'} \in \mathbf{Z}(\psi) = 1$. Consequently, x is a p-element. Since d is p-regular, we apply Theorem 2.4 and this straightforwardly contradicts the simplicity of G.

Case 3. Suppose that G is a sporadic finite simple group.

By using the character tables of the sporadic groups (for instance in GAP [7]) we can check that the equivalence of Theorem B does not hold for any of these groups and any two non-trivial conjugacy classes of it. In fact, for any sporadic simple group, the only character satisfying such assertion for fixed elements $x, d \in G$ with $x \neq 1$ is the principal character.

The non-simplicity of G when $KK^{-1} = 1 \cup D$ is a direct consequence of our previous arguments when $D = D^{-1}$ taking into account the corresponding case of Theorem B. □

We provide an example illustrating the non-simplicity of a group satisfying the hypothesis of Theorem A. Let $G = \langle a \rangle \rtimes \langle b \rangle$ where $\langle a \rangle \cong \mathbb{Z}_7$, $\langle b \rangle \cong \mathbb{Z}_3$ and $a^b = a^2$. Let K be one of the two classes of elements of order 3, which satisfies $|K| = 7$. It holds $KK^{-1} = 1 \cup D \cup D^{-1}$ where D is a conjugacy class of elements of order 7 and size 3. We have $\langle K \rangle = G$ and $\langle D \rangle \cong \mathbb{Z}_7$. In fact, this is the example of the smallest order group satisfying the property of Theorem A with $D \neq D^{-1}$.

4 Proof of Theorem C

Proof of Theorem C. Let $K = x^G$ with $x \in G$. We write $\widehat{K}\widehat{K^{-1}} = |K|\widehat{1} + m\widehat{D}$, so $|K|^2 = |K| + m|D|$ and $|D|$ divides $|K|(|K| - 1)$. The fact that $\langle K \rangle / \langle D \rangle$ is cyclic follows immediately from Lemma 2.8.

1) Suppose that $|D| = |K| - 1$. Then $|KK^{-1}| = |K|$. Note that $xK^{-1} \subseteq KK^{-1}$ and, since $|xK^{-1}| = |K|$, we obtain $xK^{-1} = KK^{-1}$. Then $K^{-1} = x^{-1}KK^{-1}$, which implies that $K^{-1} = \langle x^{-1}K \rangle K^{-1}$. This means that K^{-1} is union of right classes of $\langle x^{-1}K \rangle$. Also, $\langle x^{-1}K \rangle = \langle KK^{-1} \rangle = \langle D \rangle$, so we get that $|\langle D \rangle|$ divides $|K|$. As $|K| = |KK^{-1}| \leq |\langle KK^{-1} \rangle| = |\langle D \rangle|$, then $|\langle D \rangle| = |K|$. Since $x^{-1}K \subseteq \langle KK^{-1} \rangle$ and $|x^{-1}K| = |K| = |\langle KK^{-1} \rangle|$, we obtain $\langle D \rangle = x^{-1}K$. Thus, $\langle D \rangle = xK^{-1} \subseteq 1 \cup D \subseteq \langle D \rangle$, so $\langle D \rangle = 1 \cup D$ is p-elementary abelian for some prime p. As $\langle K \rangle / \langle D \rangle$ is cyclic, this case is finished.

2) Assume that $|K| = |D|$. It is clear that $xK^{-1} \cup x^{-1}K \subseteq K^{-1}K$. We divide the proof of this case into two subcases: whether $xK^{-1} = x^{-1}K$ or not. Suppose first that $xK^{-1} = x^{-1}K$. We have $K = x^2K^{-1}$ and, analogously, $K^{-1} = (x^g)^{-2}K$ for every $g \in G$. By replacing K^{-1} in the former equality, we deduce that $K = x^2(x^g)^{-2}K$ for every $g \in G$. We define

$$N = \langle x^2(x^g)^{-2} \mid x \in K \ , \ g \in G \rangle.$$

Then $K = NK$ and, as a consequence, $|N|$ divides $|K|$. In addition, $KK^{-1} = NKK^{-1}$, so $|N|$ also divides $|KK^{-1}| = 1 + |D| = 1 + |K|$, which allows to $N = 1$. As a result, $x^2 \in \mathbf{Z}(G)$. If $y \in K$, then $y = x^g \in K$ for some $g \in G$ and note that

$y^2 = (x^g)^2 = (x^2)^g = x^2$. On the other hand, we can write $KK^{-1} = xK^{-1} \cup \{z\}$ for some $z \in D$. Since $xK^{-1} = x^{-1}K = (xK^{-1})^{-1}$ and KK^{-1} coincides with its inverse, both facts show that $z = z^{-1}$, that is, z has order 2. Now, if we take two distinct elements $y, y^g \in K$ with $g \in G$, then $y^{-1}y^g \in D$, so we write $y^g = yd$ for some $d \in D$. Then $y^2 = (y^g)^2 = (yd)^2 = yy^d$ and consequently, $y = y^d$. This means that $[y, d] = 1$ and hence $[y, y^g] = 1$. Therefore, $\langle K \rangle$ is abelian, so the assertion 2) holds.

Assume now that $xK^{-1} \neq x^{-1}K$. We know that $xK^{-1} \cup x^{-1}K \subseteq KK^{-1}$. Since $|KK^{-1}| = |K| + 1$ and $|K| = |xK^{-1}| = |x^{-1}K|$, there exists only just one element $z \in xK^{-1} \setminus x^{-1}K$. Moreover, it is easy to prove that z^{-1} is the only element contained in $x^{-1}K \setminus xK^{-1}$ (notice that $z \neq z^{-1}$). Therefore, KK^{-1} can be decomposed as

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

From this equality and the fact that $(x^{-1}K)(xK^{-1}) = KK^{-1}$, we deduce that

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

On the other hand, $(KK^{-1})^2 = (1 \cup D)(1 \cup D) = 1 \cup D \cup D^2$. It follows that $D^2 \subseteq 1 \cup D \cup \{z^2\} \cup \{z^{-2}\}$. We distinguish two cases. If $z^2 \in D$, then $D^2 = 1 \cup D$ and hence, $\langle D \rangle$ is p-elementary abelian for some prime p. We get the assertion 2) by taking into account that $\langle K \rangle / \langle D \rangle$ is cyclic. Assume now that $z^2 \notin D$. Then $\langle z^2 \rangle \trianglelefteq G$ because either $\{z^2\}$ and $\{z^{-2}\}$ are central conjugacy classes or $\{z^2, z^{-2}\}$ is a conjugacy class. We write $\overline{G} = G/\langle z^2 \rangle$ and we obtain $\overline{D^2} \subseteq \overline{1} \cup \overline{D}$. So we have two possibilities: $\overline{D^2} = \overline{1}$ or $\overline{D^2} = \overline{1} \cup \overline{D}$. If $\overline{D^2} = \overline{1}$, then $\langle \overline{D} \rangle \cong \mathbb{Z}_2$, and as a result $\langle D \rangle$ is metacyclic. Consequently, $\langle K \rangle$ is solvable with $dl(\langle K \rangle) \leq 3$. Finally, if $\overline{D^2} = \overline{1} \cup \overline{D}$, it certainly follows that $\langle \overline{D} \rangle$ is elementary abelian. Then $\langle D \rangle$ is metabelian and, again $\langle K \rangle$ is solvable with $dl(\langle K \rangle) \leq 3$.

3) Assume that $|D| = |K|(|K|-1)$. Since $\widehat{K}\widehat{K^{-1}} = |K|\widehat{1} + m\widehat{D}$, we necessarily have $m = 1$. We write $K = \{x_1, \ldots, x_n\}$ and $K^{-1}K = x_1^{-1}K \cup \ldots \cup x_n^{-1}K$. Notice that $1 \in x_i^{-1}K$ for all $i = 1, \cdots, n$. We rewrite the previous equality as the union

$$K^{-1}K = 1 \cup (x_1^{-1}K \setminus 1) \cup \ldots \cup (x_n^{-1}K \setminus 1).$$

By counting elements we conclude that $x_i^{-1}K \cap x_j^{-1}K = 1$ for all $i = 1, \ldots, n$ with $i \neq j$. Let $g \in \mathbf{C}_G(x_i x_j^{-1})$ with $i \neq j$. Thus, $(x_i x_j^{-1})^g = x_i^g (x_j^{-1})^g = x_i x_j^{-1}$. From the last equality we have $x_i^{-1} x_i^g = x_j^{-1} x_j^g = 1$, so $g \in \mathbf{C}_G(x_i) \cap \mathbf{C}_G(x_j^{-1})$. Hence, $\mathbf{C}_G(x_i x_j^{-1}) = \mathbf{C}_G(x_i) \cap \mathbf{C}_G(x_j^{-1})$. As $x_i x_j^{-1} \in \mathbf{C}_G(x_i x_j^{-1})$, then $x_i x_j^{-1} \in \mathbf{C}_G(x_i)$, so $[x_i, x_j] = 1$. Therefore, $\langle K \rangle$ is generated by pairwise commuting elements, which means that $\langle K \rangle$ is abelian.□

We emphasize the feasibility of Theorem C by giving examples. Some of them have been found by using the SmallGroups library of GAP [7]. The

m-th group of order n in this library is identified by $n\#m$. If $G = 110\#1$, there is a class K of elements of order 5 satisfying $KK^{-1} = 1 \cup D$ where D is a class of elements of order 11. We have $\langle K \rangle \cong \mathbb{Z}_{11} \rtimes \mathbb{Z}_5$ and $\langle D \rangle \cong \mathbb{Z}_{11}$. This is an example of Case 1. Let $G = \langle a \rangle \times A_4$ where $\langle a \rangle \cong \mathbb{Z}_{10}$ and we take $K = x^G$ where $x = at$ and t is an involution of A_4. It follows that $KK^{-1} = 1 \cup D$ where $D = t^G$ and $\langle K \rangle \cong \mathbb{Z}_{10} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\langle D \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. This is an example of Case 2. The group $G = 150\#5$ has a class K of elements of order 5 which satisfies $KK^{-1} = 1 \cup D$, where D is a class of elements of order 5. We have $\langle K \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_5$. This is an example of Case 3. Finally, in the next example, $|D|$ is a divisor of $|K|(|K| - 1)$ different from those appearing in Theorem C. Take $G = SL(2, 3)$ and $K = x^G$ where $o(x) = 3$. Then $KK^{-1} = 1 \cup D$, where D is a class of elements of order 4. We have $\langle K \rangle \cong G$ and $\langle D \rangle \cong Q_8$. Note that $dl(\langle K \rangle) = 3$, so this is the best bound.

5 Analogous problems for irreducible characters

Following the parallelism between conjugacy classes and irreducible characters, we reflect on the problem of translating our results into Character Theory. As we have asserted in the Introduction by means of an example, the fact that $\eta(KK^{-1}) = 3$ does not imply the non-simplicity of the group. Something similar occurs when working with irreducible characters. For example, if we consider the simple group $\mathrm{PSL}(2, 11)$, there exist three irreducible characters χ, ψ and φ such that $\chi\overline{\chi} = 1 + \psi + \varphi$ (see for instance page 290 of [12]).

Trying to transfer Theorem A into the framework of irreducible characters, we find that in [1] the author gives the structure of a finite solvable group G with $\chi \in \mathrm{Irr}(G)$ such that $\chi\overline{\chi} = 1_G + m_1\alpha_1 + m_2\alpha_2$ where α_1, $\alpha_2 \in \mathrm{Irr}(G)$ are non-principal characters and m_1 and m_2 are strictly positive integers. We are not aware, however, whether the above equality may hold in a simple group when $\alpha_2 = \overline{\alpha_1} \neq \alpha_1$. Nevertheless, regarding the particular case of Theorem A, if we take $G = \mathrm{PSp}_{2n}(3)$, $n \geq 2$, or $G = \mathrm{PSU_n}(2)$, $(n, 3) = 1$, $n \geq 4$, it is known that there exists a non-trivial character $\psi \in \mathrm{Irr}(G)$ such that $\psi\overline{\psi} = \chi + 1$, with $\chi \in \mathrm{Irr}(G)$ (see [13] for instance). So we conclude that simplicity may occur when the particular case of Theorem A is translated into irreducible characters.

Acknowledgements

The authors gratefully acknowledge all helpful comments made by the referee. The results in this paper are part of the third author's Ph.D. thesis, and she acknowledges the predoctoral grant PREDOC/2015/46, Universitat Jaume I. The first and second authors are supported by the Valencian Government, Proyecto PROMETEOII/2015/011. The first and the third authors are also partially supported by Universitat Jaume I, grant P11B2015-77.

References

[1] E. Adan-Bante, Products of characters with few irreducible constituents. *J. Algebra*, **311** (2007), 38-68.

[2] E. Adan-Bante, Symmetric groups and conjugacy classes. *J. Group Theory*, **3** (2008), 371-379.

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

[4] Z. Arad and M. Herzog, *Products of conjugacy classes in groups*, Lecture Notes in Mathematics, 1112, Springer-Verlag, Berlin, (1985).

[5] A. Beltrán, M.J. Felipe and C. Melchor, Squares of real conjugacy classes in finite groups. DOI: 10.1007/s10231-017-0681-0. *Ann. Mat. Pura Appl.*

[6] R.W. Carter, *Finite groups of Lie Type. Conjugacy classes and complex characters*, John Wiley & Sons, Inc. New York, (1985).

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

[8] G. Glauberman, Central elements in core-free groups. *J. Algebra*, **4** (3) (1966), 403-420.

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

[10] R.M. Guralnick and G.R. Robinson, On extensions on the Baer-Suzuki theorem, *Israel J. Math.* **82** (1993), 281-297.

[11] B. Huppert, *Character theory of finite groups*, Walter de Gruyter, Berlin, New York, (1998).

[12] I.M. Isaacs, *Character theory of finite groups*, Academic Press, Inc, New York, (1976).

[13] G. Malle, Almost irreducible tensor squares, *Comm. in Algebra*, **27** (3) (1999), 1033-1051.

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

[15] J. Moori, H.P. Tong-Viet, Products of conjugacy classes in simple groups, *Quaest. Math.*, **34** (4) (2011), 433-439.