Mediterr. J. Math. (2022) 19:257
https://doi.org/10.1007/s00009-022-02171-7
1660-5446/22/060001-12
published online October 18, 2022

Mediterranean Journal of Mathematics

An Arad and Fisman's Theorem on Products of Conjugacy Classes Revisited

Antonio Beltrán, María José Felipe and Carmen Melchor

Abstract. A theorem of Z. Arad and E. Fisman establishes that if A and B are two non-trivial conjugacy classes of a finite group G such that either $AB = A \cup B$ or $AB = A^{-1} \cup B$, then G cannot be a non-abelian simple group. We demonstrate that, in fact, $\langle A\rangle = \langle B\rangle$ is solvable, the elements of A and B are p-elements for some prime p, and $\langle A\rangle$ is p-nilpotent. Moreover, under the second assumption, it turns out that $A = B$. This research is done by appealing to recently developed techniques and results that are based on the Classification of Finite Simple Groups.

Mathematics Subject Classification. 20E45, 20D15.

Keywords. Conjugacy classes, products of conjugacy classes, solvability criterium.

1. Introduction

The well-known and long-standing conjecture of Arad and Herzog claims that the product of two non-trivial conjugacy classes of a finite non-abelian simple group cannot be a conjugacy class. Taking one further step, several authors have studied more general conditions on the product of conjugacy classes that cannot either happen in a non-abelian simple group. This occurs, for instance, when the product of two conjugacy classes is the union of certain limited sets of conjugacy classes (see for instance [2,3,5]).

Our contribution is motivated by the new techniques and results that have been developed in the last few years (requiring the Classification of Finite Simple Groups) in this direction. These results not only provide the non-simplicity of a group but the solvability of certain subgroups generated by the conjugacy classes when certain conditions on their products are assumed. This is the case, for example, of the main results of [4,6,8].

Among these results, Arad and Fisman proved that when A and B are two non-trivial conjugacy classes of a group G such that either $AB = A \cup B$ or $AB = A^{-1} \cup B$, then G cannot be non-abelian simple [1]. They used elementary methods to prove it, however, the new outlined approaches allow

Birkhäuser

us to revisit this theorem and supply solvability and structural properties in the group. We prove the following.

Theorem A. *Let A and B be conjugacy classes of a finite group G and suppose that $AB = A \cup B$. Then $\langle A\rangle = \langle B\rangle$ is solvable. Furthermore, the elements of A and B are p-elements for some prime p and $\langle A\rangle$ is p-nilpotent.*

Theorem B. *Let A and B be conjugacy classes of a finite group G and suppose that $AB = A^{-1} \cup B$ with $A \neq A^{-1}$. Then $A = B$ and $\langle A\rangle$ is solvable. Furthermore, the elements of A are p-elements for some prime p and $\langle A\rangle$ is p-nilpotent.*

The case $A = B$ in Theorem B, that is, $A^2 = A \cup A^{-1}$, was already studied in Theorem D of [4]. This asserts that, under this hypothesis, $\langle A\rangle$ is solvable and the elements of A are p-elements. We will improve this result by showing that $\langle A\rangle$ is in addition p-nilpotent. Moreover, for proving Theorem B, we also need a new solvability criterion concerning the product of a conjugacy class and its inverse class, which has interest on its own.

Theorem C. *Let A be a conjugacy class of a finite group G such that $AA^{-1} = 1 \cup A \cup A^{-1}$. Then $\langle A\rangle = AA^{-1}$ is an elementary abelian group.*

The above result provides further evidence of the following conjecture posed in [6]: If A and B are conjugacy classes of a group such that $AA^{-1} = 1 \cup B \cup B^{-1}$, then $\langle A\rangle$ is solvable. The non-simplicity of G and the solvability of $\langle A\rangle$ for some specific cases were obtained in Theorems A and C of [5] and also in Theorem C of [7].

The proofs of Theorems A and B are based on the Classification. However, the proof of Theorem C is elementary. All groups are supposed to be finite and the notation is standard and essentially follows that appearing in [1].

2. Preliminary Results

We state some preliminary results. The first one is essential for proving both Theorems A and B, and part (a) requires the Classification of Finite Simple Groups. However, part (b) does not need it.

Theorem 2.1. *Let G be a finite group and let N be a normal subgroup of G. Let $x \in G$ be such that all elements of xN are conjugate in G. Then:*

(a) *N is solvable.*
(b) *If x is a p-element for some prime p, then N has a normal p-complement.*

Proof. This is Theorem 3.2 (a) and (c) of [8]. □

The following property, however, is elementary and is used for proving Theorem B. Observe that in the particular case of Theorem C, this property is trivial. This situation is addressed in [5].

Lemma 2.2. *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. See Lemma 3.1 of [5]. □

Our approach mainly utilizes the complex group algebra. We denote by $\mathbb{C}[G]$ the complex group algebra of a group G over the complex field $\mathbb{C}$. Let K be a conjugacy class of G and denote by $\widehat{K}$ the class sum of the elements of K in $\mathbb{C}[G]$. Let $g_1, \ldots, g_k$ be representatives of the conjugacy classes of a finite group G. Let $\widehat{S} = \sum_{i=1}^{k} n_i \widehat{g_i^G}$ with $n_i \in \mathbb{N}$ for $1 \leq i \leq k$. We write $(\widehat{S}, \widehat{g_i^G}) = n_i$ following [1]. Nevertheless, our notation for class sums differs from that appearing in [1] in order to facilitate the reading. The following properties are well known.

Lemma 2.3. *If D_1, D_2 and D_3 are conjugacy classes of a finite group G, then*

(i) $(\widehat{D_1}\widehat{D_2}, \widehat{D_3}) = (\widehat{D_1^{-1}}\widehat{D_2^{-1}}, \widehat{D_3^{-1}})$

(ii) $(\widehat{D_1}\widehat{D_2}, \widehat{D_3}) = |D_2||D_3|^{-1}(\widehat{D_1}\widehat{D_3^{-1}}, \widehat{D_2^{-1}})$

(iii) $(\widehat{D_1}\widehat{D_2}, \widehat{D_1}) = |D_2||D_1|^{-1}(\widehat{D_1}\widehat{D_1^{-1}}, \widehat{D_2^{-1}}) = (\widehat{D_2}\widehat{D_1^{-1}}, \widehat{D_1^{-1}}) = (\widehat{D_2^{-1}}\widehat{D_1}, \widehat{D_1})$.

Proof. This easily follows, for instance, from Theorem 4.6 of [9]. □

3. Proofs

We start by proving Theorem C, which will be used for proving Theorem B.

Proof of Theorem C. The case $A = A^{-1}$ is easy and known, so we can assume that $A \neq A^{-1}$. By Lemma 2.3 we have

$$m = (\widehat{A}\widehat{A^{-1}}, \widehat{A}) = (\widehat{A}\widehat{A^{-1}}, \widehat{A^{-1}}) = (\widehat{A}^2, \widehat{A}) = (\widehat{A^{-1}}^2, \widehat{A^{-1}}),$$

where m is a positive integer, and so we can write

$$\begin{aligned} \widehat{A}\widehat{A^{-1}} &= |A|\widehat{1} + m\widehat{A} + m\widehat{A^{-1}} \\ \widehat{A}^2 &= m\widehat{A} + \alpha\widehat{A^{-1}} + \widehat{T} \\ \widehat{A^{-1}}^2 &= m\widehat{A^{-1}} + \alpha\widehat{A} + \widehat{T^{-1}} \end{aligned} \tag{1}$$

where $\alpha \geq 0$, and $\widehat{T}$ is a sum of conjugacy classes taking into account the multiplicities and such that $(\widehat{T}, \widehat{L}) = (\widehat{T^{-1}}, \widehat{L}) = 0$ for $L \in \{1, A, A^{-1}\}$. For convenience, we write

$$\widehat{T} = l_1\widehat{L_1} + \cdots + l_s\widehat{L_s}$$

where L_i are distinct conjugacy classes of G and l_i the corresponding multiplicities, and $\widehat{T^{-1}}$ denotes $l_1\widehat{L_1^{-1}} + \cdots + l_s\widehat{L_s^{-1}}$.

Suppose first $T \neq \emptyset$ and calculate

$$\begin{aligned} \widehat{A}^2\widehat{A^{-1}}^2 &= (m\widehat{A} + \alpha\widehat{A^{-1}} + \widehat{T})(m\widehat{A^{-1}} + \alpha\widehat{A} + \widehat{T^{-1}}) \\ &= m^2\widehat{A}\widehat{A^{-1}} + m\alpha\widehat{A}^2 + m\widehat{A}\widehat{T^{-1}} + m\alpha\widehat{A^{-1}}^2 + \alpha^2\widehat{A^{-1}}\widehat{A} \\ &\quad + \alpha\widehat{A^{-1}}\widehat{T^{-1}} + m\widehat{T}\widehat{A^{-1}} + \alpha\widehat{T}\widehat{A} + \widehat{T}\widehat{T^{-1}}. \end{aligned}$$

Consequently, from the above equation, we observe

$$(\widehat{A}^2\widehat{A^{-1}}^2,\widehat{1}) = m^2|A| + \alpha^2|A| + l_1|L_1| + \cdots l_s|L_s|. \quad (2)$$

On the other hand,

$$\begin{aligned}(\widehat{A}\widehat{A^{-1}})^2 &= (|A|\widehat{1} + m\widehat{A} + m\widehat{A^{-1}})(|A|\widehat{1} + m\widehat{A} + m\widehat{A^{-1}})\\ &= |A|^2\widehat{1} + |A|m\widehat{A} + |A|m\widehat{A^{-1}} + |A|m\widehat{A} + m^2\widehat{A}^2 + m^2\widehat{A}\widehat{A^{-1}}\\ &\quad +m|A|\widehat{A^{-1}} + m^2\widehat{A^{-1}}\widehat{A} + m^2\widehat{A^{-1}}^2.\end{aligned}$$

Thus,

$$((\widehat{A}\widehat{A^{-1}})^2,\widehat{1}) = |A|^2 + 2m^2|A|. \quad (3)$$

By joining Eqs. (2) and (3) we obtain

$$l_1|L_1| + \cdots + l_s|L_s| = |A|^2 + (m^2 - \alpha^2)|A| \quad (4)$$

and from Eq. (1) we have

$$l_1|L_1| + \cdots + l_s|L_s| = |A|^2 - (m + \alpha)|A|. \quad (5)$$

Hence, from Eqs. (4) and (5), we conclude that $m = \alpha - 1$.
On the other hand, we calculate

$$\begin{aligned}\widehat{A}(\widehat{A}\widehat{A^{-1}}) &= \widehat{A}(|A|\widehat{1} + m\widehat{A} + m\widehat{A^{-1}})\\ &= |A|\widehat{A} + m(m\widehat{A} + \alpha\widehat{A^{-1}} + \widehat{T}) + m(|A|\widehat{1} + m\widehat{A} + m\widehat{A^{-1}}) \quad (6)\\ &= m|A|\widehat{1} + (|A| + 2m^2)\widehat{A} + (\alpha m + m^2)\widehat{A^{-1}} + m\widehat{T}\end{aligned}$$

and

$$\begin{aligned}\widehat{A}^2\widehat{A^{-1}} &= (m\widehat{A} + \alpha\widehat{A^{-1}} + \widehat{T})\widehat{A^{-1}}\\ &= m(|A|\widehat{1} + m\widehat{A} + m\widehat{A^{-1}}) + \alpha(m\widehat{A^{-1}} + \alpha\widehat{A} + \widehat{T^{-1}}) + \widehat{T}\widehat{A^{-1}} \quad (7)\\ &= |A|m\widehat{1} + (m^2 + \alpha^2)\widehat{A} + (m^2 + \alpha m)\widehat{A^{-1}} + \alpha\widehat{T^{-1}} + \widehat{T}\widehat{A^{-1}}.\end{aligned}$$

So, from Eqs. (6) and (7) we conclude that $T = T^{-1}$ and $m = \alpha + \beta$ for some $\beta \in \mathbb{N}^*$, a contradiction. This contradiction implies that $T = \emptyset$, and hence $A^2 = A \cup A^{-1}$.
Now we prove that $\langle A\rangle$ is elementary abelian. Indeed, we have $A^3 = AA^2 = A(A\cup A^{-1}) = A^2 \cup AA^{-1} = 1\cup A\cup A^{-1}$, so we deduce that $\langle A\rangle = 1\cup A\cup A^{-1}$. In particular, all non-trivial elements of $\langle A\rangle$ have the same order, and this forces $\langle A\rangle$ to be p-elementary for some prime p. Finally, we prove that $\langle A\rangle$ is abelian. Put $N = \langle A\rangle$ and let $x \in A$. Observe that $|x^N|$ divides $|A| = |x^G|$, but on the other hand, $|x^N|$ also divides $|N| = 1 + 2|A|$. This implies that $|x^N| = 1$, and hence N is abelian. □

Examples. The smallest group for Theorem C with A non-trivial and real is the symmetric group on 3 letters with the conjugacy class of 3-cycles. The smallest example for Theorem C with A non-real is the non-abelian group of order 21, $G = \langle x, y \mid x^y = x^2, x^7 = 1\rangle$, when we consider the conjugacy class $A = \{x, x^2, x^4\}$ where $\langle A\rangle = \langle x\rangle \cong \mathbb{Z}_7$.

We restate Theorems A and B in terms of the theorems appearing in [1]. We will divide the proofs into several steps. Although Steps 1 and 4 are identical to those appearing in [1] we are including again their proofs for the reader's convenience.

Theorem A. *Let D_1 and D_2 be conjugacy classes of a finite group G and suppose that $D_1D_2 = D_1 \cup D_2$. Then $\langle D_1\rangle = \langle D_2\rangle$ is solvable. Furthermore, the elements in D_1 and D_2 are p-elements for some prime p and $\langle D_1\rangle$ is p-nilpotent.*

Proof. First, let us prove $\langle D_1\rangle = \langle D_2\rangle$ by induction on $|G|$. If $G = \langle D_1\rangle = \langle D_2\rangle$ the proof is finished. Suppose, for instance, that $\langle D_1\rangle < G$ and write $\overline{G} = G/\langle D_1\rangle$. Then $\overline{D_1D_2} = \overline{D_1} \cup \overline{D_2}$, which implies that $\overline{D_2} = \overline{1}$, and hence $\langle D_2\rangle \subseteq \langle D_1\rangle$. Now, if we consider the factor group $G/\langle D_2\rangle$, by arguing as above we get $\langle D_1\rangle \subseteq \langle D_2\rangle$.

We continue the proof by induction on $|G|$. We write $\widehat{D_1}\widehat{D_2} = n_1\widehat{D_1} + n_2\widehat{D_2}$ with $n_1, n_2 \in \mathbb{N}^*$.

Step 1: $\widehat{D_1}\widehat{D_2^{-1}} = n_1\widehat{D_1} + n_2\widehat{D_2^{-1}}$ *and* $D_i = D_i^{-1}$ for $1 \leq i \leq 2$.

By Lemma 2.3 (iii), $n_1 = (\widehat{D_1}\widehat{D_2}, \widehat{D_1}) = (\widehat{D_1}\widehat{D_2^{-1}}, \widehat{D_1})$ and $n_2 = (\widehat{D_1}\widehat{D_2}, \widehat{D_2}) = (\widehat{D_1}\widehat{D_2^{-1}}, \widehat{D_2^{-1}})$. So $\widehat{D_1}\widehat{D_2^{-1}} = n_1\widehat{D_1} + n_2\widehat{D_2^{-1}} + \widehat{T}$ where $\widehat{T}$ is a sum of classes (counting multiplicities) with $(\widehat{T}, \widehat{L}) = 0$ for $L \in \{D_1, D_2^{-1}\}$. Since

$$\begin{aligned} n_1|D_1| + n_2|D_2^{-1}| &= n_1|D_1| + n_2|D_2| = |D_1||D_2| = |D_1||D_2^{-1}| \\ &= n_1|D_1| + n_2|D_2^{-1}| + |T|, \end{aligned}$$

then $\widehat{T} = 0$.

In addition,

$$(n_1\widehat{D_1} + n_2\widehat{D_2^{-1}})\widehat{D_2} = (\widehat{D_1}\widehat{D_2^{-1}})\widehat{D_2} = (\widehat{D_1}\widehat{D_2})\widehat{D_2^{-1}} = (n_1\widehat{D_1} + n_2\widehat{D_2})\widehat{D_2^{-1}}.$$

So $\widehat{D_1}\widehat{D_2^{-1}} = \widehat{D_1}\widehat{D_2}$ or equivalently $n_1\widehat{D_1} + n_2\widehat{D_2^{-1}} = n_1\widehat{D_1} + n_2\widehat{D_2}$ then $D_2 = D_2^{-1}$ and similarly $D_1 = D_1^{-1}$.

Step 2: *We have*

$$\begin{aligned} \widehat{D_1}^2 &= |D_1|\widehat{1} + n_1|D_1||D_2|^{-1}\widehat{D_2} + s_1\widehat{D_1} + \widehat{M_1} \\ \widehat{D_2}^2 &= |D_2|\widehat{1} + n_2|D_2||D_1|^{-1}\widehat{D_1} + s_2\widehat{D_2} + \widehat{M_2} \end{aligned}$$

where $s_i \in \mathbb{N}$ and $\widehat{M_i}$ are sums of conjugacy classes taking into account their multiplicities such that $(\widehat{M_i}, \widehat{C}) = 0$ for $C \in \{1, D_j\}$, $i, j, \in \{1, 2\}$.

By Lemma 2.3 we know that

$$\begin{aligned} (\widehat{D_1}^2, \widehat{1}) &= |D_1|(\widehat{D_1}, \widehat{D_1}) = |D_1|, \\ (\widehat{D_1}^2, \widehat{D_2}) &= |D_1||D_2|^{-1}(\widehat{D_1}\widehat{D_2}, \widehat{D_1}) = |D_1||D_2|^{-1}n_1. \end{aligned}$$

Then we can write

$$\widehat{D_1}^2 = |D_1|\widehat{1} + n_1|D_1||D_2|^{-1}\widehat{D_2} + s_1\widehat{D_1} + \widehat{M_1}$$

and analogously,

$$\widehat{D_2}^2 = |D_2|\widehat{1} + n_2|D_2||D_1|^{-1}\widehat{D_1} + s_2\widehat{D_2} + \widehat{M_2}$$

for some $s_i \in \mathbb{N}$ and $\widehat{M_i}$ such that $(\widehat{M_i}, \widehat{C}) = 0$ for $C \in \{1, D_j\}$, $i, j, \in \{1, 2\}$.

We distinguish two subcases depending on whether $M_1 = \emptyset$ or not.

Step 3: *If $M_1 = \emptyset$, then $\langle D_1 \rangle$ is p-elementary abelian, so the theorem is proved.*

If $M_1 = \emptyset$, then either $D_1^2 = 1 \cup D_1 \cup D_2$ or $D_1^2 = 1 \cup D_2$. In the first case, $D_1^3 = 1 \cup D_1 \cup D_2$ and in the second $D_1^4 = 1 \cup D_1 \cup D_2$, so in both cases it certainly follows that $\langle D_1 \rangle = 1 \cup D_1 \cup D_2$. Hence, joint with the fact that $\langle D_1 \rangle = \langle D_2 \rangle$, we deduce that $\langle D_1 \rangle$ is a minimal normal subgroup of G. Furthermore, it must be solvable due to the fact that its elements only have two possible orders. Consequently, $\langle D_1 \rangle$ is p-elementary abelian for some prime p, so the thesis of the theorem trivially follows.

Henceforth, we will assume that $M_1 \neq \emptyset$.

Step 4: *We have*

$$n_1\widehat{M_1} = n_1|D_1||D_2|^{-1}\widehat{M_2} + \widehat{M_1}\widehat{D_2} - (\widehat{M_1}\widehat{D_2}, \widehat{D_2})\widehat{D_2}$$
$$n_2\widehat{M_2} = n_2|D_2||D_1|^{-1}\widehat{M_1} + \widehat{M_2}\widehat{D_1} - (\widehat{M_2}\widehat{D_1}, \widehat{D_1})\widehat{D_1}.$$

By applying Steps 1 and 2,

$$\widehat{D_1}(\widehat{D_1}\widehat{D_2}) = \widehat{D_1}(n_1\widehat{D_1} + n_2\widehat{D_2}) = n_1(|D_1|\widehat{1} + n_1|D_1||D_2|^{-1}\widehat{D_2} + s_1\widehat{D_1} + \widehat{M_1}) + n_2(n_1\widehat{D_1} + n_2\widehat{D_2})$$

and

$$\begin{aligned}\widehat{D_1}^2\widehat{D_2} &= (|D_1|\widehat{1} + n_1|D_1||D_2|^{-1}\widehat{D_2} + s_1\widehat{D_1} + \widehat{M_1})\widehat{D_2} \\ &= |D_1|\widehat{D_2} + n_1|D_1||D_2|^{-1}(|D_2|\widehat{1} + n_2|D_2||D_1|^{-1}\widehat{D_1} + s_2\widehat{D_2} + \widehat{M_2}) \\ &\quad + s_1(n_1\widehat{D_1} + n_2\widehat{D_2}) + \widehat{M_1}\widehat{D_2}.\end{aligned}$$

Since $\widehat{D_1}(\widehat{D_1}\widehat{D_2}) = \widehat{D_1}^2\widehat{D_2}, 0 = (\widehat{M_1}\widehat{D_2}, \widehat{1})$ and

$$(\widehat{M_1}\widehat{D_2}, \widehat{D_1}) = |M_1||D_1|^{-1}(\widehat{M_1}, \widehat{D_1}\widehat{D_2}) = 0,$$

then

$$n_1\widehat{M_1} = n_1|D_1||D_2|^{-1}\widehat{M_2} + \widehat{M_1}\widehat{D_2} - (\widehat{M_1}\widehat{D_2}, \widehat{D_2})\widehat{D_2}.$$

Similarly we get

$$n_2\widehat{M_2} = n_2|D_2||D_1|^{-1}\widehat{M_1} + \widehat{M_2}\widehat{D_1} - (\widehat{M_2}\widehat{D_1}, \widehat{D_1})\widehat{D_1}.$$

Step 5: *Conclusion.*

First, let us see that $\langle D_1 \rangle$ is solvable. By applying Step 4, we have

$$\begin{aligned}n_1n_2\widehat{M_2} &= n_1n_2|D_2||D_1|^{-1}\widehat{M_1} + n_1(\widehat{M_2}\widehat{D_1} - (\widehat{M_2}\widehat{D_1}, \widehat{D_1})\widehat{D_1}) \\ &= n_2|D_2||D_1|^{-1}(n_1|D_1||D_2|^{-1}\widehat{M_2} + \widehat{M_1}\widehat{D_2} - (\widehat{M_1}\widehat{D_2}, \widehat{D_2})\widehat{D_2}) \\ &\quad + n_1\widehat{M_2}\widehat{D_1} - n_1(\widehat{M_2}\widehat{D_1}, \widehat{D_1})\widehat{D_1}.\end{aligned}$$

It follows that $n_2|D_2||D_1|^{-1}\widehat{M_1}\widehat{D_2} + n_1\widehat{M_2}\widehat{D_1} = l_1\widehat{D_1} + l_2\widehat{D_2}$ for $l_1, l_2 \in \mathbb{N}$. In particular, $\widehat{M_1}\widehat{D_2} = m_1\widehat{D_1} + m_2\widehat{D_2}$ for $m_1, m_2 \in \mathbb{N}$. As we know $(\widehat{M_1}\widehat{D_2}, \widehat{D_1}) = 0$, then $\widehat{M_1}\widehat{D_2} = m_2\widehat{D_2}$. Symmetrically, $\widehat{M_2}\widehat{D_1} = m_1\widehat{D_1}$. Hence, taking into account Step 4 and the definition of M_1, we obtain $n_1\widehat{M_1} = n_1|D_1||D_2|^{-1}\widehat{M_2}$. Thus, $M_1 = M_2$, as sets that are union of conjugacy classes, so we have $D_1M_1 = D_1$. As a result, $D_1\langle M_1\rangle = D_1$. Then, as either $D_1^2 = 1 \cup D_2 \cup D_1 \cup M_1$ or $D_1^2 = 1 \cup D_2 \cup M_1$, we easily deduce that $\langle D_1\rangle = 1 \cup D_2 \cup D_1 \cup M_1$.

We write $\overline{G} = G/\langle M_1\rangle$ and then $\langle\overline{D_1}\rangle = \overline{1} \cup \overline{D_1} \cup \overline{D_2}$. By induction, the elements in $\overline{D_1}$ and $\overline{D_2}$ are p-elements for some prime p, so $\langle\overline{D_1}\rangle$ is a p-group. Let $d \in D_1$. As all elements in $d\langle M_1\rangle$ are conjugate in G, then $\langle M_1\rangle$ is solvable by Theorem A(a). It clearly follows that $\langle D_1\rangle$ is solvable. Finally let us prove that the elements in D_1 and D_2 are p-elements too. Let $1 \neq P \in \mathrm{Syl}_p(\langle D_1\rangle)$. Note that $\langle D_1\rangle = P\langle M_1\rangle = P\langle M_1\rangle D_1 = PD_1$. In particular, we can write $1 = xd$ with $x \in P$ and $d \in D_1$. This shows that the elements in D_1 are p-elements. Analogously, we can deduce that the elements in D_2 are also p-elements. By Theorem A(b), we conclude that $\langle M_1\rangle$, and then also $\langle D_1\rangle$, has normal p-complement. □

Examples. We show different examples corresponding to distinct cases of Theorem A.

1. The easiest example is the dihedral group of order 10, in which the only two conjugacy classes of size 2 satisfy the hypotheses of the theorem. This example can be generalized by taking $G = \langle x\rangle \rtimes \langle a\rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_{(p-1)/2}$, where p is a prime such that $p \equiv 1 \pmod 4$ and a is an automorphism of order $(p-1)/2$ of $\langle x\rangle$. The subgroup $\langle x\rangle$ contains exactly the trivial class and two (real) conjugacy classes A and B of size $(p-1)/2$, which satisfy $AB = A \cup B$ and $\langle A\rangle = \langle x\rangle$. This corresponds to the case $M_1 = \emptyset$ in Step 3 of the proof of Theorem A.
2. Two examples with $\langle A\rangle$ non-cyclic are the following. Let $G = (\langle x\rangle \times \langle y\rangle) \rtimes \langle a\rangle \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_4$, where a is defined by: $x^a = x^2y$, $y^a = xy$. If we take $A = \{x, x^2y, x^2, xy^2\}$ and $B = \{y, xy, y^2, x^2y^2\}$, then we have $AB = A \cup B$ and $\langle A\rangle = \langle B\rangle = \langle x\rangle \times \langle y\rangle$. On the other hand, the group of the library of the small groups of GAP [10] with number $\mathrm{Id}(1176, 213)$ has two conjugacy classes A and B of size 24 satisfying the hypotheses of Theorem A, with $\langle A\rangle \cong \mathbb{Z}_7 \times \mathbb{Z}_7$. Also in both examples $M_1 = \emptyset$.
3. The group $\mathrm{Id}(108, 15)$ has two conjugacy classes A and B of size 12 satisfying $AB = A \cup B$ with $\langle A\rangle \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3$. This example shows that $\langle A\rangle$ is not necessarily abelian. We remark that this example corresponds to the case $M_1 \neq \emptyset$ in the proof of Theorem A (see Step 4). In fact, $\langle M_1\rangle = \mathbf{Z}(\langle A\rangle)$.
4. The smallest group that we have found with the help of [10] satisfying the hypothesis of Theorem A and $\langle A\rangle$ not being a p-group is $\mathrm{Id}(480, 1188)$. Its structure description is $(((\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_5) \rtimes \mathbb{Z}_2) \rtimes \mathbb{Z}_3$ and has two conjugacy classes A and B of size 32 of elements of order 5, such that $AB = A \cup B$ and $\langle A\rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_5$, which is 5-nilpotent but not a 5-group.

As we said in the introduction, to prove Theorem B we make a slight improvement of Theorem D of [4] by proving p-nilpotency.

Theorem 3.1. *Let G be a group and let $K = x^G$ be a conjugacy class of G. If $K^2 = K \cup K^{-1}$, then $\langle K\rangle$ is solvable. Moreover, x is a p-element for some prime p and $\langle K\rangle$ is p-nilpotent.*

Proof. Following the proof of Theorem D of [4] we have $KK^{-1} = 1 \cup K \cup K^{-1} \cup S$ where S is union of conjugacy classes of G other than 1, K and K^{-1}. If $S = \emptyset$, by the proof given in [4] we have that $\langle K \rangle$ is p-elementary abelian for some prime p and the theorem is proved. If $S \neq \emptyset$, again by following the quoted proof, $KS = K$, $\langle K \rangle / \langle S \rangle$ is p-elementary abelian for some prime p and x is a p-element. In particular, the elements of $x\langle S \rangle$ are all conjugate in G and, by applying Theorem A(b), $\langle S \rangle$ has normal p-complement. Since $\langle K \rangle / \langle S \rangle$ is a p-group, then $\langle K \rangle$ has normal p-complement too. □

Theorem B. *Let D_1 and D_2 be conjugacy classes of a finite group G and suppose that $D_1D_2 = D_1^{-1} \cup D_2$ with $D_1 \neq D_1^{-1}$. Then $D_1 = D_2$ and $\langle D_1 \rangle$ is solvable. Moreover, D_1 is a class of p-elements and $\langle D_1 \rangle$ is p-nilpotent.*

Proof. By arguing by induction on $|G|$ as at the beginning of the proof of Theorem B, we can easily deduce that $\langle D_1 \rangle = \langle D_2 \rangle$.

If $D_1 = D_2$, by Theorem 3.1 we have that $\langle D_1 \rangle$ is solvable, the elements of D_1 are p-elements, and $\langle D_1 \rangle$ is p-nilpotent. To complete the proof, in the following, we will prove by minimal counterexample that there do not exist distinct classes D_1 and D_2 in a finite group satisfying the hypotheses of the theorem. Let G be a finite group of minimal order and let D_1 and D_2 two conjugacy classes such that $D_1D_2 = D_1^{-1} \cup D_2$, with D_1 non-real and $D_1 \neq D_2$. We write $\widehat{D_1}\widehat{D_2} = n_1\widehat{D_1^{-1}} + n_2\widehat{D_2}$ with $n_1, n_2 \in \mathbb{N}^*$. We distinguish two cases: first, $D_2 = D_2^{-1}$ and second $D_2 \neq D_2^{-1}$.
Case 1: $D_2 = D_2^{-1}$.
Step 1.1: *We have*

$$\begin{aligned} \widehat{D_1}^2 &= n_1\widehat{D_2} + n_2\widehat{D_1} \\ \widehat{D_1^{-1}}\widehat{D_1} &= \widehat{D_2}^2 \\ \widehat{D_2}^2 &= |D_2|\widehat{1} + n_2(\widehat{D_1} + \widehat{D_1^{-1}}) + \widehat{L} \end{aligned}$$

with $L = L^{-1}$, $0 = (\widehat{L}, \widehat{C})$ *for* $C \in \{1, D_1, D_1^{-1}, D_2\}$.

Follow Steps c(1)(i), c(1)(ii), c(1)(iii) and c(1)(iv) of the proof of Theorem 2 of [1]. We remark that the proof of these properties do not need to assume that G is simple (as assumed in the quoted theorem).

Step 1.2: *We have* $\widehat{D_1^{-1}}\widehat{D_2} = n_1\widehat{D_1} + n_2\widehat{D_2}$.

Since $\widehat{D_1}\widehat{D_2} = n_1\widehat{D_1^{-1}} + n_2\widehat{D_2}$ and $\widehat{D_2} = \widehat{D_2^{-1}}$, we have $\widehat{D_1^{-1}}\widehat{D_2} = \widehat{D_1^{-1}}\widehat{D_2^{-1}} = n_1\widehat{D_1} + n_2\widehat{D_2^{-1}} = n_1\widehat{D_1} + n_2\widehat{D_2}$.
Step 1.3: $L \neq \emptyset$.

If $L = \emptyset$, then $D_2^2 = 1 \cup D_1 \cup D_1^{-1}$ and since D_2 is real, by Lemma 2.2, D_1 is also real, a contradiction.
Step 1.4: *Conclusion.*

We know, by Step 1.1,

$$\begin{aligned} \widehat{D_2}^2\widehat{D_1} &= (|D_2|\widehat{1} + n_2(\widehat{D_1} + \widehat{D_1^{-1}}) + \widehat{L})\widehat{D_1} \\ &= |D_2|\widehat{D_1} + n_2\widehat{D_1}^2 + n_2\widehat{D_2}^2 + \widehat{L}\widehat{D_1} \end{aligned}$$

and, by applying Step 1.2,

$$\widehat{D_2}(\widehat{D_1}\widehat{D_2}) = \widehat{D_2}(n_1\widehat{D_1^{-1}} + n_2\widehat{D_2}) = n_1(n_1\widehat{D_1} + n_2\widehat{D_2}) + n_2\widehat{D_2}^2.$$

Hence

$$|D_2|\widehat{D_1} + n_2(n_1\widehat{D_2} + n_2\widehat{D_1}) + \widehat{L}\widehat{D_1} = n_1^2\widehat{D_1} + n_1n_2\widehat{D_2}.$$

Thus $(|D_2| + n_2^2)\widehat{D_1} + \widehat{L}\widehat{D_1} = n_1^2\widehat{D_1}$. It follows that $\widehat{L}\widehat{D_1} = k\widehat{D_1}$ for some $k \in \mathbb{N}^*$. As a consequence, there exists a conjugacy class C of G other than 1, D_1, D_1^{-1} and D_2 such that $D_1C = D_1$. Thus, $D_1\langle C\rangle = D_1$, with $1 \neq \langle C\rangle \trianglelefteq G$ and we write $\overline{G} = G/\langle C\rangle$. We have $|\overline{G}| < |G|$, $\overline{D_1D_2} = \overline{D_1^{-1}} \cup \overline{D_2}$, with $\overline{D_1} \neq \overline{D_1^{-1}}$, because otherwise $D_1 = D_1\langle C\rangle = D_1^{-1}\langle C\rangle = D_1^{-1}$, a contradiction. In addition, $\overline{D_1} \neq \overline{D_2}$ because otherwise $D_1 = D_1\langle C\rangle = D_2\langle C\rangle \supseteq D_2$, which is impossible. By minimality, we get a contradiction and this case is finished.

Case 2: $D_2 \neq D_2^{-1}$.

We have

$$0 = (\widehat{D_1}\widehat{D_2}, \widehat{D_1}) = \frac{|D_2|}{|D_1|}(\widehat{D_1}\widehat{D_1^{-1}}, \widehat{D_2^{-1}}) = \frac{|D_2|}{|D_1|}(\widehat{D_1}\widehat{D_1^{-1}}, \widehat{D_2}) = (\widehat{D_1}\widehat{D_2^{-1}}, \widehat{D_1})$$

$$0 = (\widehat{D_1}\widehat{D_2}, \widehat{D_2^{-1}}) = \frac{|D_1|}{|D_2|}(\widehat{D_2}^2, \widehat{D_1^{-1}})$$

$$n_1 = (\widehat{D_1}\widehat{D_2}, \widehat{D_1^{-1}}) = \frac{|D_2|}{|D_1|}(\widehat{D_1}^2, \widehat{D_2^{-1}})$$

$$n_2 = (\widehat{D_1}\widehat{D_2}, \widehat{D_2}) = (\widehat{D_1}\widehat{D_2^{-1}}, \widehat{D_2^{-1}}) = \frac{|D_1|}{|D_2|}(\widehat{D_2}\widehat{D_2^{-1}}, \widehat{D_1^{-1}}).$$

We denote by

$$\begin{aligned} l_1 &= (\widehat{D_1}\widehat{D_2^{-1}}, \widehat{D_1^{-1}}) = \frac{|D_2|}{|D_1|}(\widehat{D_1}^2, \widehat{D_2}), \\ l_2 &= (\widehat{D_1}\widehat{D_2^{-1}}, \widehat{D_2}) = \frac{|D_1|}{|D_2|}(\widehat{D_2}^2, \widehat{D_1}) \\ j_1 &= (\widehat{D_1}^2, \widehat{D_1}) = (\widehat{D_1}\widehat{D_1^{-1}}, \widehat{D_1}), \\ j_2 &= (\widehat{D_2}^2, \widehat{D_2}) = (\widehat{D_2}\widehat{D_2^{-1}}, \widehat{D_2^{-1}}) \\ d_1 &= (\widehat{D_1}^2, D_1^{-1}), \\ d_2 &= (\widehat{D_2}^2, D_2^{-1}). \end{aligned}$$

Therefore, we can collect all these multiplicities in Table 1, which also appears in the proof given by Arad and Fisman.

In Table 1, we have $N_i = N_i^{-1}$ and $(\widehat{L}, \widehat{C}) = 0$ for $C \in \{1, D_k, D_k^{-1}\}$, $L \in \{M_{ij}, N_i\}$ for every $k, i, j \in \{1, 2\}$.

Step 2.1: $n_1\widehat{N_1} = n_1\dfrac{|D_1|}{|D_2|}\widehat{N_2}$ *and* $\widehat{N_2}\widehat{D_1} = (\widehat{N_2}\widehat{D_1}, \widehat{D_1})\widehat{D_1}$.

Follow Steps c(2)(i) to (vii) of the proof of Theorem 2 of [1]. We remark again that the assumption of simplicity of G in that theorem is not needed to prove these properties.

Table 1. Multiplicities of D_1 and D_2 and their inverse classes in their respective products

	$\widehat{1}$	$\widehat{D_1}$	$\widehat{D_1^{-1}}$	$\widehat{D_2}$	$\widehat{D_2^{-1}}$	
$\widehat{D_1}\widehat{D_2}$	0	0	n_1	n_2	0	
$\widehat{D_1}\widehat{D_2^{-1}}$	0	0	l_1	l_2	n_2	$\widehat{M_{12}}$
$\widehat{D_1}^2$	0	j_1	d_1	$l_1\dfrac{\lvert D_1\rvert}{\lvert D_2\rvert}$	$n_1\dfrac{\lvert D_1\rvert}{\lvert D_2\rvert}$	$\widehat{M_{11}}$
$\widehat{D_2}^2$	0	$l_2\dfrac{\lvert D_2\rvert}{\lvert D_1\rvert}$	0	j_2	d_2	$\widehat{M_{22}}$
$\widehat{D_1}\widehat{D_1^{-1}}$	$\lvert D_1\rvert$	j_1	j_1	0	0	N_1
$\widehat{D_2}\widehat{D_2^{-1}}$	$\lvert D_2\rvert$	$n_2\dfrac{\lvert D_2\rvert}{\lvert D_1\rvert}$	$n_2\dfrac{\lvert D_2\rvert}{\lvert D_1\rvert}$	j_2	j_2	N_2

Step 2.2: *Conclusion.*

We distinguish two cases, whether $\widehat{N_2} \neq 0$ or not. First, if $\widehat{N_2} \neq 0$, then there exists a conjugacy class C of G such that $D_1C = D_1$. We can apply the same argument as at the end of Step 1.4 of Case 1 and, by minimal counterexample, we get a contradiction.

Assume now that $\widehat{N_2} = 0$. By Step 2.1, we know that

$$n_1\widehat{N_1} = n_1\frac{|D_1|}{|D_2|}\widehat{N_2}.$$

Therefore, $\widehat{N_1} = 0$. Thus, from Table 1, we have $D_1D_1^{-1} = 1 \cup D_1 \cup D_1^{-1}$ and by Theorem C, we conclude that $\langle D_1\rangle = D_1D_1^{-1} = 1 \cup D_1 \cup D_1^{-1}$. This forces that $D_2 = D_1^{-1}$ or $D_2 = D_1$ and both certainly are contradictions. This finishes the proof. □

Examples. This is an example of Theorem B where $\langle A\rangle$ is p-nilpotent and not a p-group. We take the group $G = ((\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_7) \rtimes \mathbb{Z}_3 = \mathrm{Id}(168, 43)$ which has a conjugacy class A of elements of order 7 and size 24 satisfying $A^2 = A \cup A^{-1}$. Also, $\langle A\rangle = (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_7$.

Acknowledgements

The authors thank the referee for careful reading that helped to improve the manuscript. This research is partially supported by Ministerio de Ciencia, Innovación y Universidades, Proyecto PGC2018-096872-B-I00 and by Generalitat Valenciana, Proyecto CIAICO/2021/163. The first-named author is also supported by the National Nature Science Fund of China (No. 12071181) and by Proyecto UJI-B2019-03.

Funding Information Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

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

[2] Arad, Z., Fisman, E., Muzychuk, M.: Order evaluation of products of subsets in finite groups and its applications. I. J. Algebra **182**(3), 577–603 (1996)

[3] Arad, Z., Muzychuk, M.: Order evaluation of products of subsets in finite groups and its applications. II. Trans. Am. Math. Soc. **349**(11), 4401–4414 (1997)

[4] Beltrán, A., Camina, R.D., Felipe, M.J., Melchor, C.: Powers of conjugacy classes in a finite group. Ann. Mat. Pura Appl. **199**(2), 409–424 (2020)

[5] Beltrán, A., Felipe, M.J., Melchor, C.: Multiplying a conjugacy class by its inverse in a finite group. Isr. J. Math. **227**(2), 811–825 (2018)

[6] Beltrán, A., Felipe, M.J., Melchor, C.: Squares of real conjugacy classes in finite groups. Ann. Mat. Pura Appl. **197**(2), 317–328 (2018)

[7] Camina, R.D.: Applying combinatorial results to products of conjugacy classes. J. Group Theory **23**(5), 917–923 (2020)

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

[9] Huppert, B.: Character Theory of Finite Groups. Walter de Gruyter, Berlin (1998)

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

Antonio Beltrán
Departamento de Matemáticas
Universitat Jaume I
12071 Castellón
Spain
e-mail: abeltran@uji.es

María José Felipe
Instituto de Matemática Pura y Aplicada
Universitat Politècnica de València
46022 Valencia
Spain
e-mail: mfelipe@mat.upv.es

Carmen Melchor
Departamento de Didáctica de la Matemática
Universitat de València
Valencia
Spain
e-mail: Carmen.Melchor-Borja@uv.es

Received: May 13, 2021.
Revised: March 11, 2022.
Accepted: September 27, 2022.