

Universitat Jaume I
Escola de Doctorat



UNIVERSITAT
JAUME • **I**

CONJUGACY CLASSES AND NORMAL SUBGROUPS IN FINITE GROUPS

AUTHOR

Carmen Melchor Borja

ADVISORS

Dr. Antonio Beltrán Felip

Dr. María José Felipe Román

Castelló de la Plana, Desembre 2018



Programa de doctorat en Ciències
Escola de Doctorat de la Universitat Jaume I

CONJUGACY CLASSES AND NORMAL SUBGROUPS IN FINITE GROUPS

*Memòria presentada per Carmen Melchor Borja per a optar al
grau de doctora per la Universitat Jaume I*

DOCTORANDA:
Carmen Melchor Borja

DIRECTORS:
Dr. Antonio Beltrán Felip
Dra. María José Felipe Román

Castelló de la Plana, Desembre 2018

FINANÇAMENT REBUT

- Ajuda predoctoral per a la formació de personal investigador 2015 del Pla de Promoció de la Investigació de la Universitat Jaume I: PREDOC/2015/46.
- Beca per a realitzar estades temporals en altres centres d'investigació, per al personal docent i investigador 2017 del programa de mobilitat del personal investigador de la Universitat Jaume I: E-2017-02.

Als meus pares i a Alejandro

Acknowledgments

May the reader forgive me the discourtesy of following my wish to write the acknowledgements in my mother tongue.

En primer lugar quisiera dar las gracias a mi director de tesis Antonio Beltrán por la formación que me ha dado, por su tiempo, por sus consejos y por todas las conversaciones que hemos tenido. Tanta ayuda en tantos aspectos es un regalo. Gracias también a María José, mi codirectora, por su dedicación a nuestro trabajo, por su esfuerzo para coordinarnos y por todas sus valiosas palabras. Gracias a ellos dos ha sido posible este trabajo.

Por otra parte, quiero mostrar mi especial agradecimiento, por su compañerismo, a los miembros del Departamento de Matemáticas de la Universitat Jaume I, en el cual he trabajado como becaria financiada por el *Pla de promoció de la investigació de la Universitat Jaume I per a l'any 2015*. También quiero mencionar a los miembros del Departamento de Educación de la UJI, donde comencé mi andadura universitaria. Aún estando fuera del departamento siempre me han mostrado su apoyo y amistad y por ello me siento muy agradecida. Además, durante estos años he convivido con otros estudiantes de máster y doctorado con quienes he compartido muy buenas experiencias e inquietudes. A ellos y ellas, gracias. También quiero mencionar a las personas del Instituto Universitario de Matemática Pura y Aplicada de la Universitat Politècnica de València y del Departamento de Matemáticas de la Universitat de València que, junto con Antonio y conmigo, formamos y sentimos un equipo. Durante este tiempo me han mostrado su acogida y apoyo y por ello les doy las gracias. En especial, agradezco las estancias que he realizado en el IUMPA y la buena gente con la que allí he convivido.

I would also like to thank the Department of Pure Mathematics and Mathematical Statistics of the University of Cambridge for my stay. In particular, I greatly thank Rachel Camina for giving me the opportunity to visit her department, her hospitality and the work together. My stay in Cambridge was wonderful, thanks to Polly and her lovely family and friends. Thank you for taking care of me, I miss you. Esta estancia fue financiada con una beca para la movilidad del personal investigador del *Pla de promoció de la investigació de la Universitat Jaume I per a l'any 2017*.

Finalitze els agraïments amb els qui més m'estime. Als amics que sempre estan, pel suport. Al meu amor *Forky*, per acompanyar-me sempre, per tanta paciència i per tantíssima estima. Als meus infinitament estimats pares Juan i Lolita, per donar-m'ho tot sempre.

Contents

| | |
|---|------------|
| Acknowledgments | iii |
| Introducción | vii |
| Introduction | xi |
| I Conjugacy classes contained in normal subgroups | 1 |
| 1 Graphs associated to conjugacy classes of normal subgroups | 3 |
| 1.1 Introduction | 3 |
| 1.2 Number of connected components of $\Gamma_G(N)$ and $\Gamma_G^*(N)$ | 5 |
| 1.3 Diameter of $\Gamma_G(N)$ | 6 |
| 1.4 Diameter of $\Gamma_G^*(N)$ | 10 |
| 1.5 Structure of N in the disconnected case | 11 |
| 2 Normal subgroups whose conjugacy class graph has diameter three | 15 |
| 2.1 Introduction | 15 |
| 2.2 Proofs | 16 |
| 3 Triangles in the graph of conjugacy classes of normal subgroups | 23 |
| 3.1 Introduction | 23 |
| 3.2 Preliminary results | 25 |
| 3.3 $\Gamma_G(N)$ with one vertex | 26 |
| 3.4 $\Gamma_G(N)$ with two vertices | 26 |
| 3.4.1 $\Gamma_G(N)$ with two vertices without edge | 26 |
| 3.4.2 $\Gamma_G(N)$ with two vertices and one edge | 27 |
| 3.5 $\Gamma_G(N)$ with three vertices | 30 |
| 3.5.1 $\Gamma_G(N)$ disconnected with three vertices | 30 |
| 3.5.2 $\Gamma_G(N)$ with exactly one triangle | 31 |
| 3.5.3 $\Gamma_G(N)$ with three vertices connected in a line | 34 |
| 3.6 $\Gamma_G(N)$ without triangles | 36 |
| 4 Landau's theorem on conjugacy classes for normal subgroups | 41 |
| 4.1 Introduction | 41 |
| 4.2 Proof of Theorem A | 43 |
| 4.3 Applications of Theorem A | 44 |

| | | |
|-----------|---|-----------|
| 4.3.1 | Normal subgroups with only one non-central G -class | 45 |
| 4.3.2 | Normal subgroups with two non-central G -classes of coprime sizes | 47 |
| 4.4 | An extension of Landau's theorem for prime-power order elements | 49 |
| II | Products of conjugacy classes | 55 |
| 5 | Squares of real conjugacy classes in finite groups | 57 |
| 5.1 | Introduction | 57 |
| 5.2 | Preliminary results | 59 |
| 5.3 | Proofs | 60 |
| 6 | Multiplying a conjugacy class by its inverse in a finite group | 71 |
| 6.1 | Introduction | 71 |
| 6.2 | Preliminary results and proof of Theorem B | 73 |
| 6.3 | Proof of Theorem A | 76 |
| 6.4 | Proof of Theorem C | 79 |
| 6.5 | Analogous problems for irreducible characters | 80 |
| | Conclusiones y futuros problemas de investigación | 83 |
| | Conclusions and future research problems | 87 |
| | References of the Introduction and Conclusion | 91 |

Introducción

Esta tesis se enmarca dentro del estudio que analiza la influencia de las clases de conjugación en la estructura de grupos finitos. En los últimos treinta y cinco años ésta ha sido una línea de investigación próspera y activa. Los contenidos están divididos en dos partes que recogen un compendio de artículos cada uno de los cuales es un capítulo que tiene exactamente la misma estructura y bibliografía que la versión original publicada. La primera parte consta de cuatro capítulos sobre el tema de grafos de clases de conjugación contenidas en un subgrupo normal y su impacto estructural en este subgrupo. Además, como aplicación de las propiedades de estos grafos, presentamos una versión generalizada del conocido Teorema de Landau para este tipo de clases. Estos capítulos corresponden a los manuscritos [6], [8], [9] y [7] que aparecen en la bibliografía, respectivamente. La segunda parte contiene dos capítulos que tratan sobre la información que el producto de clases de conjugación proporciona acerca de la no simplicidad y la estructura normal de un grupo. Estos capítulos son [11] y [10], respectivamente.

Parte I

En la primera parte, centraremos nuestra atención en las clases de conjugación contenidas en subgrupos normales. Sea N un subgrupo normal de un grupo G . Para cada elemento $x \in N$, la G -clase de conjugación de x es el conjunto de elementos de N que son conjugados a x en G . Cada G -clase de elementos de N es unión de clases de conjugación de N , y se sigue fácilmente que su tamaño es múltiplo de un tamaño de una N -clase. Resultados recientes ponen de manifiesto que el conjunto de tamaños de G -clase mantienen una fuerte influencia en la estructura de N , a pesar de que pueden existir primos que dividen a los tamaños de G -clase que, sin embargo, no dividen al orden de N . Las contribuciones de esta parte de la tesis representan un avance en esta nueva línea de investigación sobre la estructura normal de un grupo finito considerando sus clases de conjugación.

El estudio de grafos de clases de conjugación y de caracteres ha sido muy amplio y continúa siendo una línea de investigación activa. Los resultados más clásicos se encuentran recogidos en los *surveys* de M.L. Lewis en [32] y A.R. Camina y R.D. Camina en [15]. Los artículos [14] y [3] son ejemplos que muestran la actualidad del tema. El origen del estudio de grafos asociados a clases de conjugación se debe a E. A. Bertram, M. Herzog y A. Mann. En 1990, definieron en [13] el grafo $\Gamma(G)$ asociado a los tamaños de las clases de conjugación ordinarias de G como sigue: los vértices de $\Gamma(G)$ están representados por las clases de conjugación no centrales de G y dos vértices están conectados por una arista si sus tamaños tienen un primo divisor

común. Probaron que el número de componentes conexas de $\Gamma(G)$ es a lo sumo 2 y que cuando el grafo es conexo, entonces su diámetro es a lo sumo 4. Además, caracterizaron el caso desconexo, en el que cada componente es un grafo completo, probando que los grupos cuasi-Frobenius con núcleo y complemento abelianos son los únicos cuyos grafos tienen dos componentes conexas. Más tarde, en [22], C. Chillag, Herzog y Mann obtuvieron la mejor cota del diámetro de este grafo cuando es conexo, la cual es 3.

En el Capítulo 1, nos fijamos en las clases de conjugación contenidas en un subgrupo normal N de G y definimos, de manera análoga a $\Gamma(G)$, el grafo $\Gamma_G(N)$, cuyos vértices son las G -clases de N , y es un subgrafo de $\Gamma(G)$. El hecho de que el número de componentes conexas y el diámetro de $\Gamma(G)$ estén acotados no implica directamente que los correspondientes parámetros para $\Gamma_G(N)$ también tengan que estar acotados. También veremos que no hay relación entre $\Gamma(N)$ y $\Gamma_G(N)$ ni entre sus diámetros. Probaremos que el número de componentes conexas de $\Gamma_G(N)$ es a lo sumo 2 y que, en el caso conexo, la mejor cota de su diámetro es 3 y en el caso desconexo cada componente conexa es un grafo completo. Además, para el caso desconexo de $\Gamma_G(N)$ obtenemos que, o bien N es cuasi-Frobenius con núcleo y complemento abelianos, o es el producto directo de un p -grupo y un subgrupo central. Contrariamente al caso ordinario, esto no es una caracterización. En [23], S. Dolfi define el grafo dual de $\Gamma(G)$, denotado $\Gamma^*(G)$, cuyos vértices son los primos divisores de los tamaños de clase de G , y dos vértices p y q están unidos por una arista si existe una clase de conjugación de G cuyo tamaño es múltiplo de pq . En este capítulo también abordamos cuestiones similares para el correspondiente grafo dual de $\Gamma_G(N)$, esto es, el grafo asociado a los primos que dividen a los cardinales de las G -clases de N que denotamos como $\Gamma_G^*(N)$.

Uno de los problemas que se plantean en el estudio de grafos asociados a grupos finitos es analizar la estructura del grupo cuando el diámetro es máximo. En [19], por ejemplo, C. Casolo, S. Dolfi, E. Pacifici y L. Sanus caracterizan el grafo asociado a los grados de los caracteres de los grupos resolubles cuando tiene diámetro 3. En cuanto a clases ordinarias, L.S. Kazarin caracteriza en [30] la estructura de un grupo G con dos "clases aisladas". En particular, Kazarin determinó, como resultado de dicha caracterización, la estructura de los grupos G con diámetro de $\Gamma(G)$ igual a 3. En cuanto a $\Gamma_G(N)$, en el Capítulo 2 se determina la estructura del subgrupo normal N cuando su diámetro es tan grande como es posible, esto es, cuando es igual a 3. Respecto a los grafos duales, en [18], Casolo y Dolfi describen todos los grupos finitos G para los cuales el grafo dual de $\Gamma(G)$ es conexo y tiene diámetro 3. Sin embargo, el problema de determinar la estructura normal cuando el diámetro de $\Gamma_G^*(N)$ es exactamente 3 todavía está abierto.

En el Capítulo 3, presentamos varios resultados en relación a la estructura de los grupos y subgrupos normales en los casos más simples del grafo $\Gamma_G(N)$: cuando consta de exactamente uno, dos o tres vértices. Estas propiedades se utilizan para obtener la estructura del subgrupo normal cuando el grafo de G -clases no tiene triángulos. En todos estos casos, hacemos una comparación entre $\Gamma(G)$ y $\Gamma_G(N)$. Los correspondientes resultados caracterizando el grafo $\Gamma(G)$ cuando no tiene triángulos se encuentran publicados en [24].

En el último capítulo de la primera parte nos centraremos en el estudio del número de clases de conjugación de un grupo en lugar de en sus tamaños. El conocido Teorema de Landau sobre clases de conjugación afirma que hay solo un número finito de grupos finitos, salvo isomorfismo, con exactamente k clases de conjugación para cualquier entero positivo k . En el teorema original, no se proporciona una cota superior en términos de k para el orden de estos grupos, pero pocos años después, M. Newman proporciona en [35] dicha cota. Cuando consideramos clases contenidas en un subgrupo normal N , una cuestión natural es si existe un número finito de grupos con un subgrupo normal tal que es unión de un número fijo de G -clases. La respuesta es negativa si no se fija el índice $|G : N|$. Por el contrario, si se fija el índice, entonces la respuesta es afirmativa y en el Capítulo 4 se proporcionan cotas superiores para $|G|$ y $|N|$ dependiendo del número de G -clases de conjugación no centrales en N (en lugar de todas las G -clases). Además, como aplicación de las propiedades obtenidas para el grafo $\Gamma_G(N)$, clasificamos explícitamente los grupos G con un subgrupo normal N y una o dos G -clases de conjugación no centrales de tamaños coprimos para algunos índices concretos.

En la literatura encontramos muchos resultados sobre cotas logarítmicas para ciertas clases de grupos, por ejemplo, grupos nilpotentes o “ceranos a nilpotentes” [17], o grupos resolubles [16], así como extensiones del resultado de Landau como [29] y [34], en las que solamente se tienen en cuenta clases de conjugación de elementos de orden potencia de primo y de elementos p -regulares, respectivamente. En 2005, L. Héthelyi y B. Külshammer [29] probaron una extensión del Teorema de Landau para elementos de orden potencia de primo. No dieron, sin embargo, una expresión numérica de la cota superior del orden del grupo. En el Capítulo 4, proporcionamos una función explícita de dicha cota para grupos resolubles y elementos de orden potencia de primo. Además, volviendo al estudio de G -clases, también proporcionamos una extensión del Teorema de Landau para elementos de orden potencia de primo contenidos en un subgrupo normal. No obstante, veremos que dicha extensión no se puede restringir solamente a G -clases de conjugación no centrales de elementos de orden potencia de primo contenidas en un subgrupo normal N de G . Esto ocurre porque se puede ver fácilmente que $|N|$ y $|G|$ no pueden acotarse en términos del número de éstas clases aunque el índice esté fijado.

Parte II

La segunda parte de esta tesis se dedica al estudio de la estructura normal de un grupo finito considerando la información proporcionada por el número de clases de conjugación que aparecen en el producto de clases. Un subconjunto X de G se dice que es G -invariante si $X^g = \{x^g \mid x \in X\} = X$ para todo $g \in G$, y en este caso, X es siempre unión de clases de conjugación. Escribimos $\eta(X)$ para denotar el número de clases de conjugación diferentes que aparecen en X . En particular, el producto de dos clases de conjugación A y B de G es un conjunto G -invariante. Existen algunos resultados sobre la estructura de un grupo finito respecto a $\eta(AB)$, algunos de los cuales están relacionados con la resolubilidad o no simplicidad del grupo. Por ejemplo, cuando $\eta(AB) = 2$, Arad y Fisman obtuvieron en [4], trabajando en el álgebra compleja de grupo $\mathbb{C}[G]$, la no simplicidad de un grupo bajo la hipótesis de que el

producto de dos clases de conjugación A y B es exactamente la unión de estas dos clases o sus inversas.

En [5], Z. Arad y M. Herzog conjeturan uno de los problemas más significativos sobre productos de clases de conjugación, esto es, si existen dos clases de conjugación A y B en un grupo G tales que $\eta(AB) = 1$, entonces G no es un grupo simple no abeliano. Esta conjetura todavía sigue abierta aunque ha sido verificada para muchas familias de grupos simples. Fue comprobada en [5] para los grupos alternados, los grupos Suzuki, $\mathrm{PSL}_2(q)$, los grupos simples no abelianos de orden menor que un millón, y 15 de los 26 grupos simples esporádicos. Más tarde, usando una caracterización del hecho de que el producto de dos clases es una clase en términos de caracteres, J. Moori y H.P. Tong-Viet probaron en [33] la conjetura para más familias de grupos simples. En realidad, esta caracterización puede utilizarse para probarla para todos los grupos simples esporádicos y todos los grupos simples cuya tabla de caracteres sea conocida. Más recientemente, R. Guralnick, G. Malle y P.H. Tiep validaron en [27] la conjetura de Arad y Herzog en varios casos más de grupos simples algebraicos. Además, un caso particular de la conjetura de Arad y Herzog ha sido probado recientemente por G. Navarro and Guralnick en [28] considerando el cuadrado de una clase de conjugación, aunque el resultado aportó más información. Obtuvieron, utilizando la Clasificación de los Grupos Finitos Simples (CGFS), la resolubilidad de $\langle K \rangle$, siendo K una clase que satisface que K^2 es clase.

Recordemos que una clase de conjugación K se dice que es real si $K = K^{-1}$. Inspirados por el anterior resultado de Guralnick y Navarro, observamos que si K es una clase de conjugación real no trivial de G , se sigue trivialmente que K^2 nunca puede ser una clase de conjugación a menos que K conste de una única involución central de G . En el Capítulo 5, estudiamos el caso más simple cuando consideramos una clase real K , esto es, K^2 es la unión de la clase trivial y otra clase. Obtenemos que entonces el subgrupo $\langle K \rangle$ es resoluble. Las técnicas para probar este resultado son bastante elementales aunque utilizamos el teorema Z^* de Glauberman [26] y un resultado de Y. Berkovich y L. Kazarin [12]. Ambos requieren herramientas de la teoría modular de representaciones, luego nuestro resultado principal también está basado en ellas. Remarcamos, sin embargo, que no utilizamos la CGFS a diferencia del resultado de Guralnick y Navarro.

En el Capítulo 6 consideramos otro caso relevante a estudiar sobre el producto de una clase de conjugación por su inversa. Los primeros resultados en esta situación fueron obtenidos para grupos superresolubles, grupos nilpotentes y p -grupos por Adan-Bante en [1] y [2]. Nos preguntamos qué ocurre en general cuando $\eta(KK^{-1}) = 2$ o $\eta(KK^{-1}) = 3$ para cualquier grupo G . En este capítulo, estudiamos el caso $\eta(KK^{-1}) = 2$ y obtenemos la no simplicidad del grupo y conjeturamos que $\langle K \rangle$ y $\langle KK^{-1} \rangle$ son resolubles. Sin embargo, solo hemos podido probarlo en algunos casos particulares. Si continuamos con el estudio de KK^{-1} observamos que el hecho de que $\eta(KK^{-1}) = 3$ no implica que $\langle K \rangle$ o $\langle KK^{-1} \rangle$ sea resoluble. En realidad, veremos que $\langle KK^{-1} \rangle$ puede ser incluso simple. Sin embargo, estudiamos el caso particular en que $KK^{-1} = 1 \cup D \cup D^{-1}$ con D una clase de conjugación de G , y demostramos que G no puede ser simple utilizando la teoría de caracteres y la CGFS. También en este caso, la resolubilidad de $\langle K \rangle$ ha quedado como cuestión abierta.

Introduction

This thesis is framed within the study that analyzes the influence of the conjugacy classes on the structure of finite groups. Over the last thirty five years this has been a flourishing and active line of research. The contents are divided into two parts each of which compiles a compendium of papers being each of them a chapter having exactly the same structure and biography as the original published version. The first part consists of four chapters about the topic of graphs of conjugacy classes contained in a normal subgroup and their structural impact in such subgroup. Furthermore, as an application of the properties of these graphs, we present a generalized version of the well-know Landau Theorem for such classes. These chapters correspond to the manuscripts [6], [8], [9] and [7] appearing in the bibliography, respectively. The second part contains two chapters about the information that the product of conjugacy classes provides about the non-simplicity and normal structure of a group. These chapters are [11] and [10], respectively.

Part I

In the first part, we will focus our attention on the conjugacy classes contained in normal subgroups. Let N be a normal subgroup of a group G . For each element $x \in N$, the G -conjugacy class of x is the set of elements of N which are conjugate to x in G . Each G -class of elements of N is the join of conjugacy classes of N , and it easily follows that its size is a multiple of a single N -class size. Recent results put forward that the set of G -class sizes continues to maintain a strong influence on the structure of N , in spite of the fact that there may exist primes dividing the G -class sizes that, however, do not divide the order of N . The contributions of this part of the thesis represent an advance in this new line of research about the normal structure of a finite group considering its conjugacy classes.

The study of graphs of conjugacy classes and characters has been very wide and it continues being an active line of research. The most classical results are included in the surveys of M.L. Lewis in [32] and A.R. Camina and R.D Camina in [15]. The papers [14] and [3] are examples showing that this is a current topic. The origin of the study of graphs associated to conjugacy classes is due to E. A. Bertram, M. Herzog and A. Mann. In 1990, they defined in [13] the graph $\Gamma(G)$ associated to the ordinary conjugacy class sizes of G as follows: the vertices of $\Gamma(G)$ are represented by the non-central conjugacy classes of G and two vertices are connected by an edge if their sizes have a common prime divisor. They proved that the number of connected components of $\Gamma(G)$ is at most 2 and that when the graph is connected, then its diameter is at most 4. Furthermore, they characterize the disconnected case, in

which each component is a complete graph, by proving that quasi-Frobenius groups with abelian kernel and complements are the only groups whose graphs have two connected components. Later, in [22], C. Chillag, Herzog and Mann obtained the best bound of the diameter of this graph when it is connected, which is 3.

In Chapter 1, we look at the conjugacy classes contained in a normal subgroup N of G and we define, analogue to $\Gamma(G)$, the graph $\Gamma_G(N)$, whose vertices are the G -classes of N , and it is a subgraph of $\Gamma(G)$. The fact that the number of connected components and the diameter of $\Gamma(G)$ are bounded does not directly imply that the corresponding parameters for $\Gamma_G(N)$ must be bounded too. We will also see that there is no relation between $\Gamma(N)$ and $\Gamma_G(N)$ nor between their diameters. We will prove that the number of connected components of $\Gamma_G(N)$ is at most 2 and that, in the connected case, the best bound of its diameter is 3 and in the disconnected case each component is a complete graph. Furthermore, for the disconnected case we have that, either N is quasi-Frobenius with abelian kernel and complement, or it is the direct product of a p -group and a central subgroup. On the contrary to the ordinary case, this is not a characterization. In [23], S. Dolfi defines the dual graph of $\Gamma(G)$, denoted by $\Gamma^*(G)$, whose vertices are the primes which occur as divisors of the class sizes of G , and two vertices p and q are joined by an edge if there exists a conjugacy class in G whose size is a multiple of pq . In this chapter we also tackle similar questions for the corresponding dual graph of $\Gamma_G(N)$, that is, the graph associated to the primes that divide the G -class sizes of N that we denote by $\Gamma_G^*(N)$.

One of the raised problems in the study of graphs associated to finite groups is to analyze the structure of the group when the diameter is maximum. In [19], for instance, C. Casolo, S. Dolfi, E. Pacifici and L. Sanus characterize the graph associated to the character degrees of the solvable groups when it has diameter 3. Concerning ordinary classes, L.S. Kazarin characterizes in [30] the structure of a group G having two "isolated classes". Particularly, Kazarin determined, as a result of such characterization, the structure of those groups G with diameter of $\Gamma(G)$ equal to 3. Regarding $\Gamma_G(N)$, in Chapter 2, the structure of the normal subgroup N is determined when its diameter is as large as possible, that is, when it is equal to 3. Concerning the dual graphs, in [18], Casolo and Dolfi describe all finite groups G for which the dual graph of $\Gamma(G)$ is connected and has diameter 3. However, the problem of determining the normal structure when the diameter of $\Gamma_G^*(N)$ is exactly 3 is still open.

In Chapter 3, we present several results in regards to the structure of groups and normal subgroups to the simplest cases of the graph $\Gamma_G(N)$: when it consists of exactly one, two or three vertices. These properties are used to obtain the structure of the normal subgroup when the graph of G -classes has no triangles. In all these cases we make a comparison between $\Gamma(G)$ and $\Gamma_G(N)$. The corresponding results characterizing the graph $\Gamma(G)$ when it has no triangles are published in [24].

In the last chapter of the first part we focus on the study of the number of conjugacy classes of a group instead of in their sizes. The well-known Landau's Theorem on conjugacy classes asserts that there are only finitely many finite groups, up to isomorphism, with exactly k conjugacy classes for any positive integer k . In the original theorem, no upper bound in terms of k for the order of such groups was pro-

vided, but a few years later, M. Newman provides in [35] such bound. When dealing with classes contained in a normal subgroup N , a natural question is whether there exist finitely many groups having a normal subgroup which is the union of a fixed number of G -classes. The answer is negative if the index $|G : N|$ is not fixed. On the contrary, if the index is fixed, then the answer is affirmative and in Chapter 4 we provide upper bounds for $|G|$ and $|N|$ depending on the number of non-central G -classes lying in N (instead of all G -classes). In addition, as an application of the properties obtained for the graph $\Gamma_G(N)$, we explicitly classify the groups G with a normal subgroup N and one or two non-central conjugacy G -classes with coprime sizes for some concrete indices.

In the literature we find many results about logarithmic bounds for certain classes of groups, for instance, nilpotent or “almost nilpotent” groups [17], or solvable groups [16], as well as extensions of Landau’s result, such as [29] and [34], where only conjugacy classes of prime power order elements and of p -regular elements are taken into account, respectively. In 2005, L. Héthelyi and B. Külshammer [29] proved an extension of Landau’s theorem for prime power order elements. They did not give, however, any numerical expression for the upper bound of the group order. In Chapter 4, we provide an explicit function of such bound for solvable groups and elements of prime power order. Furthermore, coming back to the study of G -classes, we also give an extension of Landau’s Theorem for prime power order elements lying in a normal subgroup. However, we will see that we cannot restrict this extension to just non-central G -classes of prime power order elements contained in a normal subgroup N of G . This happens because one can easily see that $|N|$ and $|G|$ cannot be bounded in terms of the number of such classes although the index is fixed.

Part II

The second part of this thesis is devoted to the study of the structure of a finite group by considering the information provided by the number of conjugacy classes appearing in the product of classes. A subset X of G is said to be G -invariant if $X^g = \{x^g \mid x \in X\} = X$ for all $g \in G$, and in this case, X is always union of conjugacy classes. We set $\eta(X)$ to denote the number of distinct conjugacy classes appearing in X . In particular, the product of two conjugacy classes A and B of G , that is, $AB = \{ab \mid a \in A, b \in B\}$, is a G -invariant set. There exist some results about the structure of a finite group regarding $\eta(AB)$, some of which are related to the solvability and non-simplicity of the group. For instance, when $\eta(AB) = 2$, Arad and Fisman obtained in [4], by working on the complex group algebra $\mathbb{C}[G]$, the non-simplicity of a group under the assumption that the product of two conjugacy classes A and B is exactly the union of these two classes or their inverses.

In [5], Z. Arad and M. Herzog conjecture one of the most significant problems about products of conjugacy classes, that is, if there exist two conjugacy classes A and B in a group G such that $\eta(AB) = 1$, then G is not a non-abelian simple group. This conjecture remains open although it has been verified for plenty of families of simple groups. It was checked in [5] for alternating groups, Suzuki groups, $\text{PSL}_2(q)$, non-abelian simple groups of order less than one million, and 15 of the 26 sporadic simple groups. Later, by using a characterization of the fact that the product of two

conjugacy classes is a conjugacy class in terms of characters, J. Moori and H.P. Tong-Viet proved in [33] the conjecture for more families of simple groups. Actually, this characterization can also be used to check it for all the sporadic simple groups and all the simple groups whose character table is known. More recently, R. Guralnick, G. Malle and P.H. Tiep validated in [27] Arad and Herzog's conjecture in several more cases of algebraic simple groups. Furthermore, a particular case of Arad and Herzog's conjecture has been recently proved by G. Navarro and Guralnick in [28] by considering the square of a conjugacy class, although the result goes much further. They obtained, by means of the Classification of the Finite Simple Groups (CFSG), the solvability of $\langle K \rangle$, being K a class satisfying that K^2 is class.

Recall that a conjugacy class K of a group G is said to be real if $K = K^{-1}$. Inspired by the above Guralnick and Navarro's result, we observe that if K is a non-trivial real conjugacy class of G , it trivially follows that K^2 can never be a conjugacy class unless K consists of a single central involution of G . In Chapter 5, we study the simplest case when considering a real class K , that is, K^2 is union of the trivial class and another class. We obtain that then the subgroup $\langle K \rangle$ is solvable. The techniques for proving this result are quite elementary although we make use of Glauberman's Z^* theorem [26] and a result of Y. Berkovich and L. Kazarin [12]. Both require tools from modular representation theory, so our main result is based on it as well. We remark, however, that we do not appeal to the CFSG unlike Guralnick and Navarro's result.

In Chapter 6 we consider another relevant case to study about the product of a conjugacy class by its inverse. The early results in this situation were obtained for supersolvable groups, nilpotent groups and p -groups by Adan-Bante in [1] and [2]. We wonder what happens in general when $\eta(KK^{-1}) = 2$ or $\eta(KK^{-1}) = 3$ for any group G . In this chapter, we study the case $\eta(KK^{-1}) = 2$ and we obtain the non-simplicity of the group and we conjecture that $\langle K \rangle$ and $\langle KK^{-1} \rangle$ are solvable. Nevertheless, we have only been able to prove it in some particular cases. If we continue with the study of KK^{-1} , we observe that the fact that $\eta(KK^{-1}) = 3$ does not imply that $\langle K \rangle$ or $\langle KK^{-1} \rangle$ is solvable. Actually, we will see that $\langle KK^{-1} \rangle$ may be even simple. Nonetheless, 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 character theory and the CFSG. Also in this case, the solvability of $\langle K \rangle$ remains an open question.

Part I

Conjugacy classes contained in normal subgroups

Chapter 1

Graphs associated to conjugacy classes of normal subgroups

Abstract

Let G be a finite group and let N be a normal subgroup of G . We attach to N two graphs $\Gamma_G(N)$ and $\Gamma_G^*(N)$ related to the conjugacy classes of G contained in N and to the set of primes dividing the sizes of these classes, respectively. These graphs are subgraphs of the ordinary ones associated to the conjugacy classes of G , $\Gamma(G)$ and $\Gamma^*(G)$, which have been widely studied by several authors. We prove that the number of connected components of both graphs is at most 2, we determine the best upper bounds for the diameters and characterize the structure of N when these graphs are disconnected.

Keywords. Finite groups, conjugacy classes, normal subgroups, graphs.

Mathematics Subject Classification (2010): 20E45, 20D15.

1.1 Introduction

Let G be a finite group and let N be a normal subgroup of G . For each element $x \in N$, the G -conjugacy class is $x^G = \{x^g \mid g \in G\}$. We will denote by $\text{Con}_G(N)$ the set of conjugacy classes in G of elements of N . The elements in $\text{Con}_G(N)$ are unions of conjugacy classes of N , and it turns out that every G -class size is a multiple of a N -class size. Recent results have showed that the G -class sizes still have a strong influence on the structure of N in spite of the fact that there may exist primes dividing the G -class sizes which, however, do not divide the order of N .

In 1990, E. A. Bertram, M. Herzog and A. Mann introduced in [3] the graph $\Gamma(G)$ associated to the sizes of the ordinary conjugacy classes of G , and later, in [4] the best bound of the diameter of this graph was attained. Our aim is to study the properties of the following subgraph of $\Gamma(G)$ regarding the G -conjugacy classes contained in N and to obtain structural properties of N in the disconnected case.

Definition 1.1.1. *Let G be a finite group and let N be a normal subgroup in G . We define the graph $\Gamma_G(N)$ in the following way: the set of vertices is the set of non-central elements of $\text{Con}_G(N)$, and two vertices x^G and y^G are joined by an edge if and only if $|x^G|$ and $|y^G|$ have a common prime divisor.*

Notice that $\Gamma(N)$ is not a subgraph of $\Gamma_G(N)$ because the set of vertices of $\Gamma(N)$ needs not to be included within the set of vertices of $\Gamma_G(N)$. Moreover, we remark that although $\Gamma_G(N)$ is subgraph of $\Gamma(G)$, the fact that the number of connected components and the diameter of $\Gamma(G)$ are bounded does not directly imply that the corresponding for $\Gamma_G(N)$ have to be bounded too. However, we show that both numbers, denoted by $n(\Gamma_G(N))$ and $d(\Gamma_G(N))$, are actually bounded. It is easy to check that the bounds in Theorems A and B are the best possible bounds.

Theorem A. *Let G a finite group and let N be a normal subgroup of G . Then $n(\Gamma_G(N)) \leq 2$.*

We want to remark that there is no relation between the connectivity of $\Gamma_G(N)$ and $\Gamma(N)$. For instance, $\Gamma(N)$ can be disconnected while $\Gamma_G(N)$ is not. We can use the semilinear affine group $\Gamma(p^n)$ for appropriate p and n in order to see this. Recall that if $GF(p^n)$ is the finite field of p^n elements, then the multiplicative group $H = GF(p^n)^*$ is cyclic of order $p^n - 1$ and acts on the elementary abelian (additive) p -group of $GF(p^n)$, say K . This action is Frobenius, so the corresponding semidirect product KH is a Frobenius group with abelian kernel and complement. Moreover, α , defined by $x^\alpha = x^p$ for all $x \in K$, is an automorphism of K of order n in such a way that $H\langle\alpha\rangle \leq \text{Aut}(K)$. Then $\Gamma(p^n)$ is defined as the semidirect product $K(H\langle\alpha\rangle)$. Now, take $n = 2$ and let S be a cyclic subgroup of H of order $s = 3$ (so we are assuming that 3 divides $p^2 - 1$). We have that $N := KS$ is normal in G and is also a Frobenius group with abelian kernel and complement. Hence $\Gamma(N)$ is disconnected by Theorem 2 of [3]. However, there are exactly two non-trivial G -classes in N consisting in the $p^2 - 1$ elements of $K \setminus \{1\}$, and the $(|S| - 1)|K| = 2p^2$ elements of $NS \setminus K$, respectively. Therefore, $\Gamma_G(N)$ is connected.

Theorem B. *Let G a finite group and let N be a normal subgroup of G .*

1. *If $n(\Gamma_G(N)) = 1$, then $d(\Gamma_G(N)) \leq 3$.*
2. *If $n(\Gamma_G(N)) = 2$, then each connected component is a complete graph.*

We notice that the diameters of $\Gamma_G(N)$ and $\Gamma(N)$ are not either related. For instance, let P be an extraspecial group of order p^3 with $p \neq 2$. If we take $G = P \times S_3$ and $N = P \times A_3$, we have that $\Gamma(N)$ is a complete graph (all N -classes have size p) while $\Gamma_G(N)$ has diameter 2, since the nontrivial G -classes of N have size $2, p$ and $2p$.

In 1995, S. Dolfi introduced in [5] the dual graph $\Gamma^*(G)$ (it was also independently studied in [1]) associated to the primes that divide the sizes of the conjugacy classes of G . In a similar way, we define the following subgraph of $\Gamma^*(G)$.

Definition 1.1.2. *Let G be a finite group and let N be a normal subgroup in G . We define the "dual" graph of $\Gamma_G(N)$, denoted by $\Gamma_G^*(N)$, as follows: the vertices are those primes which divide the size of some class in $\text{Con}_G(N)$, and two vertices p and q are joined by an edge if there exists $C \in \text{Con}_G(N)$ such that pq divides $|C|$.*

We also provide the best bounds for the number of components of $\Gamma_G^*(N)$ and for its diameter. We note again that these bounds cannot be obtained from the only fact that $\Gamma_G^*(N)$ is a subgraph of $\Gamma^*(G)$.

Theorem C. *If G is a finite group and $N \trianglelefteq G$, then $n(\Gamma_G^*(N)) \leq 2$ and $n(\Gamma_G^*(N)) = n(\Gamma_G(N))$.*

Theorem D. *Let G a finite group and $N \trianglelefteq G$.*

1. *If $n(\Gamma_G^*(N)) = 1$, then $d(\Gamma_G^*(N)) \leq 3$.*
2. *If $n(\Gamma_G^*(N)) = 2$, then each connected component is a complete graph.*

We give a characterization of a normal subgroup N whose graph $\Gamma_G(N)$, or equivalently $\Gamma_G^*(N)$, is disconnected. We recall that a group G is said to be quasi-Frobenius if $G/\mathbf{Z}(G)$ is a Frobenius group. In this case, the inverse image in G of the kernel and complement of $G/\mathbf{Z}(G)$ are called the kernel and complement of G , respectively.

Theorem E. *Let G a finite group and $N \trianglelefteq G$. If $\Gamma_G(N)$ has two connected components then, either N is quasi-Frobenius with abelian kernel and complement, or $N = P \times A$ where P is a p -group and $A \leq \mathbf{Z}(G)$.*

We point out that our proofs of Theorems B, D and E are different and independent of the proofs of the respective theorems concerning $\Gamma(G)$ and $\Gamma^*(G)$. In addition, Theorem E extends Corollary B of [2], which analyzes (with a completely different approach) the particular case in which N has exactly two coprime G -class sizes bigger than 1.

1.2 Number of connected components of $\Gamma_G(N)$ and $\Gamma_G^*(N)$

In this section we prove Theorems A and C in an easy way by using the following lemma, that is basic for our development. The distance in both graphs will be denoted by d .

Lemma 1.2.1. *Let G be a finite group and $N \trianglelefteq G$. Let $B = b^G$ y $C = c^G$ non-central elements in $\text{Con}_G(N)$. If $(|B|, |C|) = 1$. Then*

1. $\mathbf{C}_G(b)\mathbf{C}_G(c) = G$.
2. $BC = CB$ is a non-central element of $\text{Con}_G(N)$ and $|BC|$ divides $|B||C|$.
3. Suppose that $d(B, C) \geq 3$ and $|B| < |C|$. Then $|BC| = |C|$ and $CBB^{-1} = C$. Furthermore, $C\langle BB^{-1} \rangle = C$, $\langle BB^{-1} \rangle \subseteq \langle CC^{-1} \rangle$ and $|\langle BB^{-1} \rangle|$ divides $|C|$.

Proof. For 1, 2 and the first part of 3, it is enough to mimic the proofs of Lemmas 1 and 2 of [3], by taking into account that the product of two classes of $\text{Con}_G(N)$ is contained in N again. The properties $C\langle BB^{-1} \rangle = C$ and $\langle BB^{-1} \rangle \subseteq \langle CC^{-1} \rangle$ are elementary. The fact that $|\langle BB^{-1} \rangle|$ divides $|C|$ follows from the fact that C is a normal subset that can be written as the union of right coclasses of the normal subgroup $\langle BB^{-1} \rangle$. \square

Proof of Theorem A. Suppose that $\Gamma_G(N)$ has at least three connected components and take three non-central classes $B = b^G$, $C = c^G$ and $D = d^G$ in $\text{Con}_G(N)$, each of which belongs to a different connected component. Certainly, any two of them have coprime size. Moreover, we can assume without loss of generality that $|B| < |C| < |D|$. By applying Lemma 1.2.1, we get that $|\langle BB^{-1} \rangle|$ divides both $|D|$ and $|C|$. Then, $(|C|, |D|) > 1$, which is a contradiction. \square

Proof of Theorem C. Suppose that $n(\Gamma_G^*(N)) \geq 3$. We take three primes r, s and l each of which belongs to a different connected component, and let B, C and D be elements of $\text{Con}_G(N)$ such that r divides $|B|$, s divides $|C|$ and l divides $|D|$. Without loss of generality we suppose that $|D| < |C| < |B|$. We have $d(B, D) \geq 3$ and $d(B, C) \geq 3$ and by applying Lemma 1.2.1, we obtain that $|\langle DD^{-1} \rangle|$ divides $|B|$ and $|C|$, but this leads to a contradiction, because $|B|$ and $|C|$ would have a common prime divisor. This proves that $n(\Gamma_G^*(N)) \leq 2$.

Suppose now that $n(\Gamma_G(N)) = 1$ and $n(\Gamma_G^*(N)) = 2$. Let r and s be primes such that each of them belongs to a distinct connected component of $\Gamma_G^*(N)$. Then there exist $B_r, B_s \in \Gamma_G(N)$ such that r divides $|B_r|$ and s divides $|B_s|$. Let us consider the following path in $\Gamma_G(N)$ that joins B_r and B_s , which exists because $n(\Gamma_G(N)) = 1$:

$$B_r \xleftarrow{p_1} B_1 \xleftarrow{p_2} B_2 \xleftarrow{p_3} \dots \xleftarrow{p_s} B_s$$

where p_i is a prime dividing $|B_i|$. This provides a contradiction, because r and s are connected in $\Gamma_G^*(N)$ by the following path:

$$r \xleftarrow{B_r} p_1 \xleftarrow{B_1} p_2 \xleftarrow{B_2} \dots \xleftarrow{B_{s-1}} p_s \xleftarrow{B_s} s$$

So, we have proved that $n(\Gamma_G(N)) = 1$ implies that $n(\Gamma_G^*(N)) = 1$. Now, if $n(\Gamma_G(N)) = 2$ and $n(\Gamma_G^*(N)) = 1$ we can get a contradiction by arguing in a similar way. This shows that $n(\Gamma_G(N)) = n(\Gamma_G^*(N))$. \square

1.3 Diameter of $\Gamma_G(N)$

The following two lemmas, one for the disconnected case and the other for the connected case, summarize important structural properties of a normal subgroup N concerning the graph $\Gamma_G(N)$, which will be used for determining the diameters of $\Gamma_G(N)$ and $\Gamma_G^*(N)$. We start with the disconnected case.

Lemma 1.3.1. *Let G a finite group and let N be a normal subgroup of G . Suppose that $n(\Gamma_G(N)) = 2$ and let X_1 and X_2 be the connected components of $\Gamma_G(N)$. Let B_0 be a non-central element of $\text{Con}_G(N)$ of maximal size and assume that $B_0 \in X_2$. We define*

$$S = \langle C \mid C \in X_1 \rangle \text{ and } T = \langle CC^{-1} \mid C \in X_1 \rangle.$$

Then

1. S is a normal subgroup of G and every element in S , either is central, or its G -conjugacy class is in X_1 .
2. If C is a G -conjugacy class of N out of S , then $|T|$ divides $|C|$.
3. $T = [S, G]$ is normal in G and $T \leq \mathbf{Z}(S)$.
4. $\mathbf{Z}(G) \cap N \subseteq S$ and $\pi(S/(\mathbf{Z}(G) \cap N)) \subseteq \pi(T) \subseteq \pi(B_0)$. Moreover, S is abelian.
5. Let $b^G = B \in X_1$. Then $\mathbf{C}_G(b)/S$ is a q -group for some prime $q \in \pi(B_0)$.

Proof. 1. The fact that S is normal in G is elementary. Let $C \in X_2$ and $B \in X_1$. We know that BC is a G -conjugacy class of $\text{Con}_G(N)$ of maximal size between $|B|$ and $|C|$ by Lemma 1.2.1. Assume that $|BC| = |B|$. By Lemma 1.2.1 again, it follows that $|\langle CC^{-1} \rangle|$ divides $|B|$ and that $\langle CC^{-1} \rangle \subseteq \langle BB^{-1} \rangle$. On the other hand, $|B_0B| = |B_0|$ again by Lemma 1.2.1, and also $|\langle BB^{-1} \rangle|$ divides $|B_0|$. From these facts, we deduce that $(|B|, |B_0|) > 1$, which is a contradiction. Thus, $|BC| = |C|$ for all $C \in X_2$ and $B \in X_1$. Furthermore, we have proved that the size of every class in X_1 is less than the size of any class in X_2 .

Now, take $C \in X_2$ and let A be the union of all G -conjugacy classes of size $|C|$ in S and assume that $A \neq \emptyset$. By the above paragraph, we have that if $B \in X_1$, then $BA \subseteq A$. Hence, $SA = A$, and consequently, since A is a normal subset, $|S|$ divides $|A|$. This is not possible because $A \subseteq S - \{1\}$. This contradiction shows that $A = \emptyset$, that is, S does not contain any class of size $|C|$. Therefore, since S is normal in G , then S does not contain elements whose classes are in X_2 .

2. Let $B \in X_1$. As we have proved in (1), $|B| < |C|$ and then, by Lemma 1.2.1, we have $C\langle BB^{-1} \rangle = C$, and as a consequence, $CT = C$. Therefore, $|T|$ divides $|C|$, as wanted.

3. By definition, it is clear that $T = [S, G]$ and so, it is a normal subgroup of G . Let us prove that $T \leq \mathbf{Z}(S)$. In fact, if $B = b^G \in X_1$, then $(|T|, |G : \mathbf{C}_G(b)|) = (|T|, |B|) = 1$, because $|T|$ divides every class size in X_2 by (2). Now, since $|T : \mathbf{C}_T(b)|$ divides $(|T|, |B|) = 1$, we deduce that $T = \mathbf{C}_T(b)$. As the classes in X_1 generate S , we conclude that T is central in S .

4. Let $z \in \mathbf{Z}(G) \cap N$ and let $B = b^G \in X_1$. Note that $b^G z = (bz)^G$. Moreover $bz \in N$, because both elements lie in N . As $|(bz)^G| = |Bz| = |B|$, then $bz \in S$ and so $z \in S$. This proves that $\mathbf{Z}(G) \cap N \subseteq S$. Since $T = [S, G]$, then $[S/T, G/T] = 1$ and $S/T \subseteq \mathbf{Z}(G/T)$. In particular, S/T is abelian and as $T \leq \mathbf{Z}(S)$ by (3), then S is nilpotent. We can write $S = R \times Z$ where Z is the largest Hall subgroup of S which is contained in $\mathbf{Z}(G)$. Let p be a prime divisor of $|R|$ and let P be a Sylow p -subgroup of R . It is clear that $P \trianglelefteq G$ and $T = [S, G] = [R, G] \geq [P, G] > 1$. Hence p divides $|T|$ and by applying (1) and (2), $|T|$ divides $|B_0|$. Therefore, $\pi(R) \subseteq \pi(T) \subseteq \pi(B_0)$. On the other hand, it is elementary that $\pi(S/(\mathbf{Z}(G) \cap N)) \subseteq \pi(R)$, and the first part of the step is proved. We show now that $R \leq \mathbf{Z}(S)$. In fact, let $b^G = B \in X_1$. Since $(|B|, |B_0|) = 1$, we obtain in particular, $(|B|, |R|) = 1$. Thus, $|R : \mathbf{C}_R(b)| = 1$ since this index trivially divides $|R|$ and $|B|$ because $R \trianglelefteq G$. This means that $R = \mathbf{C}_R(b)$ for every generating element b of S . So, R is contained in $\mathbf{Z}(S)$ as wanted, and S is abelian.

5. By considering the primary decomposition of b , it is clear that we can write $b = b_q b_{q'}$ where b_q and $b_{q'}$ are the q -part and the q' -part of b , where q is a prime such that $b_q \notin \mathbf{Z}(G) \cap N$. Hence, $q \in \pi(B_0)$ by (4). Furthermore, it is elementary that $\mathbf{C}_G(b) \subseteq \mathbf{C}_G(b_q)$, and as a result, $|(b_q)^G|$ divides $|B|$. We claim that any element $xS \in \mathbf{C}_G(b)/S$ is a q -element. For any $x \in \mathbf{C}_G(b)$, write $x = x_q x_{q'}$ (it is possible $x_q = 1$). It is obvious that x_q and $x_{q'}$ belong to $\mathbf{C}_G(b)$. We consider $a = b_q x_{q'}$ and observe that $\mathbf{C}_G(a) = \mathbf{C}_G(b_q) \cap \mathbf{C}_G(x_{q'}) \subseteq \mathbf{C}_G(b_q)$, so $|(b_q)^G|$ divides $|a^G|$. Since $(b_q)^G \in X_1$, this forces that $a^G \in X_1$, and we conclude that $x_{q'} \in S$, that is, xS is a

q -element, as wanted. This shows that $\mathbf{C}_G(b)/S$ is a q -group. \square

Lemma 1.3.2. *Let G be a finite group and $N \trianglelefteq G$ with $\Gamma_G(N)$ connected. Let B_0 be a G -conjugacy class of $\text{Con}_G(N)$ of maximal size. Let*

$$M = \langle D \mid D \in \text{Con}_G(N) \text{ and } d(B_0, D) \geq 2 \rangle$$

$$K = \langle D^{-1}D \mid D \in \text{Con}_G(N) \text{ and } d(B_0, D) \geq 2 \rangle$$

Then

1. M and K are normal subgroups of G . Furthermore, $K = [M, G]$ and $K \leq \mathbf{Z}(M)$.
2. $\mathbf{Z}(G) \cap N \subseteq M$ and $\pi(M/(\mathbf{Z}(G) \cap N)) \subseteq \pi(K) \subseteq \pi(B_0)$. Furthermore, M is abelian.

Proof. 1. By definition, we easily see that M and K are normal subgroups of G and $K = [M, G]$. Let us prove that $K \leq \mathbf{Z}(M)$. If $C = c^G \in \text{Con}_G(N)$ satisfies that $d(B_0, C) \geq 2$, in particular we have $(|B_0|, |C|) = 1$ and then, $|B_0| = |B_0C|$. Moreover, by Lemma 1.2.1, $B_0CC^{-1} = B_0$ and as a result $|K|$ divides $|B_0|$. Therefore, $(|K|, |C|) = 1$. However, we have that $|K : \mathbf{C}_K(c)|$ divides $(|K|, |C|)$ and thus, $K = \mathbf{C}_K(c)$, which implies that $K \leq \mathbf{Z}(M)$.

2. We prove that $\mathbf{Z}(G) \cap N \subseteq M$. Let $z \in \mathbf{Z}(G) \cap N$ and let $C = c^G \in \text{Con}_G(N)$ such that $d(B_0, C) = 2$. Notice that $c^G z = (cz)^G$. As $|(cz)^G| = |c^G|$, then $d(B_0, (cz)^G) = 2$. Thus, $cz \in M$ and $\mathbf{Z}(G) \cap N \subseteq M$. Since $K = [M, G]$, then $M/K \leq \mathbf{Z}(G/K)$ and since $K \leq \mathbf{Z}(M)$ by (1), we obtain that M is nilpotent. We can write $M = R \times Z$ where Z is the largest Hall subgroup of M that is contained in $\mathbf{Z}(G)$. Let q be a prime divisor of $|R|$ and let Q be the Sylow q -subgroup of R . Then $Q \trianglelefteq G$ and $K = [M, G] \geq [R, G] \geq [Q, G] > 1$. So, q divides $|K|$ and $\pi(R) \subseteq \pi(K)$. In the proof of (1), we have seen that $\pi(K) \subseteq \pi(B_0)$. Then, $\pi(R) \subseteq \pi(B_0)$. Furthermore, it is elementary that $\pi(M/(\mathbf{Z}(G) \cap N)) \subseteq \pi(K)$ and so, the first part of the step is proved. On the other hand, given a generating class $B = b^G$ of M , we know that $d(B, B_0) \geq 2$. In particular, we have $(|B|, |B_0|) = 1$ and hence $(|Q|, |B|) = 1$, where Q is the above Sylow q -subgroup. Since $|Q : \mathbf{C}_Q(b)|$ divides $(|Q|, |B|) = 1$, we have $\mathbf{C}_G(b) = Q$ and $Q \leq \mathbf{Z}(M)$. Thus, $R \leq \mathbf{Z}(M)$ and M is abelian. \square

The following consequence, which has interest on its own, is the key to bound the diameter of $\Gamma_G(N)$ in the connected case.

Theorem 1.3.3. *Let G a finite group and N a normal subgroup of G and suppose that $\Gamma_G(N)$ is connected. Let B_0 a non-central conjugacy class of $\text{Con}_G(N)$ with maximal size. Then $d(B, B_0) \leq 2$ for every non-central $B \in \text{Con}_G(N)$.*

Proof. Suppose that the theorem is false. Let $B = b^G \in \text{Con}_G(N)$ such that $d(B_0, B) = 3$ and let

$$B_0 \longleftrightarrow B_1 \longleftrightarrow B_2 \longleftrightarrow B$$

be a shortest chain linking B and B_0 of length 3. By considering the primary decomposition of b , we write $b = b_q b_{q'}$ where b_q and $b_{q'}$ are the q -part and the q' -part of b , and q is a prime such that $b_q \notin \mathbf{Z}(G) \cap N$. Hence, $q \in \pi(B_0)$ by Lemma 1.3.2 (2). Also, the fact that $\mathbf{C}_G(b) \subseteq \mathbf{C}_G(b_q)$ implies that $|(b_q)^G|$ divides $|B|$ and then any class which is connected to $(b_q)^G$ must be connected to B . This means that $d((b_q)^G, B_0) \geq 3$.

Let M be subgroup defined in Lemma 3.2. We claim that any element $x \in \mathbf{C}_G(b_q) \setminus M$ satisfies that xM is a q -element. Write $x = x_q x_{q'}$ and suppose that $x_{q'} \notin M$. Set $a = x_{q'} b_q$ and notice that $a \notin M$. By definition of M , we have $d(a^G, B_0) \leq 1$ and since $\mathbf{C}_G(a) = \mathbf{C}_G(x_{q'}) \cap \mathbf{C}_G(b_q)$, it follows that $|(b_q)^G|$ divides $|a^G|$. These facts show that $d((b_q)^G, B_0) \leq 2$, a contradiction. Therefore, $x_{q'} \in M$ and xM is a q -element. In conclusion, $\mathbf{C}_G(b_q)/M$ is a q -group. Now, observe that $|B_2|$ divides

$$|G : \mathbf{Z}(G) \cap N| = |G : \mathbf{C}_G(b_q)| |\mathbf{C}_G(b_q) : M| |M : \mathbf{Z}(G) \cap N|.$$

Also, we know by Lemma 1.3.2 (2) that $\pi(M/\mathbf{Z}(G) \cap N) \subseteq \pi(B_0)$ and we have seen in the above paragraph that $\mathbf{C}_G(b_q)/M$ is a q -group for some $q \in \pi(B_0)$. Consequently, $|B_2|$ must divide $|(b_q)^G|$ (which divides $|B|$), because $(|B_2|, |B_0|) = 1$. This is a contradiction, since B_1 and B would be joined by an edge. \square

Proof of Theorem B. 1. Suppose that D_1 and D_2 are classes of $\text{Con}_G(N)$ such that $d(D_1, D_2) = 4$. Let B_0 be a class of maximal size in $\text{Con}_G(N)$. By Theorem 1.3.3 we know that $d(B_0, D_i) \leq 2$ for $i = 1, 2$. We can suppose then that $d(B_0, D_i) = 2$ for $i = 1, 2$. Furthermore, without loss of generality, $|D_1| > |D_2|$. Then, by Lemma 1.2.1 it is true that $|\langle D_2 D_2^{-1} \rangle|$ divides $|D_1|$. In addition, $B_0 D_2$ is a conjugacy class of $\text{Con}_G(N)$ and $|B_0 D_2| = |B_0|$ by Lemma 1.2.1 (2) and by the maximality of B_0 . It follows that $B_0 D_2 D_2^{-1} = B_0$ and $|\langle D_2 D_2^{-1} \rangle|$ divides $|B_0|$. Therefore, B_0 and D_1 are joined by an edge, which is a contradiction. This proves that $d(\Gamma_G(N)) \leq 3$.

2. Let $B_1 = b_1^G$ and $B_2 = b_2^G$ in X_1 . Notice that $b_1, b_2 \in S$ where S is the subgroup defined in Lemma 3.1. By applying the properties of that result, we know that $|b_2^G|$ divides

$$|G : \mathbf{Z}(G) \cap N| = |G : \mathbf{C}_G(b_1)| |\mathbf{C}_G(b_1) : S| |S : \mathbf{Z}(G) \cap N|$$

where the primes dividing $|\mathbf{C}_G(b_1) : S|$ and $|S : \mathbf{Z}(G) \cap N|$ are in $\pi(B_0)$. So, we have that $|b_2^G|$ divides $|b_1^G|$. By arguing symmetrically we also get that $|b_1^G|$ divides $|b_2^G|$, so we conclude that all classes in X_1 have the same size. Hence, X_1 is a complete graph. Now, we prove that X_2 is also a complete graph. It is enough to consider again S and T defined in Lemma 1.3.1 and observe that every $C \in X_2$ is out of S and that $|T|$ divides $|C|$ by Lemma 1.3.1 (1) and (2). \square

Remark 1.3.4. *In the proof of Theorem B.2, we have seen that all G -classes of N lying in the connected component X_1 (the component which does not contains the classes of maximal size), must have the same size. Moreover, in the proof of Lemma 3.1(1) we have seen that this size is less than the size of every class in X_2 .*

1.4 Diameter of $\Gamma_G^*(N)$

Proof of Theorem D. 1. Suppose that there exist two primes r and s in $\Gamma_G^*(N)$ such that $d(r, s) = 4$ and we will get a contradiction. This means that the primes r and s are connected by a path of length 4, say

$$r \xleftrightarrow{B_1} p_1 \xleftrightarrow{B_2} p_2 \xleftrightarrow{B_3} p_3 \xleftrightarrow{B_4} s$$

where $B_i \in \text{Con}_G(N)$ for $i = 1, \dots, 4$ and $p_i \in \Gamma_G^*(N)$ for $i = 1, 2, 3$. By Theorem 1.3.3 we know that $d(B_i, B_0) \leq 2$ for $i = 1, \dots, 4$ where B_0 is a non-central G -conjugacy class of maximal size. Notice that $d(B_1, B_4) = 3$ and we distinguish only two possibilities:

Case 1. $d(B_0, B_1) = 2 = d(B_0, B_4)$. By symmetry, we can assume for instance that $|B_1| > |B_4|$. Since $d(B_1, B_4) = 3$, by Lemma 1.2.1 we have that $|\langle B_4 B_4^{-1} \rangle|$ divides $|B_1|$. Moreover, $B_0 B_4$ is an element of $\text{Con}_G(N)$ such that $|B_0 B_4| = |B_0|$ and by Lemma 1.2.1, $|\langle B_4 B_4^{-1} \rangle|$ divides $|B_0|$. Therefore, $d(B_0, B_1) = 1$, because their cardinalities have a prime common divisor. This is a contradiction.

Case 2. Either $d(B_0, B_1) = 2$ and $d(B_0, B_4) = 1$, or $d(B_0, B_1) = 1$ and $d(B_0, B_4) = 2$. Without loss we assume for instance the latter case. Let us consider the subgroup M defined in Lemma 3.2 and let $B_4 = b^G$. Since $d(B_0, B_4) = 2$, then $b \in M$ by definition. Moreover, $|B_1|$ divides

$$|G : \mathbf{Z}(G) \cap N| = |G : \mathbf{C}_G(b)| |\mathbf{C}_G(b) : M| |M : \mathbf{Z}(G) \cap N|.$$

Now, notice that $r \notin \pi(B_0)$, otherwise it yields $d(r, s) \leq 3$, a contradiction, and trivially $r \notin \pi(B_4)$. Also, $\pi(M/\mathbf{Z}(G) \cap N) \subseteq \pi(B_0)$, so we have that r (which divides $|B_1|$) must divide $|\mathbf{C}_G(b) : M|$. Therefore, there exists an r -element $y \in \mathbf{C}_G(b) \setminus M$. On the other hand, $b \in M$, and by Lemma 1.3.2 (2), the r -part of b is central in G , that is, we can assume that b is an r' -element, by replacing b by its r' -part. As y and b have coprime orders, we have

$$\mathbf{C}_G(yb) = \mathbf{C}_G(y) \cap \mathbf{C}_G(b) \subseteq \mathbf{C}_G(b).$$

Consequently, $|B_4|$ divides $|(yb)^G|$. Furthermore, since $yb \notin M$, by definition of M we have $d((yb)^G, B_0) \leq 1$. As $d(B_0, B_1) = 1$ by hypothesis, we deduce that $d(B_1, (yb)^G) \leq 2$. Now, s divides $|B_1|$ and r divides $|(yb)^G|$, and this forces that $d(r, s) \leq 3$, which is a contradiction.

2. Let X_1 and X_2 be the connected components of $\Gamma_G(N)$ where X_2 is the component that contains the G -conjugacy class with the largest size. Let us prove first that X_1^*, X_2^* are the connected components of $\Gamma_G^*(N)$, where $X_i^* = \{p \in \pi(B) \mid B \in X_i\}$, and secondly, that X_1^* y X_2^* are complete graphs.

Let X be a connected component of $\Gamma_G(N)$ and let $r, s \in X^*$. Then there exist B_r, B_s such that r divides $|B_r|$ and s divides $|B_s|$. Let us consider the path in $\Gamma_G(N)$ that joins B_r and B_s :

$$B_r \xleftrightarrow{p_1} B_1 \xleftrightarrow{p_2} B_2 \xleftrightarrow{p_3} \dots \xleftrightarrow{p_s} B_s$$

where $B_i \in \text{Con}_G(N)$ for $i = 1, \dots, s-1$ and $p_i \in \Gamma_G^*(N)$ for $i = 1, \dots, s$. So, r and s are connected in $\Gamma_G^*(N)$ in the following way:

$$r \xleftrightarrow{B_r} p_1 \xleftrightarrow{B_1} p_2 \xleftrightarrow{B_2} \dots \xleftrightarrow{B_{s-1}} p_s \xleftrightarrow{B_s} s$$

Therefore, X^* is contained in a connected component Y of $\Gamma_G^*(N)$. Now, we take $q \in Y$, which is connected by an edge to some $r \in X^*$. Then there exists $B \in \text{Con}_G(N)$ such that qr divides $|B|$. It follows that $B \in X$ and $q \in X^*$. Thus, $X^* = Y$ and X^* is a connected component of $\Gamma_G^*(N)$ as wanted.

By Remark 1.3.4, all classes in X_1 have the same size, which trivially implies that X_1^* is a complete graph. Let us show that X_2^* is a complete graph too. Suppose that B_0 is a conjugacy class with maximal size, which lies in X_2 , and let $B_1 = b_1^G \in X_1$. Then, the subgroup S defined in Lemma 3.1 is abelian, and $S \subseteq \mathbf{C}_G(b_1)$. Now, if $p \in X_2^*$, there exists $D \in X_2$ such that p divides $|D|$. Notice that $|D|$ divides

$$|G : \mathbf{Z}(G) \cap N| = |B_1| |\mathbf{C}_G(b_1) : S| |S : \mathbf{Z}(G) \cap N|,$$

and by Lemma 1.3.1 (4) and (5), we know that $|\mathbf{C}_G(b_1) : S|$ is a q -power with $q \in \pi(B_0)$ and $\pi(S/(\mathbf{Z}(G) \cap N)) \subseteq \pi(B_0)$. It follows that $\pi(D) \subseteq \pi(B_0)$. Therefore, all primes in X_2^* are in $\pi(B_0)$ and so, X_2^* trivially is a complete graph. \square

1.5 Structure of N in the disconnected case

Proof of Theorem E. Suppose that X_1 and X_2 are the two connected components of $\Gamma_G(N)$, where X_2 is the one containing the classes of maximal size. Let S the subgroup defined in Lemma 3.1.

Step 1: If $S \leq \mathbf{Z}(N)$, then $N = P \times A$ with $A \leq \mathbf{Z}(G) \cap N$ and P a p -group.

We can choose a p -element x and a q -element y of N , for some primes p and q , such that $x^G \in X_1$ and $y^G \in X_2$. If $p = q$ for every election of x and y , it is clear that $N = P \times A$ with $A \leq \mathbf{Z}(G) \cap N$. Assume then that $p \neq q$. Since $x \in S \leq \mathbf{Z}(N)$, we obtain $N/S = \mathbf{C}_N(x)/S$ and this group has prime power order by Lemma 1.3.1 (5). As a consequence, N is nilpotent and $[x, y] = 1$. As x and y have coprime order, $\mathbf{C}_G(xy) = \mathbf{C}_G(x) \cap \mathbf{C}_G(y)$ and so, $|(xy)^G|$ divides $|x^G|$ and $|y^G|$, a contradiction. This proves the step.

Notice that we can assume that $S\mathbf{Z}(N) < N$, because if $S\mathbf{Z}(N) = N$ then N is abelian and $S \leq \mathbf{Z}(N)$. For the rest of the proof, we assume $\mathbf{Z}(N) < S\mathbf{Z}(N) < N$ and we will prove that N is quasi-Frobenius with abelian kernel and complement. We divide the proof into several steps. Let us denote by $\pi = \{p \text{ prime} \mid p \text{ divides } |B| \text{ with } B \in X_1\}$.

Step 2: N has a normal π -complement and abelian Hall π -subgroups.

Let us prove that N is p -nilpotent and has abelian Sylow p -subgroups for every $p \in \pi$. Let $a \in N \setminus S$, then obviously $a^G \in X_2$ and $|a^G|$ is a π' -number. If we

take $P \in \text{Syl}_p(N)$, then there exists $g \in N$ such that $P^g \subseteq \mathbf{C}_N(a)$, that is, $a \in \mathbf{C}_N(P^g) = \mathbf{C}_N(P)^g$. Thus, we can write

$$N = S \cup \bigcup_{g \in N} \mathbf{C}_N(P)^g$$

and, by counting elements, it follows that

$$|N| \leq (|S| - 1) + |N : \mathbf{N}_N(\mathbf{C}_N(P))|(|\mathbf{C}_N(P)| - 1) + 1.$$

Hence

$$1 \leq \frac{|S|}{|N|} + \frac{|\mathbf{C}_N(P)|}{|\mathbf{N}_N(\mathbf{C}_N(P))|} - \frac{1}{|\mathbf{N}_N(\mathbf{C}_N(P))|}.$$

However, if $\mathbf{C}_N(P) < \mathbf{N}_N(\mathbf{C}_N(P))$, as we are assuming that $S < N$, we have

$$1 \leq \frac{1}{2} + \frac{1}{2} - \frac{1}{|\mathbf{N}_N(\mathbf{C}_N(P))|},$$

which is a contradiction. This implies that $\mathbf{C}_N(P) = \mathbf{N}_N(\mathbf{C}_N(P))$, and in particular,

$$P \leq \mathbf{N}_N(P) \leq \mathbf{N}_N(\mathbf{C}_N(P)) \leq \mathbf{C}_N(P),$$

so $\mathbf{C}_N(P) = \mathbf{N}_N(P)$ and P is abelian. By Burnside's p -nilpotency criterion (see for instance 17.9 of [7]), we get that N is p -nilpotent for every $p \in \pi$ and so, N has normal π -complement. In particular, N is π -separable and there exists a Hall π -subgroup H of N . By reasoning with H similarly as with P , we obtain $\mathbf{C}_N(H) = \mathbf{N}_N(H)$ and so, H is abelian too. The step is finished.

Let $K/\mathbf{Z}(N)$ be the normal π -complement of $N/\mathbf{Z}(N)$. By applying Lemma 1.3.1 (4), we get that $S\mathbf{Z}(N)/\mathbf{Z}(N)$ is a normal π' -subgroup of $N/\mathbf{Z}(N)$, so $S \leq K$.

Step 3: $K = \mathbf{C}_N(x)$ for every $x \in S \setminus \mathbf{Z}(G) \cap N$ and $S \leq \mathbf{Z}(K)$.

Let $x \in S \setminus \mathbf{Z}(G) \cap N$. Then $x^G \in X_1$ by Lemma 1.3.1 (1) and $\mathbf{C}_G(x)/S$ is a π' -group by Lemma 1.3.1 (5). Since $|x^N|$ is a π -number, we obtain that $\mathbf{C}_N(x)/\mathbf{Z}(N)$ is a Hall π' -subgroup of $N/\mathbf{Z}(N)$. Thus, $K = \mathbf{C}_N(x)$ for every $x \in S \setminus \mathbf{Z}(G) \cap N$ and, in particular, $S \leq \mathbf{Z}(K)$.

Step 4: $K = S$.

Let H be an abelian Hall π -subgroup of N . We have seen in the proof of Step 2 that

$$N = S \cup \bigcup_{g \in N} \mathbf{C}_N(H)^g,$$

which trivially implies that

$$N = \bigcup_{g \in N} S\mathbf{C}_N(H)^g.$$

This forces that $N = \mathbf{C}_N(H)S$ and consequently, $HS \trianglelefteq N$. Suppose that $S < K$ and we will get a contradiction. Let $a \in K \setminus S$, then $a^G \in X_2$ by Lemma 1.3.1 (1),

so $|a^G|$ is a π' -number and as a result, $a \in \mathbf{C}_K(H^g) = \mathbf{C}_K(H)^g$ for some $g \in N$. Moreover, $S \leq \mathbf{Z}(K)$ by Step 3, so we have the following equalities

$$\mathbf{C}_K(H^g) = \mathbf{C}_K(H^g S) = \mathbf{C}_K(HS) = \mathbf{C}_K(H).$$

Thus, $a \in \mathbf{C}_K(H)$ for every $a \in K \setminus S$ and we conclude that $K = \langle K \setminus S \rangle \subseteq \mathbf{C}_N(H)$. As H is abelian and $N = HK$, we have $H \leq \mathbf{Z}(N) \leq K$. This implies that $N = K$ and then, $S \leq \mathbf{Z}(N)$ by Step 3, which contradicts the assumption made after Step 1.

Step 5: N is quasi-Frobenius with abelian kernel and complement.

Let $\bar{N} = N/\mathbf{Z}(N)$ and let $\bar{K} = K/\mathbf{Z}(N)$. If $\bar{K} = \mathbf{C}_{\bar{N}}(\bar{x})$ for all $\bar{x} \in \bar{K} \setminus \{1\}$, this is equivalent to the fact that N is quasi-Frobenius with abelian kernel K and abelian complement H . Suppose then that $\bar{K} < \mathbf{C}_{\bar{N}}(\bar{x})$ for some $\bar{x} \in \bar{K} \setminus \{1\}$. Also, we can suppose that $o(\bar{x})$ is an r -number for some prime $r \in \pi'$. Now, let $\bar{y} \in \mathbf{C}_{\bar{N}}(\bar{x}) \setminus \bar{K}$ such that $o(\bar{y})$ is a q -number for some $q \in \pi$. We can suppose without loss of generality that $o(y)$ is a q -number. Notice that $[y, x] \in \mathbf{Z}(N)$ because $\bar{y} \in \mathbf{C}_{\bar{N}}(\bar{x})$ and, since $(o(x), o(y)) = 1$, it easily follows that $[x, y] = 1$. Then $y \in \mathbf{C}_N(x) = K$ and $\bar{y} \in \bar{K}$, which is a contradiction. \square

Example 1.5.1. *We show that the converse of the above theorem is false. It is known that the special linear group $H = SL(2, 5)$ acts Frobeniusly on $K \cong \mathbb{Z}_{11} \times \mathbb{Z}_{11}$. As a consequence, the action of any subgroup of H on K is also Frobenius. We consider, in particular, a Sylow 5-subgroup P of H and $\mathbf{N}_H(P)$ acting Frobeniusly on K . We define the semidirect product $N := KP$, which is trivially a normal subgroup of $G := K\mathbf{N}_H(P)$. Thus, N is a Frobenius group with abelian kernel and complement. In fact, N decomposes into the following disjoint union*

$$N = \{1\} \cup (K \setminus \{1\}) \cup \left(\bigcup_{k \in K} P^k \setminus \{1\} \right),$$

and $K \setminus \{1\}$ is partitioned into N -classes of cardinality 5, whereas the elements of $\bigcup_{k \in K} (P^k \setminus \{1\})$ are decomposed into N -classes of cardinality 121. Therefore, the set of class sizes of N is $\{1, 5, 121\}$. Now, let us compute the G -class sizes of N . As G is a Frobenius group with kernel K and complement $\mathbf{N}_H(P)$, it follows that K is decomposed exactly into the trivial class and G -classes of size $|\mathbf{N}_H(P)| = 20$. That is, the N -classes contained in $K \setminus \{1\}$ are grouped 4 by 4 to form G -classes. And on the other hand, the four N -conjugacy classes contained in $\bigcup_{k \in K} P^k \setminus \{1\}$ of size 121, are grouped in pairs and become two G -conjugacy classes of size 121×2 . Then the set of G -class sizes of N is $\{1, 20, 242\}$ and $\Gamma_G(N)$ is a connected graph.

Example 1.5.2. *The following example shows that the case in which N is a p -group in Theorem E actually occurs. Let G be the group of the library of the small groups of GAP ([6]) with number $Id(324, 8)$ and with the presentation*

$$\langle x, y, z \mid x^3 = y^4 = z^9 = 1, [x, y] = 1, z^y = z^{-1}, z^2 = xzxzx = x^{-1}zx^{-1}zx^{-1} \rangle.$$

By using GAP, one can check that G has an abelian normal subgroup $N \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ and the set of G -class sizes of N is $\{1, 2, 3\}$, so $\Gamma_G(N)$ is disconnected.

Question 1.5.3. *The referee proposed us the following question: whether it is possible to obtain any information on the structure of G from the graph $\Gamma_G(N)$ or not. We believe that in general $\Gamma_G(N)$ may provide few information of G , although possibly one could get further information on the action of G on N . In fact, $G/\mathbf{C}_G(N)$ is always immersed in $\text{Aut}(N)$. For giving an easy example, we consider the case in which $\Gamma_G(N)$ is just one vertex, as it happens with $G = S_3$ and $N = A_3$. Now, take N any p -elementary abelian group of order p^s and let us consider the action of $G = \text{Hol}(N)$ on N . As a result of the fact that $\text{Aut}(N)$ acts transitively on $N \setminus \{1\}$, it follows that $\Gamma_G(N)$ consists only in one vertex, whilst $\text{Aut}(N) \cong GL(s, p)$ and so G might have a extremely more complex structure.*

Acknowledgements

The research of the first and second authors is supported by the Valencian Government, Proyecto PROMETEO/2011/30 and by the Spanish Government, Proyecto MTM2010-19938-C03-02. The first author is also supported by Universitat Jaume I, grant P11B2012-05.

Bibliography

- [1] G. Alfandary. On graphs related to conjugacy classes of groups. *Israel J. Math.* **86** (1994), no. 1-3, 211-220.
- [2] Z. Akhlaghi, A. Beltrán, M.J. Felipe, M. Khatami, Structure of normal subgroups with three G -class sizes. *Monatsh. Math.* **167** (2012), 1-12.
- [3] E.A. Bertram, M. Herzog, A. Mann, On a graph related to conjugacy classes of groups. *Bull. London Math. Soc.* **22** (6) (1990), 569-575.
- [4] D. Chillag, M. Herzog, A. Mann, On the diameter of a graph related to conjugacy classes of groups. *Bull. London Math. Soc.* **25** (1993), 255-262.
- [5] S. Dolfi, Arithmetical conditions on the length of the conjugacy classes of a finite group. *J. Algebra* **174** (1995), 753-771.
- [6] The GAP Group, GAP - Groups, Algorithms and Programming, Vers. 4.4.12 (2008). <http://www.gap-system.org>
- [7] B. Huppert, Character Theory of Finite groups, Vol. 25, De Gruyter Expositions in Mathematics, Berlin, New York, 1998.

Chapter 2

Normal subgroups whose conjugacy class graph has diameter three

Abstract

Let G be a finite group and let N be a normal subgroup of G . We determine the structure of N when the diameter of the graph associated to the G -conjugacy classes contained in N is as large as possible, that is, is equal to three.

Keywords. Finite groups, conjugacy classes, normal subgroups, graphs.

Mathematics Subject Classification (2010): 20E45, 20D15.

2.1 Introduction

Let G be a finite group and let N be a normal subgroup of G . If $x \in N$, we denote by $x^G = \{x^g \mid g \in G\}$ the G -conjugacy class of x . Let $\Gamma_G(N)$ be the graph associated to these G -conjugacy classes, which was defined in [2] as follows: its vertices are the G -conjugacy classes of N of cardinality bigger than 1, that is, G -classes of elements lying in $N \setminus (\mathbf{Z}(G) \cap N)$, and two of them are joined by an edge if their sizes are not coprime. It was proved in [2] that $d(\Gamma_G(N)) \leq 3$, where $d(\Gamma_G(N))$ denotes the diameter of the graph. In this note we analyze the structure properties of N when $d(\Gamma_G(N)) = 3$.

The above graph extends the ordinary graph, $\Gamma(G)$, which was formerly defined in [3], and whose vertices are the non-central conjugacy classes of G and two vertices are joined by an edge if their sizes are not coprime. The graph $\Gamma_G(N)$ can be viewed as the subgraph of $\Gamma(G)$ induced by those vertices of $\Gamma(G)$ which are vertices in $\Gamma_G(N)$. This fact does not allow us, however, to obtain directly properties of the graph of G -classes.

Concerning ordinary classes, L.S. Kazarin characterizes in [8] the structure of a group G having two "isolated classes". We recall that a group G is said to have isolated classes if there exist elements $x, y \in G$ such that every element of G has a conjugacy class size coprime to either $|x^G|$ or $|y^G|$. Particularly, Kazarin determined

the structure of those groups G with $d(\Gamma(G)) = 3$. On the other hand, the disconnected graph was studied by Bertram, Herzog and Mann in [3]. It should be noted that similar results have also been studied for other graphs. In [5], Dolfi defines the graph $\Gamma'(G)$ whose vertices are the elements of the set of all primes which occur as divisors of the lengths of the conjugacy classes of G , and two vertices p, q are joined by an edge if there exists a conjugacy class in G whose length is a multiple of pq . In [6] Dolfi and Casolo describe all finite groups G for which $\Gamma'(G)$ is connected and has diameter three.

We remark that the primes dividing the G -conjugacy class sizes do not need to divide $|N|$. This especially occurs when N is Abelian and non-central in G and consequently, we may have no control on this set of primes. For this reason, we observe that new cases appear when dealing with G -classes which are not contemplated in the ordinary case. The main result of this note is Theorem 2.1.1 and it is inspired in [8]. From now on, if G is a finite group we denote by $\pi(G)$ the set of primes dividing $|G|$, and analogously, if X is a set, then $\pi(X)$ denotes the set of primes dividing $|X|$.

Theorem 2.1.1. *Let G be a finite group and $N \trianglelefteq G$. Suppose that x^G and y^G are two non-central G -conjugacy classes of N such that any G -conjugacy class of N has size coprime with $|x^G|$ or $|y^G|$. Let $\pi_x = \pi(x^G)$, $\pi_y = \pi(y^G)$ and $\pi = \pi_x \cup \pi_y$. Then $N = \mathbf{O}_{\pi'}(N) \times \mathbf{O}_{\pi}(N)$ with $x, y \in \mathbf{O}_{\pi}(N)$, which is either a quasi-Frobenius group with Abelian kernel and complement or $\mathbf{O}_{\pi}(N) = P \times A$ with $A \leq \mathbf{Z}(N)$ and P is a p -group for a prime p .*

Notice that in the conditions of Theorem 2.1.1, we have two possibilities: $d(\Gamma_G(N)) \leq 2$ or $d(\Gamma_G(N)) = 3$. In the former case, we certainly have that the graph is disconnected, and then the structure of N is already determined by Theorem E of [2]. However, we slightly improve this result in Corollary 1.2. In the second case, the graph is connected since when the graph $\Gamma_G(N)$ is disconnected, it was proved that each connected component is a complete graph (Theorem B of [2]). Therefore, we deduce the following consequences for each of these cases.

Corollary 2.1.2. *Let G be a finite group and $N \trianglelefteq G$. Suppose that $\Gamma_G(N)$ is disconnected and let $x, y \in N$ such that $(|x^G|, |y^G|) = 1$. Set $\pi = \pi(x^G) \cup \pi(y^G)$. Then $x, y \in \mathbf{O}_{\pi}(N)$, $N = \mathbf{O}_{\pi'}(N) \times \mathbf{O}_{\pi}(N)$ with $\mathbf{O}_{\pi'}(N) \leq \mathbf{Z}(G)$, and either $\mathbf{O}_{\pi}(N)$ is a quasi-Frobenius group with Abelian kernel and complement or $\mathbf{O}_{\pi}(N) = P \times A$ with $A \leq \mathbf{Z}(G)$ and P is a p -group for a prime p .*

Corollary 2.1.3. *Let G be a finite group and $N \trianglelefteq G$. Suppose that $\Gamma_G(N)$ is connected with $d(\Gamma_G(N)) = 3$. Let $x, y \in N$ such that $d(x^G, y^G) = 3$. Set $\pi = \pi(x^G) \cup \pi(y^G)$. Then $x, y \in \mathbf{O}_{\pi}(N)$, $N = \mathbf{O}_{\pi'}(N) \times \mathbf{O}_{\pi}(N)$ where either $\mathbf{O}_{\pi}(N)$ is a quasi-Frobenius group with Abelian kernel and complement or $\mathbf{O}_{\pi}(N) = P \times A$ with $A \leq \mathbf{Z}(N)$ and P is a p -group for a prime p .*

2.2 Proofs

First, we state three elementary results which are needed to prove the main result.

Lemma 2.2.1. *Let G be a π -separable group. Then the conjugacy class size of every π -element of G is a π -number if and only if $G = H \times K$, where H and K are a Hall π -subgroup and a π -complement of G , respectively.*

Proof. This is Lemma 8 of [1]. □

In the particular case in which $\pi = p'$, the complement of some prime p , Lemma 2.2.1 is true without assuming p -separability (or equivalently p -solvability). We recall that the class size of an element is also sometimes called the index of the element.

Lemma 2.2.2. *If every p' -element of a group G has index prime to p , for some prime p , then the Sylow p -subgroup of G is a direct factor of G .*

Proof. This is Lemma 1 of [4]. □

Lemma 2.2.3. *Let G be a finite group and $N \trianglelefteq G$. Let $B = b^G$ and $C = c^G$ be two non-central G -conjugacy classes of N . If $(|B|, |C|) = 1$. Then*

1. $\mathbf{C}_G(b)\mathbf{C}_G(c) = G$.
2. $BC = CB$ is a non-central G -class of N and $|BC|$ divides $|B||C|$.
3. Suppose that $d(B, C) \geq 3$ and $|B| < |C|$. Then $|BC| = |C|$ and $CBB^{-1} = C$. Furthermore, $C\langle BB^{-1} \rangle = C$, $\langle BB^{-1} \rangle \subseteq \langle CC^{-1} \rangle$ and $|\langle BB^{-1} \rangle|$ divides $|C|$.

Proof. This is Lemma 2.1 of [2]. □

Proof of Theorem 2.1.1. We proceed by induction on $|N|$. Notice that the hypotheses are inherited by every normal subgroup in G which is contained in N and contains x and y . By using the primary decomposition we can assume that both x and y have order a power of a prime, say p and q , respectively.

Step 1. $q = p$ if and only if $xy = yx$.

Suppose that $xy = yx$ and that $p \neq q$. Observe that $\mathbf{C}_G(xy) = \mathbf{C}_G(x) \cap \mathbf{C}_G(y)$ and consequently, both $|x^G|$ and $|y^G|$ divide $|(xy)^G|$. Thus, we obtain a G -conjugacy class connected with x^G and y^G , which contradicts the hypotheses. Conversely, suppose that $p = q$. We know that p cannot divide either $|x^G|$ or $|y^G|$. Furthermore, the hypotheses imply that $(|x^G|, |y^G|) = 1$, so we have $G = \mathbf{C}_G(x)\mathbf{C}_G(y)$ and $|x^G| = |G : \mathbf{C}_G(x)| = |\mathbf{C}_G(y) : \mathbf{C}_G(x) \cap \mathbf{C}_G(y)|$. Now, since y is a p -element in $\mathbf{Z}(\mathbf{C}_G(y))$, we deduce that $y \in \mathbf{C}_G(x) \cap \mathbf{C}_G(y)$ and hence $xy = yx$.

Step 2. We have $p \in \pi_y$ and $q \in \pi_x$. Hence $p, q \in \pi$.

We define $K = \mathbf{C}_G(x) \cap \mathbf{C}_G(y)$. First, we assume that $p \neq q$ and $xy \neq yx$. We have $|G : K| = |G : \mathbf{C}_G(x)||\mathbf{C}_G(x) : \mathbf{C}_G(x) \cap \mathbf{C}_G(y)| = |x^G||y^G|$, which is a π -number. Since $x \in \mathbf{Z}(\mathbf{C}_G(x))$ and x is a p -element but $x \notin K$, we know that p divides $|\mathbf{C}_G(x) : K| = |y^G|$. This means that $p \in \pi_y$. Similarly we obtain that q divides $|x^G|$, that is, $q \in \pi_x$. As a result, $p, q \in \pi$.

Suppose now that $p = q$ and $xy = yx$. Let us see that $p \in \pi$. We denote $X = x^G$ and $Y = y^G$ and we assume for instance that $|X| > |Y|$. By hypothesis, the distance between X and Y in $\Gamma_G(N)$ is bigger than or equal to 3. We can apply Lemma 2.2.3 (iii) and we get $X\langle YY^{-1} \rangle = X$, $\langle YY^{-1} \rangle \subseteq \langle XX^{-1} \rangle$ and $|\langle YY^{-1} \rangle|$ divides $|X|$. On the other hand, since $G = \mathbf{C}_G(x)\mathbf{C}_G(y)$ we have $X \subseteq \mathbf{C}_G(y)$. As a

result, $\langle YY^{-1} \rangle \subseteq \langle XX^{-1} \rangle \subseteq \mathbf{C}_G(y)$. In particular, if we take $z = y^g \neq y$, for some $g \in G$, we have $w = zy^{-1} \in \langle YY^{-1} \rangle \subseteq \mathbf{C}_G(y)$, so $[z, y] = 1$. We obtain that w is a non-trivial p -element and, since p divides $|\langle YY^{-1} \rangle|$, which divides $|X|$, we conclude that $p \in \pi_x$. If $|Y| > |X|$ we can argue similarly to get $p \in \pi_y$.

Step 3. We can assume that $N/\mathbf{Z}(N)$ is neither a p -group nor a q -group. Particularly, we can assume that N is not Abelian.

Suppose that $N/\mathbf{Z}(N)$ is a p -group. The argument is analogous if we suppose that it is a q -group. Hence we can write $N = P \times A$ where $A \leq \mathbf{Z}(N)$ and A is a p' -group. If $p \neq q$, it follows that $x \in P$ and $y \in A$, which leads to a contradiction with Step 1. Thus, $p = q$ and $x, y \in P$, so the theorem is proved.

Step 4. We can suppose that N is not a π -group.

Let us see that if N is a π -group, then N is a quasi-Frobenius group with Abelian kernel and complement or $N = P \times A$ with $A \leq \mathbf{Z}(N)$ and A a p' -group. Assume that N is a π -group. As N is non-Abelian by Step 3, there exists a conjugacy class z^N such that $|z^N| \neq 1$. Since $|z^N|$ divides $|z^G|$, then either $(|z^N|, |x^G|) = 1$ or $(|z^N|, |y^G|) = 1$. As N is a π -group, then $|z^N|$ either is a π_x -number or a π_y -number. If $\Gamma(N)$ is disconnected, we know by Theorem 2 of [3] that N is quasi-Frobenius group with Abelian kernel and complement. Moreover, $\Gamma(N)$ cannot be empty because by Step 3, N can be assumed to be non-Abelian. Consequently, we can assume that $\Gamma(N)$ is connected and this forces to either $|x^N| = 1$ or $|y^N| = 1$. Suppose for instance that $|x^N| = 1$, that is, $x \in \mathbf{Z}(N)$. Again by Step 3, we can take w an s -element of $N \setminus \mathbf{Z}(N)$ with $s \neq p$. Observe that $|w^N|$ must be a π_y -number, so w^G is connected to y^G in $\Gamma_G(N)$. As x and w have coprime orders and $x \in \mathbf{Z}(N)$ we have that $|w^G|$ and $|x^G|$ both divide $|(wx)^G|$. As a consequence, we have a contradiction because $|(wx)^G|$ has primes in π_x and π_y . Then we can suppose that N is not a π -group.

Step 5. Conclusion in case $p \neq q$.

Let z be a π' -element of $K \cap N$ and let us prove that $|z^G|$ is a π' -number. Suppose that $s \in \pi$ is a prime divisor of $|z^G|$. We can assume for instance that $s \in \pi_y$, otherwise we proceed analogously. Since $|z^G|$ divides $|(zx)^G|$ we deduce that s divides $|(zx)^G|$. Also, we know by Step 2 that $q \in \pi_x$. This forces $|(zx)^G|$ to be divisible by primes in π_x and π_y , a contradiction. Consequently, $s \notin \pi$ and $|z^G|$ is a π' -number, as wanted.

Let M be the subgroup generated by all π' -elements of $K \cap N$. We prove that M is a non-trivial normal subgroup of G . If $M \neq 1$, then $K \cap N$ would be a π -group and, since $|N : K \cap N| = |KN : K|$ divides $|G : K|$, which is a π -number too, then N would be a π -group, against Step 4. Let α be a generator of M , so $|\alpha^G|$ is π' -number. As $(|G : K|, |\alpha^G|) = 1$ we have $G = K\mathbf{C}_G(\alpha)$ and hence, $\alpha^G = \alpha^K \subseteq K \cap N$. Therefore $\alpha^G \subseteq M$, as wanted.

Let $D = \langle x^G, y^G \rangle$. Notice that $D \trianglelefteq G$ and $D \subseteq N$. Let α be a generator of M . As

we have proved in the above paragraph $|\alpha^G|$ is π' -number, and then $(|\alpha^G|, |x^G|) = 1$, so $G = \mathbf{C}_G(x)\mathbf{C}_G(\alpha)$. Thus, $x^G = x^{\mathbf{C}_G(\alpha)} \subseteq \mathbf{C}_G(\alpha)$ because $\alpha \in K$. The same happens for y , that is, $y^G \subseteq \mathbf{C}_G(\alpha)$, so we conclude that $[M, D] = 1$.

We define $L = MD$ and we distinguish two cases. Assume first that $L < N$. Note that $x, y \in L \trianglelefteq G$ and L trivially satisfies the hypotheses of the theorem. By applying induction to L we have $L = \mathbf{O}_\pi(L) \times \mathbf{O}_{\pi'}(L)$. Observe that the fact that $M \neq 1$ implies that $\mathbf{O}_{\pi'}(L) > 1$. Now, by definition of M , we have that $|K \cap N : M|$ is a π -number. As $|N : K \cap N|$ is also a π -number, it follows that $|N : \mathbf{O}_{\pi'}(L)|$ is a π -number too. Then $\mathbf{O}_{\pi'}(L) = \mathbf{O}_{\pi'}(N)$ is a Hall π' -subgroup of N . We can apply Lemma 2.2.1 so as to conclude that $N = \mathbf{O}_\pi(N) \times \mathbf{O}_{\pi'}(N)$ with $x, y \in \mathbf{O}_\pi(N)$. Since $\mathbf{O}_{\pi'}(N) > 1$, we apply the inductive hypotheses to $\mathbf{O}_\pi(N) < N$ and we deduce that $\mathbf{O}_\pi(N)$ is a quasi-Frobenius group with Abelian kernel and complement or $\mathbf{O}_\pi(N) = P \times A$ with $A \leq \mathbf{Z}(N)$ and P is a p -group, so the proof is finished.

From now on, we assume that $L = N$ and let us see that $\mathbf{Z}(N) = 1$ and $N = M \times D$ with $x, y \in D$. If $\mathbf{Z}(N) \neq 1$, we take $\bar{N} = N/\mathbf{Z}(N)$ and $\bar{G} = G/\mathbf{Z}(N)$. If $|\bar{x}^{\bar{G}}| = 1$, then $[\bar{x}, \bar{y}] = 1$, and thus $[x, y] \in \mathbf{Z}(N)$. Since $(o(x), o(y)) = 1$, it is easy to prove that $[x, y] = 1$, a contradiction. Analogously, we have $|\bar{y}^{\bar{G}}| \neq 1$. Consequently, \bar{N} satisfies the assumptions of the theorem. By induction, we have $\bar{N} = \mathbf{O}_{\pi'}(\bar{N}) \times \mathbf{O}_\pi(\bar{N})$ with $\bar{x}, \bar{y} \in \mathbf{O}_\pi(\bar{N})$ and $\mathbf{O}_\pi(\bar{N})$ is either a quasi-Frobenius group with Abelian kernel and complement or $\bar{N} = \bar{P} \times \bar{A}$ with $\bar{A} \leq \mathbf{Z}(\bar{N})$ and \bar{P} a p -group. In the latter case, $[\bar{y}, \bar{x}] = 1$ which leads to a contradiction as we have seen before. So we are in the former case. It follows that $N = \mathbf{O}_{\pi'}(N) \times \mathbf{O}_\pi(N)$ with $x, y \in \mathbf{O}_\pi(N)$ and by applying induction to $\mathbf{O}_\pi(N) < N$, we have the result. Therefore, $\mathbf{Z}(N) = 1$. On the other hand, we have proved that $[M, D] = 1$. Hence, $M \cap D \subseteq \mathbf{Z}(N) = 1$ and $N = M \times D$ with $x, y \in D$.

Since $M \neq 1$, we can apply induction to D and get $D = \mathbf{O}_{\pi'}(D) \times \mathbf{O}_\pi(D)$ with $x, y \in \mathbf{O}_\pi(D)$ and $\mathbf{O}_\pi(D)$ is a Frobenius group with Abelian kernel and complement (notice that $\mathbf{Z}(\mathbf{O}_\pi(D)) = 1$ because $\mathbf{Z}(N) = 1$). The p -group case cannot occur because x and y do not commute. Notice that if M is π' -group then the theorem is proved. Assume that M is not a π' -group and we seek a contradiction. Let $s \in \pi$ such that s divides $|M|$. We can assume that $s \in \pi_x$ (we proceed analogously if $s \in \pi_y$). Suppose that there exists an s' -element $z \in M$ such that $|z^M|$ is divisible by s . Since N is the direct product of M and D , we have that $(zy)^N = z^N y^N$ is a non-trivial class of N whose size is divisible by s and by some prime of $|y^N| \neq 1$. This is not possible because $|(zy)^G|$ would have primes in π_x and π_y . Thus, the class size of every s' -element of M is a s' -number. By Lemma 2.2.2, we have $M = M_1 \times S$ with $S \in \text{Syl}_s(M)$. In this case, $\mathbf{Z}(S) \subseteq \mathbf{Z}(N) = 1$, which is a contradiction.

Step 6. Conclusion in case $p = q$.

Let $K = \mathbf{C}_G(x) \cap \mathbf{C}_G(y)$ as in Step 2. Let z be a p' -element of $K \cap N$ and let us prove that $|z^G|$ is a π' -number. Suppose that $s \in \pi$ is a prime divisor of $|z^G|$. We can assume without loss that $s \in \pi_y$. Since $|z^G|$ divides $|(zx)^G|$ we obtain that s divides $|(zx)^G|$. On the other hand, we know by the proof of Step 2 that $q \in \pi_x$. Therefore, $|(zx)^G|$ is divisible by primes in π_x and π_y , a contradiction. As a consequence, $s \notin \pi$

and $|z^G|$ is a π' -number, as wanted.

Let T be the subgroup generated by all p' -elements of $K \cap N$. We prove that T is a non-trivial normal subgroup of G . In fact, $T \neq 1$ because otherwise $K \cap N$ would be a π -group and this implies that N is a π -group by arguing as in Step 5, and this contradicts Step 4. If α is a generator of T , we know that $|\alpha^G|$ is π' -number. Then $(|G : K|, |\alpha^G|) = 1$, so we have $G = K\mathbf{C}_G(\alpha)$ and $\alpha^G = \alpha^K \subseteq K \cap N$. This proves that $\alpha^G \subseteq T$, as we wanted to prove.

As the class size of every p' -element of T is a p' -number then, by using Lemma 2.2.2, we have $T = \mathbf{O}_p(T) \times \mathbf{O}_{p'}(T)$. However, by definition of T , we have $\mathbf{O}_p(T) = 1$, or equivalently $M = \mathbf{O}_{p'}(T)$. Notice that if $s \in \pi$ and $s \neq p$, then the class size of every element of T is an s' -number so, it is elementary that T has a central Sylow s -subgroup and we can write $T = \mathbf{O}_\pi(T) \times \mathbf{O}_{\pi'}(T)$. On the other hand, $|N : T| = |N : K \cap N| |K \cap N : T|$ where $|N : K \cap N| = |KN : K|$ is a π -number and $|K \cap N : T|$ is a power of $p \in \pi$. Therefore $\mathbf{O}_{\pi'}(T) = \mathbf{O}_{\pi'}(N)$ and $\mathbf{O}_{\pi'}(N)$ is a Hall π' -subgroup of N . We have proved that the class size of every p' -element of N is a π' -number, so by Lemma 2.2.1, we have $N = \mathbf{O}_{\pi'}(N) \times \mathbf{O}_\pi(N)$. We apply induction to $\mathbf{O}_\pi(N) < N$ and the proof is finished. \square

Proof of Corollary 2.1.2. It follows immediately by Theorem 2.1.1. We only have to notice that if $x, y \in \mathbf{O}_{\pi'}(N)$ and $z \in \mathbf{O}_{\pi'}(N) \setminus \mathbf{Z}(G)$ it is easy to get that there is a path connecting x^G and y^G because $(xz)^G$ is connected to x^G and $(yz)^G$ which is connected to y^G . This contradicts the hypotheses of the theorem. Thus, $\mathbf{O}_{\pi'}(N) \leq \mathbf{Z}(G)$. By the same argument, we obtain $A \leq \mathbf{Z}(G)$ when $\mathbf{O}_\pi(N) = P \times A$. \square

Proof of Corollary 2.1.3. It trivially follows by Theorem 2.1.1. \square

We give an example showing that the converse of Theorem 2.1.1 is not true.

Example 2.2.4. We take the Special Linear group $H = \mathrm{SL}(2, 5)$ which is a group of order 120 that acts Frobeniusly on $K = \mathbb{Z}_{11} \times \mathbb{Z}_{11}$. Let $P \in \mathrm{Syl}_5(H)$ and we consider $\mathbf{N}_H(P)$. Then we define $N := KP$, which trivially is a normal subgroup of $G := K\mathbf{N}_H(P)$. We have that the set of the G -conjugacy class sizes of N is $\{1, 20, 242\}$. The graph $\Gamma_G(N)$ consists of exactly two vertices joint by an edge. Obviously, N is a Frobenius group with Abelian kernel and complement and there do not exist two non-central G -classes in N such that any non-central G -class of N has size coprime with one of both.

Let us see two examples illustrating each of the cases that appear in Theorem 2.1.1.

Example 2.2.5. We take the following groups from the library SmallGroups of GAP ([7]). Let $G_1 = \mathrm{Id}(324, 8)$ and $G_2 = \mathrm{Id}(168, 44)$ (in fact, G_2 is the Semi Linear Affine group of order 168) that have the normal subgroups: the Abelian 3-subgroup $P = \mathbb{Z}_3 \times \mathbb{Z}_3$ and $A = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, respectively. It is easy to check that P has four G_1 -classes which sizes are 1, 2, 3 and 3, and A has two G_2 -classes of size 1 and 7. We construct $N = P \times A$ and $G = G_1 \times G_2$. We have that N is a normal subgroup of G and the set of G -conjugacy class sizes of N is $\{1, 2, 3, 7, 14, 21\}$. Therefore, $d(\Gamma_G(N)) = 3$ and N is the direct product of a 3-group and $A \leq \mathbf{Z}(N)$. Notice that in this example we have $\mathbf{O}_{\pi'}(N) = 1$ and $\pi = \{2, 3, 7\}$.

Example 2.2.6. *The quasi-Frobenius case in Theorem 2.1.1 is the natural extension of the ordinary case. It is enough to consider any group G and $N = G$ such that $\Gamma(G) = \Gamma_G(N)$ has two connected components. By the main theorem of [3], we know that G is a quasi-Frobenius group with Abelian kernel and complement.*

Acknowledgements

The results in this paper are part of the third author's Ph.D. thesis at the University Jaume I of Castellón. We would like to thank Professor A. Mann for his English translation of [8]. The research of the first and second authors is 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.

Bibliography

- [1] A. Beltrán and M.J. Felipe, Prime powers as conjugacy class lengths of π -elements. *Bull. Austral. Math. Soc.* **69** (2004), 317-325.
- [2] A. Beltrán, M.J. Felipe and C. Melchor, Graphs associated to conjugacy classes of normal subgroups in finite groups. *J. Algebra*, **443** (2015), 335-348.
- [3] E.A. Bertram, M. Herzog and A. Mann, On a graph related to conjugacy classes of groups. *Bull. London Math. Soc.*, **22** (6) (1990), 569-575.
- [4] A.R. Camina, Arithmetical conditions on the conjugacy class numbers of a finite group. *J. London Math. Soc. (2)* **5** (1972), 127-132.
- [5] S. Dolfi, Arithmetical conditions of the length of the conjugacy classes in finite groups. *J. Algebra*, **174**, (3) (1995), 753-771.
- [6] C. Casolo, S. Dolfi, The diameter of a conjugacy class graph of finite groups. *Bull. London Math. Soc.* **28** (1996), 141-148.
- [7] The GAP Group, GAP - Groups, Algorithms and Programming, Vers. 4.4.12 (2008). <http://www.gap-system.org>
- [8] L.S. Kazarin, On groups with isolated conjugacy classes, *Izv. Vyssh. Uchebn. Zaved. Mat.* (7) (1981), 40-45.

Chapter 3

Triangles in the graph of conjugacy classes of normal subgroups

Abstract

Let G be a finite group and N a normal subgroup of G . We determine the structure of N when the graph $\Gamma_G(N)$, which is the graph associated to the conjugacy classes of G contained in N , has no triangles and when the graph consists in exactly one triangle.

Keywords. Finite groups, conjugacy classes, normal subgroups, graphs.

Mathematics Subject Classification (2010): 20E45, 20D15.

3.1 Introduction

Let G be a finite group and let N be a normal subgroup of G and let $x \in N$. We denote by $x^G = \{x^g \mid g \in G\}$ the G -conjugacy class of x . Let $\Gamma_G(N)$ be the graph associated to these G -conjugacy classes, which was defined in [2] as follows: its vertices are the G -conjugacy classes of N of cardinality bigger than 1, that is, G -classes of elements in $N \setminus (\mathbf{Z}(G) \cap N)$, and two of them are joined by an edge if their sizes are not coprime.

The above graph extends the ordinary graph, $\Gamma(G)$, which was formerly defined in [1], whose vertices are the non-central conjugacy classes of G and two vertices are joined by an edge if their sizes are not coprime. The graph $\Gamma_G(N)$ can be viewed as the subgraph of $\Gamma(G)$ induced by those vertices of $\Gamma(G)$ which are contained in N . This fact does not allow us to obtain directly properties of the graph of G -classes.

On the other hand, the graph $\Gamma_G(N)$ is not related to $\Gamma(N)$. In fact, the action of a finite group G on a normal subgroup N determines that the conjugacy classes of N are grouped into G -classes and it is possible to find primes dividing some G -class sizes of N which do not divide the order of N . However, the study of these classes and their sizes has emerged as a new useful tool to obtain information regarding normal subgroups from a new point of view.

In this paper we analyze the structure properties of N in two particular cases: when $\Gamma_G(N)$ has no triangles and when it consists in exactly one triangle. In the

following theorem, we extend known results appeared for the graph $\Gamma(G)$ when it has no triangles. In fact, in [6] Fang and Zhang gave a complete list of those groups G whose graph $\Gamma(G)$ has no triangles. These groups are exactly: the symmetric group S_3 , the dihedral group D_{10} , the three pairwise non-isomorphic non-abelian groups of order 12, and the non-abelian group of order 21. In order to obtain our result we firstly need to study the structure of N when $\Gamma_G(N)$ has few vertices: exactly one, two or three. The structure of normal subgroups which are union of three or four G -conjugacy classes already appeared in [10] and [9], respectively. However, in these papers central G -classes are also contemplated, and we need to exclude them. We remark that some of the results that we obtain for $\Gamma_G(N)$ are not possible for $\Gamma(G)$.

Theorem A. *Let N be a non-central normal subgroup of a finite group G such that $\Gamma_G(N)$ has no triangles. Then N is a $\{p, q\}$ -group and satisfies one of these properties*

1. N is a p -group.
2. $N = P \times Q$ with P a p -group and $Q \subseteq \mathbf{Z}(G) \cap N$, $Q \cong \mathbb{Z}_2$.
3. $N = P \times Q$ with P a p -group and Q a q -group both elementary abelian with p and q odd primes. In this case $\mathbf{Z}(G) \cap N = 1$.
4. N is a quasi-Frobenius group with abelian kernel and complement and $\mathbf{Z}(G) \cap N \cong \mathbb{Z}_2$.
5. N is a Frobenius group with complement isomorphic to \mathbb{Z}_q , \mathbb{Z}_{q^2} or Q_8 . In the first case, the kernel of N is a p -group with exponent less or equal than p^2 and in the two latter cases, the kernel of N is p -elementary abelian.

We recall that a group G is said to be quasi-Frobenius if $G/\mathbf{Z}(G)$ is Frobenius and then the preimage in G of its kernel and complement are called the kernel and complement of G .

Returning to the ordinary case, the structure of a group G having exactly three non-central classes forming a triangle in $\Gamma(G)$ is very limited. We give a proof here.

Theorem B. *Let G be a finite group such that $\Gamma(G)$ consists exactly of one triangle. Then $G \cong Q_8$ or $G \cong D_8$.*

We study the structure of a normal subgroup N when $\Gamma_G(N)$ consists in exactly one triangle.

Theorem C. *Let N be a normal subgroup of a finite group G . If $\Gamma_G(N)$ has exactly one triangle, then one of the following possibilities holds:*

1. N is a p -group for some prime p .
2. $N = P \times Q$, with P p -elementary abelian and Q q -elementary abelian for some primes p and q , and $\mathbf{Z}(G) \cap N = 1$.
3. $N = P \times Q$, with P a p -group for a prime $p \neq 3$, and $Q \subseteq \mathbf{Z}(G) \cap N$, $Q \cong \mathbb{Z}_3$ and $P/(\mathbf{Z}(G) \cap P)$ has exponent p .

4. $N = PQ$, where P is a Sylow p -subgroup, $p \neq 2$ and Q is a Sylow 2-subgroup of N . In addition, P has exponent p , $|\mathbf{Z}(G) \cap N| = 2$ and $Q/(\mathbf{Z}(G) \cap N)$ is 2-elementary abelian.
5. Either N is a Frobenius group with complement \mathbb{Z}_q , \mathbb{Z}_{q^2} or Q_8 for a prime q , or there are two primes p and q such that $N/\mathbf{O}_p(N)$ is a Frobenius group of order pq and $\mathbf{O}_p(N)$ has exponent p . In this case, $\mathbf{Z}(G) \cap N = 1$.
6. $N \cong A_5$ and $G = (N \times K)\langle x \rangle$ for some $K \leq G$ and $x \in G$, with $x^2 \in N \times K$ and $G/K \cong N\langle x \rangle \cong S_5$.

We will provide examples for all the cases with the help of [11]. In particular, we see that the still open S_3 -conjecture, which asserts that any finite group in which distinct conjugacy classes have distinct sizes is isomorphic to the symmetric group S_3 , does not hold for G -conjugacy classes lying in a normal subgroup. All groups are supposed to be finite.

3.2 Preliminary results

We state some preliminary results which are necessary for the proofs. In [2], the authors obtained the following three theorems, which concern the case where the graph $\Gamma_G(N)$ is disconnected. We denote by $n(\Gamma_G(N))$ the number of connected components of $\Gamma_G(N)$.

Theorem 3.2.1. *Let G be group and let N be a normal subgroup of G , then $n(\Gamma_G(N)) \leq 2$.*

Theorem 3.2.2. *Let G be a group and let N be a normal subgroup of G . If $\Gamma_G(N)$ has two connected components then, either N is quasi-Frobenius with abelian kernel and complement, or $N = P \times A$ where P is a p -group and $A \leq \mathbf{Z}(G)$.*

Theorem 3.2.3. *Let G be a group and let N be a normal subgroup of G . If $n(\Gamma_G(N)) = 2$, each of its connected components is a complete graph.*

It will be hugely important to use the following two results concerning CP-groups, that is, those groups having all elements of prime-power order, due to Higman ([7]) and Deaconescu ([4]), respectively.

Theorem 3.2.4. *Let G be a solvable group all of whose elements have prime power order. Let p be the prime such that G has a normal p -subgroup greater than 1, and let P be the greatest normal p -subgroup of G . Then $G = P$ or G/P is either*

1. a cyclic group whose order is a power of a prime other than p ; or
2. a generalized quaternion group, p being odd; or
3. a group of order $p^a q^b$ with cyclic Sylow subgroups, q being a prime of the form $kp^a + 1$.

Thus, G has order divisible by at most two primes, and G/P is metabelian.

We note that in cases 1 and 2 of the above theorem, G is a Frobenius group since it is immediate that a p -complement of G acts fixed-point-freely on P . In 3, however, G/P is a Frobenius group.

Theorem 3.2.5. *Let G be a group having all nontrivial elements of prime order. Then one of the following cases occurs:*

1. G is a p -group of exponent p .
2. (a) $|G| = p^a q$, $3 \leq p < q$, $a \geq 3$, $|F(G)| = p^{a-1}$, $|G : G'| = p$.
 (b) $|G| = p^a q$, $3 \leq q < p$, $a \geq 1$, $|F(G)| = |G'| = p^a$.
 (c) $|G| = 2^a p$, $p \geq 3$, $a \geq 2$, $|F(G)| = |G'| = 2^a$.
 (d) $|G| = 2p^a$, $p \geq 3$, $a \geq 1$, $|F(G)| = |G'| = p^a$. and $F(G)$ is elementary abelian.
3. $G \cong A_5$.

3.3 $\Gamma_G(N)$ with one vertex

We start with some properties of those normal subgroups having exactly one non-central G -conjugacy class. We stress, however, that for any group G , it is elementary that the case in which $\Gamma(G)$ has exactly one vertex cannot happen.

Theorem 3.3.1. *If G is a group and N is a normal subgroup of G such that $\Gamma_G(N)$ has only one vertex, then N is a p -group for some prime p and $N/(N \cap \mathbf{Z}(G))$ is an elementary abelian p -group.*

Proof. Since $\Gamma_G(N)$ has one vertex, the set $N \setminus (N \cap \mathbf{Z}(G))$ consists of exactly one G -conjugacy class and so, $N/(N \cap \mathbf{Z}(G))$ is characteristically simple. Thus, $N/(N \cap \mathbf{Z}(G))$ is p -elementary abelian for some prime p . Moreover, $N \cap \mathbf{Z}(G)$ is also a p -group, and as a consequence, N is a p -group too. In fact, if a prime $q \neq p$ divides $|N \cap \mathbf{Z}(G)|$, then $N/(N \cap \mathbf{Z}(G))$ would have elements of order divisible by p and q , a contradiction. \square

Example 3.3.2. *Let $G = SL(2, 3)$ and let N be the normal subgroup of G isomorphic to Q_8 . Then $\Gamma_G(N)$ has exactly one vertex of size 6 and $N/(\mathbf{Z}(G) \cap N)$ has exponent 2.*

3.4 $\Gamma_G(N)$ with two vertices

We divide this section into two cases: when there are exactly two vertices joined by an edge, and when they are not joined.

3.4.1 $\Gamma_G(N)$ with two vertices without edge

It was proved in [1] that if $\Gamma(G)$ has vertices but no edges, then G is isomorphic to S_3 , and this is clearly not true for $\Gamma_G(N)$, just take for instance $G = S_3$ and $N = A_3$ or Example 1. The following property helps us to further refine the structure of these normal subgroups.

Lemma 3.4.1. *Let N be a normal subgroup of a group G . If $\Gamma_G(N)$ has two vertices but no edges, then $\mathbf{Z}(G) \cap N = 1$.*

Proof. Let A and B be the two vertices of $\Gamma_G(N)$ and let $z \in \mathbf{Z}(G) \cap N$. Then zA is a G -class of N of cardinality $|A|$. Hence, $zA = A$ and $\langle z \rangle A = A$. Thus, $|\langle z \rangle|$ divides $|A|$. Similarly, we deduce that $|\langle z \rangle|$ divides $|B|$ and since $(|A|, |B|) = 1$, we conclude that $z = 1$. Thus, $\mathbf{Z}(G) \cap N = 1$. \square

Recall that a conjugacy class A of a group G is said to be real if $A^{-1} = A$, and an element $g \in G$ is real if there exists $x \in G$ such that $g^x = g^{-1}$. Of course, all elements of order 2 in G are real. We note that if A is the unique class of size $|A|$ inside a certain set of classes containing A^{-1} , then the fact that $|A| = |A^{-1}|$ proves that A is necessarily real. Another elementary property, which is used in the sequel, is that if x^G is real and $|x^G|$ is odd, then $x^2 = 1$.

Theorem 3.4.2. *Let N be a normal subgroup of a group G such that $\Gamma_G(N)$ has two vertices and no edge. Then N is a 2-group or a Frobenius group with p -elementary abelian kernel K , and complement H , which is cyclic of order q , for two different primes p and q . In particular, $|N| = p^n q$ with $n \geq 1$.*

Proof. By Theorem 3.2.2 we know that either $N = P \times A$ with $A \leq \mathbf{Z}(G)$ or N is quasi-Frobenius with abelian kernel and complement. In the first case, by Lemma 3.4.1 we obtain that A is trivial. On the other hand, notice that one of the G -classes of the graph has odd size, so it is real, and this implies that N has elements of order 2. Consequently, N is a 2-group.

Suppose now that N is quasi-Frobenius with kernel K and complement H , both abelian. It is trivial that there must exist elements of order p and order q in N for two different primes p and q . If $\mathbf{Z}(N) \neq 1$, then N would have elements of at least three different orders. Thus, $\mathbf{Z}(N) = 1$, which means that N is a Frobenius group. Now, since p and q are the only possible orders for the elements of N , we have that all nontrivial elements in K must have the same order, say p , and since K is abelian, we conclude that K is p -elementary abelian. Furthermore, it is well-known that the Sylow subgroups of H are cyclic or generalized quaternion. Nevertheless, since all elements of H have the same order, we conclude that H is cyclic of order q . \square

Example 3.4.3. *Let $G = S_4$ and let $N = A_4$. The G -classes of N have sizes $\{1, 3, 8\}$ and accordingly, $\Gamma_G(N)$ has two vertices and no edge.*

3.4.2 $\Gamma_G(N)$ with two vertices and one edge

We remark that this case does not occur when dealing with the ordinary graph $\Gamma(G)$. In fact, as we pointed out in the Introduction, the complete list of those groups G whose graph $\Gamma(G)$ has no triangles proves that the graph $\Gamma(G)$ can never have exactly two vertices joined by an edge.

Hereafter $\pi(G)$ will denote the set of primes dividing the order of G . We prove first the following property, which will also be used to prove Theorem A.

Lemma 3.4.4. *Let N be a normal subgroup of a group G . Suppose that $\Gamma_G(N)$ is non-empty, has no triangles and that $|N|$ is not a prime power. Then either $\mathbf{Z}(G) \cap N = 1$ or $|\mathbf{Z}(G) \cap N|_2 = 2$.*

Proof. Suppose that $\mathbf{Z}(G) \cap N > 1$. Since N is not abelian and has not prime power order, we can trivially take a q -element $z \in \mathbf{Z}(G) \cap N$ and a p -element $x \in N \setminus \mathbf{Z}(G) \cap N$ for two distinct primes p and q . If $q > 2$, then x^G , $(zx)^G$ and $(z^2x)^G$ would be three distinct G -classes of N forming a triangle in $\Gamma_G(N)$, a contradiction. This implies that $q = 2$. Now, if $|\mathbf{Z}(G) \cap N|_2 > 2$, we can take two distinct nontrivial 2-elements $z_1, z_2 \in \mathbf{Z}(G) \cap N$, whence the G -classes x^G , $(xz_1)^G$ and $(xz_2)^G$ are distinct too and again we have a triangle in $\Gamma_G(N)$. Therefore, $|\mathbf{Z}(G) \cap N|_2 = 2$. \square

Theorem 3.4.5. *Let N be a normal subgroup of a group G such that $\Gamma_G(N)$ has exactly two vertices and one edge. Then one of the following possibilities holds:*

1. N is a p -group for a prime p .
2. $N = P \times Q$ with $P/(\mathbf{Z}(G) \cap P)$ an elementary abelian p -group with p an odd prime, and $Q \subseteq \mathbf{Z}(G) \cap N$ and $Q \cong \mathbb{Z}_2$.
3. N is a Frobenius group with p -elementary abelian kernel K and complement $H \cong \mathbb{Z}_q$ for some distinct primes p and q . In particular, $|N| = p^a q$ for some $a \geq 1$ and the G -classes of N have cardinality 1, $(p^a - 1)$ and $p^a(q - 1)$.

Proof. We divide the proof into two cases, depending on whether $\overline{N} = N/(\mathbf{Z}(G) \cap N)$ is a p -group or not.

a) Suppose first that \overline{N} is a p -group for some prime p . If $\mathbf{Z}(G) \cap N$ is also a p -group, we trivially have the first assertion. Thus, we can assume that $\mathbf{Z}(G) \cap N$ is nontrivial and apply Lemma 3.4.4, so $|\mathbf{Z}(G) \cap N|_2 = 2$.

Now, observe that N is nilpotent because \overline{N} is a p -group. We prove that $\mathbf{Z}(G) \cap N$ is a $\{2, p\}$ -group and consequently, N will be a $\{2, p\}$ -group too. In fact, if there exists $r \in \pi(\mathbf{Z}(G) \cap N)$ with $r \neq 2, p$, then we can find in $N \setminus (\mathbf{Z}(G) \cap N)$ elements of order divisible by $2r$ and pr , which is a contradiction. Therefore, N is a nilpotent $\{2, p\}$ -group and we can write $N = P \times Q$ with P a p -group (p odd) and Q a 2-group. Also, we have proved that $Q \cong \mathbb{Z}_2$ and $Q \subseteq \mathbf{Z}(G)$. Now, the G -classes of N are exactly the products of the G -classes of P by the two (central) classes of Q and, by the structure of the graph, it follows that P has exactly one nontrivial G -class. This forces $P/(\mathbf{Z}(G) \cap P)$ to be p -elementary abelian by Theorem 3.3.1, and this completes the structure of N described in 2.

b) Assume that \overline{N} has not prime power order and take two distinct primes $p, q \in \pi(\overline{N})$. Hence there exist p -elements and q -elements in $N \setminus (\mathbf{Z}(G) \cap N)$. Moreover, all p -elements of $N \setminus (\mathbf{Z}(G) \cap N)$ form a single non-central G -class and the q -elements form the other one. No more primes can be involved in $\pi(\overline{N})$. We note that $\mathbf{Z}(G) \cap N = 1$ because otherwise, the product of one element of prime order of $N \cap \mathbf{Z}(G)$ by the elements of $N \setminus (\mathbf{Z}(G) \cap N)$ produce elements in $N \setminus (\mathbf{Z}(G) \cap N)$ whose order is divisible by more than one prime. This means that N is a $\{p, q\}$ -group, and in particular, by $p^a q^b$ -Burnside's Theorem, N is solvable. Let $M \leq N$ be a minimal normal subgroup of G , which is elementary abelian, say for instance, a p -group. As M is proper in N and is the union of G -classes, M is equal to the union of the trivial class and one of the non-central G -classes of N . Then every element of

$N \setminus M$ is a q -element, so $M \in \text{Syl}_p(N)$.

Now, if $Q \in \text{Syl}_q(N)$, then Q acts Frobeniusly on M , because N cannot have elements of order divisible by pq . Moreover, Q must be cyclic or generalized quaternion. As we have seen that all nontrivial q -elements have the same order, we conclude that Q is cyclic of order q . \square

The following examples illustrate the results obtained in the above theorem.

Example 3.4.6. Let $G = SL(2, 3) \times \langle z \rangle$ with $\langle z \rangle \cong \mathbb{Z}_2$. The group $SL(2, 3)$ has a normal subgroup $K \cong Q_8$ and we set $N = K \times \langle z \rangle$. Then $\mathbf{Z}(G) \cap N = \mathbf{Z}(K) \times \langle z \rangle$, so $|\mathbf{Z}(G) \cap N| = 4$, and the non-central G -classes of N are:

$$\begin{aligned} (x, 1)^G &= \{(x, 1) | x \in K \setminus \mathbf{Z}(K)\} \\ (x, z)^G &= \{(x, z) | x \in K \setminus \mathbf{Z}(K)\}. \end{aligned}$$

Moreover, $|(x, 1)^G| = |(x, z)^G| = 6$, so $\Gamma_G(N)$ has two vertices joined by an edge. This example corresponds to case 1.

We show two examples of case 2. In the first one, N is abelian whereas in the second, it is not. We also give an example of case 3 of Theorem 3.4.5.

Example 3.4.7. Let p be an odd prime and let $N = \langle x_1 \rangle \times \dots \times \langle x_n \rangle \times \langle z \rangle$ with $\langle x_i \rangle \cong \mathbb{Z}_p$ for $i = 1, \dots, n$ and $\langle z \rangle \cong \mathbb{Z}_2$, so $|N| = 2p^n$. Let us consider $H \cong GL(n, p)$ the group of automorphisms of $K = \langle x_1 \rangle \times \dots \times \langle x_n \rangle$ and suppose that H acts trivially on $\langle z \rangle$. We construct the corresponding semidirect product $G = NH$. Then $\mathbf{Z}(G) \cap N = \langle z \rangle$, so $|\mathbf{Z}(G) \cap N| = 2$, and the non-central G -classes of N are

$$\begin{aligned} \{x_1^{i_1} \dots x_n^{i_n} \mid (i_1, \dots, i_n) \neq (0, \dots, 0), 0 \leq i_j \leq p-1\}. \\ \{x_1^{i_1} \dots x_n^{i_n} z \mid (i_1, \dots, i_n) \neq (0, \dots, 0), 0 \leq i_j \leq p-1\}. \end{aligned}$$

Thus, $\Gamma_G(N)$ has exactly two vertices, corresponding to the above two classes, both of size $p^n - 1$ and trivially joined by an edge.

Example 3.4.8. Let P be the extraspecial p -group of order p^3 and exponent p (p odd):

$$P = \langle a, b, c \mid a^p = 1, b^p = 1, c^p = 1, [a, b] = [b, c] = 1, [a, c] = b \rangle.$$

We have $P = \{a^i b^j c^k \mid 0 \leq i, j, k \leq p-1\}$ and observe that $\mathbf{Z}(P) = \langle b \rangle$. The group $\text{Aut}(P)$ is known (see for instance, Theorem 20.8 of [5]), has order $p^3(p-1)^2(p+1)$ and it turns out that every $\varphi \in \text{Aut}(P)$ is determined by: $\varphi(a) = a^i b^j c^k$; $\varphi(b) = b^m$, with $0 < m \leq p-1$; and $\varphi(c) = a^q b^r c^s$, satisfying further that $m \equiv is - qk \not\equiv 0 \pmod{p}$ with $0 \leq i, j, k, q, r, s \leq p-1$.

Notice that there always exists an automorphism of P leading a to any non-central element of P . Furthermore, we can set $m = 1$, that is, the image of a can be chosen in such a way that all elements of $\mathbf{Z}(P)$ are fixed element by element. Set $H = \{\varphi \in \text{Aut}(P) \mid \varphi(b) = b\}$ and let us consider the semidirect product $G = (P \times \langle z \rangle) \rtimes H$, where $\langle z \rangle \cong \mathbb{Z}_2$, and H acts naturally on P and trivially on $\langle z \rangle$. Let $N = P \times \langle z \rangle$. It follows that $\mathbf{Z}(G) \cap N = \langle b \rangle \times \langle z \rangle$, so $|\mathbf{Z}(G) \cap N| = 2p$, and the non-central G -classes of N are $(x, 1)^G = \{(x, 1) \mid x \in P \setminus \mathbf{Z}(P)\}$ and $(x, z)^G = \{(x, z) \mid x \in P \setminus \mathbf{Z}(P)\}$. Then $|(x, 1)^G| = |(x, z)^G| = p^3 - p$ and $\Gamma_G(N)$ has two vertices joined by an edge.

Example 3.4.9. We use the semilinear affine group $\Gamma(p^n)$ for appropriate p and n . We remind the construction of this group, although for a more detailed description we refer the reader to Section 2 of [8]. Let $GF(p^n)$ be the finite field of p^n elements. The multiplicative group $H = GF(p^n)^*$ is cyclic of order $p^n - 1$ and acts on the additive group of $GF(p^n)$, say $K = \langle x_1 \rangle \oplus \dots \oplus \langle x_n \rangle \cong \mathbb{Z}_p \times \dots \times \mathbb{Z}_p$ in the following way: if $a \in H$ and $x \in K$, then $x^a = ax$. This action is Frobenius, so KH is a Frobenius group with abelian kernel and complement. On the other hand, we know that α , defined by $x^\alpha = x^p$ for all $x \in K$, is another automorphism of K of order n in such a way that $H\langle\alpha\rangle \leq \text{Aut}(K)$. Then $\Gamma(p^n)$ is defined by the semidirect product $\Gamma(p^n) = K \rtimes (H\langle\alpha\rangle)$.

Now, suppose that p is odd, $n = 2$ and $S \leq H$ is a cyclic subgroup of order $s = 3$ (note that we need to assume that 3 divides $p^2 - 1$). One can easily check that $N = KS$ is normal in G , and that N is a Frobenius group with abelian kernel and complement. The two nontrivial G -classes of N consist of the $p^2 - 1$ elements of $K \setminus \{1\}$, and all the elements of $\bigcup_{g \in G} (S^g \setminus \{1\}) = \bigcup_{k \in K} (S^k \setminus \{1\})$, which are exactly $(|S| - 1)|K| = 2p^2$ elements. As $(2p^2, p^2 - 1) = 2$, we obtain case 3.

3.5 $\Gamma_G(N)$ with three vertices

We distinguish the following three possibilities: $\Gamma_G(N)$ is disconnected with three vertices, $\Gamma_G(N)$ is connected having exactly one triangle or $\Gamma_G(N)$ has three vertices in a line. The former two possibilities may happen for the ordinary graph $\Gamma(G)$. In fact, $\Gamma(G)$ is disconnected with three vertices if and only if $G \cong D_{10}$ or $G \cong A_4$ (see [6]). In subsection 5.2, we will study the case in which $\Gamma(G)$ is exactly a triangle, by showing that $G \cong Q_8$ or $G \cong D_8$. However, the latter case, three vertices in a line, do not occur for the ordinary graph ([6]).

3.5.1 $\Gamma_G(N)$ disconnected with three vertices

Theorem 3.5.1. Let N be a normal subgroup of a group G . If $\Gamma_G(N)$ has three vertices and one edge, then N is a $\{p, q\}$ -group for two primes p and q . Furthermore, either

- 1) N is a p -group, or
- 2) N is a quasi-Frobenius group with abelian kernel and complement. In this case, $|N \cap \mathbf{Z}(G)| = 1$ or 2.

Proof. The graph $\Gamma_G(N)$ has the form:



and by Theorem 3.2.2, we know that either N is quasi-Frobenius with abelian kernel and complement, or $N = P \times A$ where P is a p -group and $A \leq \mathbf{Z}(G)$. Suppose the second case. We can certainly assume that A is a p' -group. If $A > 1$, then every non-central G -class of N is the product of a non-central G -class of P by a (central) class of A . By hypothesis, the number of non-central G -classes of N is 3 and this occurs if and only if either $|A| = 3$ and P has exactly one non-central G -class, or

$|A| = 1$ and P has 3 non-central G -classes. However, in the former case, the three G -classes would form a triangle, so we conclude that N is a p -group.

Assume now that N is quasi-Frobenius with abelian kernel and complement. We claim that N is a $\{p, q\}$ -group for two primes p and q . First, suppose that $\mathbf{Z}(G) \cap N = 1$. If $|N|$ is divisible by three distinct primes, then the existence of exactly three G -classes implies that all elements of N necessarily have prime order and, by Theorem 3.2.5, N is a $\{p, q\}$ -group or $N \cong A_5$. Since N is clearly solvable, we are finished. Now, if $\mathbf{Z}(G) \cap N > 1$, by Lemma 3.4.4, we can assume $|\mathbf{Z}(G) \cap N|_2 = 2$. If $|N/(\mathbf{Z}(G) \cap N)|$ is divisible by two primes p and q , both different from 2, then we can multiply a central 2-element by a p -element and a q -element of N in order to get non-central elements of order divisible by $2p$ and $2q$, respectively, and this contradicts the hypothesis. Hence, for instance $p = 2$, and N is a $\{2, q\}$ -group. In order to conclude this case it is enough to see that $|N \cap \mathbf{Z}(G)|_q = 1$. In fact, if there exists a nontrivial q -element in $x \in \mathbf{Z}(G) \cap N$, we choose a 2-element $y \in N \setminus (\mathbf{Z}(G) \cap N)$, and then y^G , $(xy)^G$ and $(x^2y)^G$ are three non-central G -classes of N with the same cardinality, a contradiction. \square

Example 3.5.2. *If we consider $G = N = A_4$, then $\Gamma_G(N)$ has three vertices and one edge. This example illustrates case 1. On the other hand, the group of the Small groups library of GAP with number Id (324, 8) has an abelian normal subgroup $N \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ whose G -class sizes are 1, 2, 3 and 3. This example shows case 2.*

3.5.2 $\Gamma_G(N)$ with exactly one triangle

In this section we prove Theorems B and C. We analyze first the ordinary case.

Proof of Theorem B. By the class equation, we have

$$|G| = |\mathbf{Z}(G)| + |a^G| + |b^G| + |c^G|,$$

where a^G, b^G and c^G are the three non-central classes of G . Since $\mathbf{Z}(G) \subset \mathbf{C}_G(x) \subset G$, for $x = a, b, c$, then

$$1 = \frac{|\mathbf{Z}(G)|}{|G|} + \frac{1}{|\mathbf{C}_G(a)|} + \frac{1}{|\mathbf{C}_G(b)|} + \frac{1}{|\mathbf{C}_G(c)|} \leq \frac{|\mathbf{Z}(G)|}{|G|} + \frac{3}{2|\mathbf{Z}(G)|}.$$

Therefore,

$$\frac{3}{4} \leq 1 - \frac{|\mathbf{Z}(G)|}{|G|} \leq \frac{3}{2|\mathbf{Z}(G)|}$$

and thus, $|\mathbf{Z}(G)| \leq 2$. If $|\mathbf{Z}(G)| = 2$, then

$$1 \leq \frac{|\mathbf{Z}(G)|}{|G|} + \frac{3}{2|\mathbf{Z}(G)|} \leq \frac{2}{|G|} + \frac{3}{4}.$$

This implies that $|G| \leq 8$ and necessarily $G \cong Q_8$ or $G \cong D_8$.

Suppose now that $\mathbf{Z}(G) = 1$ and we seek a contradiction. If $|G|$ is divisible by three different primes, then by applying the hypotheses, G should have all nontrivial elements of prime order, so by applying Theorem 3.2.5, we get $G \cong A_5$, which has exactly four non-central classes, a contradiction. Thus, we can assume that G is a p -group or a $\{p, q\}$ -group for two distinct primes p and q . Since $\Gamma(G)$ consists exactly of one triangle, one prime, say for instance p , must divide the size of every non-central class of G , and then by the class equation, p must divide $|\mathbf{Z}(G)|$, a contradiction too, as wanted. \square

The authors would like to thank Professor Haipeng Qu from Shanxi Normal University of Linfen, PR China, for his improvements in the original proof of the above theorem.

Proof of Theorem C. If N is a p -group, we have case 1, so we can assume that $|N|$ is divisible by at least two distinct primes. Let $\bar{N} = N/(\mathbf{Z}(G) \cap N)$ and distinguish two possibilities, whether \bar{N} is a CP-group or not.

a) \bar{N} is not a CP-group. Let $\bar{x} \in \bar{N}$ of order pq with $p \neq q$. We write $x = x_p x_q$ and may assume that x_p and x_q are non-central of order p and q , respectively, so the three non-central G -conjugacy classes of N are x_p^G , x_q^G and x^G . Notice that $\mathbf{Z}(G) \cap N = 1$, otherwise we could obtain more than three non-central G -classes in N . As a result, N is a $\{p, q\}$ -group. We prove now that $\mathbf{Z}(N) > 1$. Suppose on the contrary that $\mathbf{Z}(N) = 1$ and let P and Q be a Sylow p and q -subgroup of N , respectively. Let $z \in \mathbf{Z}(P)$. Since all p -elements of N are G -conjugate, they lie in x_p^G and we have $|z^G| = |x_p^G| = |G : \mathbf{C}_G(x_p)N| |x_p^N|$. Moreover, $\mathbf{C}_G(z)N = (\mathbf{C}_G(x_p)N)^q$, so $|z^N| = |x_p^N|$ is a power of q . Consequently, $|z^N| = |x_p^N| = |n^N|$ for every p -element $n \in N$. Similarly, we get that $|x_q^N|$ is power of p and $|x_q^N| = |m^N|$ for every q -element $m \in N$. Furthermore, as the N -class sizes of x_p and x_q are coprime, we have $N = \mathbf{C}_N(x_p)\mathbf{C}_N(x_q)$, and since $\mathbf{C}_N(x) = \mathbf{C}_N(x_p) \cap \mathbf{C}_N(x_q)$, it follows that $|x^N| = |x_p^N| |x_q^N|$. Thus, the set of class sizes of N is $\text{cs}(N) = \{1, |x_p^N|, |x_q^N|, |x^N|\}$ and we can apply the main result of [3] to deduce that N is nilpotent. In particular, it would have nontrivial center, a contradiction. This contradiction proves that $\mathbf{Z}(N) \neq 1$, as wanted. Now, if $\mathbf{Z}(N)$ has p -elements (analogously for q), then $P \subseteq \mathbf{Z}(N)$ and $N = P \times Q$. Since the three non-central classes of N are obtained as the products of classes of the factors, we deduce that both P and Q can only have a non-central G -conjugacy class. By Theorem 3.3.1, P and Q are elementary abelian. Therefore, we get case 2.

b) \bar{N} is a CP-group. By assumption, we have that $|\bar{N}|$ may be divisible at most by three different primes. We distinguish three subcases:

b.1) \bar{N} is a p -group. Let us see that \bar{N} has exponent p . Let $\bar{x} \in \bar{N}$ with $x \in N$ a p -element and suppose that $o(x) = p^n$ with $n > 1$. We know that there exists a q -element $z \in \mathbf{Z}(G) \cap N$ with $q \neq p$ because N is not a p -group. In fact, N has a central Sylow q -subgroup and we can write $N = P \times Q$. Thus, x^G , $(x^p)^G$, $(zx)^G$ and $(zx^p)^G$ would be four different conjugacy classes, a contradiction. As a consequence, $o(x) = p$ and $o(\bar{x}) = p$. Now, let us see that $|\mathbf{Z}(G) \cap N|$ is divisible at most by p and q with $q \neq p$. If another prime r divides $|\mathbf{Z}(G) \cap N|$, then N has non-central p -elements, $\{p, q\}$ -elements, $\{p, r\}$ -elements and $\{p, q, r\}$ -elements, again a contradiction. We prove now that $Q \cong \mathbb{Z}_3$. Since $N = P \times Q$, we have that the G -classes of N are the product of the G -classes of P and Q . Particularly, since $Q \leq \mathbf{Z}(G)$, the non-central G -classes of N are the product of the G -classes of P (distinct from 1) multiplied by all G -classes of $Q > 1$. As there are three non-central G -classes in N , then Q necessarily has exactly three central G -classes, so $Q \cong \mathbb{Z}_3$ and we get case 3.

b.2) \bar{N} is $\{p, q\}$ -group. Note that N is also a $\{p, q\}$ -group. On the contrary, if there is a prime $r \neq q, p$ dividing $|\mathbf{Z}(G) \cap N|$, then there are non-central elements

whose order is divisible by pr and qr in N , giving a contradiction. We distinguish two cases. If $\mathbf{Z}(G) \cap N = 1$, then N is a CP-group. By applying Theorem 3.2.4 and taking into account that there are only three non-central G -classes in N , one easily obtains the possibilities described in case 5. Suppose now that $\mathbf{Z}(G) \cap N \neq 1$ and we see that $|\mathbf{Z}(G) \cap N| = 2$. Suppose that for one prime, say q for instance, $|\mathbf{Z}(G) \cap N|_q > 2$ and take two distinct nontrivial q -elements $z_1, z_2 \in \mathbf{Z}(G) \cap N$. We choose a p -element $x \in N \setminus \mathbf{Z}(G) \cap N$ and we have that $x^G, (z_1x)^G$ and $(z_2x)^G$ are three distinct G -classes. However, we also have non-central q -elements in N , so there are at least four non-central G -classes inside N , a contradiction. Hence $|\mathbf{Z}(G) \cap N| = 2$, and we obtain case 4.

b.3) \overline{N} is $\{p, q, r\}$ -group. It clearly follows that $\mathbf{Z}(G) \cap N = 1$ by counting order of elements. This means that N is $\{p, q, r\}$ -group and that all elements have prime order. By Theorem 3.2.5, we have $N \cong A_5$. Now, it is known that $G/\mathbf{C}_G(N)$ is immersed in $\text{Aut}(N) \cong S_5$. Then

$$N \cong N\mathbf{C}_G(N)/\mathbf{C}_G(N) \subseteq G/\mathbf{C}_G(N) \cong A_5 \quad \text{or} \quad S_5.$$

We have two possibilities: either $G = N\mathbf{C}_G(N)$ or $G/\mathbf{C}_G(N) \cong S_5$. In the first case, $G = N \times \mathbf{C}_G(N)$ and the N -classes of N are G -classes, so N has four non-central G -classes, a contradiction. Consequently, $G/\mathbf{C}_G(N) \cong S_5$. It is enough to take $K = \mathbf{C}_G(N)$ and $x \in G \setminus (N \times K)$, so as to obtain case 6. \square

Example 3.5.3. *We show examples for each of the cases of Theorem C. The groups $G = D_8$ and $G = Q_8$ with $N = G$ are examples of case 1.*

Let us take $A \cong \mathbb{Z}_6$ acting Frobeniusly on a group $H \cong \mathbb{Z}_7$. Let us consider the action of A on another group $K \cong \mathbb{Z}_3$ in such a way that the kernel of the action is $A_0 \cong \mathbb{Z}_3$ and $A/A_0 \cong \mathbb{Z}_2$ acts Frobeniusly on K . Then we construct the corresponding semidirect product $G = (H \times K) \rtimes A$ and take $N = K \times H$. We have that the sizes of the G -classes of N are 1, 2, 6 and 12. This example shows case 2.

Let $G = SL(2, 3) \times \mathbb{Z}_3$ and let $N = K \times \mathbb{Z}_3$, where K is the normal subgroup of $SL(2, 3)$ isomorphic to Q_8 . Then the three non-central G -classes of N have size 6, so we have an example of case 3.

If we consider $G = GL(2, 3)$ with $N = SL(2, 3)$, then the G -classes of N have size 1, 1, 6, 8, 8, and this illustrates case 4.

The same construction of Example 6, that is, $G = \Gamma(p^2)$ may work for case 5. We have to take $s = 5$ instead of 3, (so we need that 5 divides $p^2 - 1$), and set $N = KS$ with $S \leq H$ a cyclic group of order 5. Then the sizes of the G -classes of N are $\{1, p^2 - 1, 2p^2, 2p^2\}$, so $\Gamma_G(N)$ is just a triangle when p is odd.

Finally, of course $G = S_5$ with $N = A_5$ is an example of case 6.

Remark 3.5.4. *As we have pointed out in the introduction, the S_3 -conjecture does not hold for conjugacy classes lying in a normal subgroup. The examples given in Sections 3, 4 and 5 show that even there are infinitely many normal subgroups having all G -classes (central and non-central) with distinct size.*

3.5.3 $\Gamma_G(N)$ with three vertices connected in a line

Theorem 3.5.5. *Let N be a normal subgroup of a group G . If $\Gamma_G(N)$ has three vertices in a line then $\mathbf{Z}(G) \cap N = 1$ and one of the following cases is satisfied:*

1. N is a 2-group of exponent at most 4.
2. $N = P \times Q$, where P and Q are elementary abelian p and q -groups.
3. N is a Frobenius group with complement isomorphic to \mathbb{Z}_q , \mathbb{Z}_{q^2} or Q_8 . In the former case, the kernel of N is a p -group with exponent $\leq p^2$ and in the two latter cases, the kernel of N is p -elementary abelian.

In all cases, $|N|$ is divisible by at most two prime numbers.

Proof. The graph $\Gamma_G(N)$ has the form:



Since the vertices of the ends, say x^G and y^G , are not joined, then x^G and y^G are the only G -classes with cardinality $|x^G|$ and $|y^G|$, respectively. If $z \in \mathbf{Z}(G) \cap N$, then $(zx)^G = x^G$ and $(zy)^G = y^G$, so $|\langle z \rangle|$ divides $|x^G|$ and $|y^G|$. Therefore, $\mathbf{Z}(G) \cap N = 1$. We will distinguish three cases:

a) Suppose that N is a p -group. By the graph form x^G and y^G are real classes and obviously one of them needs to have odd size, say y^G . Thus, the order of y is 2 and $p = 2$. Notice that necessarily the order of x is also 2, otherwise $|(x^2)^G|$ would divide $|x^G|$, and this would force $\Gamma_G(N)$ to have a triangle. If z^G is the third G -class of N , then the order of z is at most 4 and we obtain case 1.

b) Suppose now that N is not a p -group and not a CP-group. Hence it has elements whose order is divisible by two different primes p and q . Let $x = x_p x_q$ be one of them, where x_p and x_q are the (non-central) p -part and q -part, respectively. Hence, the three G -classes of N are x_p^G , x_q^G and x^G , so N is a $\{p, q\}$ -group. Let us prove that $\mathbf{Z}(N) \neq 1$. Suppose that $\mathbf{Z}(N) = 1$. Since all p -elements of N lie in x_p^G , any p -element $w \in N$ satisfies $w = x_p^g$, for some $g \in G$ and

$$|x_p^G| = |G : \mathbf{C}_G(x_p)N| |x_p^N| = |G : \mathbf{C}_G(w)N| |w^N| = |w^G|.$$

It follows that $|x^N| = |w^N|$. We can argue similarly for the N -classes of q -elements and $\{p, q\}$ -elements, which have sizes $|x_q^N|$ and $|x^N|$, respectively. In addition, since $|x_p^N|$ and $|x_q^N|$ divide $|x^G|$ and $|x_q^G|$ respectively, we have $(|x_p^N|, |x_q^N|) = 1$ by the structure of the graph. Furthermore, $|x_p^N|$ and $|x_q^N|$ must be a power of p and a power of q greater than 1 because $\mathbf{Z}(N) = 1$. On the other hand, $N = \mathbf{C}_N(x_p)\mathbf{C}_N(x_q)$, $\mathbf{C}_N(x) = \mathbf{C}_N(x_p) \cap \mathbf{C}_N(x_q)$ and this leads to $|x^N| = |x_p^N| |x_q^N|$. Therefore, the set of class sizes of N is $\text{cs}(N) = \{1, |x_p^N|, |x_q^N|, |x^N|\}$ and by the main result of [3], N is nilpotent and has nontrivial center, a contradiction. Now, let us prove that N is abelian. If p divides $|\mathbf{Z}(N)|$, since all p -elements of N are G -conjugate, N has a central Sylow p -subgroup, so N is nilpotent and factorize $N = P \times Q$. As there are only 3 nontrivial G -classes, this implies that P and Q are minimal normal subgroups of G , so P and Q are elementary abelian. We get case 2.

c) Assume that N is a CP-group but not a p -group. By Theorem 3.2.4, we know that $|N|$ is divisible by at most two primes. We will prove that case 3 of Theorem 4 cannot happen and, consequently, we obtain the properties described in case 3 of the statement. Suppose that $N/\mathbf{O}_p(N)$ is a $\{p, q\}$ -group having cyclic Sylow subgroups and let $K/\mathbf{O}_p(N)$ and $H/\mathbf{O}_p(N)$ be the kernel and complement of the Frobenius group $N/\mathbf{O}_p(N)$, respectively. Observe that $K/\mathbf{O}_p(N)$ is a cyclic q -group and $H/\mathbf{O}_p(N)$ is a cyclic p -group. By the hypotheses, we can write

$$\begin{aligned}\mathbf{O}_p(N) &= 1 \cup x^G, \\ K &= 1 \cup x^G \cup y^G, \\ N &= 1 \cup x^G \cup y^G \cup z^G,\end{aligned}$$

where x has order p and y has order q . Notice that y^G is the only class of elements of order exactly q because $K/\mathbf{O}_p(N) \cong \mathbb{Z}_q$. Also, we can write $K = \mathbf{O}_p(N)Q$ where $Q \cong \mathbb{Z}_q$ is a Sylow q -subgroup of G , and $|K| = p^a q$. On the other hand, the elements of $N \setminus K$ form a G -class, say z^G . Moreover,

$$\frac{N}{K} \cong \frac{N/\mathbf{O}_p(N)}{K/\mathbf{O}_p(N)} \cong H/\mathbf{O}_p(N)$$

and $|N| = p^{a+1}q$. Therefore,

$$\begin{aligned}|x^G| &= |\mathbf{O}_p(N)| - 1 = p^a - 1, \\ |y^G| &= |K| - |\mathbf{O}_p(N)| = p^a(q - 1), \\ |z^G| &= |N| - 1 - |x^G| - |y^G| = p^a q(p - 1).\end{aligned}$$

If both p and q are odd, we have that $|x^G|$, $|y^G|$ and $|z^G|$ are even, a contradiction. If $q = 2$, then $|K/\mathbf{O}_p(N)| = 2$, and $K/\mathbf{O}_p(N)$ would be central in $N/\mathbf{O}_p(N)$, again a contradiction. Thus, $p = 2$ and $|N| = 2^{a+1}q$. In particular, $|H/\mathbf{O}_2(N)| = 2$. By the Frattini argument, $N = K\mathbf{N}_N(Q) = \mathbf{O}_2(N)\mathbf{N}_N(Q)$. On the other hand, $[\mathbf{N}_N(Q) \cap \mathbf{O}_2(N), Q] \subseteq Q \cap \mathbf{O}_2(N) = 1$ and, in particular, $\mathbf{N}_N(Q) \cap \mathbf{O}_2(N) \subseteq \mathbf{C}_N(Q) \cap \mathbf{O}_2(N) = 1$. Then, $|\mathbf{N}_N(Q)| = |N|/|\mathbf{O}_2(N)| = 2q$ and there must exist a 2-element $w \in \mathbf{N}_N(Q)$. If H were abelian, then $H \subseteq \mathbf{C}_N(\mathbf{O}_2(N))$. However, we know that $\mathbf{O}_{2'}(N) = 1$, so $\mathbf{C}_N(\mathbf{O}_2(N)) \subseteq \mathbf{O}_2(N)$, which provides a contradiction. As a result, H is not abelian and z^G consists of elements of order 4. In particular, w has order 4 and satisfies $(w\mathbf{O}_2(N))^2 = \mathbf{O}_2(N)$, which means that $w^2 \in \mathbf{O}_2(N)$. Then $w^2 \in \mathbf{N}_N(Q) \cap \mathbf{O}_2(N) = 1$, the final contradiction. \square

Example 3.5.6. We take $G = ((\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_7) \times A_4$ which has been obtained from [11] by using the code `SmallGroup(672, 1258)`. Then $N = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is a normal subgroup of G and the sizes of the G -classes are $\{1, 3, 7, 21\}$. Thus, $\Gamma_G(N)$ has three vertices in a line and N is a 2-group.

Example 3.5.7. We consider $N = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ and construct an action of $H = \mathbb{Z}_7 \times \mathbb{Z}_2$ on K . We know that \mathbb{Z}_7 can act Frobeniusly on $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, because this group has a fixed-point-free automorphism of order 7. Also, we consider the trivial action of \mathbb{Z}_7 on \mathbb{Z}_3 . On the other hand, we consider \mathbb{Z}_2 acting trivially on $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and Frobeniusly on \mathbb{Z}_3 . We set the corresponding semidirect product $G = N \rtimes H$ and we have that N has three nontrivial G -classes whose sizes are 2, 7 and 14. Accordingly, $\Gamma_G(N)$ has three vertices in a line.

Example 3.5.8. We take $G = ((\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes Q_8) \rtimes \mathbb{Z}_3$, which has been obtained with [11] by using the code `SmallGroup(600, 150)`. Then $N = (\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes Q_8$ is a normal subgroup of G and the sizes of the G -classes of N are $\{1, 24, 25, 150\}$. Notice that $\Gamma_G(N)$ has three vertices in a line and N is a Frobenius group with complement Q_8 .

3.6 $\Gamma_G(N)$ without triangles

Theorem 3.6.1. *Let N be a normal subgroup of a group G such that $\Gamma_G(N)$ has no triangles. Then N is solvable.*

Proof. The case in which $\Gamma_G(N)$ is empty is trivial, since N is clearly abelian. We use induction on $|N|$. Take N/K a chief factor of N with $K < N$ and suppose that $K \neq 1$. If $\Gamma_G(K)$ has triangles, then $\Gamma_G(N)$ trivially has triangles too. By induction, we conclude that K is solvable. On the other hand, if $\Gamma_{G/K}(N/K)$ has a triangle, formed by $(xK)^{G/K}$, $(yK)^{G/K}$ and $(zK)^{G/K}$, then we have that x^G, y^G and z^G form a triangle of $\Gamma_G(N)$. In fact, if for instance, $x^G = y^G$, then $(xK)^{G/K} = (yK)^{G/K}$. Again by induction, N/K is solvable too. Therefore, we can assume that N is a minimal normal subgroup of G . We assume that it is the direct product of isomorphic copies of a non-abelian simple group N_1 , otherwise N is solvable and we are finished. Bertram, Herzog y Mann proved in [1] that the graph of a simple group is always complete. Thus, we can choose a triangle of $\Gamma(N_1)$, formed by a^{N_1} , b^{N_1} and c^{N_1} , such that the orders of a , b and c are different prime numbers. Since $N_1 \trianglelefteq N \trianglelefteq G$, we deduce that $|n^{N_1}|$ divides $|n^G|$, for every element $n \in N_1$, so we obtain three elements of different orders in N , whose corresponding G -classes are distinct and form a triangle in $\Gamma_G(N)$, a contradiction. Therefore, N is solvable. \square

Theorem 3.6.2. *If $\Gamma_G(N)$ has no triangles and N is a CP-group, then N is a p -group for some prime p or a Frobenius group.*

Proof. The case in which $\Gamma_G(N)$ is empty and N is a CP-group, trivially leads to that N is a p -group. Suppose that N has not prime power order. By hypothesis, it is clear that $\mathbf{Z}(N) = 1$ (and $\mathbf{Z}(G) \cap N = 1$). By Theorem 3.6.1, we know that N is solvable, and one of the three options of Theorem 3.2.4 holds. We prove that case 3 cannot occur. Suppose that N satisfies case 3 of Theorem 3.2.4, so N has the following normal series:

$$1 < \mathbf{O}_p(N) < K := \mathbf{O}_p(N)Q < N,$$

where Q is a Sylow q -subgroup of N .

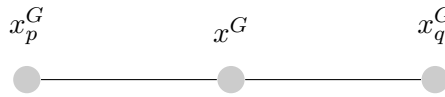
Since $K = \mathbf{O}_p(N)Q$ is a Frobenius group, the K -classes of $\mathbf{O}_p(N) \setminus 1$ have cardinality divisible by q , then the cardinalities of the respective N -classes and G -classes also are. On the other hand, the elements of $K \setminus \mathbf{O}_p(N)$ have a K -conjugacy class of cardinality divisible by p , and again the respective N -class sizes and G -class sizes are divisible by p too. Furthermore, if z is a p -element of $N \setminus K$, we see that $|z^N|$ is divisible by p and q . It is obvious that q divides $|z^N|$, otherwise there are elements of order pq in N . In addition, $|z^N|$ is divisible by p , otherwise $\mathbf{C}_N(z)$ contains a Sylow p -subgroup of N , so in particular, contains $\mathbf{O}_p(N)$. Then, $z \in \mathbf{C}_N(\mathbf{O}_p(N)) \subseteq \mathbf{O}_p(N)$. As a result, there exist at least three nontrivial G -classes in N , one of them in $\mathbf{O}_p(N)$, whose cardinality is divisible by q , another one in

$K \setminus \mathbf{O}_p(N)$ of cardinality divisible by p , and a third class in $N \setminus K$ whose cardinality is divisible by pq . Since the G -classes are union of N -classes, there are not no more nontrivial G -classes in N , otherwise, there would be a triangle in $\Gamma_G(N)$. Therefore, $\Gamma(N)$ has exactly three vertices connected in a line. However, this is not possible for the ordinary graph by the main result in [6]. In conclusion, case 3 of Theorem 3.2.4 does not happen and so, N is a p -group or a Frobenius group. \square

We are ready to prove Theorem A of the Introduction.

Proof of Theorem A. By Theorem 3.6.1 we know that N is solvable. We will distinguish two cases depending on whether $N/(\mathbf{Z}(G) \cap N)$ is a CP-group or not.

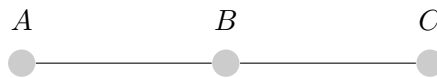
a) Suppose first that $N/(\mathbf{Z}(G) \cap N)$ is not a CP-group. Let $x \in \mathbf{Z}(G) \cap N$ of order divisible by exactly two different prime numbers p and q . We can write $x = x_p x_q$, where x_p and x_q are the p -part and q -part of x , respectively, which are trivially non-central in G . Since $\mathbf{C}_G(x) = \mathbf{C}_G(x_p) \cap \mathbf{C}_G(x_q)$, we have that both $|x_p^G|$ and $|x_q^G|$ divide $|x^G|$, so x^G is connected to x_p^G and x_q^G . Moreover, by the orders of the elements, these classes are different. Thus, we have a subgraph of $\Gamma_G(N)$ with the following form:



As $\Gamma_G(N)$ has no triangles, then $|x_p^G|$ and $|x_q^G|$ are coprime and as a consequence, $G = \mathbf{C}_G(x_p)\mathbf{C}_G(x_q)$ and $|x^G| = |x_p^G||x_q^G|$. Hence, any prime dividing $|x_p^G|$ or $|x_q^G|$ is a divisor of $|x^G|$ and consequently, if there exists a vertex in $\Gamma_G(N)$ different from x^G , x_p^G and x_q^G , it must lie in another connected component of $\Gamma_G(N)$. This means that $\Gamma_G(N)$ is disconnected and we get a contradiction by applying Theorem 3.2.3. Therefore, $\Gamma_G(N)$ coincides exactly with the subgraph above. By Theorem 3.5.5, we obtain $\mathbf{Z}(G) \cap N = 1$ and one of the assertions 1, 3 and 5 follow.

b) Suppose that $N/(\mathbf{Z}(G) \cap N)$ is a CP-group. By Theorem 3.2.4, its order is divisible by at most two primes. For the rest of the proof, we exclude the case in which N has prime power order, otherwise, we have case 1. Notice that if $\mathbf{Z}(G) \cap N = 1$, then by applying Theorems 6.2 and 3.2.4, we obtain case 5. Therefore, by applying Lemma 3.4.4, we can also assume for the rest of the proof that $|\mathbf{Z}(G) \cap N|_2 = 2$. We distinguish two subcases depending on the connectivity of $\Gamma_G(N)$.

b.1) Suppose that $\Gamma_G(N)$ is connected. If it consists only of one vertex, N would be a p -group by Theorem 3.3.1, but we are excluding this case. If $\Gamma_G(N)$ has two vertices joined by an edge, by applying Theorem 3.4.5, we obtain case 2. In any other case, $\Gamma_G(N)$ always contains a subgraph of the following way:



and this turns to a contradiction. Observe that A and C are the unique G -classes with cardinalities $|A|$ and $|C|$, respectively, because otherwise there would exist triangles in $\Gamma_G(N)$. If we take a nontrivial 2-element $z \in \mathbf{Z}(G) \cap N$, then $zA = A$ and

$zC = C$, so $|\langle z \rangle|$ divides $|A|$ and $|C|$, which is a contradiction.

b.2) Assume that $\Gamma_G(N)$ is disconnected. We distinguish all the possibilities by taking into account Theorem 3.2.3. First, if $\Gamma_G(N)$ has the form:



we have $\mathbf{Z}(G) \cap N = 1$ by Lemma 3.4.1. Also, by Theorem 3.4.2, N is a $\{p, q\}$ -group and N satisfies a particular case of 5. Secondly, if $\Gamma_G(N)$ has three G -classes, the graph is:



By Theorem 3.5.1, N is a $\{p, q\}$ -group and since N is not a p -group, then N is quasi-Frobenius with abelian kernel and complement, so we get case 4.

The only remaining case is when the structure of $\Gamma_G(N)$ is:



Then by Theorem 3.2.2, we know that either $N = P \times A$ with $A \neq 1$ a central p' -subgroup of G , or N is quasi-Frobenius with kernel K and complement H , both of them abelian. In the former case, since the G -classes of N are equal to the product of the G -classes of P by the classes of A , necessarily we have $A \cong \mathbb{Z}_2$.

We assume then the second possibility, that is, N is quasi-Frobenius with kernel K and complement H , both abelian. As $N/(\mathbf{Z}(G) \cap N)$ is a CP-group, it certainly follows that $Z := \mathbf{Z}(G) \cap N = \mathbf{Z}(N)$. We have proved above that N/Z is a $\{p, q\}$ -group and now we prove that $Z \cong \mathbb{Z}_2$. If $z \in Z$ is an r -element with r an odd prime, then r needs to be distinct from p or q , say for instance $p \neq r$. We take a p -element $x \in N \setminus Z$ and then the G -classes x^G , $(xz)^G$ and $(xz^2)^G$ form a triangle in $\Gamma_G(N)$, a contradiction. We conclude that $Z \cong \mathbb{Z}_2$, as wanted. Finally, we prove that either p or q has to be 2, that is, N is a $\{2, p\}$ -group (or a $\{2, q\}$ -group), and we obtain case 4 and the theorem is finished. Suppose that p and q are odd primes. It easy to see that the graph $\Gamma_{G/Z}(N/Z)$ has exactly two vertices without edge, and by using Theorem 3.4.1, we have $|K/Z| = p^n$, $|H/Z| = q$, with $n \geq 1$. We take a p -element $a \in K$, a q -element $b \in H$ and $1 \neq z \in \mathbf{Z}(G) \cap N$. It follows that the four vertices of $\Gamma_G(N)$ are exactly a^G , $(az)^G$, b^G and $(bz)^G$. Moreover, observe that $a^G \cup (az)^G = K \setminus Z$ and $b^G \cup (bz)^G = N \setminus K$. By taking cardinalities, we have

$$2|a^G| = 2p^n - 2 \quad \text{and} \quad 2|b^G| = 2p^n q - 2p^n,$$

so $|a^G| = p^n - 1$ and $|b^G| = p^n(q - 1)$. However, both numbers are even because p and q are odd, and this leads to a contradiction. \square

Acknowledgements

The results in this paper are part of the third author's Ph.D. thesis at the University Jaume I of Castellón. The research of the first and second authors is 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.

Bibliography

- [1] E.A. Bertram, M. Herzog and A. Mann, On a graph related to conjugacy classes of groups. *Bull. London Math. Soc.* **22** (6) (1990), 569-575.
- [2] A. Beltrán, M.J. Felipe and C. Melchor, Graphs associated to conjugacy classes of normal subgroups in finite groups. *J. Algebra.* **443** (2015), 335-348.
- [3] A.R. Camina, Arithmetical conditions on the conjugacy class numbers of a finite group. *J. London Math. Soc.* **2** (5) (1972), 127-132.
- [4] M. Deaconescu, Classification of finite groups with all elements of prime order. *Proc. Amer. Math. Soc.* **106** (3) (1989), 625-629.
- [5] K. Doerk, T. Hawkes, Finite soluble groups. de Gruyter Expositions in Mathematics, 4. Walter de Gruyter, Berlin, 1992.
- [6] M. Fang and P. Zhang, Finite groups with graphs containing no triangles. *J. Algebra* **264** (2) (2003), 613-619.
- [7] G. Higman, Finite groups in which every element has prime power order. *J. London Math. Soc.* (32) (1957), 335-342.
- [8] O. Manz and T.R. Wolf, Representations of Solvable Groups, Cambridge Univ. Press, Cambridge, UK, 1993.
- [9] U. Riese and M.A. Shahabi, Subgroups which are the union of four conjugacy classes. *Comm. Algebra.* **29** (2) (2001), 695-701.
- [10] M. Shahryari and M.A. Shahabi, Subgroups which are the union of three conjugate classes. *J. Algebra.* **207** (1) (1998), 326-332.
- [11] The GAP Group, GAP - Groups, Algorithms and Programming, Vers. 4.4.12 (2008). <http://www.gap-system.org>

Chapter 4

Landau's theorem on conjugacy classes for normal subgroups

Abstract

Landau's theorem on conjugacy classes asserts that there are only finitely many finite groups, up to isomorphism, with exactly k conjugacy classes for any positive integer k . We show that, for any positive integers n and s , there exist finitely many finite groups G , up to isomorphism, having a normal subgroup N of index n which contains exactly s non-central G -conjugacy classes. Upper bounds for the orders of G and N are obtained; we use these bounds to classify all finite groups with normal subgroups having a small index and few G -classes. We also study the related problems when we consider only the set of G -classes of prime-power order elements contained in a normal subgroup.

Keywords. Conjugacy classes; Normal subgroups; Number of conjugacy classes.

Mathematics Subject Classification (2010): 20E45, 20D15.

4.1 Introduction

The renowned theorem of Landau [9] states that there are only finitely many finite groups, up to isomorphism, with exactly k conjugacy classes, for any positive integer k . No upper bound in terms of k for the order of such groups was provided. M. Newman [12] demonstrated that $|G| \leq k^{2^{k-1}}$, or equivalently, that k goes to infinity with the order of G according to the inequality

$$k \geq \frac{\log_2(\log_2|G|)}{2}.$$

Since then many results have appeared in the literature regarding logarithmic bounds for some specific classes of groups, for instance, nilpotent or "almost nilpotent" groups [5], or solvable groups [6], as well as extensions of Landau's theorem, such as [8], [11], where only conjugacy classes of prime-power order elements and of p -regular elements are taken into account. A generalization of Landau's theorem for irreducible characters is proved in [10] by considering the above result on classes of elements of prime-power order and the number of irreducible characters of G with values in fields where \mathbb{Q} is extended by prime-power roots of unity.

Let G be a finite group and let N be a normal subgroup of G . For each $x \in N$, the G -conjugacy class of x is $x^G = \{x^g \mid g \in G\}$. Bearing in mind that N is the

union of G -classes, the aim of this paper is to extend Landau's theorem for conjugacy classes of N . A natural question is whether there exist finitely many groups having a normal subgroup which is the union of a fixed number of G -classes. The answer is negative. In fact, if we take N to be a p -elementary abelian group of order p^s and G the holomorph group of N , then since $\text{Aut}(N)$ acts transitively on $N \setminus \{1\}$, it follows that N consists only of two G -classes, $\{1\}$ and $N \setminus \{1\}$. Nevertheless, $\text{Aut}(N) \cong \text{GL}(s, p)$ and so $|G : N| = |\text{GL}(s, p)|$ may increase as much as we wish. In Section 2, our result establishes that if we fix the index $|G : N|$, then the answer to our question is affirmative. We provide upper bounds for $|G|$ and $|N|$ depending on the number of non-central G -classes lying in N (instead of all G -classes).

Theorem A. *Let $s, n \in \mathbb{N}$ such that $s, n \geq 1$. There exists at most a finite number of isomorphism classes of finite groups G which contain a normal subgroup N such that $|G : N| = n$ and N has exactly s non-central G -classes. Moreover,*

$$|G| < n^{2^s+1} (s+1) \prod_{i=0}^{s-1} (s+1-i)^{2^{s-1-i}}$$

and

$$|N| < n^{2^s} (s+1) \prod_{i=0}^{s-1} (s+1-i)^{2^{s-1-i}}.$$

In the above theorem we take $s \geq 1$, because considering $s = 0$ is equivalent to N being central in G and a classification of such groups makes no sense because these are infinitely many. When $n = 1$, we obtain an improvement of Newman's bound in terms of the number of non-central classes in a group.

In Sec. 4.3, we present two applications of the above bounds: the classification of groups G with normal subgroups having either one or two non-central G -classes of coprime size and for certain small indices. We use GAP [7] and particularly the SMALGROUPS library [4]. We recall that the classification of finite groups according to their number of conjugacy classes has been a widely studied problem (see for instance [13], [14]).

In Sec. 4.4, we tackle the problem of extending Landau's theorem for prime-power order elements lying in a normal subgroup N of a group G . We prove that there also exist finitely many finite groups, up to isomorphism, having a normal subgroup with fixed index and with a fixed number of G -classes of prime-power order elements. We show by example that every G -class instead of only non-central G -classes must be considered. Furthermore, we obtain a bound for the orders of G and N when G is solvable.

Theorem B. *For any two positive integers k and n , there are only finitely many finite groups G , up to isomorphism, with a normal subgroup N of index n and containing k G -classes of prime-power order elements. Moreover, when G is solvable,*

$$|G| \leq n \prod_{i=0}^{nk-1} (nk-i)^{2^i} \quad \text{and} \quad |N| \leq \prod_{i=0}^{nk-1} (nk-i)^{2^i}.$$

4.2 Proof of Theorem A

We need the following elementary result, which is a slight improvement of a lemma in [12].

Lemma 4.2.1. *Let $s, n \in \mathbb{N}$ with $s, n \geq 1$ and let n_1, \dots, n_{s+1} be integers such that $n_1 \leq n_2 \leq \dots \leq n_{s+1}$ and $1/n = 1/n_1 + \dots + 1/n_{s+1}$. Then*

$$n_1 \leq n(s+1)$$

and

$$n_k \leq n^{2^{k-1}}(s+2-k) \prod_{i=0}^{k-2} (s+1-i)^{2^{k-2-i}} \quad (4.1)$$

for all $2 \leq k \leq s+1$.

Proof. We obtain the first inequality trivially. We argue by induction on k for $2 \leq k \leq s+1$. First, since

$$1/n - 1/n_1 = 1/n_2 + \dots + 1/n_{s+1} \leq s/n_2$$

we deduce that $n_2 \leq s n n_1 / (n_1 - n)$ and this denominator is at least one because $n_1 > n$. By using the hypothesis we obtain

$$n_2 \leq s n n_1$$

and since $n_1 \leq n(s+1)$

$$n_2 \leq n^2(s+1)s.$$

Suppose that Eq. (4.1) holds for k with $2 \leq k \leq s$ and let us prove it for $k+1$. We know that

$$0 < 1/n - (1/n_1 + \dots + 1/n_k) = 1/n_{k+1} + \dots + 1/n_{s+1} \leq (s+1-k)/n_{k+1},$$

so we conclude that

$$n_{k+1} \leq (s+1-k) n n_1 \dots n_k / (n_1 \dots n_k - (n n_2 \dots n_k + \dots + n n_1 \dots n_{k-1}))$$

and this denominator is bigger than 0 because $1/n - (1/n_1 + \dots + 1/n_k) > 0$. Thus,

$$n_{k+1} \leq (s+1-k) n n_1 \dots n_k \leq$$

$$(s+1-k) n [n(s+1)] [n^2(s+1)s] \dots [n^{2^{k-1}}(s+2-k) \prod_{i=0}^{k-2} (s+1-i)^{2^{k-2-i}}].$$

Rearranging the terms on the right of the inequality it is easily computed that

$$n_{k+1} \leq n^{2^k} (s+2-(k+1)) \prod_{i=0}^{(k+1)-2} (s+1-i)^{2^{(k+1)-2-i}}$$

and so Eq.(4.1) is proved. \square

Proof of Theorem A. Let $C_i = x_i^G$ for $i = 1, \dots, s$ be the non-central G -conjugacy classes contained in N . Then $|C_i| = |G : \mathbf{C}_G(x_i)|$. By the class equation

$$|N| = |\mathbf{Z}(G) \cap N| + |C_1| + \dots + |C_s|$$

and by dividing by $|G|$,

$$1/n = 1/|G : \mathbf{Z}(G) \cap N| + 1/|\mathbf{C}_G(x_1)| + \dots + 1/|\mathbf{C}_G(x_s)|.$$

We rewrite the previous expression in the following way

$$1/n = 1/n_1 + \dots + 1/n_{s+1}$$

where each n_i is either $|\mathbf{C}_G(x_j)|$ or $|G : \mathbf{Z}(G) \cap N|$. Without loss of generality, we can suppose that $n_1 \leq \dots \leq n_{s+1}$, so

$$1/n = 1/n_1 + \dots + 1/n_{s+1} \leq (s+1)/n_1.$$

Thus,

$$n_1 \leq n(s+1). \quad (4.2)$$

We know that there exists some i with $1 \leq i \leq s+1$ such that $n_i = |G : \mathbf{Z}(G) \cap N|$. Furthermore, for every $j \neq i$ we know that $n_j > |\mathbf{Z}(G) \cap N|$. Then $n_i > |G|/n_j$. Hence, $|G| < n_i n_j$ for every $j \neq i$, with $1 \leq j \leq s+1$. In particular, if $i = 1$, then $|G| < n_1 n_{s+1}$ and if $i > 1$, then $|G| < n_1 n_i \leq n_1 n_{s+1}$. In all cases, by using Eq. (4.2) and by replacing k by $s+1$ in Eq. (4.1), we get

$$|G| < n_1 n_{s+1} \leq n(s+1)n^{2^s} \prod_{i=0}^{s-1} (s+1-i)^{2^{s-1-i}} = n^{2^s+1} (s+1) \prod_{i=0}^{s-1} (s+1-i)^{2^{s-1-i}}.$$

The bound for $|N|$ trivially follows just dividing by n . Once the bound for $|G|$ is obtained, the first assertion in the theorem is clear. \square

4.3 Applications of Theorem A

As an application of Theorem A we classify groups and normal subgroups with certain number of non-central classes of G by using GAP. In order to expedite this classification, we employ properties of the graph $\Gamma_G(N)$ defined in [1], associated to a normal subgroup N of G , as well as some results of [2] concerning this graph when it has few vertices. These properties give us relevant information about the structure of the normal subgroup. We recall that the graph $\Gamma_G(N)$ is defined in the following way: the vertices are the non-central G -classes contained in N and two vertices x^G and y^G are joined by an edge if and only if $|x^G|$ and $|y^G|$ have a common prime divisor.

We classify explicitly those groups G having a normal subgroup N with one or two non-central G -conjugacy classes of coprime sizes for some concrete indices. The reason we do not deal with the case of two non-central G -classes with non-coprime size is because we cannot ensure that $\mathbf{Z}(G) \cap N = 1$, whereas when the sizes are coprime we will see that this equality always holds, allowing us to improve the algorithm efficiency.

The specific indices that we have chosen give rise to groups available in the library SMALLGROUPS [4] of GAP. We provide information about the classified groups through tables in which the index of the normal subgroup and the SMALLGROUP identifier of the corresponding group satisfying the properties appear. The m th group of order n in the SMALLGROUPS library is identified by $n\#m$.

4.3.1 Normal subgroups with only one non-central G -class

We consider groups having a normal subgroup N with only one non-central G -conjugacy class, which means that $\Gamma_G(N)$ has exactly one vertex. It is trivial that this case cannot occur for ordinary classes of G .

To improve the algorithm efficiency, we specialize the bound of Theorem A and use Theorem 3.2 of [2].

Theorem 4.3.1. *Let N be a normal subgroup of a group G with $|G : N| = n$. If N has exactly one non-central G -conjugacy class, then $|G| < n(n + 1)^2$.*

Proof. Let x^G be the only non-central G conjugacy class of N . By the class equation,

$$|N| = |N \cap \mathbf{Z}(G)| + |x^G|. \tag{4.3}$$

Dividing by $|G|$,

$$\frac{1}{n} = \frac{1}{n_1} + \frac{1}{n_2} \leq \frac{2}{n_1} \tag{4.4}$$

where n_i is either $|G : N \cap \mathbf{Z}(G)|$ or $|\mathbf{C}_G(x)|$, and we suppose without loss of generality that $n_1 \leq n_2$. It follows that $n < n_1 \leq 2n$. We observe that $n_2 = nn_1/(n_1 - n)$ is uniquely determined by n_1 . By arguing similarly as in the proof of Theorem A we get $|G| < n_1n_2 = nn_1^2/(n_1 - n)$, which is a function that takes its maximum value for $n_1 = n + 1$. We conclude that $|G| < n(n + 1)^2$. \square

To obtain our classification, we discard those normal subgroups that do not satisfy the following conditions.

Theorem 4.3.2 (see [2], Theorem 3.1). *If G is a group and N is a normal subgroup of G such that $\Gamma_G(N)$ has only one vertex, then N is a p -group for some prime p and $N/(N \cap \mathbf{Z}(G))$ is an elementary abelian p -group.*

In Table 4.1, we indicate for each index the bound for $|G|$ of Theorem 4.3.1 and the number of groups with a normal subgroup containing a single non-central conjugacy class of G . In Table 4.2, we show the complete classification for the indices that appear in Table 4.1.

Figure 4.1: Number of groups with normal subgroups having one non-central G -class.

| Index of N | $ G \leq n(n+1)^2$ (Theorem 4.3.1) | Number of groups |
|--------------|--|------------------|
| 2 | 18 | 3 |
| 3 | 48 | 2 |
| 4 | 100 | 21 |
| 5 | 180 | 0 |
| 6 | 294 | 16 |
| 7 | 448 | 1 |

The idea of the algorithm implemented in GAP is to list only integers at most the bound obtained in Theorem 4.3.1, say c , which are divisible by n , n_1 and n_2 , appearing in that theorem, with $c/n_1 > 1$ and $c/n_2 > 1$. For $n = 4$, among the possible orders that satisfy the above conditions is 64. This is the most difficult possibility because there exist 267 groups. However, we can discard this case by proving the following property for p -groups. For $n = 8$, in some cases, specifically 2-groups, although the groups of the relevant orders are in the library, we could not complete the classification because the number of possibilities is too large.

Theorem 4.3.3. *Let G be a group such that $|G| = p^k$ with p prime, and let N be a normal subgroup of G of order p^a such that N has only one non-central G -conjugacy class. Then $p = 2$, N is abelian and $a \leq (k+1)/2$.*

Proof. Suppose that G has a normal subgroup with one non-central G -conjugacy class, say $|x^G|$. It follows that $|N| = |\mathbf{Z}(G) \cap N| + |x^G|$ which means that $p^a = p^c + p^d = p^c(1 + p^{d-c})$ with $c \leq d$. This equation only holds if $p = 2$. Accordingly, $2^a = 2^c(1 + 2^{d-c})$ with $c \leq d$. This forces $c = d = a - 1$, so $|\mathbf{Z}(G) \cap N| = |x^G| = 2^{a-1}$. Since $\mathbf{Z}(G) \cap N \subseteq \mathbf{Z}(N)$ and $|N : \mathbf{Z}(G) \cap N| = 2$ we conclude that N is abelian. Thus, $N \subseteq \mathbf{C}_G(x)$ and, since $2^{a-1} = |x^G| = |G : \mathbf{C}_G(x)|$ divides $|G : N| = 2^{k-a}$, we obtain $a - 1 \leq k - a$, that is, $a \leq (k+1)/2$. \square

Figure 4.2: Groups having normal subgroups with one non-central G -class for certain indices.

| n | G |
|-----|--|
| 2 | 6#1 8#3 8#4 |
| 3 | 12#3 24#3 |
| 4 | 12#1 12#4 16#3 16#4 16#6 16#7 16#8 16#9 16#11 16#12 16#13 20#3 32#27 32#28 32#29 32#30 32#31 32#32 32#33 32#34 32#35 |
| 6 | 18#1 18#3 18#4 24#12 24#13 24#4 24#6 24#8 24#10 24#11 42#1 48#28 48#29 48#32 48#33 54#8 |
| 7 | 56#11 |

Remark 4.3.4. *Every group in Table 4.2 has only one normal subgroup satisfying the conditions except for indices $n = 2, 4, 6$. In these cases there are 1, 8 and 1 groups, respectively, having two normal subgroups. In Table 4.2, the only case in which N is not abelian is when $N \cong Q_8$. This happens for $n = 3$ and $G = 24\#3 \cong SL(2, 3)$, and for $n = 6$ and four groups of order 48.*

4.3.2 Normal subgroups with two non-central G -classes of coprime sizes

It was proved in [3] that this case for ordinary classes only happens when $G \cong S_3$. However, for G -classes lying in a normal subgroup this is not the unique possibility (see [2]). We use the following lemma to improve the efficiency of the algorithm.

Lemma 4.3.5 ([2], Lemma 4.1.1). *Let N be a normal subgroup of a group G . If $\Gamma_G(N)$ has two vertices but no edges, then $\mathbf{Z}(G) \cap N = 1$.*

The following improves the bounds of Theorem A.

Theorem 4.3.6. *Let N be a normal subgroup of a group G with $|G : N| = n$. Suppose that G has exactly two non-central conjugacy classes x_1^G and x_2^G in N and these two classes have coprime sizes. Let $n_1 = |\mathbf{C}_G(x_1)|$ and $n_2 = |\mathbf{C}_G(x_2)|$ such that $n_1 < n_2$. Then*

- (i) $n + 1 \leq n_1 \leq 3n - 1$.
- (ii) $E[\frac{nn_1}{n_1-n}] + 1 \leq n_2 \leq E[\frac{2n_1n}{n_1-n}]$, where $E[x]$ denotes the integer part of x .
- (iii) $|G| \leq n(n+1)(n^2+n+1)$.

Proof. By the class equation and Lemma 3.4.

$$|N| = 1 + |x_1^G| + |x_2^G|. \tag{4.5}$$

Dividing by $|G|$,

$$\frac{1}{n} = \frac{1}{|G|} + \frac{1}{n_1} + \frac{1}{n_2} < \frac{3}{n_1}. \tag{4.6}$$

Therefore, $n_1 < 3n$ and $n < n_1$, so (i) holds. Furthermore, since $n < n_1 < n_2 < |G|$,

$$\frac{1}{n} - \frac{1}{n_1} = \frac{1}{n_2} + \frac{1}{|G|} < \frac{2}{n_2}$$

and this means that

$$n_2 \leq E[\frac{2n_1n}{n_1-n}].$$

On the other hand,

$$\frac{1}{n} - \frac{1}{n_1} = \frac{1}{n_2} + \frac{1}{|G|} > \frac{1}{n_2},$$

so

$$n_2 > E[\frac{nn_1}{n_1-n}].$$

Then (ii) is proved. Also, Eq. (4.6) reduces to

$$|G| = nn_1n_2/(n_1n_2 - nn_2 - nn_1). \tag{4.7}$$

Eq. (4.7) is equivalent to the equation $|G| = (1/n - (1/n_1 + 1/n_2))^{-1}$, from which it immediately follows that this function (of n_1 and n_2) takes its maximum value when n_1 and n_2 are at their minimum values, which are $n + 1$ and $n(n + 1) + 1$ according to (i) and (ii), respectively. We deduce that $|G| \leq n(n + 1)(n^2 + n + 1)$. \square

We use the following theorem to limit the search.

Theorem 4.3.7 (see [2], Theorem 4.1.2). *Let N be a normal subgroup of a group G such that $\Gamma_G(N)$ has two vertices and no edge. Then N is a 2-group or a Frobenius group with p -elementary abelian kernel K , and complement H which is cyclic of order q , for two different primes p and q . In particular, $|N| = p^n q$ with $n \geq 1$.*

In Table 4.3 we indicate, for each index, the improved bound for $|G|$ of Theorem 4.3.6 and the number of groups with a normal subgroup containing two non-central classes of G of coprime sizes. In Table 4.4, we show the complete classification for the indices that appear in Table 4.3.

Figure 4.3: Groups with normal subgroups having two non-central G -classes with coprime sizes.

| Index of N | $ G \leq n(n + 1)(n^2 + n + 1)$ (Theorem 4.3.6) | Number of groups |
|--------------|---|------------------|
| 2 | 42 | 3 |
| 3 | 156 | 2 |
| 4 | 420 | 7 |
| 5 | 930 | 2 |
| 6 | 1806 | 8 |
| 7 | 3192 | 1 |
| 8 | 5256 | 22 |
| 9 | 8190 | 5 |
| 10 | 12210 | 7 |
| 11 | 17556 | 2 |
| 13 | 33306 | 2 |
| 17 | 93942 | 1 |

The idea of the algorithm implemented in GAP is to list only those integers at most the bound obtained in Theorem 4.3.6, say c , satisfying that n , n_1 and n_2 divide c , with $(c/n_1, c/n_2) = 1$, $c/n_1 > 1$ and $c/n_2 > 1$. For $n = 12$, we have not been able to give a complete classification because 2184 is a possible value for $|N|$ but this order is not included in the SMALLGROUPS library of GAP. The same problem arises for the indices 14, 15, 16 and 18.

Figure 4.4: Groups having normal subgroups with two non-central G -classes with coprime sizes for certain indices.

| n | G | | | | | |
|-----------|--------|--------|---------|---------|---------|---------|
| 2 | 24#12 | 20#3 | 12#4 | | | |
| 3 | 42#1 | 18#3 | | | | |
| 4 | 48#30 | 48#48 | 72#39 | 72#41 | 40#12 | 24#5 |
| | 24#14 | | | | | |
| 5 | 110#1 | 30#1 | | | | |
| 6 | 72#42 | 72#43 | 156#7 | 84#7 | 60#6 | 60#7 |
| | 36#10 | 36#12 | | | | |
| 7 | 42#3 | | | | | |
| 8 | 96#65 | 96#185 | 96#186 | 96#187 | 96#194 | 96#195 |
| | 96#226 | 272#50 | 144#120 | 144#182 | 144#185 | 144#187 |
| | 80#28 | 80#30 | 80#31 | 80#34 | 80#50 | 48#4 |
| | 48#35 | 48#38 | 48#40 | 48#51 | | |
| 9 | 342#7 | 126#1 | 126#7 | 54#4 | 54#12 | |
| 10 | 120#37 | 120#38 | 220#7 | 100#9 | 100#10 | 60#8 |
| | 60#11 | | | | | |
| 11 | 506#1 | 66#1 | | | | |
| 13 | 702#47 | 78#3 | | | | |
| 17 | 102#1 | | | | | |

Remark 4.3.8. *Every group in Table 4.4 has only one normal subgroup with the desired conditions. Also, for every index, the symmetric group S_3 always appears as a normal subgroup. This happens because we can construct groups in the following way: $G = N \times A$ where $N \trianglelefteq G$ and A is abelian. Consequently, the G -classes of N are exactly the classes of N . Thus, by taking $N \cong S_3$, the G -classes sizes of N are $\{1, 2, 3\}$. In fact, for $n = 7$ and $n = 17$ this is the unique possibility.*

4.4 An extension of Landau's theorem for prime-power order elements

Let G be a finite group and let $N \trianglelefteq G$. We denote by $k(G)$ the number of conjugacy classes of G and by $k_G(N)$ the number of G -conjugacy classes of elements of N . Analogously, we denote by $k_{pp}(G)$ the number of conjugacy classes of prime-power order elements of G and by $k_{pp_G}(N)$ the number of G -classes of prime-power order elements of N .

The aim of this section is to extend Landau's result to elements of prime-power order lying in a normal subgroup of a finite group. However, if we restrict our attention to just non-central G -classes of prime-power order elements contained in a normal subgroup N of G , one can easily see that $|N|$ and $|G|$ cannot be bounded in terms of the number of such classes although the index $|G : N|$ is fixed. For instance, suppose that $N \trianglelefteq G$ with $|G : N| = n$ and that N has just one non-central G -class (necessarily of prime-power order elements), as in any example of Section 4.3.1. Then N is a p -group for some prime p and we can take an arbitrary abelian finite p' -group

H and construct $N_0 = N \times H$ and $G_0 = G \times H$. It follows that $N_0 \trianglelefteq G_0$, with index n too, and N_0 contains exactly one non-central G_0 -class of prime-power order elements. However, $|N_0|$ and $|G_0|$ need not be bounded.

Therefore, in this section, we consider all G -classes, central and non-central, contained in a normal subgroup, and prove that there are finitely many groups G having a normal subgroup N of index n and with $kpp_G(N) = k$. We also provide an upper bound for $|G|$ and $|N|$ as a function of k when G is solvable.

As we pointed out in the introduction, Héthelyi and Külshammer [8] prove an extension of Landau's theorem for prime-power order elements. They did not give any numerical expression for the upper bound of the group order.

Theorem 4.4.1 ([8], Theorem 1.1). *For a positive integer k , there are only finitely many finite groups, up to isomorphism, satisfying $k = kpp(G)$.*

This theorem is a direct consequence of the next result, which uses the classification of the Finite Simple Groups.

Lemma 4.4.2 ([8], Lemma 1.5). *There exists a function $\alpha : \mathbb{N} \rightarrow \mathbb{N}$ satisfying that whenever k is a positive integer and G is a finite group with $kpp(G) = k$ then $|G| \leq \alpha(k)$.*

Analogous results can be obtained when we work with conjugacy classes lying in a normal subgroup. For this purpose, we state and prove the following well-known elementary facts; see [5], Lemma 2.1.

Lemma 4.4.3. *If G is a finite group and $N \trianglelefteq G$, then*

- (i) *For every $x \in N$, the class x^G decomposes into the union of exactly $|G : N\mathbf{C}_G(x)|$ conjugacy classes of N ,*
- (ii) $k_G(N) \geq k(N)/|G : N|$,
- (iii) $kpp_G(N) \geq kpp(N)/|G : N|$.

Proof. (i) By taking a set of representatives of the right (or left) classes of N in G , we can write $x^G = \cup_{i=1}^k x_i^N$ for certain $x_i \in N$, which are G -conjugate. Furthermore, the fact that the x_i are G -conjugate implies that the classes x_i^N all have the same cardinality, and hence $|x^G| = k|x^N|$. On the other hand,

$$|x^G| = |G : \mathbf{C}_G(x)N| |\mathbf{C}_G(x)N : \mathbf{C}_G(x)| = |G : \mathbf{C}_G(x)N| |x^N|,$$

so $|G : \mathbf{C}_G(x)N| = k$, as required.

(ii) By (i), each G -conjugacy class of $x \in N$ decomposes into exactly $|G : N\mathbf{C}_G(x)|$ classes of N . Since this number divides $|G : N|$, we deduce that the G -class of every element in N decomposes into at most $|G : N|$ classes of N . Moreover, the N -classes in such a decomposition are trivially distinct, so the inequality follows.

(iii) The same argument of (ii) works, by restricting to prime-power order elements of N . □

Lemma 4.4.4. *There exists a function $\gamma : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ with the following property. If $n, l \in \mathbb{N}^+$ and G is a finite group with $N \trianglelefteq G$ such that $|G : N| = n$ and $kpp_G(N) = l$, then $|G| \leq \gamma(n, l)$.*

Proof. By Lemma 4.4.3, $nl = kpp_G(N)|G : N| \geq kpp(N)$. Now, by Lemma 4.4.2, there exists $\alpha : \mathbb{N} \rightarrow \mathbb{N}$ such that for every i , with $1 \leq i \leq nl$, if we assume that $kpp(N) = i$, then $|N| \leq \alpha(i)$. Therefore, if we define

$$\gamma(n, l) = |G : N| \max\{\alpha(1), \dots, \alpha(nl)\},$$

we conclude that $|G| \leq \gamma(n, l)$. □

We have now proved the first part of Theorem B.

Theorem 4.4.5. *For any two positive integers k, n , there are only finitely many finite groups G , up to isomorphism, with a normal subgroup N of index n satisfying $k = kpp_G(N)$.*

Proof. This is a direct consequence of Lemma 4.4.4. □

From now on we assume that G is a solvable group and we get first an specific upper bound for $|G|$ when $kpp(G) = k$. The idea of our proof is inspired by [8], Lemma 1.5. If we take a normal subgroup N of G with a fixed index and with $kpp_G(N) = k$, we obtain in Corollary 4.4.8 a formula for bounding $|N|$ and $|G|$, so Theorem B will be proved.

To get the upper bound for $|G|$, we need one more result of [8] concerning G -classes and factor groups. This holds for every finite group, not only for solvable groups.

Lemma 4.4.6 ([8], Lemma 1.2(ii)). *If N is a normal subgroup of a finite group G , then $kpp(G/N) < kpp(G)$ unless $N = 1$.*

Theorem 4.4.7. *If G is a finite solvable group such that $kpp(G) = k$, then*

$$|G| \leq \gamma(k)$$

where γ is defined as follows: $\gamma(1) = 1$ and $\gamma(k) = k\gamma(k - 1)^2$ for every $k \geq 2$. Consequently,

$$|G| \leq \prod_{i=0}^{k-1} (k - i)^{2^i}.$$

Proof. We argue by induction on k to prove both that $|G| \leq \gamma(k)$ and that γ is an increasing function in $[1, k]$. When $k = 1$ it is trivial that $|G| = 1$, so we define $\gamma(1) = 1$. If $k = 2$, we take N a minimal normal subgroup G , and by applying Lemma 4.4.6, since $N \neq 1$, $kpp(G/N) < kpp(G) = 2$. Then $kpp(G/N) = 1$, that is, $N = G$. On the other hand, since N is abelian, certainly $|N| = 2$. Therefore, $|G| \leq 2 = 2\gamma(1)^2 =: \gamma(2)$. Also, in particular $\gamma(1) < \gamma(2)$. Now, assume by induction that when $kpp(G) = k$ then $|G| \leq k\gamma(k - 1)^2$ and that γ is an increasing function in $[1, k]$. Suppose that $kpp(G) = k + 1$ and let N be a minimal normal subgroup of G . Again by Lemma 4.4.6, $kpp(G/N) < kpp(G) = k + 1$. Then $|G/N| \leq$

$\max\{\gamma(1), \dots, \gamma(k)\} = \gamma(k)$ by the inductive hypothesis. Furthermore, N trivially contains at most $k + 1$ G -classes of elements of prime-power order. Each of these splits into at most $|G/N|$ N -classes of elements of prime-power order. As a result, N has at most $(k + 1)\gamma(k)$ conjugacy classes of elements of prime-power order by Lemma 4.4.3 (iii). As N is an abelian prime-power order group, we conclude that $|N| \leq (k + 1)\gamma(k)$. Therefore, $|G| = |N||G/N| \leq (k + 1)\gamma(k)^2 =: \gamma(k + 1)$ and also, in particular, $\gamma(k) < \gamma(k + 1)$. The last inequality of the statement follows easily. \square

Corollary 4.4.8. *Let G be a finite solvable group and let $N \trianglelefteq G$ such that $|G : N| = n$ and $kpp_G(N) = k$. Then*

$$|N| \leq \prod_{i=0}^{nk-1} (nk - i)^{2^i}$$

and

$$|G| \leq n \prod_{i=0}^{nk-1} (nk - i)^{2^i}.$$

Proof. By Lemma 4.4.3, we know that $kpp_G(N) \geq kpp(N)/|G : N|$, so $kpp(N) \leq |G : N|kpp_G(N) = nk$. Thus, by applying Theorem 4.4.7 to N we get $|N| \leq \gamma(nk) = \prod_{i=0}^{nk-1} (nk - i)^{2^i}$. This implies that $|G| = n|N| \leq n\gamma(nk) \leq n \prod_{i=0}^{nk-1} (nk - i)^{2^i}$. \square

Figure 4.5: Classification of solvable groups with small $kpp(G)$.

| k | G |
|-----|--|
| 2 | 2#1 |
| 3 | 3#1 6#1 |
| 4 | 4#1 4#2 6#2 10#1 12#3 |
| 5 | 5#1 8#3 8#4 12#1 12#4 14#1 20#3 21#1 24#3 24#12 30#3 42#1 |

We finish this section by showing in Table 4.5 a classification, obtained with GAP, of those solvable groups G with $kpp(G) = k$ for small values of k . We note that for $k = 5$ the bound of Corollary 4.4.8 is too large to be used with GAP, but we improve it by using the same argument as in Theorem 4.4.7. Let N be a minimal normal subgroup of G . By Lemma 4.4.6 we know that $kpp(G/N) < kpp(G) = 5$, so $kpp(G/N) \leq 4$. We observe in Table 5 that the largest size of $|G|$ for $k = 4$ is 12. Consequently, $|G/N| \leq 12$. Furthermore, N trivially contains at most 5 G -classes of elements of prime-power order and each of these splits into at most $|G/N|$ N -classes. Thus, N has at most $5 \times 12 = 60$ conjugacy classes of elements of prime-power order by Lemma 4.4.3 (iii). As a consequence, $|G| = |N||G/N| \leq 60 \times 12 = 720$. This bound is computationally useful.

Acknowledgements

The results in this paper are part of the third author's Ph.D. thesis at the Jaume I University of Castellón, who is financially supported by a predoctoral grant of the Jaume I University. The research of the first and second authors is supported by the

Valencian Government, Proyecto PROMETEOII/2015/011. The first and the third authors are also partially supported by the Jaume I University, grant P11B2015-77.

Bibliography

- [1] A. Beltrán, M.J. Felipe and C. Melchor, Graphs associated to conjugacy classes of normal subgroups in finite groups. *J. Algebra*, **443** (2015), 335-348.
- [2] A. Beltrán, M.J. Felipe and C. Melchor, Triangles in the graph of conjugacy classes of normal subgroups. *Monatshefte für Mathematik*, 10.1007/s00605-015-0866-9. To appear.
- [3] E.A. Bertram, M. Herzog, A. Mann, On a graph related to conjugacy classes of groups. *Bull. London Math. Soc.* **22** (6) (1990), 569-575.
- [4] H.U. Besche, B. Eick and E.A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.* **12**, 623 - 644 (2002).
- [5] M. Cartwright. The number of conjugacy classes of certain finite groups. *Quart. J. Math. Oxford Ser.* **36** (1985), no. 144, 393-404.
- [6] M. Cartwright. A bound on the number of conjugacy classes of a finite soluble group. *J. London Math. Soc.* (2) (1987), 229-244.
- [7] The GAP Group, GAP - Groups, Algorithms and Programming, Vers. 4.7.7; 2015. (<http://www.GAP-system.org>)
- [8] L. Héthelyi and B. Külshammer. Elements of prime-power order and their conjugacy classes in finite groups. *J. Aust. Math. Soc.* **78** (2005), 291-295.
- [9] E. Landau, Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante. *Math Ann.* **56** (1903), 671-676.
- [10] M.L. Lewis, Landau's theorem, fields of values for characters, and solvable groups. Preprint (2015).
- [11] A. Moretó, H.N. Nguyen, Variations of Landau's theorem for p -regular and p -singular conjugacy classes. *Israel J. Math.* **212** (2016), no. 2, 961-987.
- [12] M. Newman, A bound for the number of conjugacy classes in a group. *J. London Math. Soc.* **43** (1968), 108-110.
- [13] A. Vera, J. Vera, Classification of finite groups according to the number of conjugacy classes. *Israel J. Math.* **51** (1985), no. 4, 305-338.
- [14] A. Vera, J. Vera, Classification of finite groups according to the number of conjugacy classes. II. *Israel J. Math.* **56** (1986), no. 2, 188-221.

Part II

Products of conjugacy classes

Chapter 5

Squares of real conjugacy classes in finite groups

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 non-central conjugacy classes and when every conjugacy class satisfies that its square is the union of all central conjugacy classes except at most one.

Keywords. Finite groups, conjugacy classes, product of classes, characters, real conjugacy classes.

Mathematics Subject Classification (2010): 20E45, 20C15, 20D15.

5.1 Introduction

There exist many results about the structure of a finite group focused on the product of its conjugacy classes. Some of them are related to the solvability and non-simplicity of the group. Perhaps, one of the most relevant problems was stated in 1985 by Z. Arad and M. Herzog who 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 although it has been obtained for several families of simple groups (see [11]). A particular case of the conjecture was recently given by G. Navarro and R. Guralnick in [7]. They proved that when a conjugacy class K in a finite group G satisfies that K^2 is again a conjugacy class, then $\langle K \rangle$ is a solvable (normal) subgroup of G . Another result concerning products of classes was given by Z. Arad and E. Fisman [1] who demonstrated 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.

In this paper we present a contribution to the study of the solvability and non-simplicity of a group from the square of a conjugacy class. Suppose that K is a non-trivial real conjugacy class of G , that is, a class satisfying that $K^{-1} = K$. It trivially follows that K^2 can never be a conjugacy class unless K consists of only a single 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 the join of conjugacy classes of G . In this note, we

study the extreme case in which A is a single class, and we wonder whether one may obtain somewhat information concerning solvability 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 result needs to be a real class. In fact, this is not a very unusual 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 . Since $|\langle K \rangle / \langle D \rangle| \leq 2$, then $\langle K \rangle = \langle x \rangle [x, G]$ is solvable. More precisely,*

1. *Suppose that $|K| = 2$.*
 - (a) *If $o(x) = 2$, then $\langle K \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \cong \langle D \rangle \subseteq \mathbf{Z}(G)$.*
 - (b) *If $o(x) = n > 2$, then $\langle K \rangle \cong \mathbb{Z}_n$ and $\langle D \rangle$ is cyclic.*
2. *Suppose that $|K| \geq 3$.*
 - (a) *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.*
 - (b) *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 $o(x) = 2p$.*

Observe that in case 2 we determine the order of the elements of K , which may be either 2, p or $2p$ with p an 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 [6] and a result of Y. Berkovich and L. Kazarin in [3]. Both require tools from modular representation theory, so our results are based on it as well. 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 appeal to the Classification of Finite Simple Groups.

On the other hand, we prove that the property $K^2 = 1 \cup D$ in a group G , stated in Theorem A, can be characterized by means of an arithmetical property of the set of irreducible characters of G . As usual, $\text{Irr}(G)$ will denote this set.

Theorem B. *Let G be a group and $x, d \in G \setminus \{1\}$. Let $K = x^G$ and $D = d^G$. The following are equivalent:*

- a) $K^2 = 1 \cup D$
- b) *For every $\chi \in \text{Irr}(G)$ we have*

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

As an application of our main result we obtain the following corollaries. The first one is related to groups in which every non-central conjugacy class satisfies the hypothesis of Theorem A and its proof is a trivial consequence. The second concerns conjugacy classes whose square is the join of classes all central except at most one.

Corollary C. *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 D. *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. It is trivial that every real element must lie in $\mathbf{Z}(G)$ and must have order 2. In [4], D. Chillag and A. Mann described the groups in which every real element is a central element. Particularly, in Remark 5.5 of [4], the authors also announce, with omitted proof, that any group satisfying this property is nilpotent. We include here an extension of this result which will be needed in order to study the structure of those groups in which all conjugacy classes satisfy the hypothesis of Corollary C. Note that these groups are solvable by Theorem A and we show that they are close to nilpotent groups.

Corollary E. *Let G be a finite group and 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 F. *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.*

5.2 Preliminary results

We begin by stating the Z^* theorem version appearing in [8].

Theorem 5.2.1. *Let G be a finite group. Suppose that $P \in \text{Syl}_2(G)$ 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 often used in the proofs. The reader interested in further properties related to products and powers of conjugacy classes can refer to [2].

Lemma 5.2.2. *Let K be a real conjugacy class of a finite 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 consider the factor group $\langle K \rangle / N$ which is generated by the set of 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 of G and all non-trivial elements of K^2 are conjugate, so all of them have the same order. \square

As we have already indicated in the Introduction, we use the following result of Berkovich and Kazarin of [3], which is based on the well-known Kazarin's Theorem (see for instance [8]), which asserts that any conjugacy class of prime-power size generates a solvable normal subgroup.

Lemma 5.2.3 (Lemma 3 of [3]). *Let G be a finite group and 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.*

The following result, to which we have referred at the beginning of the Introduction, will be used in the proof of Corollaries C and D. We remark that we do need it to prove Theorem A.

Theorem 5.2.4 (Theorem A of [7]). *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 [7] 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 here, can be easily obtained without using characters. The solvability in Theorem 5.2.4, however, needs the Classification of Finite Simple Groups.

Finally, we will also use a Burnside's classic result whose proof can be found in [10] for instance.

Lemma 5.2.5 (Theorem 1.2.6 of [10]). *A non-cyclic 2-group P has only one involution if and only if P is a generalized quaternion group.*

5.3 Proofs

We start by proving the equalities concerning commutators that appear in Theorem A. Recall that the conjugacy classes K and D of the statement are real classes.

Lemma 5.3.1. *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 $K = \{x_1, \dots, x_n\}$, it is clear that $K^2 = x_1K \cup \dots \cup x_nK$. Let $y \in x_iK$. Since K is real, then $y = x_i g^{-1} x_i^{-1} g \in [x_i^{-1}, G] = [x_i, G]$ for some $g \in G$. Also, 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, since any element $[x, t]$ lies in K^2 for all $t \in G$, then $[x, G] \subseteq \langle K^2 \rangle = \langle D \rangle$ 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

We are ready to prove our main result.

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

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

Case 1.a. 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.a is proved.

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

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

Case 2.a. 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 $K = \{x_1, \dots, x_s\}$ and we have $K^2 = 1 \cup \{x_i x_j | i \neq j\}$. Since $o(x_i x_j) = 2$ for every $1 \leq i, j \leq s$ with $i \neq j$, then $1 = x_i^2 x_j^2 = x_i x_i x_j x_j = x_i x_j x_i x_j$, so x_i and x_j commute. Consequently, $\langle K \rangle$ is generated by pairwise commuting involutions, so $\langle K \rangle$ is 2-elementary abelian (and $\langle D \rangle$ too) and we obtain the first assertion of 2.a.

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 $P \in \text{Syl}_2(G)$. Therefore, $P \cap K = \{x\}$ and we deduce that $\mathbf{O}_{2'}(G)\langle x \rangle \trianglelefteq G$ by Theorem 5.2.1.

The Frattini argument gives $G = \mathbf{N}_G(\langle x \rangle)\mathbf{O}_{2'}(G)$. 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 $|\mathbf{O}_{2'}(G) : \mathbf{C}_{\mathbf{O}_{2'}(G)}(x)|$. As $\mathbf{O}_{2'}(G)$ 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. Let $P \in \text{Syl}_p(\mathbf{O}_{2'}(G))$ such that $P^x = P$. Thus, $[x, P] \subseteq P$. Now, if $[x, P] = 1$ this contradicts that p divides $|\mathbf{O}_{2'}(G) : \mathbf{C}_{\mathbf{O}_{2'}(G)}(x)|$, 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 lying in D , so all elements of D are p -elements and in particular, 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 $m \geq 1$, as we wanted to prove. By applying Lemma 5.2.3, we deduce that $\langle K \rangle / \mathbf{O}_p(\langle K \rangle)$ is an abelian 2-group. As a consequence, $\mathbf{O}_{2'}(\langle K \rangle) = \mathbf{O}_p(\langle K \rangle)$. By

Lemma 5.2.2 (a), we have that $\langle K \rangle / \langle D \rangle$ is necessarily cyclic of order 2 and then $\langle D \rangle = \mathbf{O}_p(\langle K \rangle)$. The second assertion of case 2.a is complete.

Case 2.b. Suppose that $o(x) > 2$. We prove first that $|D| = |K|$. We know that $|K| \leq |K^2| = 1 + |D|$ and $D = (x^2)^G$. Note that $|D|$ divides $|K|$ because $\mathbf{C}_G(x) \subseteq \mathbf{C}_G(x^2)$. Thus, either $|D| = |K|$ or $|D| \leq |K|/2$. However, if $|D| \leq |K|/2$, the first inequality implies that $|K| \leq 1 + |K|/2$, so $|K| \leq 2$, a contradiction. Consequently, $|K| = |D|$ as wanted. Now, notice that $xK \cup x^{-1}K \subseteq K^2$ and we claim that $xK \neq x^{-1}K$. Indeed, if $xK = x^{-1}K$, 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 K is union of right classes of $\langle D \rangle$ and then $|\langle D \rangle|$ divides $|K|$. But this is a contradiction because $|K| = |D| < |\langle D \rangle|$.

We have proved that $xK \neq x^{-1}K$ 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 $x^{-1}K \setminus xK$ (notice that $z, z^{-1} \in D$). Therefore, K^2 can be decomposed as

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

From the fact that $(xK)(x^{-1}K) = K^2$ 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 $D^2 = 1 \cup A_1 \cup \dots \cup A_r$ 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, $g \in A_i$ 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 $z^2 \in K^2$ or $z^2 \notin K^2$.

- 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 that $D^2 = K^2 = 1 \cup D$, and then $\langle D \rangle$ is p -elementary abelian for some prime p by applying Lemma 5.2.2 (b). Furthermore, $\langle D \rangle = \langle K^2 \rangle$, so $|\langle K \rangle / \langle D \rangle| \leq 2$ by Lemma 5.2.2 (a). Observe that $(x^2)^G = D$, so $o(x)$ divides $2p$ and hence, either $o(x) = p$ or $o(x) = 2p$. If $o(x) = p > 2$, then $\langle x \rangle = \langle x^2 \rangle$ and $\langle K \rangle = \langle D \rangle$ is p -elementary abelian. Let us prove 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. As K is real, then $o(x) = 2$, a contradiction. Thus, we obtain the assertion of 2.b.
- b) Suppose that $z^2 \notin K^2$, what is equivalent to say 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 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 $P \in \text{Syl}_2(\langle D \rangle)$ 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 $\overline{D^2} = \overline{D}^2 = \overline{1} \cup \overline{D}$. By Lemma 5.2.2 (b), $\langle \overline{D} \rangle$ is p -elementary abelian 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 hence, $D \subseteq \mathbf{C}_G(z^2)$. This means that $\langle z^2 \rangle \subseteq \mathbf{Z}(\langle D \rangle)$, so $\langle D \rangle / \mathbf{Z}(\langle D \rangle)$ is abelian and $\langle D \rangle$ is nilpotent of class at most 2. The decomposition for $\langle D \rangle$ of the statement certainly 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 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 of cardinality 2 for the rest of this step. Suppose that $o(z^2) = k$ is odd and notice 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 $zz^g \in D^2 = 1 \cup D \cup \{z^2, z^{-2}\}$. Also, $zz^g = z^k z^2 (z^k)^g z^{-2} = z^k (z^k)^g \in P$ 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 order $2k$. 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, $o(z^2)$ must be even.

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 $k \geq 2$, $D^{k-1} \subseteq D^k \subseteq 1 \cup D \cup \langle z^2 \rangle \cup D \langle z^2 \rangle$. We can deduce that there exists $l \in \mathbb{N}$, depending on the order of z , such that $\langle D \rangle = D^l \subseteq 1 \cup D \cup \langle z^2 \rangle \cup D \langle z^2 \rangle \subseteq \langle D \rangle$. This yields to

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

Accordingly, it is enough to show that there exists no element $dz^{2i} \in D z^{2i}$ with $d \in D$ such that $o(dz^{2i}) = 2$. Otherwise, we assume $(dz^{2i})^2 = d^2 z^{4i} = 1$ 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 5.2.5, P must be cyclic or generalized quaternion. We will get a contradiction in both cases. Assume first that P is cyclic. Since

$\langle \bar{D} \rangle = \langle D \rangle / \langle z^2 \rangle \cong P/P \cap \langle z^2 \rangle$ is 2-elementary abelian by Step 1 and P is cyclic, then either $\langle \bar{D} \rangle \cong \mathbb{Z}_2$ or $\langle \bar{D} \rangle$ is trivial. Furthermore, $\langle z \rangle \neq \langle z^2 \rangle$. Otherwise, $\mathbf{C}_G(z) = \mathbf{C}_G(z^2)$ and then $|K| = |D| = |(z^2)^G|$ would be either 1 or 2, contradicting the fact that $|K| \geq 3$. Thus, $\langle z^2 \rangle \subset \langle z \rangle \subseteq \langle D \rangle$ and this forces that $\langle D \rangle = \langle z \rangle$. As the elements of D have the same order that z , which is even, 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 $D \subseteq D^2$.

From now on, P can be assumed to be generalized quaternion. We denote $\tilde{G} = G/H$ and then $\langle \tilde{D} \rangle = \langle \bar{D} \rangle \cong P$. Notice that $\mathbf{Z}(P) \cong \mathbf{Z}(\langle \tilde{D} \rangle) = \mathbf{Z}(\langle D \rangle / H) = \mathbf{Z}(\langle D \rangle) / H$, because $\langle D \rangle = P \times H$, and that $\langle \tilde{D} \rangle / \mathbf{Z}(\langle \tilde{D} \rangle)$ is dihedral. Also, $\langle \tilde{D} \rangle / \mathbf{Z}(\langle \tilde{D} \rangle) \cong \langle D \rangle / \mathbf{Z}(\langle D \rangle)$ is 2-elementary abelian by Step 1. By joining both facts, we conclude that $\langle \tilde{D} \rangle / \mathbf{Z}(\langle \tilde{D} \rangle) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore, $\langle \tilde{D} \rangle \cong Q_8$ and $\langle D \rangle \cong Q_8 \times H$. Note that $\langle \tilde{z}^2 \rangle \subseteq \mathbf{Z}(\langle \tilde{D} \rangle)$ which has order 2. Then the order of $\langle \tilde{z}^2 \rangle$ is either 1 or 2. If $\langle \tilde{z}^2 \rangle$ is trivial, from Step 3, we get

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

and by Lemma 5.2.2 (b), $\langle \tilde{D} \rangle$ is elementary abelian, a contradiction. Thus, we can assume that $o(\tilde{z}^2) = 2$. Again, by Step 3,

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

and we distinguish two cases. When \tilde{D} and $\tilde{D} \tilde{z}^2$ are equal or distinct. If $\tilde{D} \neq \tilde{D} \tilde{z}^2$, then $8 = 2 + 2|\tilde{D}| = 2(1 + |\tilde{D}|)$, what means that $|\tilde{D}| = 3$. The fact that \tilde{D} is real forces that $o(\tilde{z}) = 2$, a contradiction. Therefore, $\tilde{D} = \tilde{D} \tilde{z}^2$ and $8 = |\langle \tilde{D} \rangle| = 2 + |\tilde{D}|$, so $|\tilde{D}| = 6$. Now we prove that $|\tilde{K}| = |\tilde{D}|$. We have $\tilde{K}^2 = \tilde{1} \cup \tilde{D}$. Since $o(\tilde{z}^2) = 2$ and \tilde{x}^2 and \tilde{z} are \tilde{G} -conjugate, we know that $o(\tilde{x}) > 2$. So, $\tilde{D} = (\tilde{x}^2)^{\tilde{G}}$ and, since $\mathbf{C}_{\tilde{G}}(\tilde{x}) \subseteq \mathbf{C}_{\tilde{G}}(\tilde{x}^2) \subseteq \tilde{G}$, we conclude that $|\tilde{D}|$ divides $|\tilde{K}|$. As $6 = |\tilde{D}| \leq |\tilde{K}| \leq |\tilde{K}^2| = 1 + |\tilde{D}|$, we get $|\tilde{D}| = |\tilde{K}|$, as wanted.

On the other hand, by taking into account that \tilde{K} is a real class and Lemma 5.2.2 (a), we know that $\langle \tilde{K} \rangle / \langle \tilde{K}^2 \rangle = \langle \tilde{K} \rangle / \langle \tilde{D} \rangle$ is trivial or cyclic of order 2. In the former case, that is, if $\langle \tilde{K} \rangle = \langle \tilde{D} \rangle = \tilde{1} \cup \{ \tilde{z}^2 \} \cup \tilde{D}$, we see that this leads to a contradiction. We know that $\tilde{1} \neq \tilde{x} \in \langle \tilde{K} \rangle$. If $\tilde{x} = \tilde{z}^2$, then $o(\tilde{x}) = 2$. Then $x^2 \in H$, which implies that $z \in H$ and $o(z^2)$ is odd, a contradiction. So $\tilde{x} \in \tilde{D}$ 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, as a result, $\langle z \rangle = \langle z^2 \rangle$. So, $\mathbf{C}_G(z) = \mathbf{C}_G(z^2)$ and $|D| = |(z^2)^G| = 2$, which contradicts that $|K| \geq 3$. We can assume then that $\langle \tilde{K} \rangle / \langle \tilde{D} \rangle \cong \mathbb{Z}_2$. Therefore, $\langle \tilde{K} \rangle$ is a 2-group of order 16, which has a normal subgroup isomorphic to Q_8 , and moreover, $\langle \tilde{K} \rangle$ possesses at least 6 elements of order 8 (the elements of \tilde{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 former two groups possess exactly 4 elements of order 8 and the latter two groups have no elements of order 8. All cases give a contradiction.

□

Example 5.3.2. *Let us show several examples of each case of Theorem A. In some of them, we use the SMALLGROUPS library of GAP [5]. The m -th group of order n in this library is identified by $n\#m$.*

Case 1.a. We take G the group

$$M_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^2 = 1, a^b = a^{2^{n-1}+1} \rangle$$

with $n \geq 3$. We consider the conjugacy class $K = b^G$ that satisfies $K^2 = 1 \cup D$ where $D = (a^{2^{n-1}})^G$.

Case 1.b. We consider $G = D_{2n} = \langle a, b \mid a^n = b^2 = 1, a^b = a^{-1} \rangle$ with $n \geq 3$ and $K = a^G$. Then $K^2 = 1 \cup D$ where $D = (a^2)^G$. Remark that if n is odd, then $\langle D \rangle = \langle K \rangle$ whereas if n is even, $|\langle K \rangle / \langle D \rangle| = 2$.

Case 2.a. 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, $K = \{x_1, \dots, x_r\}$ is a conjugacy class of G such that $K^2 = 1 \cup D$ where $D = \{x_i x_j \mid i \neq j\}$ 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.a 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 is another example where K is the conjugacy class of involutions. In this case, $\langle K \rangle = \langle D \rangle$.

Let $G = 216\#88 = \langle a, b, c \mid c^3 = 1, a^4 = 1, a^2 = b^2, a^b = a^{-1}, c^{-1}a^{-1}ca^{-1}bcb = 1, c^{-1}a^{-1}c^{-1}b^{-1}ca^{-1}b = 1, b^{-1}ca^{-1}c^{-1}abc = 1 \rangle \cong ((\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3) \rtimes Q_8$. The conjugacy class $K = (a^2)^G$ satisfies that $K^2 = 1 \cup D$ where $D = c^G$. Moreover, $o(a^2) = 2$, $o(c) = 3$, $|K| = 9$ and $|D| = 24$. This is an example of case 2.a in which $\langle D \rangle$ is a non-abelian extraspecial 3-group of order 27 and exponent 3.

Case 2.b. Let $\langle a \rangle \cong \mathbb{Z}_5$ and let $\langle b \rangle \cong \mathbb{Z}_8$ acting on $\langle a \rangle$ by $a^b = a^2$. Let G be the associated semidirect product $\langle a \rangle \rtimes \langle b \rangle$ 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.b of Theorem A with $\langle D \rangle \cong \mathbb{Z}_5$ and $\langle K \rangle \cong \mathbb{Z}_{10}$.

We get another example for the case in which the order of the elements of K is a prime. Take $G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes Q_8 \cong \text{PSU}(3, 2) = \langle a, b, c, d \mid a^4 = c^3 = d^3 = 1, a^2 = b^2, a^b = a^{-1}, c^a = cd^2, d^a = c^2 d^2, c^b = d, d^b = c^2 \rangle$ and $K = c^G$, with c an element of order 3. This class satisfies that $K^2 = 1 \cup K$ with $|K| = 8$. Furthermore, $\langle K \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Observe that both examples satisfy $|K| = |D|$, as it is explicitly showed in the proof of Theorem A.

Now we prove the characterization of the property stated in Theorem A in terms of irreducible characters. For our purposes, we use the following result which characterizes when the product of two conjugacy classes is again a conjugacy class.

Lemma 5.3.3. *Let G be a group and let $a, b, c \in G$ be nontrivial elements of G . The following conditions are equivalent:*

$$a) a^G b^G = c^G$$

$$b) \chi(a)\chi(b) = \chi(c)\chi(1) \text{ for all } \chi \in \text{Irr}(G).$$

Proof. See for instance Lemma 5.2.2 of [11]. \square

Proof of Theorem B. Suppose that $K^2 = 1 \cup D$ and let $\chi \in \text{Irr}(G)$. Notice that K is real. By applying problem 3.12 of [9],

$$\chi(x)^2 = \chi(x)\chi(x^{-1}) = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(x(x^{-1})^g).$$

We can divide the sum into two parts, so the above formula is equal to

$$\begin{aligned} & \frac{\chi(1)}{|G|} \left(\sum_{g \in \mathbf{C}_G(x)} \chi(x(x^{-1})^g) + \sum_{g \in G \setminus \mathbf{C}_G(x)} \chi(x(x^{-1})^g) \right) = \\ & \frac{\chi(1)}{|G|} (|\mathbf{C}_G(x)|\chi(1) + (|G| - |\mathbf{C}_G(x)|)\chi(d)). \end{aligned}$$

We obtain b) by simply multiplying by $|K|$.

Suppose now that b) holds. Again by problem 3.12 of [9] we have that for every $h \in G$,

$$\begin{aligned} & \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(x(x^h)^g) = \chi(x)\chi(x^h) = \chi(x)^2 = \\ & \frac{\chi(1)}{|G|} (|\mathbf{C}_G(x)|\chi(1) + (|G| - |\mathbf{C}_G(x)|)\chi(d)). \end{aligned}$$

Thus,

$$\sum_{g \in G} \chi(x(x^h)^g) = |\mathbf{C}_G(x)|\chi(1) + (|G| - |\mathbf{C}_G(x)|)\chi(d). \quad (5.1)$$

Let $h \in G$ and suppose that $xx^h \notin D$. We will prove that $xx^h = 1$. By Eq.(5.1) and taking into account the second orthogonality relation,

$$\begin{aligned} & \sum_{g \in G} \sum_{\chi \in \text{Irr}(G)} \chi(x(x^h)^g) \overline{\chi(d)} = \\ & |\mathbf{C}_G(x)| \sum_{\chi \in \text{Irr}(G)} \chi(1) \overline{\chi(d)} + (|G| - |\mathbf{C}_G(x)|) \sum_{\chi \in \text{Irr}(G)} \chi(d) \overline{\chi(d)} = \\ & (|G| - |\mathbf{C}_G(x)|) |\mathbf{C}_G(d)|. \end{aligned}$$

On the other hand, since $xx^h \notin D$, then

$$\begin{aligned} & \sum_{g \in \mathbf{C}_G(x^h)} \sum_{\chi \in \text{Irr}(G)} \chi(x(x^h)^g) \overline{\chi(d)} + \sum_{g \in G \setminus \mathbf{C}_G(x^h)} \sum_{\chi \in \text{Irr}(G)} \chi(x(x^h)^g) \overline{\chi(d)} = \\ & \sum_{g \in G \setminus \mathbf{C}_G(x^h)} \sum_{\chi \in \text{Irr}(G)} \chi(x(x^h)^g) \overline{\chi(d)}. \end{aligned}$$

Therefore,

$$\sum_{g \in G \setminus \mathbf{C}_G(x^h)} \sum_{\chi \in \text{Irr}(G)} \chi(x(x^h)^g) \overline{\chi(d)} = (|G| - |\mathbf{C}_G(x)|) |\mathbf{C}_G(d)|.$$

Again by using the second orthogonality relation, we deduce that there are exactly $(|G| - |\mathbf{C}_G(x)|)$ elements $g \in G \setminus \mathbf{C}_G(x^h)$ such that

$$\sum_{\chi \in \text{Irr}(G)} \chi(x(x^h)^g) \overline{\chi(d)} = |\mathbf{C}_G(d)|.$$

So, for every $g \in G \setminus \mathbf{C}_G(x^h)$, we have $x(x^h)^g \in D$. Now, if we come back to Eq.(5.1), we have

$$\begin{aligned} & \sum_{g \in \mathbf{C}_G(x^h)} \chi(x(x^h)^g) + \sum_{g \in G \setminus \mathbf{C}_G(x^h)} \chi(x(x^h)^g) = \\ & |\mathbf{C}_G(x)| \chi(1) + (|G| - |\mathbf{C}_G(x)|) \chi(d) \quad \forall \chi \in \text{Irr}(G). \end{aligned}$$

As a result,

$$\begin{aligned} & |\mathbf{C}_G(x^h)| \chi(xx^h) + (|G| - |\mathbf{C}_G(x)|) \chi(d) = \\ & |\mathbf{C}_G(x)| \chi(1) + (|G| - |\mathbf{C}_G(x)|) \chi(d) \quad \forall \chi \in \text{Irr}(G). \end{aligned}$$

This implies that $\chi(xx^h) = \chi(1)$ for every $\chi \in \text{Irr}(G)$, that is, $xx^h = 1$. Therefore, we have proved that for every $h \in G$, either $xx^h = 1$ or $xx^h \in D$, that is, $K^2 \subseteq 1 \cup D$. Since K^2 is a G -invariant set, the only possibilities are $K^2 = D$ or $K^2 = 1 \cup D$. However, if $K^2 = D$, by Lemma 5, we have $\chi(x)^2 = \chi(1)\chi(d)$ and by replacing in the equation of b), we get $|K|\chi(1)\chi(d) = \chi(1)^2 + (|K| - 1)\chi(1)\chi(d)$ for every $\chi \in \text{Irr}(G)$. This forces that $\chi(d) = \chi(1)$ for every $\chi \in \text{Irr}(G)$, so $d = 1$, a contradiction. Then $K^2 = 1 \cup D$, as wanted. \square

Proof of Corollary C. For every non central 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. \square

Proof of Corollary D. It may occur that K^2 is a conjugacy class and then, by applying Theorem 5.2.4, $\langle K \rangle$ is solvable. Otherwise, it happens that either $K^2 = A_1 \cup A_2 \cup \dots \cup A_n$ or $K^2 = A_1 \cup A_2 \cup \dots \cup A_n \cup D$ with A_i a central class for every i and D a non-central class. If we consider $\overline{G} = G/\mathbf{Z}(G)$, 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, so $\langle K \rangle$ is solvable too. \square

Proof of Corollary E. 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 $\mathbf{O}_{\pi'}(G) = 1$. For every $p \in \pi$, we choose $1 \neq x_p \in \mathbf{Z}(P)$ for some $P \in \text{Syl}_p(G)$. The hypotheses imply that $(x_p^G)^2$ is a conjugacy class and, by applying Theorem 5.2.4, $|x_p^G| = |[x_p, G]|$ and hence, $[x_p, G]$ has p' -order.

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 $K_{p'} \subseteq \mathbf{O}_{p'}(G)$. By induction,

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

is nilpotent. Now, we consider the natural homomorphism

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

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

Proof of Corollary F. The hypotheses are inherited by quotients. 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 obtain 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.

We assume first that there exists a $2'$ -element $x \in G \setminus \mathbf{F}(G)$ 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 conclude that $x^2 \in \langle D \rangle \subseteq \mathbf{F}(G)$ and, since $\langle x \rangle = \langle x^2 \rangle$, we get a contradiction.

Therefore, if we consider $\widehat{G} = G/\mathbf{F}(G)$, we can assume that every non-trivial $2'$ -element $\widehat{x} \in \widehat{G}$ satisfies that $(\widehat{x}^{\widehat{G}})^2$ is a conjugacy class of \widehat{G} . Observe that 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 Corollary E with $\pi = \{2\}'$ in order to deduce that $\widehat{G}/\mathbf{O}_2(\widehat{G})$ is nilpotent, which implies that G/M is nilpotent, and the proof is finished. \square

Bibliography

- [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** (1), 7-22 (1987).
- [2] Z. Arad and M. Herzog, *Products of conjugacy classes in groups*, *Lecture Notes in Mathematics*, 1112 (Springer-Verlag, Berlin, 1985).
- [3] Y. Berkovich and L. Kazarin, 'Indices of elements and normal structure of finite groups', *J. Algebra* **283**(2), 564-583 (2005).
- [4] D. Chillag and A. Mann, 'Nearly odd-order and nearly real finite group', *Comm. in Algebra* **26**(7), 2041-2064 (1998).
- [5] GAP Group, *GAP-Groups, Algorithms and Programming*, Vers. 4.7.7 (2015) (<http://www.gap-system.org>)
- [6] G. Glauberman, 'Central elements in core-free groups', *J. Algebra* **4**(3), 403-420 (1966).

-
- [7] R. Guralnick and G. Navarro, ‘Squaring a conjugacy class and cosets of normal subgroups’, *Proc. Am. Math. Soc.* **144**(5), 1939-1945 (2016) .
- [8] B. Huppert, *Character Theory of Finite Groups*, Walter de Gruyter, Berlin. New York, (1998).
- [9] I.M. Isaacs, *Character theory of finite groups*, Academic Press, Inc, New York, (1976).
- [10] G.O. Michler, *Theory of finite simple groups. New Mathematical Monographs, 8* Cambridge University Press, Cambridge, (2006).
- [11] J. Moori, H.P. Tong-Viet, Products of conjugacy classes in simple groups, *Quaest. Math.***34** (4), 433-439 (2011).

Chapter 6

Multiplying a conjugacy class by its inverse in a finite group

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.

6.1 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 $\{ab \mid a \in A, b \in B\}$) 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 Herzog'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 $\text{Irr}(G)$ 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 $\chi \in \text{Irr}(G)$

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

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

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

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 $\chi, \psi \in \text{Irr}(G)$ such that $\chi\bar{\chi} = 1 + \psi$. A possible problem could be to classify the groups of this type satisfying the conjugacy class condition, but we are not attempting that.

6.2 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 6.2.1 (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 6.2.2 (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 6.2.2.

Theorem 6.2.3 (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 6.2.2 is the following.

Theorem 6.2.4. *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 6.2.2, 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 $P \in \text{Syl}_p(G)$ 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 6.2.3.

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. \square

We state a very well-known Burnside's result.

Lemma 6.2.5 (Lemma 15.1 of [11]). *Let $\chi \in \text{Irr}(G)$ 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, \dots, 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,

$$|K|^2 = |K| + 2m|D|. \quad (6.1)$$

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 $\chi \in \text{Irr}(G)$. Taking into account Eq.(6.1) 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

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

and c_k is a representative of C_k . In particular,

$$\widehat{K}\widehat{K}^{-1} = \sum_k \alpha_k \widehat{C}_k \quad \text{with} \quad \alpha_k = \frac{|K|^2}{|G|} \sum_{\chi \in \text{Irr}(G)} \frac{|\chi(x)|^2 \chi(c_k^{-1})}{\chi(1)}. \quad (6.2)$$

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

$$|\chi(x)|^2 = \frac{(|K| - 1)\chi(1)(\chi(d) + \chi(d^{-1})) + 2\chi(1)^2}{2|K|}, \quad (6.3)$$

and by replacing Eq.(6.3) in Eq.(6.2) and making easy calculations, it follows that

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

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

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

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

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

Lemma 6.2.6. *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 $K = \{x_1, \dots, x_n\}$, then $K^{-1}K = x_1^{-1}K \cup \dots \cup x_n^{-1}K$. 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. \square

6.3 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 6.3.1. *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 $KK^{-1} = 1 \cup \{xx^g, x^gx\}$. Notice that $\{xx^g, x^gx\}$ cannot be decomposed into two central classes. In fact, if xx^g and x^gx are central elements, then x and x^g would commute. Therefore, $|K| \geq 3$ and we write $K = \{x_1, \dots, x_n\}$ 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. \square

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 6.2.1, 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 $\psi := \chi - 1 \in \text{Irr}(G)$ 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 $\psi \in \text{Irr}(G)$ 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

$$|K| |\mathbf{C}_G(x)|_p^2 - |G|_p^2 = \frac{|K| - 1}{2} |G|_p (\psi(d) + \psi(d^{-1})). \quad (6.4)$$

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.(6.4) 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 6.2.5 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 6.2.5 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 6.2.4 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. \square

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 $D \neq D^{-1}$.

6.4 Proof of Theorem C

Proof of Theorem C. Let $K = x^G$ with $x \in G$. We write $\widehat{KK^{-1}} = |K|\widehat{1} + m\widehat{D}$, 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 $xK^{-1} \cup x^{-1}K \subseteq KK^{-1}$. 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 $K = \{x_1, \dots, x_n\}$ and $K^{-1}K = x_1^{-1}K \cup \dots \cup x_n^{-1}K$. Notice that $1 \in x_i^{-1}K$ for all $i = 1, \dots, n$. We rewrite the previous equality as the union

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

By counting elements we conclude that $x_i^{-1}K \cap x_j^{-1}K = 1$ for all $i = 1, \dots, n$ 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. \square

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.

6.5 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 $\chi\bar{\chi} = 1 + \psi + \varphi$ (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 $\chi\bar{\chi} = 1_G + m_1\alpha_1 + m_2\alpha_2$ where $\alpha_1, \alpha_2 \in \mathrm{Irr}(G)$ 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 $\alpha_2 = \bar{\alpha}_1 \neq \alpha_1$. 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 $\psi\bar{\psi} = \chi + 1$, 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.

Bibliography

- [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.

Conclusiones y futuros problemas de investigación

Todos los resultados presentados en esta tesis se encuentran publicados en revistas indexadas en el Journal Citation Report (JCR). Todos ellos han supuesto un avance en el campo de investigación sobre clases de conjugación de grupos finitos ya que, o bien son generalizaciones de resultados anteriores, o son contribuciones totalmente novedosas.

Sintetizamos a continuación los resultados más significativos en cuanto a grafos de clases de conjugación contenidas en un subgrupo normal. Sea G un grupo finito y N un subgrupo normal de G . En los Teoremas A, B, C y D de [6] se estudian el número de componentes conexas de los grafos $\Gamma_G(N)$ y $\Gamma_G^*(N)$, que en ambos grafos coincide y es a lo sumo 2, y la cota de sus diámetros, que en el caso conexo es a lo sumo 3 y en el caso desconexo es 1, pues cada componente conexa es un grafo completo. En el Teorema E de [6], se obtiene la estructura de N cuando $\Gamma_G(N)$ es desconexo. Además, en el Teorema 1.1 de [8] se determina la estructura de N cuando el diámetro de $\Gamma_G(N)$ es tan grande como es posible, esto es, 3. En el Teorema A de [9] se obtiene la estructura de N en el caso en que $\Gamma_G(N)$ no tiene triángulos y en los Teoremas B y C de [9] se proporciona la estructura de G cuando $\Gamma(G)$ es exactamente un triángulo y la estructura de N cuando $\Gamma_G(N)$ es exactamente un triángulo, respectivamente. Los resultados que cabe destacar sobre la generalización del Teorema de Landau para clases de conjugación contenidas en un subgrupo normal son los Teoremas A y B de [7]. En el primero se obtienen cotas del orden de G y de N , siendo N un subgrupo normal de G de índice fijo, con un determinado número de G -clases de conjugación no centrales. El segundo es un resultado análogo cuando se fija el número de G -clases de elementos de orden potencia de primo de N .

Resumimos ahora los resultados sobre el producto de clases de conjugación más relevantes. En el Teorema A de [11] se obtiene la resolubilidad del subgrupo generado por una clase de conjugación K cuyo cuadrado es unión de la clase trivial y otra clase D . Cabe destacar que éste es el caso más sencillo que aparece cuando consideramos el cuadrado de una clase real. Además, se proporciona exactamente la estructura de los subgrupos generados por las clases K y D . En el Teorema B de [11] se aporta una caracterización de la anterior propiedad en términos de los caracteres irreducibles del grupo. En el Teorema A de [10] se prueba la no simplicidad de un grupo que posee una clase K tal que al multiplicarla por su inversa, o bien es de la forma $KK^{-1} = 1 \cup D$ donde D es una clase, o bien $KK^{-1} = 1 \cup D \cup D^{-1}$. Estas dos propiedades se caracterizan en el Teorema B de [10] en términos de los caracteres

irreducibles del grupo. Además se conjetura que bajo estas hipótesis $\langle K \rangle$ es resoluble. En el Teorema C de [10] se prueba que si $KK^{-1} = 1 \cup D$, entonces $|D|$ divide a $|K|(|K| - 1)$ y se obtiene la resolubilidad de $\langle K \rangle$ cuando $|D| = |K|$, $|D| = |K| - 1$ o $|D| = |K|(|K| - 1)$. Para el resto de divisores, la resolubilidad queda como problema abierto.

En las temáticas estudiadas en las dos partes que forman esta tesis todavía pueden ser planteados problemas abordables de los que se pueden obtener resultados interesantes. Por una parte, respecto a los grafos $\Gamma_G(N)$ y $\Gamma_G^*(N)$ se pueden investigar cuestiones sobre regularidad, diámetro, completitud o incompletitud de vértices análogas a las planteadas en [14], [18], [21] y [20], respectivamente. En particular, nos planteamos qué ocurre cuando el diámetro de $\Gamma_G^*(N)$ alcanza su valor máximo, es decir, 3.

Respecto al Teorema de Landau, se podrían estudiar más generalizaciones trabajando con G -clases contenidas en un subgrupo normal. Podríamos considerar, por ejemplo, únicamente los elementos p -regulares tal y como se ha hecho para clases ordinarias.

En cuanto al producto de clases de conjugación, cabe destacar que la literatura es escasa y nos proponemos seguir estudiando los casos abiertos que han sido mencionados anteriormente y nos planteamos diversas cuestiones nuevas sobre las que podemos trabajar en este campo. En primer lugar, tal y como se ha visto en la segunda parte de la tesis, la conjetura de Arad y Herzog sigue abierta pues todavía no se ha podido probar para todos los grupos simples de tipo Lie. Además, nos proponemos estudiar el siguiente problema el cual es una variación más débil de la conjetura de Arad y Herzog:

En un grupo simple no abeliano el producto de n clases de conjugación con n un número natural fijo y $n \geq 2$ no es una clase de conjugación.

De la misma manera que la conjetura de Arad y Herzog se prueba para el cuadrado de una clase, estamos estudiando si el anterior problema es cierto para la potencia n -ésima de una clase con un n fijo y si el subgrupo generado por ésta clase es resoluble.

En los Capítulos 5 y 6 hemos probado que si K y D son clases de conjugación de un grupo G tales que $K^2 = 1 \cup D$ o $KK^{-1} = 1 \cup D$, respectivamente, entonces G es no simple. Además en el primer caso se obtiene la resolubilidad de $\langle K \rangle$ y en el segundo, se conjetura dicha resolubilidad y se obtiene en algunos casos particulares. Una cuestión natural es qué ocurre si la potencia de una clase es unión de, o bien la clase trivial y otra clase, o de una clase y su inversa. Estudiaremos los siguientes problemas:

Sea G un grupo finito y sea K una clase de conjugación. Si $K^n = 1 \cup D$ o $K^n = D \cup D^{-1}$ para algún $n \in \mathbb{N}$ y $n \geq 2$, y alguna clase de conjugación D , entonces $\langle K \rangle$ es resoluble. En particular, G no es un grupo simple no abeliano

En los problema anteriores, se pueden obtener caracterizaciones en términos de

caracteres que pueden ser utilizadas a la hora de obtener la no simplicidad del grupo.

Por otra parte nos preguntamos de qué manera se pueden aunar los dos temas abarcados en esta tesis. Esto se traduciría, por ejemplo, en estudiar la información sobre la estructura normal de un grupo obtenida a partir del producto de G -clases contenidas en un normal. Si suponemos, por ejemplo, que una G -clase de conjugación contenida en un subgrupo normal N satisface que alguna de sus potencias vuelve a ser clase, sabemos que el subgrupo generado por dicha clase es resoluble. Este subgrupo está contenido en N , por lo que concluimos que N no es simple. Sin embargo, podría ocurrir que ninguna potencia de N -clase volviera a ser clase. Con esto concluimos que tendría sentido estudiar los problemas de productos de clases tratados en la segunda parte de la tesis para el caso de G -clases contenidas en un subgrupo normal con el objetivo de analizar su estructura como hicimos en la primera parte de la tesis.

Conclusions and future research problems

All the results presented in this thesis are published in indexed journals in the Journal Citation Report (JCR). All of them have led an advance in the research line about conjugacy classes of finite groups because, either they are generalizations of previous results, or they are totally new contributions.

Now we synthesize the most significant results about graphs of conjugacy classes contained in a normal subgroup. Let G be a finite group and N a normal subgroup of G . In Theorems A, B, C and D of [6] we study the number of connected components of the graphs $\Gamma_G(N)$ and $\Gamma_G^*(N)$, that in both graphs is the same and it is at most 2, and the bound of their diameters, that in the connected case it is at most 3 and in the disconnected case it is 1, because each connected component is a complete graph. In Theorem E of [6], we obtain the structure of N when $\Gamma_G(N)$ is disconnected. Furthermore, in Teorema 1.1 of [8] we determine the structure of N when the diameter of $\Gamma_G(N)$ is as large as possible, that is, 3. In Theorem A of [9] we obtain the structure of N in the case in which $\Gamma_G(N)$ has no triangles and in Theorems B and C of [9] we provide the structure of G when $\Gamma(G)$ is exactly a triangle and the structure of N when $\Gamma_G(N)$ is exactly a triangle, respectively. The results that are worth stressing about the generalization of Landau's theorem for conjugacy classes contained in a normal subgroup are Theorem A and B of [7]. In the first, we obtain the bounds of the order of G and N , being N a normal subgroup of G of fixed index, with a determined number of non-central conjugacy G -classes. The second is an analogue when we fix the number of G -classes of elements of prime power order of N .

Now we summarise the most relevant results about the product of conjugacy classes. In Theorem A of [11] we obtain the solvability of the subgroups generated by a conjugacy class K such that its square is a union of the trivial class and another class D . It is worth stressing that this is the simplest case that appears when we consider the square of a real class. Furthermore, we provide exactly the structure of the subgroups generated by the classes K and D . In Theorem B of [11] we address a characterization of the previous property in terms of the irreducible characters of the group. In Theorem A of [10] we prove the non-simplicity of a group having a class K such that when we multiply it by its inverse, either it is of the form $KK^{-1} = 1 \cup D$, where D is a class, or $KK^{-1} = 1 \cup D \cup D^{-1}$. These two properties are characterized in Theorem B of [10] in terms of the irreducible characters of the group. Furthermore, we conjecture that, under these hypotheses, $\langle K \rangle$ is solvable. In Theorem C of [10] we prove that if $KK^{-1} = 1 \cup D$, then $|D|$ divides $|K|(|K| - 1)$ and we obtain

the solvability of $\langle K \rangle$ when $|D| = |K|$, $|D| = |K| - 1$ or $|D| = |K|(|K| - 1)$. To the rest of divisors, the solvability remains an open problem.

In the topics studied in both parts of the thesis it still can be raised tackled problems from which interesting results can be obtained. On the one hand, regarding the graphs $\Gamma_G(N)$ and $\Gamma_G^*(N)$ we can investigate questions about regularity, diameter, completeness and incompleteness of vertices analogue to those that have been raised in [14], [18], [21] and [20], respectively. In particular, we raise what happens when the diameter of $\Gamma_G^*(N)$ get the maximum value, that is, 3.

With regard to the product of conjugacy classes, we have to say that literature is scarce and we propose ourselves to continue studding the open cases mentioned before and we raise several new questions about we can work on in this topic. In the first place, as it have been seen in the second part of the thesis, Arad and Herzog's conjecture remains open because it has not yet been tested for all the simple groups of Lie type. Furthermore, we propose ourselves to study the following problem, which is a weaker variation of Arad and Herzog's conjecture:

In a non-abelian simple group the product of n conjugacy classes with n a fixed natural number and $n \geq 2$ is not a conjugacy class.

In the same way that Arad and Herzog's conjecture is proved for the square of a class, we are studding if the above problem is true for the n th power with n fixed and if the subgroup generated by this class is solvable.

In Chapters 5 and 6 we have proved that if K and D are conjugacy classes of a group G such that $K^2 = 1 \cup D$ or $KK^{-1} = 1 \cup D$, respectively, then G is not simple. Furthermore, in the first case we obtain the solvability of $\langle K \rangle$ and in the second, we conjecture this solvability and we obtain it in some particular cases. A natural question is what happens if the power of a class is a union of, either the trivial class and another class, or of a class and its inverse. We will study the following problems:

Let G be a finite group and let K be a conjugacy class. If $K^n = 1 \cup D$ or $K^n = D \cup D^{-1}$ for some $n \in \mathbb{N}$ and $n \geq 2$, and some conjugacy class D , then $\langle K \rangle$ is solvable. In particular, G is not a non-abelian simple group.

In the above problems, we can obtain characterizations in terms of characters that can be used to study the non-simplicity of the group.

On the other hand we wonder how we can join the two topics tackled in this thesis. This would be, for instance, to study the information about the normal structure of a group obtained when considering the product of G -classes contained in a normal. If we suppose, for example, that a G -conjugacy class contained in a normal subgroup N satisfies that some of its powers is again a class, we know that the subgroup generated by such class is solvable. This subgroup is contained in N , so we conclude that N is not simple. However, it could happen that there is no power of N -class being again a class. According to this, we conclude that it made sense to study the problems about product of classes tackled in the second part of the

thesis for the case of G -classes contained in a normal subgroup in order to analyse its structure as we made in the first part of the thesis.

References of the Introduction and Conclusion

- [1] E. Adan-Bante, Conjugacy classes and finite p -groups. *Arch. Math. (Basel)*. **85**(4) (2005), 297-303.
- [2] E. Adan-Bante, Derived length and products of conjugacy classes. *Israel J. Math.* **168** (2008), 93-100.
- [3] Z. Akhlaghi, C. Casolo, S. Dolfi, K. Khedri, E. Pacifici, On the character degree graph of solvable groups. *Proc. Amer. Math. Soc.* **146**(4) (2018), 1505-1513.
- [4] Z. Arad and E. Fisman, An analogy between products of two conjugacy classes and products of two irreducible characters in finite groups. *Proc. Edinburgh Math. Soc.* **30** (1987), 7-22.
- [5] Z. Arad and M. Herzog, *Products of conjugacy classes in groups*, Lecture Notes in Mathematics, 1112, Springer-Verlag, Berlin, (1985).
- [6] A. Beltrán, M.J. Felipe and C. Melchor, Graphs associated to conjugacy classes of normal subgroups in finite groups. *J. Algebra.* **443** (2015), 335-348.
- [7] A. Beltrán, M.J. Felipe and C. Melchor, Landau's Theorem on conjugacy classes for normal subgroups. *Internat. J. Algebra Comput.* **26**(7) (2016), 1453-1466.
- [8] A. Beltrán, M.J. Felipe and C. Melchor, Normal subgroups whose conjugacy class graph has diameter three. *Bull. Aust. Math. Soc.* **94** (2016), 266-272.
- [9] A. Beltrán, M.J. Felipe and C. Melchor, Triangles in the graph of conjugacy classes of normal subgroups. *Monatshefte für Mathematik.* **182**(1) (2017), 5-21.
- [10] A. Beltrán, M.J. Felipe and C. Melchor, Multiplying a conjugacy class by its inverse in a finite group. Accepted in *Israel J. Math.*
- [11] A. Beltrán, M.J. Felipe and C. Melchor, Squares of real conjugacy classes in finite groups, *Ann. Mat. Pura Appl.* **197**(2) (2018), 317-328.
- [12] Y. Berkovich and L. Kazarin, Indices of elements and normal structure of finite groups, *J. Algebra.* **283**(2), 564-583 (2005).
- [13] E.A. Bertram, M. Herzog and A. Mann, On a graph related to conjugacy classes of groups. *Bull. London Math. Soc.* **22**(6) (1990), 569-575.
- [14] M. Bianchi, R. D. Camina, M. Herzog, E. Pacifici, Conjugacy classes of finite groups and graph regularity. *Forum Math.* **27**(6) (2015), 3167-3172.
- [15] A. R. Camina, R. D. Camina, The influence of conjugacy class sizes on the structure of finite groups: a survey. *Asian-Eur. J. Math.* **4**(4) (2011), 559-588.

-
- [16] M. Cartwright. A bound on the number of conjugacy classes of a finite soluble group. *J. London Math. Soc.* (2) (1987), 229-244.
- [17] M. Cartwright. The number of conjugacy classes of certain finite groups. *Quart. J. Math. Oxford Ser.* **36**(144) (1985), 393-404.
- [18] C. Casolo and S. Dolfi, The diameter of a conjugacy class graph of finite groups. *Bull. London Math. Soc.* **28** (1996), 141-148.
- [19] C. Casolo, S. Dolfi, E. Pacifici, L. Sanus, Groups whose character degree graph has diameter three. *Israel J. Math.* **215**(2) (2016), 523-558.
- [20] C. Casolo, S. Dolfi, E. Pacifici, L. Sanus, Groups whose prime graph on conjugacy class sizes has few complete vertices. *J. Algebra.* **364** (2012), 1-12.
- [21] C. Casolo, S. Dolfi, E. Pacifici, L. Sanus, Incomplete vertices in the prime graph on conjugacy class sizes of finite groups. *J. Algebra* **376** (2013), 46-57.
- [22] D. Chillag, M. Herzog and A. Mann, On the diameter of a graph related to conjugacy classes of groups. *Bull. London Math. Soc.* **25** (1993), 255-262.
- [23] S. Dolfi, Arithmetical conditions of the length of the conjugacy classes in finite groups. *J. Algebra.* **174**(3) (1995), 753-771.
- [24] M. Fang and P. Zhang, Finite groups with graphs containing no triangles. *J. Algebra.* **264**(2) (2003), 613-619.
- [25] GAP Group, *GAP-Groups, Algorithms and Programming, Vers. 4.7.7* (2015). <http://www.gap-system.org>
- [26] G. Glauberman, Central elements in core-free groups, *J. Algebra.* **4**(3), 403-420 (1966).
- [27] R. Guralnick, G. Malle and Pham Huu Tiep, Products of conjugacy classes in finite and algebraic simple groups, *Adv. Math.* **234** (2013), 618-652.
- [28] R. Guralnick and G. Navarro, Squaring a conjugacy class and cosets of normal subgroups. *Proc. Am. Math. Soc.* **144**(5) (2016), 1939-1945.
- [29] L. Héthelyi and B. Külshammer. Elements of prime-power order and their conjugacy classes in finite groups. *J. Aust. Math. Soc.* **78** (2005), 291-295.
- [30] L.S. Kazarin, On groups with isolated conjugacy classes, *Izv. Vyssh. Uchebn. Zaved. Mat.* (7) (1981), 40-45.
- [31] E. Landau, Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante. *Math Ann.* **56** (1903), 671-676.
- [32] M. L. Lewis, An overview of graphs associated with character degrees and conjugacy class sizes in finite groups. *Rocky Mountain J. Math.* **38**(1) (2008), 175-211.
- [33] J. Moori and H.P. Tong-Viet, Products of conjugacy classes in simple groups, *Quaest. Math.* **34**(4) (2011), 433-439.
- [34] A. Moretó, H.N. Nguyen, Variations of Landau's theorem for p -regular and p -singular conjugacy classes. *Israel J. Math.* **212**(2) (2016), 961-987.
- [35] M. Newman, A bound for the number of conjugacy classes in a group. *J. London Math. Soc.* **43** (1968), 108-110.