Relaciones entre la estructura de grupos finitos y sus clases de conjugación

TESIS DE MÁSTER
Máster en Investigación Matemática
Departamento de Matemática Aplicada

PRESENTADA POR:
Elena Alemany Martínez

DIRIGIDA POR:
Antonio Beltrán Felip
María José Felipe Román

Valencia, septiembre de 2010

D. Antonio Beltrán Felip, profesor titular de universidad del Departamento de Matemáticas de la Universidad Jaume I de Castellón.

y María José Felipe Román, profesora titular de universidad del Departamento de Matemática Aplicada de la Universidad Politécnica de Valencia.

CERTIFICAN:

Que la presente Memoria, titulada "Relaciones entre las estructuras de grupos finitos y sus clases de conjugación", ha sido realizada bajo su dirección por D$^{\text{ña}}$ Elena Alemany Martínez para optar al título de Máster en Investigación Matemática.

Lo que se hace constar en cumplimiento de la legislación vigente.

Valencia, 14 de septiembre de 2010

Fdo. Antonio Beltrán Felip

Fdo. María José Felipe Román

Quiero agradecer ante todo a mis directores de tesis, María José Felipe y Antonio Beltrán, el apoyo incondicional que me han mostrado durante estos últimos años, introduciéndome y formándome en un área de investigación básicamente nueva para mí. Antonio y María José han sabido encontrar en sus agendas el tiempo y la dedicación que esta tarea requiere. Su constante motivación ha hecho posible que hoy escriba esta memoria.

También quiero agradecer a Ana Martínez Pastor, del Instituto Universitario de Matemática Pura y Aplicada de la Universidad Politécnica de Valencia, el haberme considerado en todo momento un miembro más de su grupo de investigación.

Finalmente mi especial agradecimiento a Quique, mi compañero de viaje, por haber estado a mi lado en todo momento, ayudándome tanto a nivel personal como profesional.

Índice general

Introducción

En esta memoria de investigación se culminan varios años de estudio y preparación en tercer ciclo, encaminados a la obtención de mi DEA y parte de mi futura tesis doctoral, enmarcada dentro de la teoría general de grupos finitos y, concretamente, en el estudio de la estructura de los grupos a partir de los tamaños de clase de conjugación.

Consideramos al lector familiarizado con los conceptos y resultados básicos de la teoría general de grupos. La memoria consta de tres capítulos. En el capítulo 1 se va a realizar un "survey" sobre la relación entre las estructuras de los grupos finitos y sus clases de conjugación. A continuación, en el capítulo 2 se presenta una recopilación de resultados preliminares necesarios para el seguimiento del resultado principal de esta memoria que se desarrolla en el capítulo 3. La memoria concluye con una última sección en la que se recoge la bibliografía utilizada.

La teoría de Grupos surge como respuesta a problemas en tres áreas distintas de las matemáticas: la teoría de números, la teoría de ecuaciones algebraicas y el desarrollo de las nuevas geometrías que tuvo lugar a principios del siglo XIX. Las investigaciones realizadas por J.L. Lagrange (1736-1813), A.L. Cauchy (1789-1857) y P. Ruffini (1765-1822) dentro de la teoría de ecuaciones algebraicas propiciaron el estudio y análisis de las permutaciones. Posteriormente las investigaciones relativas al problema del criterio general de la resolubilidad en radicales de ecuaciones algebraicas, llevados a cabo por N.G. Abel (1802-1829) y finalmente resuelto por Evaristo Galois (1811-1832), dieron origen en el Álgebra a una serie de conceptos generales abstractos, entre los cuales el primer lugar pertenece al concepto de grupo.

La resolución de ecuaciones algebraicas fue el problema para el que Galois desarrolló la teoría de grupos. Galois probó que no existe ningún método de resolución de ecuaciones basado en las operaciones de adición, sustracción, multiplicación, división y extracción de raíces para ecuaciones de grado $n \geq 5$. Definió para cada ecuación de grado n un grupo, actualmente conocido como grupo de Galois de la ecuación, y demostró que sólamente serán resolubles por métodos aritméticos y de extracción de raíces aquellas ecuaciones cuyo grupo sea resoluble, es decir, grupos

con series normales cuyos factores son cíclicos.

La importancia y necesidad del concepto de grupo era ya evidente para muchos matemáticos a comienzos del siglo XIX. Desde el año 1815, Cauchy llevó a cabo una serie de investigaciones sobre la teoría de grupos finitos demostrando en particular el teorema de que cada grupo cuyo orden es divisible por un número primo p contiene al menos un subgrupo de orden p. Hacia finales del siglo se formalizó la teoría de grupos finitos, alcanzando un alto nivel de desarrollo. Los trabajos de Jordan, Hölder, Cayley, Frobenius, Netto y Von Dyck, entre otros, afianzaron los pilares en dicha teoría. El libro **Theory of groups of finite order**, publicado por W. Burnside en 1897, y los dos volúmenes **Lehrbüch der Algebra** escritos por H. Weber en 1895, influyeron considerablemente en la formación de nuevos algebristas en la teoría de grupos. En esta misma época aparecieron las primeras aplicaciones de la teoría. En los años 1890-1891, el cristalógrafo y geómetra ruso E.S. Fiódorov y el matemático aleman A. Schoenflies, independientemente uno del otro, resolvieron con los métodos de la teoría de grupos, el problema de la clasificación de todas las redes cristalinas espaciales. Establecieron la existencia de 230 grupos de simetría espacial.

Los grupos discretos finitos obtuvieron extensión en la teoría de los espacios multidimensionales en relación con la teoría de los poliedros regulares. En la confluencia de los siglos XIX y XX, la teoría de grupos obtuvo aplicación en la teoría de las integrales algebraicas de las ecuaciones diferenciales lineales, las superficies de Riemann y otras. Así, por ejemplo, Jordan indicó la relación entre las ecuaciones diferenciales lineales que tienen integrales algebraicas y los grupos finitos.

Hacia finales del siglo XIX, la teoría de grupos finitos se desarrolló en tal grado que para ella adquirió actualidad el problema de la clasificación de los grupos simples. Este problema tuvo que esperar hasta finales del siglo XX para ser resuelto. Se plantean nuevos problemas sobre la estructura y propiedades de los grupos, como es el caso de la resolubilidad de los grupos de orden impar, problema que fue resuelto en el año 1963 por W. Feit y J.G. Thompson en un artículo de gran dificultad que ocupó un total de 254 páginas.

Se inicia entonces una época de desarrollo en las investigaciones de los grupos infinitos tanto continuos como discretos. Los logros fundamentales en esta área pertenecen a los discípulos de C.Jordan, F. Klein y S. Lie, los cuales emprendieron el estudio sistemático de la teoría de grupos y sus posibles generalizaciones y aplicaciones. Una aplicación importante de la teoría de grupos continuos fue realizada por F.Klein alrededor del año 1872, el cual llega a concebir que cualquier geometría (euclideana, afín, proyectiva, ...) tiene en su base cierto grupo continuo de transformaciones y es en esencia el estudio de los invariantes de este grupo.

El matemático noruego Sophus Lie extendió los métodos de la teoría de grupos al problema de la integración de ecuaciones diferenciales. Introdujo alrededor del año 1873 un nuevo tipo de grupo que él denominó *grupo continuo de transformaciones*, asociado a las transformaciones que dejan invariante cada ecuación. Estos grupos recibieron posteriormente el nombre de grupos de Lie. La estructura de los grupos de Lie resultó estar relacionada con el problema de la integrabilidad de ecuaciones diferenciales en cuadraturas.

La teoría de representaciones fue desarrollada por G. Frobenius durante las dos últimas décadas del siglo XIX. Posteriormente, W. Burnside y G. Frobenius hicieron que esta teoría jugara un papel importante dentro de la teoría abstracta de grupos finitos. El primer libro que relacionó ambas teorías aparece en 1911, escrito por W. Burnside usando los caracteres del grupo. Quizás el más famoso de los resultados expuestos es el teorema $p^a q^b$ de Burnside que afirma que un grupo cuyo orden es un $\{p, q\}$-número, para dos primos p y q, es resoluble. Recientemente, este teorema ha sido probado utilizando únicamente teoría de grupos por J.G. Thompson, pero esta última demostración no supera en facilidad la demostración original que utiliza la teoría de caracteres.

A principios del siglo XX la teoría de grupos se ramificó desmesuradamente, dando lugar a toda una serie de teorías altamente desarrolladas: los grupos finitos, los grupos discretos infinitos, los grupos continuos, entre ellos los grupos de Lie, ... Los métodos teóricos de grupos penetraron en otras disciplinas matemáticas y en sus aplicaciones. Los descubrimientos de Broglie, Schrödinger, Dirac y otros, en la mecánica cuántica y en la teoría de la estructura de la materia, mostraron que la física moderna debe apoyarse en la teoría de grupos, particularmente de grupos continuos, en la teoría de representaciones de grupos por operadores lineales y en la teoría de caracteres. Desde el punto de vista de las aplicaciones, esta teoría presenta un especial interés para la geometría diferencial, para la teoría de las ecuaciones diferenciales, la mecánica teórica y la teoría general de la relatividad. En la actualidad, se han obtenido nuevas aplicaciones de la teoría de grupos dentro del campo de la informática y de la computación. Este es el caso de la teoría de códigos, cuyas posibilidades futuras están todavía por descubrir.

Ante este panorama científico, las líneas de investigación actuales dentro de la teoría de grupos se caracterizan por su diversidad: grupos de permutaciones, teoría de representaciones, teoría de caracteres, estructura y clasificación de grupos finitos e infinitos, métodos probabilísticos en teoría de grupos, semigrupos, subgrupos especiales (Frattini, Fitting, ...) y sus generalizaciones a grupos infinitos, producto de subgrupos, subgrupos subnormales, π-estructura para un conjunto de primos π,

grupos resolubles, teoría de formaciones, clases de Schunck, clases de Fitting, grupos simples, aplicaciones al álgebra computacional, ...

Dentro de la teoría de grupos finitos, el estudio de propiedades sobre la estructura de un grupo a partir de sus clases de conjugación es un campo clásico. Durante la década de los 90 resurgió el interés por el estudio de ciertas propiedades aritméticas de las clases de conjugación y su influencia en la estructura del grupo. Lejos de ser un tema cerrado, en las dos últimas décadas se han obtenido nuevos e interesantes resultados como comentaremos en los dos capítulos siguientes. Recientemente, nuevas lineas de investigación se están abriendo para dar cabida al estudio de las clases de conjugación para determinados elementos del grupo. Es el caso de elementos reales, elementos racionales, elementos de orden potencia de primo y elementos p-regulares, por citar algunos de ellos. Concretamente, el estudio sobre la influencia de los tamaños de clases de conjugación de elementos p-regulares sobre la p-estructura del grupo, contexto en el que se desarrolla la presente memoria, es un tema poco investigado que está aportando interesantes resultados.

Nuestro principal interés es determinar qué información puede obtenerse sobre la estructura del grupo a partir de los tamaños de clase de conjugación de todos o parte de sus elementos, cuando dichos tamaños satisfacen determinadas condiciones. En 1953, N. Itô demostró ([31]) que si G es un grupo finito con todas las clases de conjugación de elementos no centrales del mismo tamaño, entonces $G = P \times A$, donde P es un p-subgrupo de Sylow de G, para algún primo p, y $A \subseteq \mathbf{Z}(G)$. En [3], A. Beltrán y M.J. Felipe obtienen una generalización de este teorema para tamaños de clase de conjugación de elementos p-regulares, para un cierto primo p, bajo la hipótesis de que el grupo G es p-resoluble. En 1974, A.R. Camina probó en [17] que si G es un grupo finito con todas las clases de conjugación de elementos p-regulares no centrales del mismo tamaño y $|G/\mathbf{Z}(G)|$ es divisible al menos por dos primos distintos de p, entonces G es resoluble. En su trabajo Camina utiliza la clasificación de D. Gorenstein y J.H. Walter ([27]), sobre los grupos cuyos 2-subgrupos de Sylow son diédricos, resultado profundo que se utilizaría posteriormente en la clasificación de grupos simples. En [1], E. Alemany, A. Beltrán y M.J. Felipe obtenemos una demostración alternativa más simple del resultado de A.R. Camina y, por tanto, probamos que la condición de p-resolubilidad del grupo, en la hipótesis del teorema principal de [3], no es realmente necesaria.

En el capítulo 3 de esta memoria se presenta un resultado conjunto de los trabajos realizados en [3] y [1].

A lo largo de toda la memoria consideraremos que los grupos con los que se trabaja son finitos.

Capítulo 1

Clases de conjugación en un grupo finito

1.1. Clases de conjugación ordinarias

Sea G un grupo finito. Denotaremos por $x^G = \{g^{-1}xg : g \in G\}$ a la clase de conjugación de un elemento x de G. El cardinal de la clase de conjugación de x,

$$|x^G| = |G : C_G(x)|$$

se denomina tamaño de clase o índice de x en G. Denotaremos por

$$cs(G) = \{|x^G| : x \in G\}$$

al conjunto de tamaños de clases de conjugación de elementos de G.

Con el fin de obtener un mayor conocimiento sobre la estructura de los grupos, algunos autores se han interesado por determinar qué información puede extraerse de los tamaños de clase de conjugación de todos o parte de los elementos del grupo, cuando estos tamaños de clases verifican determinadas condiciones.

Así por ejemplo, varios autores han estudiado la estructura de un grupo cuando todos o parte de sus elementos tienen tamaño de clase potencia de primo. Los primeros resultados son los de Sylow ([47]) y W. Burnside ([15]). Sylow demuestra que un grupo cuyos índices son todos potencia de un primo dado tiene centro no trivial, y W. Burnside demuestra que si G tiene un elemento x con tamaño de clase de conjugación potencia de un primo, entonces es no simple. Posteriormente en 1990, S.L. Kazarin ([34]) obtiene una extensión de este resultado demostrando que en tales circunstancias el grupo generado por el elemento x, $\langle x^G \rangle$, es subgrupo normal resoluble de G. Utilizando este resultado, A.R. Camina y R.D. Camina ([18])

muestran que cualquier elemento con índice potencia de primo está en el segundo Fitting. A.R. Camina también prueba en [16], que si G es un grupo finito y p^a es la mayor potencia del primo p que divide a un tamaño de clase en G, entonces, si existe un p-elemento en G con índice p^a, el grupo posee p-complemento normal.

La información que podemos obtener sobre la estructura del grupo depende de lo que se conoce sobre los tamaños de clase. Así por ejemplo, sabemos que G es abeliano si y sólo si G tiene un único tamaño de clase, es decir $cs(G) = \{1\}$, pero no sabemos de qué grupo abeliano se trata. ¿Qué información se conoce cuando el grupo tiene dos tamaños de clase?

N. Itô demostró en 1953 ([31]) que si $cs(G) = \{1, m\}$, entonces $m = p^a$ para algún primo p y G es nilpotente. En particular, $G = P \times A$ con P un p-subgrupo de Sylow de G y A un p'-grupo abeliano, y además P tiene un subgrupo normal abeliano H tal que P/H tiene exponente p. Este resultado, que permite enfocar el estudio de la estructura de los grupos con dos tamaños de clase de conjugación a través del conocimiento de los p-grupos, motivó la obtención y aplicación de algunos resultados importantes como los que se mencionan a continuación.

En 1951 Knoche demostró ([36]) que G es un p-grupo con tamaños de clase 1 y p si y sólo si el orden del grupo derivado es p, mientras que en 1953 Itô prueba que si los tamaños de clase de un p-grupo son 1 y 2^a el grupo es metabeliano. En 1970 Isaacs demostró que si los tamaños de clase del p-grupo son 1 y p^a entonces el grupo cociente $G/\mathbf{Z}(G)$ tiene exponente p, y en el año 2002, Ishikawa demuestra ([30]) que para estos grupos la clase de nilpotencia del grupo es menor o igual que 3 y el grupo derivado es elemental abeliano.

En cuanto al estudio de los grupos con dos tamaños de clase de conjugación, podemos citar el resultado de E. Fisman y Z. Arad ([2]) del año 1987, que prueban que si G tiene dos tamaños de clase coprimos, entonces es no simple. Cabe mencionar que en su demostración utilizan la Clasificación de Grupos Simples. Asímismo, en 1996, S. Li ([37]) obtiene una extensión del citado teorema de Itô ([31]) que dice que si G es un grupo finito, x un elemento de G y m un número natural, asumiendo que siempre que x tiene orden potencia de primo entonces x tiene índice 1 ó m, se verifica que G es resoluble.

El estudio de la estructura de los grupos finitos con tres tamaños de clase de conjugación tiene su principal resultado en un teorema de Itô de 1970 ([32]) que dice que si $cs(G) = \{1, m, n\}$, entonces G es resoluble. En su demostración, N. Itô utiliza el Teorema de Feit-Thompson y algunos resultados profundos de la Clasificación de Grupos Simples de M. Suzuki. Poco después, en 1971, J.Rebmann ([44]) simplifica

este resultado para el caso de F-grupos, determinando la estrutura de este tipo de grupos. Recordemos que un grupo G verifica la propiedad F, ó es F-grupo, si para cualquier par de elementos no centrales x, y de G se verifica que $C_G(x) \not\leq C_G(y)$. Por su parte, S.L. Kazarin prueba en 1981 ([35]) que si $cs(G) = \{1, m, n\}$, donde m y n son enteros coprimos, entonces $G/\mathbf{Z}(G)$ es grupo Frobenius.

En 1971, A. R. Camina ([17]) utiliza la descripción de los grupos finitos con 2-subgrupos de Sylow diédricos, dada por D. Gorenstein y J.H. Walter, para demostrar que si G es un grupo con tres tamaños de clase que no es F-grupo, entonces es producto directo de un grupo abeliano por un $\{p, q\}$-grupo. Recientemente, S. Dolfi y E. Jabara, mejoran el anterior resultado, caracterizando los grupos con tres tamaños de clase utilizando el resultado de resolubilidad debido a N. Itô. ([23]). Por otro lado, usando técnicas más elementales, se analiza en [16] la estructura de los grupos con $cs(G) = \{1, p^a, p^a q^b\}$. Este resultado ha sido generalizado por A. Beltrán y M.J. Felipe en ([11]) probando que si G es un grupo finito tal que $cs(G) = \{1, m, mn\}$, con m y n dos enteros coprimos, entonces $G = G_0 \times L$, con L abeliano, y se verifica que

1. $m = p$, para algún primo p.
2. $M = \{x \in G : |x^G| = 1 \text{ ó } m\}$ es subgrupo normal de G_0 y $|G_0 : M| = p$.
3. $M = H \times P_0$ es abeliano, siendo H un p-complemento de G_0.
4. Si P es un p-subgrupo de Sylow de G, entonces P/P_0 actúa libre de puntos fijos sobre $H/\mathbf{Z}(G_0)_{p'}$ y $|H/\mathbf{Z}(G_0)_{p'}| = n$.
5. p divide a $n - 1$.

El estudio de los grupos con cuatro tamaños de clase de conjugación nos lleva al año 1970, año en que N. Itô ([32]) demuestra que los únicos grupos simples con $|cs(G)| = 4$ son los grupos $SL(2, 2^m)$, con $m \geq 2$. Poco después, en 1972, A. R. Camina ([16]) prueba que si $cs(G) = \{1, p^a, q^b, p^a q^b\}$, entonces G es nilpotente.

En el año 2006, A. Beltrán y M.J. Felipe ([6], [7]) extienden el resultado de A.R. Camina a grupos G con $cs(G) = \{1, m, n, mn\}$, y m y n coprimos, probando que para estos grupos $n = p^a$ y $m = q^b$, con p y q primos distintos, y G nilpotente. Resultado que generalizaron poco después en el año 2008 ([10]), al caso de un grupo resoluble G con $cs(G) = \{1, m, n, mk\}$, m y n coprimos y k un divisor estricto de n, concluyendo que si $\pi = \pi(m)$, entonces $k = q^a$ para un primo q, G posee un π-subgrupo de Hall abeliano y los π-complementos de G son de la forma QA, siendo Q un q-subgrupo de Sylow de G y A abeliano. Más recientemente, A. Beltrán y M.J.

Felipe han clasificado los grupos con cuatro tamaños de clase tales que dos de ellos son coprimos (ver [12]). Por otro lado, A.R. Camina y R.D. Camina prueban en [19] que cuando un grupo tiene más de tres tamaños de clase y dos de ellos son coprimos con un tercero, entonces el grupo tiene como máximo cuatro tamaños y es resoluble (en la demostración utilizan la Clasificación de Grupos Simples).

Considerando aquellos primos que dividen el orden del grupo y no dividen a ningún tamaño de clase en G, obtenemos resultados como el de D. Chillag y M. Herzog ([20]) de 1990. Estos autores demuestran que si ningún elemento de $cs(G)$ es divisible por 4, entonces G es resoluble. Por su parte A.R. Camina obtiene como corolario del resultado principal obtenido en ([16], 1972) que G tiene un p-subgrupo de Sylow central si y sólo si el primo p divide a $|G|$ y no divide a ningún elemento de $cs(G)$.

Un grupo se dice que es superresoluble si tiene una serie normal cuyos factores son todos cíclicos. Algunos autores han estudiado los grupos cuyos tamaños de clase son todos libres de cuadrados. Por ejemplo, J. Cossey y Y. Wang demuestran ([22]) que estos grupos son superresolubles y que ambos, $G/F(G)$ y G' son grupos cíclicos de orden libre de cuadrados. Además concluyen que la clase de nilpotencia $F(G)$ es como mucho 2 y que G es metabeliano. Utilizando los resultados en [26], S. Li refuerza este resultado demostrando ([38]) que si p es el primo más pequeño que divide el orden del grupo G, y asumiendo que p^2 no divide el tamaño de clase de ningún elemento de orden potencia de q, para un primo $q \neq p$, entonces G es p-nilpotente y, en particular, resoluble.

Como se ha comentado en la introducción, nuevas líneas de investigación aparecen en el estudio de las clases de conjugación de elementos reales y, en particular, de elementos racionales. En 1979, en [33], S. Iwasaki caracteriza los grupos que tienen exactamente dos clases de conjugación reales. Por otro lado, D. Chillag y A. Mann, [21], caracterizan aquellos grupos tales que todo elemento racional es central. Este resultado ha sido posteriormente generalizado por G. Navarro y L. Sanus en [40] para clases racionales. Recientemente, S. Dolfi, E. Pacifici y L. Sanus determinan en [24] la estructura de los grupos que tienen todas las clases reales no centrales de tamaño un primo, probando que el grupo es resoluble (citeDol3).

1.2. Clases de conjugación de elementos p-regulares

A continuación vamos a citar algunos resultados sobre la estructura de un grupo cuando los tamaños de clase de conjugación de sus elementos p-regulares verifican

determinadas condiciones aritméticas. Estos resultados, que extienden o generalizan propiedades conocidas en el caso ordinario al caso p-regular, no son siempre directas y ello se debe, principalmente, al hecho de que los tamaños de clase en un p-complemento no necesariamente dividen a los tamaños de clase en el grupo. Por otro lado, en las demostraciones de algunos de estos resultados para clases p-regulares se introducen métodos nuevos que dan lugar a demostraciones más sencillas que sus análogas para el caso ordinario. Si además, el grupo no es p-resoluble, las extensiones o generalizaciones se complican, al no poder garantizarse la existencia de p-complementos.

Denotaremos por $G_{p'}$ al conjunto de elementos p-regulares de G,

$$G_{p'} = \{g \in G \,|\, p \text{ no divide } o(g)\}$$

y por $cs_{p'}(G)$ al conjunto de tamaños de clase de conjugación de elementos p'-regulares de G

$$cs_{p'}(G) = \{|x^G| : x \in G_{p'}\}$$

El interés por estudio de los tamaños de clases de conjugación de los elementos p-regulares y su influencia en la p-estructura del grupo es reciente. Durante los años 90 aparecen algunos resultados, entre los que podemos citar el trabajo de Y.C. Ren ([43]) o los trabajos de Y.Ninomiya ([41],[42]). Ren determina la estructura de los grupos con valores de $rc_q(G)$ pequeños, siendo q el menor primo que divide a $|G|$ y $rc_q(G)$ la mayor potencia de q que divide a los cardinales de las clases p-regulares de G.

En 1972, A. Camina demuestra que ([16]) si G es un grupo y p un primo tal que todo tamaño de clase de conjugación en $G_{p'}$ es un p'-número, entonces $G = P \times H$ donde P es un p-subgrupo de Sylow y H un p-complemento de G. Posteriormente X. Liu, Y. Wang y H. Wei obtienen una variante debilitada de este resultado ([39]) que dice que si p es un primo que no divide ningún tamaño de clase de elementos de orden potencia de primo en $G_{p'}$, entonces el p-subgrupo de Sylow de G es un factor directo de G.

En el año 2001, S. Dolfi y M.S. Lucido introducen la siguiente definición: un grupo finito G verifica la propiedad $P(p,q)$ si cada p'-elemento tiene q'-índice. Estos autores demuestran que si G es un grupo que satisface la propiedad $P(p,q)$, con $p \neq q$, entonces $\mathbf{O}^p(G)$ es q-nilpotente y G tiene q-subgrupos de Sylow abelianos. También obtienen una clasificación de este tipo de grupos haciendo uso de la Clasificación de los Grupos Simples. Posteriormente S. Dolfi, A. Moreto y G. Navarro demuestran que si G es un grupo finito que tiene exactamente una clase de conjugación de

tamaño un múltiplo de un primo p, entonces una de las siguientes afirmaciones se verifica:

1. G es un grupo Frobenius con un complemento Frobenius de orden 2 y un núcleo de Frobenius de orden divisible por p.

2. G es un grupo Frobenius doblemente transitivo cuyo complemento Frobenius tiene un p-subgrupo de Sylow central no trivial.

3. $G = KH$, con $K = F(G)$ un q-grupo de G para un primo q, $H = C_G(P)$ siendo P un p-subgrupo de Sylow de G. Además $K \cap H = \mathbf{Z}(K)$ y $G/\mathbf{Z}(K)$ es un grupo Frobenius doblemente transitivo.

A. Beltrán y M.J. Felipe obtienen en [3] una caracterización de los grupos con p-complementos abelianos que dice que si G es un grupo finito y p un primo que divide a $|G|$, todo tamaño de clase en $G_{p'}$ es potencia de p si y sólo si G tiene p-complementos abelianos.

Por su parte, A.R. Camina y R.D. Camina demuestran en un reciente "survey"sobre la influencia de los tamaños de clases de conjugación sobre la estructura de los grupos finitos que si G es un grupo resoluble y p un primo, asumiendo que ningún tamaño de clase en $G_{p'}$ es divisible por p^2, entonces $G/\mathbf{O}_{p'}(G)$ es un π'-grupo, siendo $\pi = \{q : q \neq p$ es primo y q no divide $p-1\}$.

También se han obtenido algunos resultados importantes para grupos p-resolubles. Así por ejemplo en [3], A. Beltrán y M.J. Felipe obtienen una extensión del teorma de N. Itô ([31]) sobre la estructura de los grupos con dos tamaños de clase, mostrando que si G es un grupo p-resoluble tal que $cs_{p'}(G) = \{1, m\}$, entonces una de las siguientes afirmaciones se verifica:

1. $m = p^a$ y G tiene p-complemento abeliano

2. $m = q^b$, con q un primo distinto de p, y G es nilpotente con todos sus subgrupos de Sylow abelianos, excepto, como mucho, los q-sbugrupos de Sylow

3. $m = p^a q^b$, con $q \neq p$, y $G = PQ \times A$, con P un p-subgrupo de Sylow y Q un q-subgrupo de Sylow de G, respectivamente, y $A \subseteq \mathbf{Z}(G)$.

También se demuestra que si $a = 0$ entonces $G = P \times Q \times A$. Posteriormente, en [1], los autores obtienen una generalización de este resultado en la que se muestra que la condición de p-resolubilidad del grupo en la hipótesis del teorema no es necesaria.

En el Teorema A de [4] se extiende el resultado principal de [13] para clases ordinarias y se demuestra que si G es un grupo p-resoluble y m y n son dos elementos maximales de $cs_{p'}(G)$, con m y n coprimos y $m, n > 1$, suponiendo que $(m, n) = 1$, y p es un primo que no divide a m, entonces G es resoluble y

1. $cs_{p'}(G) = \{1, m, n\}$
2. un p-complemento de G es un grupo cuasi-Frobenius con núcleo y complemento abelianos. Es más los tamaños de clase del p-complemento son $\{1, m, n\}$

Como corolario del teorema se obtiene que si G es un grupo p-resoluble y $cs_{p'}(G) = \{1, m, n\}$, con m y n coprimos y $m, n > 1$, entonces G es resoluble y los p-complementos de G son cuasi-Frobenius con núcleo y complementos abelianos. Recordemos que un grupo G se dice que es cuasi-Frobenius si $G/\mathbf{Z}(G)$ es Frobenius. En tal caso, la imagen inversa en G del núcleo y de un complemento se conocen como núcleo y complemento de G.

Aplicando este último corolario, A. Beltrán y M.J. Felipe obtienen también en [4] la estructura de los grupos p-resolubles cuyos tamaños de clase p-regulares no centrales son números enteros consecutivos. Los autores demuestran que si $cs_{p'}(G) = \{1, n, n+1, ..., n+r\}$, entonces se verifica una de las siguientes afirmaciones:

1. $r = 0$, $n = p^a$, para algún entero positivo a y G tiene p-complementos abelianos.
2. $r = 0$, $n = p^a q^b$, para algún primo $q \neq p$ y enteros $a \geq 0$ y $b \geq 1$, y $G = PQ \times A$, siendo P y Q un p-subgrupo de Sylow y un q-subgrupo de Sylow de G, respectivamente, y $A \leq \mathbf{Z}(G)$. Además si $a = 0$ entonces $G = P \times Q \times A$.
3. $r = 1$ y cada p-complemento de G es cuasi-Frobenius con núcleo y complemento abelianos. Además si p no divide a n, entonces G es p-nilpotente . Si además, p tampoco divide a $n + 1$, entonces $G = P \times H$, siendo H el p-complemento de G.

M.G. Bianchi et al. obtuvieron en 1992 ([14]) el correspondiente resultado para clases de conjugación ordinarias.

El teorema D de [4] determina la estructura de los grupos p-resolubles cuyas clases de conjugación p-regulares tienen cardinal potencia de primo. El teorema extiende dos resultados de D. Chillag y M. Herzog para clases de conjugación ordinarias (Teorema 2 y corolario 2.2 de [20]) demostrando que si G es un grupo p-resoluble, entonces, fijado un primo p, cada clase de conjugación p-regular de G tiene cardinal potencia de primo si y sólo si se satisface una de las siguientes condiciones:

1. G tiene p-complementos abelianos. Esto ocurre si y sólo si cada clase p-regular tiene cardinal potencia de p.

2. G es nilpotente y todos sus r-subgrupos de Sylow son abelianos para todo primo $r \neq p$, q. Esto ocurre si y sólo si el cardinal de cada clase p-regular de G es potencia de un primo $q \neq p$.

3. $G = P \times H$, donde P es un p-subgrupo de Sylow de G y H es un p-complemento de G. Además, H es un grupo cuasi-Frobenius en el que el núcleo y los complementos son abelianos y los cardinales de sus clases p-regulares son exactamente $\{1, q^n, r^m\}$, siendo n y m dos enteros positivos, y q y r dos primos distintos entre sí y distintos de p. Esto ocurre si y sólo si los cardinales de las clases p-regulares de G son exactamente $\{1, q^n, r^m\}$.

Un resultado análogo al obtenido en [5], comentado en el último párrafo de la página 3, para grupos p-resolubles con condiciones similares en clases de conjugación p-regulares, es el obtenido por A. Beltrán y M. J. Felipe en [8] donde demuestran que si G es un grupo p-resoluble con $cs_{p'}(G) = \{1, m, n, mn\}$, siendo m y n enteros positivos coprimos, y p no divide a m y n, o $n = p^a$, entonces los p-complementos de G son nilpotentes y m y n son potencias de algún primo.

En 1974 A.R. Camina demuestra ([17]) que si G es un grupo finito con todas las clases de conjugación de elementos p-regulares no centrales del mismo tamaño y $|G/\mathbf{Z}(G)|$ es divisible al menos por dos primos distintos de p, entonces G es resoluble. En [1], E. Alemany, A. Beltrán y M.J. Felipe presentamos una demostración alternativa más sencilla de este resultado y la utilizamos para eliminar la condición de p-resolubilidad del grupo en la hipótesis del teorema principal de [3]. En el capítulo 3 de esta memoria presentamos una prueba unificada de estos resultados. En definitiva demostramos que si G es un grupo finito cuyos elementos p-regulares no centrales tienen todos el mismo tamaño de clase de conjugación, entonces G tiene p-complemento abeliano ó bien $G = PQ \times A$, con $P \in Syl_p(G)$, $Q \in Syl_q(G)$ y $A \in \mathbf{Z}(G)$.

Capítulo 2

Resultados preliminares

En este capítulo se realiza una recopilación de todos los resultados que hemos utilizado en la obtención del resultado principal de este trabajo, que se presenta en el capítulo siguiente.

2.1. Resultados de la Teoría General de Grupos

El primer resultado que presentamos pone de manifiesto una propiedad fundamental del subgrupo de Fitting de los subgrupos resolubles. El subgrupo de Fitting de un grupo G, denotado por $F(G)$ es el mayor subgrupo normal nilpotente de G.

Lema 2.1 *Si G es un grupo finito resoluble entonces $F(G) \neq 1$ y $C_G(F(G)) \subseteq F(G)$.*

Demostración. Como G es resoluble se tiene que la serie derivada

$$G \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq ... \trianglerighteq G^{(n-1)} \trianglerighteq G^{(n)} = 1$$

termina en 1. Consideremos el primer factor $G^{(n-1)}/G^{(n)} = G^{(n-1)}$ de la serie, que es normal, abeliano y nilpotente en G. Es decir $G^{(n-1)} \subseteq F(G) \neq 1$.

Sea $T = C_G(F(G))$ y $F_1 = F(T) \neq 1$. Como G es resoluble, T también lo es. Además $T \trianglelefteq G$, por ser el centralizador de un subgrupo normal de G. Por otro lado F_1 es subgrupo nilpotente de G, característico en T y, por tanto, normal en G. Por consiguiente $F_1 \subseteq F(G)$. Y, tomando centralizadores, $C_G(F(G)) \subseteq C_G(F_1)$.

Veamos que si $|T| < |G|$ el lema se tiene. Como T es resoluble y $|T| < |G|$, podemos aplicar inducción sobre el orden del grupo concluyendo que $C_T(F_1) \subseteq F_1 \subseteq F(G)$, por lo que acabamos de ver. Pero

$$C_T(F_1) = C_G(F_1) \cap T = C_G(F_1) \cap C_G(F(G)) = C_G(F(G))$$

por estar un centralizador contenido en otro, y se tendría que $C_G(F(G)) \subseteq F(G)$, como se quiere demostrar.

Veamos, por tanto, que $|T| < |G|$ aplicando reducción al absurdo. Supongamos que $|T| = |G|$.Como T es subgrupo de G se sigue que $T = G$, es decir $C_G(F(G)) = G$ y concluimos que $F(G)$ es subgrupo central de G. Pero como $\mathbf{Z}(G)$ es subgrupo nilpotente de G se tiene que $F(G) \subseteq \mathbf{Z}(G) \subseteq F(G)$ y, por tanto, $F(G) = \mathbf{Z}(G)$.

Podemos concluir que el grupo cociente $G/F(G)$ es resoluble y, aplicando el resultado que acabamos de obtener, $F(G/F(G))$ es un subgrupo no trivial, nilpotente del cociente. Pero, por definición, $F(G/F(G)) = F_2(G)/F(G)$, donde el subgrupo $F_2(G)$ se conoce como segundo grupo de Fitting de G, y se tiene que $F_2(G)/\mathbf{Z}(F_2(G))$ es subgrupo no trivial nilpotente de $F_2(G)/F(G)$, por ser $\mathbf{Z}(G) \subseteq \mathbf{Z}(F_2(G))$. Como $F_2(G)/\mathbf{Z}(F_2(G))$ es nilpotente entonces $F_2(G)$ es nilpotente y por tanto, $F_2(G) \subseteq F(G)$. Como por definición $F(G) \leq F_2(G)$, se tiene que $F(G) = F_2(G)$ de donde $F(G/F(G)) = F_2(G)/F(G) = 1$, obteniéndose una contradicción. Por tanto $|T| < |G|$, y el resultado se obtiene por inducción.

A continuación, exponemos una propiedad básica del p-residual de un grupo G, $\mathbf{O}^p(G)$, que se define como el menor subgrupo normal H de G tal que G/H es p-grupo. Es inmediato probar que dicho subgrupo es único y que $G = \mathbf{O}^p(G)$ si y sólo si G no posee cocientes p-grupo.

Lema 2.2 *Si Q es un q-subgrupo de Sylow de G y $q \neq p$ entonces $Q \subseteq \boldsymbol{O}^p(G)$. Por tanto $G = P\,\boldsymbol{O}^p(G)$, siendo P un p-subgrupo de Sylow de G.*

Demostración. Por definición se tiene que $G/\mathbf{O}^p(G)$ es p-grupo. Sea Q un q subgrupo de Sylow de G y $w \in Q$. Entonces la coclase $w\mathbf{O}^P(G)$ pertenece al grupo cociente $G/\mathbf{O}^p(G)$. Como $o(w) = q^r$ se tiene que

$$(w\mathbf{O}^p(G))^{q^r} = w^{q^r}\mathbf{O}^p(G) = \mathbf{O}^p(G)$$

por lo que $o(w\mathbf{O}^p(G))$ divide a q^r. Pero el grupo cociente es p-grupo y, por tanto, $o(w\mathbf{O}^p(G))$ es un p-número. Se concluye que $w\mathbf{O}^p(G) = \mathbf{O}^p(G)$ y $w \in \mathbf{O}^p(G)$ para todo $w \in Q$. Es decir, $Q \subseteq \mathbf{O}^p(G)$, como se quería demostrar.

Como consecuencia se tiene que si H es p'-subgrupo de G entonces $H \subseteq \mathbf{O}^p(G)$.

El siguiente resultado permite clasificar todos los grupos finitos cuyos subgrupos de Sylow son cíclicos.

Lema 2.3 ***(Hölder, Burnside, Zassenhaus).*** *Si G es un grupo finito con todos sus subgrupos de Sylow cíclicos, entonces G tiene representación*

$$G =< a,\, b | a^m = 1 = b^n,\, a^b = a^r >$$

donde $r^n \equiv 1 (mod\ m)$, m es impar, $0 \leq r < m$, y m y $n(r-1)$ son coprimos.

Recíprocamente en un grupo con tal representación todos los subgrupos de Sylow son cíclicos.

Demostración. Véase 10.1.10 de [46].

Un grupo con tal representación se dice que es metacíclico. Como consecuencia el grupo tiene una serie normal cuyos factores son todos cíclicos y es superresoluble. Por tanto es resoluble.

La siguiente propiedad elemental establece que un grupo finito no puede ser unión de conjugados de un subgrupo propio.

Lema 2.4 *Si G es un grupo finito y $U \leq G$ es un subgrupo de G tal que $G = \bigcup_{g \in G} U^g$, entonces $G = U$.*

Demostración. Como sabemos, el número de conjugados de U, U^g con $g \in G$, viene dado por $|G : N_G(U)|$. Por tanto, teniendo en cuenta que todos los conjugados son del mismo orden y que el elemento neutro del grupo pertenece a todos ellos, contando elementos se tiene:

$$|G| = |\bigcup_{g \in G} U^g| \leq 1 + |G : N_G(U)|(|U| - 1) \leq 1 + |G : U|(|U| - 1)$$

ya que $U \leq N_G(U) \leq G$ y por tanto $|G : N_G(U)| \leq |G : U| = |G|/|U|$. Es decir

$$|G| \leq 1 + \frac{|G|}{|U|}|U| - \frac{|G|}{|U|} = 1 + |G| - \frac{|G|}{|U|}$$

de donde, simplificando, se obtiene que $|G : U| \leq 1$. Como $|G : U| \geq 1$ se concluye que $|G : U| = 1$ y $G = U$.

Para abordar el estudio de los elementos p-regulares y de sus clases de conjugación es imprescindible conocer la $\{p, p'\}$-factorización de un elemento cualquiera de un grupo. Esta factorización puede extenderse hasta obtener la factorización de un elemento como producto de elementos de orden potencia de primo.

Lema 2.5 *Sea G un grupo finito, $g \in G$ y p un número primo que divide $|G|$. Entonces existen dos elementos únicos, g_p y $g_{p'}$ tales que:*

1. *g_p es de orden potencia de p.*
2. *$g_{p'}$ es de orden no divisible por p.*
3. *$g = g_p g_{p'} = g_{p'} g_p$.*

A g_p se denomina la p-parte de g y $g_{p'}$ se le denomina la p'-parte de g.

Demostración. Sea $n = o(g)$ y consideremos la descomposición de n como producto de potencia de números primos $n = p^a q^b r^s ...$ Denotaremos por $n_p = p^a$ a la mayor potencia de p que divide a n y por $n_{p'} = n/n_p$, de forma que $n = n_p\, n_{p'}$. Como $(n_p, n_{p'}) = 1$, por la Identidad de Bezout, existen enteros positivos a, $b \in \mathbb{Z}^+$ tales que $a.n_p + b.n_{p'} = 1$, de forma que

$$g = g^1 = g^{a.n_p + b.n_{p'}} = g^{a.n_p} g^{b.n_{p'}} = g_p g_{p'}$$

Tomaremos $g_p = g^{b.n_{p'}}$ y $g_{p'} = g^{a.n_p}$, de forma que $g = g_p g_{p'}$, como acabamos de ver. Además g_p y $g_{p'}$ conmutan

$$g = g_p g_{p'} = g^{b.n_{p'}} g^{a.n_p} = g^{b.n_{p'} + a.n_p} = g^{a.n_p + b.n_{p'}} = g^{a.n_p} g^{b.n_{p'}} = g_{p'} g_p = g$$

y por tanto

$$g^n = (g_p g_{p'})^n = {g_p}^n {g_{p'}}^n = ((g_p)^{n_p})^{n_{p'}} ((g_{p'})^{n_{p'}})^{n_p} = 1$$

Veamos que g_p es de orden potencia de p y que $g_{p'}$ es de orden no divisible por p.

$$(g_p)^{n_p} = (g^{b.n_{p'}})^{n_p} = g^{b.n_p.n_{p'}} = (g^n)^b = 1$$

$$(g_{p'})^{n_{p'}} = (g^{a.n_p})^{n_{p'}} = g^{a.n_p.n_{p'}} = (g^n)^a = 1$$

Por tanto, $o(g_p)$ divide a n_p y es p-número, mientras que $o(g_{p'})$ divide a $n_{p'}$ y es p'-número. Se concluye también que $o(g_p)o(g_{p'})$ divide a $n_p n_{p'} = n = o(g)$. Como además

$$g^{o(g_p)o(g_{p'})} = (g_p g_{p'})^{o(g_p)o(g_{p'})} = (g_p)^{o(g_p)o(g_{p'})}(g_{p'})^{o(g_p)o(g_{p'})} = 1$$

se sigue que $o(g) = n = n_p n_{p'}$ divide a $o(g_p)o(g_{p'})$. Por tanto $o(g_p)o(g_{p'}) = n_p n_{p'}$, de donde $o(g_p) = n_p$ y $o(g_{p'}) = n_{p'}$.

Además g_p y $g_{p'}$ son únicos. Supongamos que existen g_1 y g_2 tales que $g = g_1 g_2$, con $o(g_1)$ un p-número distinto de $o(g_p) = p^a$, y $o(g_2)$ un p'-número distinto de $o(g_{p'}) = n_{p'}$. Entonces $o(g_1) = p^\alpha$ con $\alpha < a$ y $o(g_2) = n'_{p'}$ con $n'_{p'}$ un divisor de $n_{p'}$. Pero entonces

$$g^{o(g_1)o(g_2)} = (g_1 g_2)^{o(g_1)o(g_2)} = ((g_1)^{o(g_1)})^{o(g_2)}((g_2)^{o(g_2)})^{o(g_1)} = 1$$

de donde $o(g_1)o(g_2) = p^\alpha n'_{p'} < n$, lo que implica que $o(g_1)o(g_2) = o(g)$, llegándose a una contradicción.

Otra herramienta que utilizaremos es la acción coprima de un grupo sobre otro y sus propiedades. Supongamos que un grupo A actúa como grupo de automorfismos de otro grupo G, es decir, que podemos considerar A como subgrupo del grupo de automorfismos de G.

Se dice que A actúa coprimamente sobre el grupo G si $(|G|, |A|) = 1$. En tal caso, si $S = AG$ es el producto semidirecto de A con G, se tiene que $G \trianglelefteq S$ y A es un complemento de G en S. El siguiente teorema, conocido como el Lema de Fitting, recoge algunas de las propiedades de la acción coprima que vamos a necesitar.

Teorema 2.1 *Sea A un grupo que actúa coprimamente sobre otro grupo abeliano G. Entonces $G = C_G(A) \times [G, A]$.*

Demostración. Sea $S = AG$ el grupo semidirecto que resulta de la acción de A sobre G. Como G es abeliano, $[G, A]$ y $C_G(A)$ son subgrupos normales de G. Dividiremos la demostración en tres pasos:

Paso 1. $[G, A]$ es subgrupo normal de S.

Sea $[g, a]$ un elemento generador de $[G, A]$, con $g \in G$ y $a \in A$, y sea $a_1 \in A$, entonces:

$$[g, a]^{a_1} = (g^{-1}g^a)^{a_1} = (g^{-1})^{a_1}(g^a)^{a_1}$$

Pero

$$(g^a)^{a_1} = {a_1}^{-1}a^{-1}a_1{a_1}^{-1}ga_1{a_1}^{-1}aa_1 = (a^{a_1})^{-1}g^{a_1}a^{a_1} = (g^{a_1})^{a^{a_1}}$$

por lo que

$$[g,a]^{a_1} = (g^{-1})^{a_1}(g^{a_1})^{a^{a_1}} = (g^{a_1})^{-1}(g^{a_1})^{a^{a_1}} = [g^{a_1}, a^{a_1}] \in [G,A]$$

Es decir $[G,A]$ es A-invariante y, por tanto, normal en S, como se quería demostrar.

Paso 2. $G = [G,A]C_G(A)$.

Como $[G,A]$ es A-invariante, si $\bar{g} \in C_{G/[G,A]}(A)$ se tiene que

$$(g[G,A])^a = g^a[G,A] = g[G,A] \text{ para todo } a \in A$$

Fijado un elemento $\bar{g} \in C_{G/[G,A]}(A)$, definimos la aplicación de A en $[G,A]$ que a cada $a \in A$ le hace corresponder $f(a) = g^{-1}g^a$. Entonces $f(a) = [g,a] \in [G,A]$ y el conjunto $K = \{af(a) : a \in A\}$ es subgrupo del grupo semidirecto $S = AG$ ya que

$$f(a_1a_2) = g^{a_1a_2}(g^{-1})^{a_2}g^{a_2}g^{-1} = (g^{a_1}g_{-1})^{a_2}g^{a_2}g^{-1} = f(a_1)^{a_2}f(a_2)$$

y por tanto

$$a_1f(a_1)a_2f(a_2) = a_1a_2f(a_1)^{a_2}f(a_2) = a_1a_2f(a_1a_2) \in K$$

Al ser $[G,A]$ A-invariante, se tiene que $[G,A] \trianglelefteq [G,A]A \leq S$. Si $af(a) \in K \cap [G,A]$, entonces $a \in [G,A]$, y, por tanto, $a \in [G,A] \cap A = 1$, por ser $(|[G,A]|, |A|) = 1$. Concluimos que $K \cap [G,A] = 1$.

Pero $A[G,A] = K[G,A]$ ya que si $ah \in A[G,A]$ entonces $ah = af(a)f(a)^{-1}h \in K[G,A]$. Por tanto A y K son dos complementos de $[G,A]$ en $A[G,A] \leq S$. Como $(|A|, |[G,A]|) = 1$ se tiene que $[G,A]$ es un subgrupo Hall de $A[G,A]$, normal y abeliano, por lo que los complementos de $[G,A]$ en $A[G,A]$ son todos conjugados (vease 10.29 de [45]). Es decir, existe $y = ah \in A[G,A]$ tal que $K = A^y = A^{ah} = A^h$. Entonces para todo $a \in A$ obtenemos que

$$a^h \in K \text{ y } a^h = aa^{-1}h^{-1}ah = a(h^{-1})^a h \in a[G,A]$$

por lo que $a^h \in a[G,A] \cap K = \{af(a)\}$. Como $f(a) = g^a g^{-1}$ y $a^h = af(a)$ se sigue que

$$(hg)^a = h^a g^a = a^{-1}hag^a = a^{-1}haf(a)g = a^{-1}ha^h g = hg \text{ para todo } a \in A$$

Denotaremos por $g_0 = hg \in G$ y se tiene que ${g_0}^a = g_0$. Como $h \in [G, A]$, podemos poner $[G, A]g = [G, A]hg = [G, A]g_0$. Concluimos que dado un elemento $\bar{g} \in C_{G/[G,A]}(A)$, existe un elemento $g_0 \in C_G(A)$ tal que $[G, A]g = [G, A]g_0$. Es decir $\bar{g} = \overline{g_0}$ y, como $\bar{g_0} \in [G, A]C_G(A)/[G, A] = C_G(A)[G, A]/[G, A]$, se sigue que $C_{G/[G,A]}(A) = C_G(A)[G, A]/[G, A]$.

Sea ahora $g \in G$. Entonces

$$g^a = a^{-1}gag^{-1}g = [a, g^{-1}]g \in [A, G]g = [G, A]g$$

por lo que $[G, A]g = [G, A]g^a = ([G, A]g)^a$ para todo $g \in G$ y para todo $a \in A$, por lo que $G/[G, A] = C_{G/[G,A]}(A) = C_G(A)[G, A]/[G, A]$, y se tiene que $G = C_G(A)[G, A]$, como se quería demostrar. (Esta propiedad es cierta, en general, en toda acción coprima).

Paso 3. $G = C_G(A) \times [G, A]$.

Como G es abeliano, sólo tenemos que ver que $[G, A] \cap C_G(A) = 1$. Sea $\mu : G \to G$ un homomorfismo de grupos tal que si $x \in G$, entonces

$$\mu(x) = \prod_{a \in A} x^a$$

Como G es abeliano, si $\alpha \in A$ y $x \in G$, entonces $\mu(x^\alpha) = \mu(x)$, ya que x,$x^\alpha \in x^A$. Si $g = [x, a] \in [G, A]$, entonces $g = x^{-1}x^a$ con $x \in G$ y $a \in A$, de manera que

$$\mu(g) = \mu(x^{-1}x^a) = \mu(x^{-1})\mu(x^a) = \mu(x^{-1})\mu(x) = \mu(1) = 1$$

Por otra parte, si $g \in C_G(A)$ entonces $g^a = g$ para todo $a \in A$ y por tanto

$$\mu(g) = \prod_{a \in A} g^a = \prod_{a \in A} g = g^{|A|}$$

Es decir, si $g \in [G, A] \cap C_G(A)$ se tiene que $o(g)$ divide a $|A|$ y $o(g)$ divide a $|[G, A]|$. Pero $(|[G, A]|, |A|) = 1$, por lo que $o(g) = 1$ y $g = 1$. Es decir, $[G, A] \cap C_G(A) = 1$. Como G es abeliano y $G = [G, A]C_G(A)$, concluimos que $G = C_G(A) \times [G, A]$ como se quería demostrar.

Lema 2.6 *Sea P un p-grupo abeliano para un cierto primo p. Sea K un grupo de automorfismos de P tal que $|K|$ es divisible por p. Supongamos que $C_P(x) = C_P(y)$ para todo x, $y \in K - \{1\}$. Entonces $\boldsymbol{O}_{p'}(K) = 1$.*

Demostración. Asumiremos que $H = \mathbf{O}_{p'}(K) > 1$ hasta llegar a una contradicción. Supongamos primero que $C_P(H) = 1$ y tomemos un $x \in H - \{1\}$. Si existe algún elemento $w \in C_P(x) - \{1\}$, entonces $w \in C_P(H)$. Por tanto $C_P(x) = \{1\} = C_P(y)$, para todo $y \in K - \{1\}$.

El grupo K actúa sobre P de modo que para cada $g \in P$ podemos considerar el estabilizador $Stab_K(g) = \{\alpha \in K : g^\alpha = g\}$. Como $C_P(\alpha) = 1$ para todo $\alpha \in K$, si $g = 1$ el estabilizador $Stab_K(g) = K$ y si $g \neq 1$ entonces $Stab_K(g) = 1$. Contando elementos en P se tiene que

$$|P| = \sum_{g \in P} |Orb_K(g)| = \sum_{g \in P} |K : Stab_K(g)| = \sum_{g \in P} \frac{|K|}{|Stab_K(g)|} = 1 + |K|l$$

donde l es el número de órbitas de cardinalidad mayor que 1. Pero esto no puede ser porque $p/|K|$ y $|P|$ es potencia de p. Por tanto $C_P(H) \neq 1$. Por las propiedades de la acción coprima (véase Teorema 2.1) se tiene que $P = C_P(H) \times [P, H]$.

Si $[P, H] = 1$ entonces

$$C_P(H) = \{g \in P : g^\alpha = g, \text{ para todo } \alpha \in H\} = P = C_P(K)$$

Pero esto no puede darse, ya que K es grupo de automorfismos de P. Concluimos que $P = C_P(H) \times [P, H]$, con $[P, H] \neq 1$.

Veamos ahora que $C_{[P,H]}(\alpha) = 1$, para todo $\alpha \in K$. Sea $\alpha \in K - \{1\}$. Entonces

$$\begin{aligned} C_P(x) = \{g \in P : g^x = g\} &= \{g_1 g_2 \in C_P(H) \times [P, H] : (g_1 g_2)^\alpha = g_1 g_2\} \\ &= \{g_1 g_2 \in C_P(H) \times [P, H] : (g_1)^\alpha = g_1,\ (g_2)^\alpha = g_2\} \\ &= \{g_1 \in C_P(H) : (g_1)^\alpha = g_1\} \times \{g_2 \in [P,\ H] : (g_2)^\alpha = g_2\} \\ &= C_P(\alpha) \times C_{[P,\ H]}(\alpha) = C_P(K) \times C_{[P,\ H]}(\alpha) \end{aligned}$$

Si $w \in C_{[P,H]}(x) - \{1\}$ entonces $w \in C_P(K)$ y $w \in [P,\ H]$. Es decir $w \in C_P(K) \cap [P,\ H]$. Pero $C_P(K) \cap [P,\ H] = 1$, ya que si $g \in C_P(K) \cap [P,\ H] - \{1\}$ entonces $g^\alpha = g$ ($g \in C_P(K)$) y $g = {g_1}^{-1} {g_1}^\alpha$ ($g \in [P,\ H]$). Sustituyendo $g = {g_1}^{-1} {g_1}^\alpha$ en la expresión $g^\alpha = g$ se tiene

$$\begin{aligned} ({g_1}^{-1} {g_1}^\alpha)^\alpha &= {g_1}^{-1} {g_1}^\alpha \\ ({g_1}^{-1})^\alpha ({g_1}^\alpha)^\alpha &= {g_1}^{-1} {g_1}^\alpha \end{aligned}$$

de donde

$$({g_1}^{-1})^{\alpha} = {g_1}^{-1} \text{ y } ({g_1}^{\alpha})^{\alpha} = {g_1}^{\alpha}$$

Es decir, $({g_1}^{-1})^{\alpha} = ({g_1}^{\alpha})^{-1} = {g_1}^{-1}$ y ${g_1}^{\alpha} = g_1$. Por tanto, $g = {g_1}^{-1}{g_1}^{\alpha} = {g_1}^{-1}g_1 = 1$. Concluimos pues que $C_{[P,H]}(\alpha) = 1$, para todo $\alpha \in K - \{1\}$.

Ahora bien, K actúa sobre $[P, H]$ de forma que, para cada $g \in [P, H]$, el estabilizador $Stab_K(g) = \{\alpha \in K : g^{\alpha} = g\}$. Como $C_{[P,\ H]}(\alpha) = 1$, si $g = 1$ se tiene que $Stab_K(g) = K$ y si $g \neq 1$ entonces $Stab_K(g) = 1$. Razonando como en el párrafo anterior, se tiene

$$|[P,H]| = \sum_{g \in [P,H]} |Orb_K(g)| = \sum_{g \in [P,H]} |K : Stab_K(g)| = \sum_{g \in [P,H]} \frac{|K|}{|Stab_K(g)|} = 1 + |K|.l$$

donde l es de nuevo el número de órbitas de cardinalidad mayor que 1. Pero esto no puede ser porque $p/|K|$ y $[P, H] \leq P$ es p-grupo, llegando a una contradicción. Concluimos por tanto que $\mathbf{O}_{p'}(K) = 1$.

Lema 2.7 *Sea G un grupo finito cuyos subgrupos de Sylow son todos cíclicos. Si r y s son dos primos distintos que dividen a $|G|$, entonces existe un subgrupo U de G tal que $|U| = rs$.*

Demostración. Trabajamos por inducción sobre el orden de G. Por el Lema 2.3, un grupo finito cuyos subgrupos de Sylow son todos cíclicos es resoluble. Como G es resoluble existe una serie abeliana

$$1 \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq \ \ldots \ \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

tal que G_{n-1} es normal maximal en G, y G/G_{n-1} es un factor abeliano simple, y por tanto, cíclico de orden primo. Es decir, G tiene un subgrupo $M = G_{n-1}$ normal maximal tal que $|G : M| = p$, para algún primo p.

Supongamos que la hipótesis es cierta para todo subgrupo $H \leq G$, con $|H| < |G|$, y tomemos un subgrupo normal maximal $M < G$ tal que $|G : M| = p$, para un cierto primo p. Aplicando la hipótesis de inducción, para cada par de primos r, s que dividen $|M|$ existe un subgrupo $U \leq M \leq G$ tal que $|U| = rs$.

Como $|G| = |G : M||M|$, cada par de enteros que divide a $|M|$ también divide a $|G|$. Y si p divide $|M|$, cada par de enteros que divide $|G|$ también divide $|M|$. En todos estos casos el resultado se sigue por inducción.

Si M es p'-grupo entonces para cada par de enteros r, $s \neq p$ que dividen $|M|$, y por tanto $|G|$, el resultado se sigue por inducción. Veamos que para cada entero q que divide $|M|$ existe un subgrupo $U < G$ de orden pq.

Sea P un p-subgrupo de Sylow de G, entonces $|P| = |G : M| = p$. Además $(|P|, |M|) = 1$, y P actúa coprimamente sobre M. De forma que, por las propiedades de la acción coprima, para cada $q \neq p$ que divide $|M|$ existe un q-subgrupo de Sylow Q de G, P-invariante, es decir, tal que $Q^g = Q$, para todo $g \in P$. Además Q es cíclico por ser q-subgrupo de Sylow de G.

Vamos a demostrar una propiedad elemental de los grupos cíclicos, concretamente que Q tiene un único subgrupo de orden q. Por ser un q-subgrupo, Q tiene elementos de orden q. Por ser cíclico, existe un elemento $y \in Q$ tal que $Q = \langle y \rangle$ y $|Q| = q^a = o(y)$. Sea $x = y^{q^{a-1}}$ un elemento de orden q de Q (ya que $x^q = 1$). Entonces el subgrupo generado por x, $\langle x \rangle$, es un subgrupo de orden q de Q.

Supongamos que existe otro elemento $w \in Q$ de orden q. Entonces $w = y^\alpha$ y $w^q = y^{\alpha q} = 1$. Es decir $o(y) = q^a$ divide a αq y por tanto q^{a-1} divide a α. Podemos poner $\alpha = nq^{a-1}$ con n un entero positivo coprimo con q. Pero entonces $w = y^{nq^{a-1}} = x^n$ y se obtiene que $\langle w \rangle = \langle x \rangle$.

Entonces el subgrupo generado por x, $\langle x \rangle$, es característico en Q, por ser único. Y como Q es P-invariante, P actúa como grupo de automorfismos sobre Q, por lo que $\langle x \rangle$ es P-invariante y por tanto P normaliza a $\langle x \rangle$ y los grupos conmutan. Concluimos que $U = P\langle x \rangle$ es subgrupo de G de orden pq.

Teorema 2.2 *Supongamos que $H \leq Aut(G)$ actúa, libre de puntos fijos, sobre G. Entonces:*

1. *Si $Q \in Syl_q(H)$, entonces Q es grupo cíclico o cuaternio generalizado. Si $P \in Syl_p(G)$ y P es invariante por H, entonces H actúa libre de puntos fijos sobre $P/\Phi(P)$.*

2. *Si p y q son primos, entonces cada subgrupo de H de orden pq es cíclico.*

Demostración. Véase Teorema 16.12 de [29].

A continuación enunciamos algunos resultados clásicos de la Teoría General de Grupos que hemos utilizado para la obtención de algunos de los resultados que se presentan en este trabajo. El primero de ellos es el famoso teorema de Kegel-Wielandt

sobre la resolubilidad de un grupo que es producto de subgrupos nilpotentes.

Teorema 2.3 ***(Kegel - Wielandt).*** *Si G tiene subgrupos nilpotentes G_1 y G_2 tales que $G = G_1G_2$ entonces G es resoluble.*

Demostración. Véase Theorem VI.4.3 de [28].

Obsérvese que, como consecuencia del teorema, si G tiene subgrupos nilpotentes G_1 y G_2 tales que $(|G : G_1|, |G : G_2|) = 1$, entonces es resoluble.

La existencia, conjugación y dominancia de los π-subgrupos de Hall está garantizada en la clase de grupos resolubles y también en la clase de grupos π-separables para un conjunto de primos π. Sin embargo, Wielandt demuestra que la nilpotencia de los subgrupos de Hall permite obtener resultados similares en grupos finitos no necesariamente resolubles.

Teorema 2.4 ***(Wielandt).*** *Sea G un grupo finito con algún π-subgrupo Hall nilpotente H. Entonces cada π-subgrupo de G está contenido en un conjugado de H. En particular todos los π-subgrupos Hall de G son conjugados.*

Demostración. Véase 9.1.10 de [46].

Terminamos este apartado, con dos resultados fundamentales de Burnside: el criterio de no simplicidad sobre los grupos que poseen una clase de cardinal potencia de primo; y el conocido Lema p^aq^b de Burnside. A su vez, el criterio de no simplicidad de Burnside ha sido mejorado por Kazarin que obtiene para dichos grupos un subgrupo normal resoluble.

Teorema 2.5 ***(Burnside).*** *Si el grupo finito G tiene una clase de conjugación con p^m elementos ($p^m > 1$), para algún primo p, entonces G no es simple.*

Demostración. Véase 15.2 de [29].

Teorema 2.6 ***(Kazarin).*** *Sea G un grupo finito que tiene una clase de conjugación x^G de tamaño potencia de un primo $p > 1$, entonces $< x^G >$ es subgrupo normal resoluble de G.*

Demostración. Véase 15.7 de [29].

Teorema 2.7 ***(Burnside).*** *Si $|G| = p^a q^b$ con p y q dos números primos distintos, entonces G es resoluble.*

Demostración. Véase 15.3 de [29].

2.2. Resultados de tamaños de clases de conjugación

Lema 2.8 *Sea G un grupo finito, $N \trianglelefteq G$, $x \in N$ y $g \in G$. Entonces:*

1. *$|x^N|$ divide a $|x^G|$.*
2. *$|gN^{G/N}|$ divide a $|g^G|$.*
3. *Si x, $y \in G$ tales que $xy = yx$ y $(o(x), o(y)) = 1$, entonces*

$$C_G(xy) = C_G(x) \cap C_G(y)$$

Demostración. (1) Como $N \trianglelefteq G$ y $C_G(x) \leq G$ se tiene que $N\,C_G(x) \leq G$. Aplicando el Teorema de Lagrange sobre la transitividad de índices se tiene que

$$|G : C_N(x)| = |G : C_G(x)||C_G(x) : C_N(x)|$$

Como además $C_N(x) \leq N \leq N\,C_G(x) \leq G$, aplicando de nuevo la transitividad de índices

$$|G : C_N(x)| = |G : N\,C_G(x)||N\,C_G(x) : N||N : C_N(x)| \tag{2.1}$$

Por el segundo Teorema de Isomorfía de grupos

$$N\,C_G(x)/N \cong C_G(x)/C_G(x) \cap N$$

por lo que,

$$|N\,C_G(x)/N| = |C_G(x)/C_G(x) \cap N|$$

Es decir, $|NC_G(x) : N| = |C_G(x) : C_G(x) \cap N| = |C_G(x) : C_N(x)|$, y sustituyendo este resultado en la ecuación 2.1, se tiene

$$|G : C_N(x)| = |G : N\, C_G(x)||C_G(x) : C_N(x)||N : C_N(x)| \tag{2.2}$$

De manera análoga, $|G : C_N(x)| = |G : C_G(x)||C_G(x) : C_N(x)|$, de donde

$$|G : C_G(x)| = |G : C_N(x)|/|C_G(x) : C_N(x)|$$

Y sustituyendo ahora en la ecuación 2.2 y simplificando se obtiene que

$$|G : C_G(x)| = |G : NC_G(x)||N : C_N(x)|$$

y por tanto $|x^N|$ divide a $|x^G|$.

(2) Veamos en primer lugar que

$$C_G(g)\, N/N \leq C_{G/N}(gN)$$

Si hN es un elemento de $C_G(g)\, N/N$ entonces $h \in C_G(g)\, N$ y, por tanto, existen $h_1 \in C_G(g)$ y $n_1 \in N$ tales que $h = h_1 n_1$. Es decir $hN = h_1 n_1 N = h_1 N$.

Ahora, $(hN)(gN) = (h_1 N)(gN) = (h_1 g)N = (gh_1)N = (gN)(h_1 N) = (gN)(hN)$ ya que $h_1 \in C_G(g)$. Por tanto $(hN) \in C_{G/N}(gN)$ como se quería demostrar.

Como

$$C_G(g)\, N/N \leq C_{G/N}(gN) \leq G/N$$

aplicando el Teorema de transitividad de índices se obtiene que

$$|G/N : C_{G/N}(gN)|\, |C_{G/N}(gN) : C_G(g)\, N/N| = |G/N : C_G(g)\, N/N|$$
$$|G|/|N| \;/\; |C_G(g)\, N|/|N| = |G|/|C_G(g)\, N| = |G : C_G(g)\, N|$$

Como $|G : C_G(g)| = |G : C_G(g)\, N||C_G(g)\, N : C_G(g)|$, despejando $|G : C_G(g)\, N|$ e igualando con la ecuación anterior, nos queda

$$|G : C_G(g)| \;/\; |C_G(g)\, N : C_G(g)| = |G : C_G(g)\, N| =$$
$$|G/N : C_{G/N}(gN)|\, |C_{G/N}(gN) : C_G(g)\, N\; /N|$$

Por tanto

$$|G : C_G(g)| = |C_G(g)\, N : C_G(g)|\, |G/N : C_{G/N}(gN)|\, |C_{G/N}(gN) : C_G(g)\, N \;/\; N|$$

$$|g^G| = |C_G(g)\, N : C_G(g)|\, |(gN)^{G/N}|\, |C_{G/N}(gN) : C_G(g)\, N\ /N$$

y $|gN^{G/N}|$ divide a $|g^G|$, como se quería demostrar.

(3) Es fácil ver que $C_G(x) \cap C_G(y) \leq C_G(xy)$. Demostraremos que también se verifica el recíproco.

Sea $w \in C_G(xy)$, $o(x) = r$ y $o(y) = s$. Entonces $(xy)^w = xy$, y elevando la ecuación a $o(y)$ se tiene que $((xy)^w)^s = (xy)^s$. Pero $((xy)^w)^s = ((xy)^s)^w = w^{-1}x^s y^s w = x^s y^s$, ya que x e y conmutan, y por tanto

$$w^{-1}x^s w = x^s \tag{2.3}$$

De manera análoga, elevando ahora la ecuación a $o(x)$ se obtiene que

$$w^{-1}y^r w = y^r \tag{2.4}$$

Como $(r,\, s) = 1$, aplicando la Identidad de Bezout, existen a y $b \in \mathbb{Z}^+$ tales que $ar + bs = 1$, por lo que

$$x = x^{ar+bs} = (x^r)^a (x^s)^b = (x^s)^b = x$$

De igual forma se obtiene que $(y^r)^a = y$. Elevando ahora la ecuación 2.3 a b obtenemos que

$$(w^{-1}x^s w)^b = (x^s)^b \implies w^{-1}(x^s)^b w = (x^s)^b \implies w^{-1}xw = x \implies w \in C_G(x)$$

Siguiendo los mismos pasos, al elevar la ecuación 2.4 se obtiene que $w \in C_G(y)$, y por tanto $w \in C_G(x) \cap C_G(y)$.

Lema 2.9 *Sea p un primo que divide a $|G|$. Entonces existe un p-subgrupo de Sylow P de G tal que $P \subseteq \boldsymbol{Z}(G)$ si y sólo si p no divide $|x^G|$, para todo $x \in G$.*

Demostración. Sea $A = \{p \in \mathbb{Z}^+ : p \text{ divide } |x^G|,\ x \in G\}$ y sea $B = \{p \in \mathbb{Z}^+ : p \text{ divide } |G : \mathbf{Z}(G)|\}$. Veremos que $A = B$.

Demostraremos primero que $A \subseteq B$, por reducción al absurdo. Sea $p \in A$ y supongamos que $p \notin B$. Como $p \in A$, existe algún elemento $x \in G$ tal que p divide $|x^G| = |G : C_G(x)| = |G|/|C_G(x)|$ y, por tanto, p divide $|G|$.

Por hipótesis p no divide $|G : \mathbf{Z}(G)|$, por lo que

$$|G : \mathbf{Z}(G)| = \frac{|G|}{|\mathbf{Z}(G)|} = \frac{|G|_p|G|_{p'}}{|\mathbf{Z}(G)|_p|\mathbf{Z}(G)|_{p'}} = \frac{|G|_{p'}}{|\mathbf{Z}(G)|_{p'}}$$

y se tiene que $|G|_p = |\mathbf{Z}(G)|_p$. Si p divide a $|G|$ y no divide a $|G : \mathbf{Z}(G)|$, aplicando el Teorema de transitividad de índices podemos concluir que p divide $|\mathbf{Z}(G)|$ y, por tanto, si P es un p-subgrupo de Sylow de $\mathbf{Z}(G)$ entonces P es p-subgrupo de Sylow de G (por ser $|P| = |\mathbf{Z}(G)|_p = |G|_p$). Es decir, $|G : P| = |G|_{p'}$ es p'-número y $P \leq \mathbf{Z}(G) \leq C_G(x) \leq G$.

Por tanto, $|G : P| = |G : C_G(x)||C_G(x) : P|$ es producto de p'-números, por lo que p no divide a $|G : C_G(x)| = |x^G|$, llegándose a una contradicción. Concluimos que p divide a $|G : \mathbf{Z}(G)|$ y $A \subseteq B$.

Demostraremos ahora que $B \subseteq A$. Sea $p \in B$ y supongamos que $p \notin A$. Como $p \in B$ y divide a $|G : \mathbf{Z}(G)|$, también divide a $|G|$. Sea $g \in G$. Como $p \notin A$, p no divide a $|g^G| = |G : C_G(g)| = |G|/|C_G(g)|$, lo que sólo puede darse si $|G|_p = |C_G(g)|_p$. Además, como p divide a $|G|$ pero no divide a $|G : C_G(g)|$, aplicando el Teorema de transitividad de índices se sigue que p divide a $|C_G(g)|$, y por lo tanto, si P es un p-subgrupo de Sylow de $C_G(g)$ entonces $|P| = |C_G(g)|_p = |G|_p$ y P también es p-subgrupo de Sylow de G.

Sea P_1 un p-subgrupo de Sylow de G. Entonces existe $h \in G$ tal que $P = (P_1)^h$. Como $P \subseteq C_G(g)$, se tiene que $g \in C_G(P) = C_G((P_1)^h) = C_G(P_1)^h$. Es decir, para todo $g \in G$ existe $h \in G$ tal que $g \in C_G(P_1)^h$, de forma que

$$G \leq \bigcup_{h \in G} C_G(P_1)^h \leq G \implies G = \bigcup_{h \in G} C_G(P_1)^h$$

y, aplicando el Lema 2.4, se obtiene que $G = C_G(P_1)$, de donde $P_1 \in \mathbf{Z}(G)$. Entonces $|P| = |\mathbf{Z}(G)|_p = |G|_p$ y $|G : \mathbf{Z}(G)| = |G|/|\mathbf{Z}(G)|$ es p'-número, llegando a una contradicción. Concluimos que $B \subseteq A$.

Recordemos que si p es un primo fijo, $G_{p'} = \{g \in G : o(g) \text{ es } p'\text{-número } \}$ denota el conjunto de elementos p-regulares de G. A continuación presentamos algunos resultados preliminares que relacionan la estructura del grupo con sus tamaños de clases de conjugación de elementos p-regulares. Empezaremos con un resultado que determina la estructura de los grupos cuyos tamaños de clases p-regulares son p'-números, generalizando así el Lema 2.9 al caso p-regular.

Lema 2.10 *Sea G un grupo finito y p un entero que no divide al tamaño de las clases de conjugación de elementos p-regulares. Entonces $G = P \times H$ donde P es un p-subgrupo de Sylow de G y H es un p-complemento de G.*

Demostración. Sea $g \in G$. Consideremos la descomposición de g en su p-parte y en su p'-parte, $g = g_p g_{p'}$. Si $g_{p'}$ es central entonces $g_p \in C_G(g_{p'})$ y se tiene que $g_p \in P^t \subseteq C_G(g_{p'})$ para algún $t \in G$.

Si $g_{p'}$ no es central, como $|g_{p'}^G| = |G : C_G(g_{p'})|$ es un p'-número, fijado un p-subgrupo de Sylow P de G, g_p estará en algún conjugado P^t de P. Aplicando el Teorema de transitividad de índices se obtiene que $g_p \in P^t \subseteq C_G(g_{p'})$ y $g_{p'} \in C_G(P^t)$. Por lo tanto

$$G = \bigcup_{t \in G} P^t C_G(P^t) = \bigcup_{t \in G} [PC_G(P)]^t.$$

Por el Lema 2.4 se tiene que $G = PC_G(P)$. Como P y $C_G(P)$ conmutan, se sigue que $P \trianglelefteq G$ y, por tanto G tiene una serie, $1 \trianglelefteq P \trianglelefteq G$, cuyos factores son, alternadamente, p-grupos y p'-grupos. Por lo tanto G es p-resoluble.

Se concluye en particular que el $C_G(P)$ es p-resoluble y tiene un p-complemento H que también es p-complemento de G. Por tanto, $G = PH$ donde P y H conmutan y $P \cap H = 1$. Es decir, $G = P \times H$ siendo H un p-complemento de G.

En el siguiente lema caracterizamos los grupos cuyos tamaños de clase de conjugación de elementos p-regulares no centrales son potencias del primo p.

Lema 2.11 *Sea G un grupo finito. Entonces todos los tamaños de clase de conjugación en $G_{p'}$ son p-números si y sólo si G tiene p-complemento abeliano.*

Demostración. Primero mostraremos que G es resoluble en ambas direcciones del lema. Supongamos que todos los tamaños de clases de conjugación de elementos p-regulares de G son p-números. Demostraremos que G es resoluble aplicando inducción sobre $|G|$. Por el Teorema 2.5 sabemos que un grupo simple no puede tener un tamaño de clase de conjugación potencia de primo, por lo que existe $N \lhd G$, $N \neq 1$. Si $x \in N_{p'}$ entonces por el Lema 2.8(a), $|x^N|$ divide $|x^G|$ y por tanto $|x^N|$ es p-número y podemos concluir por inducción que N es resoluble.

Por otro lado, sea $\overline{G} = G/N$ y sea $\overline{x} \in \overline{G}_{p'}$. Aplicando ahora el Lema 2.8(b), $|\overline{x}^{\overline{G}}|$ divide $|x^G|$ y, por tanto, $|\overline{x}^{\overline{G}}|$ es p-número y podemos concluir por inducción que $\overline{G}$

es resoluble. Como N y G/N son resolubles obtenemos que G es resoluble.

Si G tiene p-complemento abeliano, entonces se puede escribir como producto de dos subgrupos nilpotentes, esto es, un p-complemento abeliano y un p-subgrupo de Sylow de G. Por el Teorema 2.3 se sigue que G es resoluble también.

Supongamos ahora que $|x^G|$ es un p-número para todo $x \in G_{p'}$. Trabajaremos por inducción sobre $|G|$ para mostrar que G tiene p-complemento abeliano. Como G es resoluble, en particular, es p-resoluble y por tanto $\mathbf{O}_p(G) \neq 1$ o bien $\mathbf{O}_{p'}(G) \neq 1$.

Supongamos primero que $\mathbf{O}_p(G) \neq 1$. Entonces $|\overline{G}| = |G/\mathbf{O}_p(G)| < |G|$ y por inducción obtenemos que $\overline{G}$ tiene p-complemento abeliano $\overline{H}$. Como $\overline{H}$ es p-resoluble, entonces H puede escribirse como $H = H_1\mathbf{O}_p(G)$, siendo H_1 un p-complemento de H. Entonces

$$\overline{H} = H/\mathbf{O}_p(G) = H_1\mathbf{O}_p(G)/\mathbf{O}_p(G) \simeq H_1/H_1 \cap \mathbf{O}_p(G) = H_1$$

y obtenemos por isomorfía que H_1 es subgrupo abeliano de G de orden un p'-número. Como

$$|\overline{G} : \overline{H}| = \frac{|\overline{G}|}{|\overline{H}|} = \frac{|G/\mathbf{O}_p(G)|}{|H/\mathbf{O}_p(G)|} = \frac{|G|}{|H|} = |G : H|$$

es p-número también, se tiene que $|G : H_1| = |G : H||H : H_1|$ es p-número y H_1 es p-complemento abeliano de G. Podemos suponer, por tanto, que $\mathbf{O}_p(G) = 1$ y $\mathbf{O}_{p'}(G) \neq 1$. Consideremos el primer factor N_1 de la serie derivada de G

$$1 \lhd N_1 \lhd N_2 \lhd ... \lhd N_r = G$$

donde $N_i \lhd G$, y N_i/N_{i-1} abeliano. N_1 es abeliano y por tanto nilpotente por lo que $N_1 \subseteq F(G) \neq 1$. Sea x un elemento no central de $G_{p'}$. Como G y $C_G(x)$ son resolubles, y $|G : C_G(x)|$ es potencia del primo p, existe al menos un p-complemento H de G en $C_G(x)$ con $x \in H \subseteq C_G(x)$. Por otro lado, como $\mathbf{O}_p(G) = 1$ y $F(G)$ es el producto de todos los $\mathbf{O}_p(G)$ para todos los primos p que dividen $|G|$, se tiene que $F(G)$ es un p'-subgrupo normal de G y

$$x \in C_G(H) \subseteq C_G(F(G)) \subseteq F(G) \subseteq \mathbf{O}_{p'}(G).$$

Por tanto cualquier elemento p-regular (central o no) de G pertenece a $\mathbf{O}_{p'}(G)$ y $H = \mathbf{O}_{p'}(G)$ es p-complemento normal de G. Además, para todo $x \in H$, $x \in C_G(H) \subseteq H$. Es decir, $H = C_G(H)$ y por tanto H es p-complemento abeliano.

Supongamos ahora que G tiene p-complemento abeliano H. Entonces por el Teorema 2.4 todo p'-grupo está contenido en algún conjugado de H que, además,

son todos abelianos. Sea $x \in G_{p'}$. Entonces $< x > \subseteq H^g$ es abeliano, por lo que $H^g \leq C_G(x) \leq G$. Como H^g es p-complemento de G y por tanto de $C_G(x)$, se tiene que $|G : C_G(x)| = |x^G|$ es p-número y $|x^G|$ es potencia de p para todo $x \in G_{p'}$.

Lema 2.12 *Sea G un grupo finito, $x \in G_{p'}$ y $C_G(x) < G$. Supongamos que para todo par de elementos a, $b \in G_{p'}$ se verifica que si $C_G(a) \leq C_G(b)$ entonces $C_G(a) = C_G(b)$ ó $b \in \boldsymbol{Z}(G)$.*

Entonces $C_G(x) = P \times L$, con P un p-subgrupo de Sylow de $C_G(x)$ y $L \leq \boldsymbol{Z}(C_G(x))$, ó $C_G(x) = PQ \times A$, con P un p-subgrupo de Sylow de $C_G(x)$, Q un q-subgrupo de Sylow de $C_G(x)$, para un cierto primo $q \neq p$, y $A \leq \boldsymbol{Z}(G)$.

Demostración. Teniendo en cuenta la factoriazción dada en el Lema 2.5, el elemento x se puede factorizar como $x = x_1 x_2 \dots x_s$, donde cada x_i es una componente de x de orden potencia de un primo distinto de p, y las componentes conmutan dos a dos. Como $x \notin \mathbf{Z}(G)$, existe alguna componente $x_i \notin \mathbf{Z}(G)$. Como $C_G(x) \leq C_G(x_i)$, por la hipótesis del Lema se tiene que $C_G(x) = C_G(x_i)$, por lo que podemos asumir que x es un q-elemento para un cierto primo $q \neq p$.

Si $|C_G(x)| = p^a q^b$ entonces, por el teorema $\{p^a q^b\}$ de Burnside (Véase Teorema 2.7), el $C_G(x)$ es resoluble y el Lema se sigue trivialmente. Supongamos que existe un primo r divisor de $|C_G(x)|$ tal que $p \neq r \neq q$ y sea R un r-subgrupo de Sylow de $C_G(x)$.

Si $y \in R$, como x e y son de orden coprimo y conmutan, por el Lema 2.8(c), $C_G(xy) = C_G(x) \cap C_G(y)$. Luego $C_G(xy) \leq C_G(x)$ y, como x e y conmutan $xy \in G_{p'}$. Aplicando la hipótesis del Lema se tiene que $C_G(x) = C_G(xy) \subseteq C_G(y)$. Por tanto $y \in \mathbf{Z}(C_G(x))$ y se sigue que $R \leq \mathbf{Z}(C_G(x))$, es decir $C_G(x) = PQ \times A$, para algún $P \in Syl_p(C_G(x))$, $Q \in Syl_q(C_G(x))$ y $A \leq \mathbf{Z}(C_G(x))$.

Si $A \subseteq \mathbf{Z}(G)$ el lema se sigue. Supongamos por tanto que existe un elemento no central $u \in A$. Como u es un $\{p, q\}'$-elemento, u y x son de orden coprimos y conmutan, por lo que aplicando el Lema 2.8(c) se tiene que $C_G(ux) = C_G(u) \cap C_G(x)$. Luego $C_G(ux) \leq C_G(x)$ y por la hipótesis del Lema se sigue que $C_G(ux) = C_G(x) \subseteq C_G(u)$. Aplicando ahora la hipótesis del Lema a la segunda desigualdad, se obtiene que $C_G(ux) = C_G(x) = C_G(u)$.

Sea $z \in Q$, como $u \in A \leq \mathbf{Z}(C_G(x))$, z y u conmutan y son de orden coprimo y aplicando de nuevo el Lema 2.8(c) se tiene que $C_G(uz) = C_G(u) \cap C_G(z)$. Es decir, $C_G(uz) \leq C_G(u) = C_G(x)$ y por la hipótesis del Lema $C_G(uz) = C_G(x) \leq C_G(z)$,

por lo que $z \in \mathbf{Z}(C_G(x))$. Por tanto $Q \leq \mathbf{Z}(C_G(x))$ y $A \leq \mathbf{Z}(C_G(x))$. Podemos escribir $L = Q \times A$, de forma que $C_G(x) = P \times L$ con $L \leq \mathbf{Z}(C_G(x))$, y el resultado se sigue.

Capítulo 3

Grupos finitos con dos tamaños de clases de conjugación de elementos p-regulares

Como ya hemos comentado, N. Itô demostró que si los tamaños de clases de conjugación en G son 1 y m, entonces G es producto directo de un p-subgrupo de Sylow de G, para algún primo p, y un subgrupo central de G. En [3] se presenta una generalización de este teorema para tamaños de clase de p'-elementos, para un cierto primo p, bajo la hipótesis de p-resolubilidad del grupo. También hemos comentado que A.R. Camina probó, utilizando resultados profundos de la Clasificación de Grupos Simples, que si los tamaños de clases de conjugación de elementos p-regulares de G son 1 y m entonces G es resoluble. En este capítulo presentamos una demostración alternativa más simple de este resultado, y la utilizamos para eliminar la condición de p-resolubilidad del grupo en el teorema principal de [3]. Es decir, desarrollamos una demostración que conduce al resultado conjunto derivado del trabajo en [3] y de la extensión a grupos en general obtenida en [1].

Siguiendo el esquema de la demostración dada en [3], el resultado principal se divide en dos partes. En una se estudia el caso en que los centralizadores de los elementos p-regulares no centrales no son todos conjugados, que es análogo al caso ordinario, y en la otra, el caso en que sí lo son, que plantea una situación nueva, difícil de resolver.

Es más, con las condiciones del teorema de Itô para clases ordinarias es fácil ver que no puede darse el caso en que todos los centralizadores de elementos no centrales del grupo sean conjugados; sin embargo, podemos encontrar ejemplos en los que todos los centralizadores de elementos p-regulares no centrales son conjugados,

como veremos a continuación (observemos que en este caso G tiene exactamente dos tamaños de clase de conjugación de p'-elementos para algún primo p).

Consideremos el producto semidirecto del grupo cuaternio $Q_8 = \langle a, b : \ a^4 = 1, a^b = a^3, a^2 = b^2 = (ab)^2 \rangle$ con el grupo cíclico de orden 3, $C_3 = \langle \alpha \rangle$, y la acción definida por la permutación cíclica de orden 3

$$\begin{aligned} a^\alpha &= b \\ b^\alpha &= ab \\ (ab)^\alpha &= a \end{aligned}$$

Claramente $G = Q_8 < \alpha >$ es grupo de orden 24 y tiene elementos de orden 2, 4 y 3. Si se considera $p = 3$ y $q = 2$, los elementos p-regulares no centrales de G son exactamente los elementos de $Q_8 - \mathbf{Z}(Q_8) = \{a, b, ab, a^3, b^3, (ab)^3\}$. Es fácil ver que

$$\begin{aligned} C_G(a) = \langle a \rangle = C_G(a^3) \\ C_G(b) = \langle b \rangle = C_G(b^3) \\ C_G(ab) = \langle ab \rangle = C_G((ab)^3) \end{aligned}$$

por lo que sólo existen tres centralizadores distintos y todos ellos son de orden 4. Por tanto, en este caso $m = 6$ y $cs_{p'}(G) = \{1, 6\}$. Además, por la acción y las propiedades de la conjugación, se tiene que $C_G(a) = C_G(ab)^\alpha = C_G(b)^{\alpha^2}$.

Nótese que en las dos situaciones que aparecen en la tesis del Teorema A, se sigue que el grupo es resoluble. En efecto, en el primer caso, basta aplicar el Teorema de Kegel-Wielandt, pues G factoriza como producto de un p-grupo y un p-complemento abeliano, y en el segundo, se sigue por el Teorema p^aq^b de Burnside. También se demuestra que el tamaño de clase de conjugación de los elementos p-regulares no centrales de G es de la forma $m = p^aq^b$ con $a, b \geq 0$.

Teorema A. *Sea G un grupo finito con tamaños de clase de conjugación de elementos p-regulares $\{1, m\}$. Entonces $m = p^aq^b$, con q un primo distinto de p y $a, b \geq 0$. Si $b = 0$ entonces G tiene p-complemento abeliano. Si $b \neq 0$, entonces $G = PQ \times A$, con $P \in Syl_p(G)$, $Q \in Syl_q(G)$ y $A \leq \boldsymbol{Z}(G)$. Si $a = 0$ entonces $G = P \times Q \times A$, con $A \leq \boldsymbol{Z}(G)$. En particular, se obtiene que G es resoluble.*

Demostración. Por el Lema 2.11, si $m = p^a$ entonces G tiene p-complemento abeliano y este caso está demostrado. Por lo tanto asumiremos que m no es potencia de p, es decir $b \neq 0$, y veremos que $m = p^aq^b$, con $a \geq 0$. Si $a = 0$ la afirmación en

la tesis se seguirá como consecuencia trivial del Lema 2.10.

Procederemos por inducción sobre $|G|$ en varios pasos para probar que G tiene la estructura especificada.

Paso 1. Podemos asumir que $C_G(x) = P_x \times L_x$, con P_x un p-subgrupo de Sylow de $C_G(x)$ y $L_x \leq \mathbf{Z}(C_G(x))$, para todo $x \in G_{p'}$ no central.

Por el Lema 2.12 sabemos que para cualquier $x \in G_{p'}$ no central $C_G(x) = P_x \times L_x$, con P_x un p-subgrupo de Sylow de $C_G(x)$ y $L_x \leq \mathbf{Z}(C_G(x))$, o $C_G(x) = P_x Q_x \times A$, con P_x y Q_x un p-subgrupo y un q-subgrupo de Sylow de $C_G(x)$, respectivamente, y $A \leq \mathbf{Z}(G)$.

Supongamos que existe $x \in G_{p'}$ no central tal que $C_G(x) = P_x Q_x \times A$. Veremos por reducción al absurdo que $G = PQ \times A$ con P y Q un p-subgrupo y un q-subgrupo de Sylow de G, respectivamente, y $A \leq \mathbf{Z}(G)$. Supongamos que $G \neq PQ \times A$. Entonces podemos asumir que existe un r-elemento no central, z, para algún primo r distinto de p y de q, tal que:

$$A < \langle A, z \rangle \leq C_G(z)$$

Comparando el orden de los grupos se tiene que:

$$|A| < |\langle A, z \rangle| \leq |C_G(z)|_{\{p,q\}'} = |C_G(x)|_{\{p,q\}'} = |A|$$

obteniéndose una contradicción, por lo que $G = PQ \times A$ para algún $P \in Syl_p(G)$ y $Q \in Syl_q(G)$, y el teorema queda demostrado.

Paso 2. Sean x e y dos elementos p-regulares no centrales de G. Si $C_G(x) \neq C_G(y)$, entonces $(C_G(x) \cap C_G(y))_{p'} = \mathbf{Z}(G)_{p'}$.

Supongamos que existe un elemento no central $a \in (C_G(x) \cap C_G(y))_{p'}$. Como a es un elemento p-regular de $C_G(x)$ y de $C_G(y)$, por la forma de los centralizadores dada en el *Paso 1*, tiene que estar en el p-complemento. Es decir, $a \in L_x \leq \mathbf{Z}(C_G(x))$. De manera análoga $a \in L_y \leq \mathbf{Z}(C_G(y))$. Por tanto $C_G(x) \subseteq C_G(a)$ y $C_G(y) \subseteq C_G(a)$ y por órdenes se tiene que $C_G(x) = C_G(y) = C_G(a)$, llegando a una contradicción.

Para el resto de la demostración distinguiremos dos casos, según que los centralizadores de los elementos p-regulares no centrales sean todos conjugados o no.

CASO 1. Supongamos que los centralizadores de los elementos no centrales de $G_{p'}$ no son todos conjugados en G.

Denotaremos por $\overline{G} = G/\mathbf{Z}(G)_{p'}$ y utilizaremos barras para trabajar en el grupo cociente.

Paso 3. Sean $\bar{x}$ e $\bar{y}$ dos elementos p-regulares de $\overline{G}$ tales que $\bar{x}\bar{y} = \bar{y}\bar{x}$ siendo $C_G(x) \neq C_G(y)$. Entonces $o(\bar{x}) = o(\bar{y})$ es primo.

Nótese que x, y y xy son también elementos p-regulares de G. Supongamos que $o(\bar{x}) < o(\bar{y})$, entonces $(\bar{x}\bar{y})^{o(\bar{x})} = (\bar{y})^{o(\bar{x})} \neq 1$. Por lo tanto, $1 \neq (\bar{x}\bar{y})^{o(\bar{x})} = (\overline{xy})^{o(\bar{x})} \in \overline{C_G(xy)} \cap \overline{C_G(y)}$. Es decir, existe un p'-elemento no central en $C_G(xy) \cap C_G(y)$ y, aplicando el resultado del *Paso 2*, se tiene que $C_G(y) = C_G(xy)$, es decir y, xy y $x \in C_G(y)$. Aplicando nuevamente el *Paso 2*, como $x \in C_G(x) \cap C_G(y)$ se obtiene que $C_G(x) = C_G(y)$, contradiciendo la hipótesis. Concluimos que $o(\bar{x}) = o(\bar{y})$.

Veamos ahora que $o(\bar{x}) = o(\bar{y})$ es primo. Si s es un primo divisor de $o(\bar{x})$ y $\bar{x}^s \neq 1$, entonces $C_G(x) \subseteq C_G(x^s) < G$ y como los centralizadores de elementos p-regulares no centrales son del mismo orden, obtenemos que $C_G(x) = C_G(x^s)$. Es más, $\bar{x}^s\bar{y} = \bar{y}\bar{x}^s$ y como $C_G(x^s) = C_G(x) \neq C_G(y)$, por lo que se acaba de demostrar, $o(\bar{y}) = o(\bar{x}) = o(\bar{x}^s)$ y llegamos a una contradicción.

Paso 4. Sea g un elemento no central de $G_{p'}$ y consideremos la clase de conjugación de $\bar{g}$ en $\overline{G}$, $\bar{g}^{\overline{G}}$. Entonces existe algún elemento no central $x \in G_{p'}$ tal que $\bar{g}^{\overline{G}} \cap \overline{C_G(x)} = \emptyset$.

Supongamos que no es cierto. Entonces para cada elemento no central $x \in G_{p'}$, $\overline{C_G(x)}$ contiene algún conjugado de $\bar{g}$, $\bar{g}^{\bar{n}}$ para algún $\bar{n} \in \overline{G}$. Por tanto $\overline{g^n} = \bar{g}^{\bar{n}} \in \overline{C_G(x)}$, y como g es p'-elemento de G, $g^n \in C_G(x)_{p'} = L_x$. Por el *Paso 1*, $g^n \in L_x \leq \mathbf{Z}(C_G(x)))$ y por tanto $C_G(x) \leq C_G(g^n)$, y por órdenes, la igualdad se verifica. Es decir $C_G(x) = C_G(g^n) = C_G(g)^n$ y se sigue que dos centralizadores cualesquiera son conjugados en G, contradicción.

Paso 5. El orden de cada elemento p-regular no trivial de $\overline{G}$ es primo.

Supongamos que existe algún elemento p-regular $\bar{g} \neq \bar{1}$ tal que $o(\bar{g})$ es compuesto. Notemos que g es p-regular también, ya que si $o(\bar{g}) = n$, entonces $\bar{g}^n = \overline{g^n} = \bar{1}$ y, por tanto, g^n, $g \in \mathbf{Z}(G)_{p'}$. Por el *Paso 4* existe algún elemento no central $x \in G_{p'}$ tal que $\bar{g}^{\overline{G}} \cap \overline{C_G(x)} = \emptyset$. Supongamos que existe algún elemento no trivial $\bar{y} \in \overline{C_G(x)_{p'}}$ que centralice a algún conjugado de $\bar{g}$, $\bar{g}^{\bar{n}}$. Como x es no central por el *Paso 2* se tiene que $C_G(x) = C_G(y)$. Entonces, o bien

$$\overline{C_G(x)} = \overline{C_G(y)} = \overline{C_G(g^n)}$$

lo que nos lleva a que $\overline{g^n} \in \bar{g}^{\overline{G}} \cap \overline{C_G(x)}$, contradiciendo el *Paso 4*, o bien

$$\overline{C_G(x)} = \overline{C_G(y)} \neq \overline{C_G(g^n)}$$

lo que nos lleva, por el *Paso 3*, a que $\bar{x}$, $\overline{g^n}$ y por tanto $\bar{g}$ son de orden primo, y obtenemos de nuevo una contradicción. Concluimos que no existen elementos no triviales en $\overline{C_G(x)}$ que centralicen a conjugados de $\bar{g}$.

Denotaremos por $\overline{C_{p'}}$ a $\overline{C_G(x)_{p'}}$. Tenemos que $\overline{C_{p'}}$ actúa como grupo de permutaciones sobre $\bar{g}^{\overline{G}}$ por conjugación, de manera que a cada $\bar{w} \in \overline{C_{p'}}$ le corresponde la biyección $\Phi_{\bar{w}}$ definida por

$$\begin{aligned} \Phi_{\bar{w}} : \bar{g}^{\overline{G}} &\longrightarrow \bar{g}^{\overline{G}} \\ \bar{g}^{\bar{h}} &\longrightarrow \Phi_{\bar{w}}(\bar{g}^{\bar{h}}) = (\bar{g}^{\bar{h}})^{\bar{w}} = \bar{g}^{\overline{hw}} \end{aligned}$$

Para cada $\bar{g}^{\bar{h}} \in \bar{g}^{\bar{G}}$, el estabilizador del elemento $\bar{g}^{\bar{h}}$ por la acción de $\overline{C_{p'}}$ es

$$Stab_{\overline{C_{p'}}}(\bar{g}^{\bar{h}}) = \{\overline{w} \in \overline{C_{p'}} | (\bar{g}^{\bar{h}})^{\bar{w}} = \bar{g}^{\bar{h}}\} = \{\bar{1}\}$$

y por tanto todas las órbitas de $\overline{C_{p'}}$ en $\bar{g}^{\overline{G}}$ tienen el mismo tamaño

$$|\text{Órbita}(\bar{g}^{\bar{h}})| = \frac{|\overline{C_{p'}}|}{|Stab_{\overline{C_{p'}}}(\bar{g}^{\bar{h}})|} = |\overline{C_{p'}}|$$

Como $\bar{g}^{\overline{G}}$ es unión disjunta de sus órbitas, se tiene que, para algún n natural, $|\bar{g}^{\overline{G}}| = n.|\overline{C_{p'}}|$, por lo que $|\overline{C_{p'}}|$ divide a $|\bar{g}^{\overline{G}}|$.

Consideremos ahora un $\bar{g} \in \overline{C_G(g)_{p'}} \neq \overline{C_{p'}}$ y la acción de $\overline{C_G(g)_{p'}}$ sobre el conjunto $\bar{g}^{\overline{G}} - \bar{g}^{\overline{G}} \cap \overline{C_G(g)}$. De manera análoga, y aplicando de nuevo el *Paso 3*, se deduce que no hay elementos de $\overline{C_G(g)_{p'}}$ que centralicen a elementos de $\bar{g}^{\overline{G}} - \bar{g}^{\overline{G}} \cap \overline{C_G(g)}$, por lo que si $\bar{g}^{\bar{h}} \in \bar{g}^{\bar{G}}$ entonces el estabilizador $Stab_{\overline{C_G(g)_{p'}}}(\bar{g}^{\bar{h}}) = \{1\}$ y el tamaño de las órbitas de $\overline{C_G(g)_{p'}}$ en el conjunto $\bar{g}^{\overline{G}} - \bar{g}^{\overline{G}} \cap \overline{C_G(g)}$ es $|\overline{C_G(g)_{p'}}| = |\overline{C_{p'}}|$. Concluimos que $|\overline{C_G(g)_{p'}}|$ divide a $|\bar{g}^{\overline{G}}| - |\bar{g}^{\overline{G}} \cap \overline{C_G(g)}|$, y por tanto a $|\bar{g}^{\overline{G}} \cap \overline{C_G(g)}|$, lo que es una contradicción ya que $\bar{g}^{\overline{G}} \subseteq \overline{G_{p'}}$ y

$$0 < |\overline{C_G(g)_{p'}}| < |\bar{g}^{\overline{G}} \cap \overline{C_G(g)}| < |\overline{C_G(g)_{p'}}|$$

Paso 6. Conclusión en el Caso 1.

Por el *Paso 1* todos los $C_G(x)_{p'} = L_x$ de elementos no centrales $x \in G_{p'}$ son abelianos del mismo orden. Aplicando el *Paso 5*, si $\bar{x} \in \overline{L_x} \subseteq \overline{G}$ entonces $o(\bar{x}) = q$,

para un cierto primo $q \neq p$. Sea $\bar{w} \in overline L_x \subseteq C_{\overline{G}}(\bar{x})_{p'}$. Como $\bar{w} \in \overline{G}$, por el *Paso 5* $o(\bar{w}) = r$ con $r \neq p$, primo. Además $\bar{w}\bar{x} = \bar{x}\bar{w}$ y $\bar{w}\bar{x} \in \overline{G}$ por lo que $o(\bar{w}\bar{x})$ es primo. Como$(\bar{w}\bar{x})^{rq} = (\bar{w}^r)^q(\bar{x}^q)^r = \bar{1}$, se deduce que $o(\bar{w}\bar{x})$ es q o r. Si $o(\bar{w}\bar{x}) = q$ entonces $\bar{x}^q = \bar{1}$ y $q = r$. Concluimos que todo elemento de $overline L_x$ es de orden potencia de un cierto primo $q \neq p$. Utilizando el hecho de que todos los centralizadores de los elementos p-regulares no centrales son conjugados se obtiene que $\overline{G} = G/\mathbf{Z}(G)_{p'}$ es un $\{p, q\}$-grupo y puede escribirse en la forma $G = PQ \times A$, con $P \in Syl_p(G)$, $Q \in Syl_q(G)$ y $A \leq \mathbf{Z}(G)$.

CASO 2. Supongamos que para cualquier par de elementos no centrales x, $y \in G_{p'}$, $C_G(x)$ y $C_G(y)$ son conjugados en G.

Paso 7. Podemos asumir que $\mathbf{O}^p(G) = G$.

Aplicaremos inducción para demostrar que si $\mathbf{O}^p(G) < G$ el teorema se cumple, por lo que podemos suponer que $\mathbf{O}^p(G) = G$. Sea x un elemento p-regular no central de $\mathbf{O}^p(G)$, y por tanto no central en G. Por el *Paso 1*, $C_G(x) = P_x \times L_x$, con P_x un p-subgrupo de Sylow de $C_G(x)$ y $L_x \leq \mathbf{Z}(C_G(x))$. Por ser p'-grupo, $L_x \subseteq \mathbf{O}^p(G)$, y por tanto, aplicando la igualdad de Dedekind a $\mathbf{O}^p(G) \cap C_G(x)$ se tiene que:

$$\mathbf{O}^p(G) \cap C_G(x) = L_x(P_x \cap \mathbf{O}^p(G))$$

De donde:

$$\frac{|G|}{|\mathbf{O}^p(G)|}\frac{|\mathbf{O}^p(G)|}{|\mathbf{O}^p(G) \cap C_G(x)|} = \frac{|G|}{|C_G(x)|}\frac{|C_G(x)|}{|\mathbf{O}^p(G) \cap C_G(x)|}$$

$$= \frac{|G|}{|C_G(x)|}\frac{|P_x||L_x|}{|L_x||P_x \cap \mathbf{O}^p(G)|} = m\frac{|P_x|}{|P_x \cap \mathbf{O}^p(G)|}$$

Por tanto,

$$\frac{|G|}{|\mathbf{O}^p(G)|}\frac{|\mathbf{O}^p(G)|}{|\mathbf{O}^p(G) \cap C_G(x)|} = m\frac{|P_x|}{|P_x \cap \mathbf{O}^p(G)|}$$

$$\frac{|\mathbf{O}^p(G)|}{|\mathbf{O}^p(G) \cap C_G(x)|} = \frac{m\,|P_x|}{|G : \mathbf{O}^p(G)|\,|P_x \cap \mathbf{O}^p(G)|}$$

$$\frac{|\mathbf{O}^p(G)|}{|C_{\mathbf{O}^p(G)}(x)|} = \frac{m\,|P_x|}{|G : \mathbf{O}^p(G)||P_x \cap \mathbf{O}^p(G)|}$$

$$|x^{\mathbf{O}^p(G)}| = \frac{m\,|P_x|}{l\,|P_x \cap \mathbf{O}^p(G)|}$$

donde $l = |G : \mathbf{O}^p(G)|$ es un entero positivo. Si y es otro elemento p-regular no central de $\mathbf{O}^p(G)$, como los centralizadores de elementos no centrales en $G_{p'}$ son todos conjugados, existe $h \in G$ tal que $C_G(y) = C_G(x)^h = {P_x}^h \times {L_x}^h$ y, por tanto,

$$|P_y| = |(P_x)^h| = |P_x| \text{ y } |L_y| = |(L_x)^h| = |L_x|$$

Además,

$$|P_y \cap \mathbf{O}^p(G)| = |(P_x)^h \cap \mathbf{O}^p(G)| = |(P_x)^h \cap (\mathbf{O}^p(G))^h| = |(P_x \cap \mathbf{O}^p(G))^h| = |P_x \cap \mathbf{O}^p(G)|$$

lo que implica que

$$|y^{\mathbf{O}^p(G)}| = \frac{m\,|P_y|}{l\,|P_y \cap \mathbf{O}^p(G)|} = |x^{\mathbf{O}^p(G)}| = k$$

y se tiene que $\mathbf{O}^p(G)$ sólo tiene dos tamaños de clase de conjugación de p'-elementos. Como $|\mathbf{O}^p(G)| < |G|$, aplicando la hipótesis inductiva obtenemos que $\mathbf{O}^p(G)$ tiene p-complemento abeliano o se puede expresar en la forma $\mathbf{O}^p(G) = P_0Q \times A_0$, con P_0 un p-subgrupo de Sylow de $\mathbf{O}^p(G)$, Q un q subgrupo de Sylow de $\mathbf{O}^p(G)$ para algún primo $q \neq p$, y $A_0 \leq \mathbf{Z}(\mathbf{O}^p(G))$.

Si H es un p-complemento abeliano de $\mathbf{O}^p(G)$, se tiene que

$$H \leq \mathbf{O}^p(G) \leq G$$

y por tanto, $|G : \mathbf{O}^p(G)|$ y $|\mathbf{O}^p(G) : H|$ son p-números, por lo que

$$|G : H| = |G : \mathbf{O}^p(G)||\mathbf{O}^p(G) : H|$$

también es p-número. Como $|H|$ es p'-número, H es p-complemento de G.

Si $\mathbf{O}^p(G) = P_0Q \times A_0$ con $Q \leq \mathbf{O}^p(G) \leq G$, entonces $|G : \mathbf{O}^p(G)|$ es p-número y $|\mathbf{O}^p(G) : Q|$ es q'-número, por lo que $|G : Q|$ es un q'-número y, como $|Q|$ es q-número, $Q \in Syl_q(G)$.

Veamos que $A_0 \leq \mathbf{Z}(G)_{p'}$. Sean x, y elementos no centrales de $G_{p'}$ tales que $C_G(x) \neq C_G(y)$. Por el *Paso 2*, $(C_G(x) \cap C_G(y))_{p'} = \mathbf{Z}(G)_{p'}$. Como $x, y \in \mathbf{O}^p(G)$ y A_0 es p'-grupo central del $\mathbf{O}^p(G)$ se tiene que $A_0 \subseteq (C_G(x) \cap C_G(y))_{p'} = \mathbf{Z}(G)_{p'} \leq \mathbf{Z}(G)$. Por tanto, el grupo $T = Q \times A_0$ es p-complemento de $\mathbf{O}^p(G)$ y también de G por lo que podemos escribir $G = PQ \times A_0$, con $P \in Syl_p(G)$, $Q \in Syl_q(G)$ y $A_0 \leq \mathbf{Z}(G)$,

y el teorema está probado.

Si no existen dos elementos no centrales en $G_{p'}$ tales que $C_G(x) \neq C_G(y)$, entonces dados $x, y \in G_{p'}$ se tiene que $C_G(x) = C_G(y) = P_y \times L_y$ por lo que $x \in L_y \leq C_G(y)$. Es decir, si $Q \in Syl_q(G)$ con $q \neq p$, entonces $Q \leq L_y \leq G$ lo que implica que $|G : C_G(x)| = |x^G|$ es p-número y por el Lema 2.11 se concluye que G tiene p-complemento abeliano, llegando a una contradicción.

Paso 8. $C_G(x) < N_G(C_G(x))$ para todo $x \in G_{p'}$ no central.

Supongamos que $N_G(C_G(x)) = C_G(x)$ para algún $x \in G_{p'}$ no central. Como m no es potencia de p, existe algún primo $q \neq p$ que divide a m. Por el *Paso 1*, $C_G(x) = P_x \times L_x$, con $P_x \in Syl_p(C_G(x))$ y L_x abeliano. Veamos que q también divide a $|L_x/\mathbf{Z}(G)_{p'}|$. Supongamos que q no divide a $|L_x/\mathbf{Z}(G)_{p'}|$ y sea g un q-elemento no central de G. Como $C_G(g) = P_g \times L_g$ y los centralizadores de elementos p-regulares no centrales son del mismo orden, se tiene que $|L_g| = |L_x|$ y por tanto q no divide $|L_g/\mathbf{Z}(G)_{p'}|$, es decir, el grupo cociente no tiene elementos de orden q. Pero $g\mathbf{Z}(G)_{p'}$ es un elemento del grupo cociente y $o(g\mathbf{Z}(G)_{p'}) = o(g) = q$, por lo que llegamos a una contradicción y q divide $|L_x/\mathbf{Z}(G)_{p'}|$.

Como L_x tiene q-elementos no centrales, existe algún q-subgrupo de Sylow L_i del $C_G(x)$, con $L_i \subseteq L_x$, no central en G, estrictamente contenido en un q-subgrupo de Sylow Q_i de G. En particular, $L_i < N_{Q_i}(L_i) \subseteq N_G(L_i)$, por ser Q_i nilpotente. Luego existe un $y \in N_{Q_i}(L_i) - L_i \subseteq N_G(L_i) - L_i$.

Si $(L_x)^y \neq L_x$, consideramos $C_G(x^y) = C_G(x)^y = (P_x)^y \times (L_x)^y$ y se obtiene $C_G(x^y)_{p'} = L_x^y$. Como $C_G(x)_{p'} = L_x \neq {L_x}^y = C_G(x^y)_{p'}$, se sigue que $C_G(x^y) \neq C_G(x)$, y por el *Paso 2* se tiene $C_G(x)_{p'} \cap C_G(x^y)_{p'} = L_x \cap (L_x)^y = \mathbf{Z}(G)_{p'}$.

Pero $L_i \leq L_x$ y $L_i = {L_i}^y \leq {L_x}^y$, por lo que $L_i \leq (L_x)^y \cap L_x = \mathbf{Z}(G)_{p'}$, llegando a una contradicción. Concluimos pues que $(L_x)^y = L_x$. Además como $L_x < \mathbf{Z}(C_G(x))$,

$$P_x \subseteq C_G(L_x) = C_G((L_x)^y) \subseteq C_G(x^y) = (P_x)^y \times (L_x)^y$$

Por tanto $P_x = {P_x}^y$, es decir $C_G(x) = C_G(x)^y$ e $y \in N_G(C_G(x)) = C_G(x)$ por hipótesis, lo que implica que $y \in L_i$ por ser q-elemento del $C_G(x)$ y obtenemos de nuevo contradicción, concluyendo que $C_G(x) < N_G(C_G(x))$.

Paso 9. Si el grupo es resoluble el teorema se verifica.

Por el *Paso 7*, podemos considerar $\mathbf{O}^{p'}(G) < G$. Sea $x \in G_{p'}$ un elemento fijo no central y sea $g \in G$. Podemos escribir $g = g_p g_{p'}$ (véase el Lema 2.5), donde g_p

y $g_{p'}$ son la p-parte y la p'-parte de g, respectivamente. Si $g_{p'} \in \mathbf{Z}(G)$, entonces $g \in \mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}$. Si $g_{p'} \notin \mathbf{Z}(G)$, como los centralizadores de los elementos p-regulares no centrales son todos conjugados, existe un $n \in G$ tal que $C_G(g) \subseteq C_G(g_{p'}) = C_G(x)^n$ y $g \in C_G(x)^n$. Por tanto,

$$G = \bigcup_{n \in G} C_G(x)^n \bigcup \mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}$$

Como $|G : N_G(C_G(x))|$ es el número de conjugados distintos de $C_G(x)$ y, teniendo en cuenta que el elemento neutro está en todos ellos y en $\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}$, contando elementos se tiene:

$$|G| \leq |G : N_G(C_G(x))|(|C_G(x)| - 1) + |\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}|$$

Además,

$$|G| = |G : N_G(C_G(x))||N_G(C_G(x))|$$

y dividiendo por $|G|$ se sigue que

$$1 \leq \frac{|C_G(x)| - 1}{|N_G(C_G(x))|} + \frac{\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}}{|G|} \tag{3.1}$$

Por el *Paso 8*, tenemos que $C_G(x) < N_G(C_G(x))$, por lo que existen al menos 2 coclases de $C_G(x)$ en $N_G(C_G(x))$. Aplicando el teorema de la transitividad de índices de Lagrange se obtiene

$$|N_G(C_G(x)| = |N_G(C_G(x)) : C_G(x)||C_G(x)| \geq 2|C_G(x)|$$

Sea $|N_G(C_G(x))| = n_1$. Si $\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'} < G$, entonces aplicando de nuevo el teorema de la transitividad de índices de Lagrange se obtiene que $|G| \geq 2|\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}|$ y sustituyendo en la ecuación 3.1

$$1 \leq \frac{|C_G(x)|}{2|C_G(x)|} - \frac{1}{n_1} + \frac{|\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}|}{2|\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}|}$$

$$1 \leq \frac{1}{2} - \frac{1}{n_1} + \frac{1}{2}$$

y llegamos a una contradicción. Por tanto, podemos asumir que $\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'} = G$.

Si $\mathbf{O}^{p'}(G)$ es p-grupo entonces G tiene p-complemento abeliano, y obtenemos una contradicción. Por lo tanto, existen elementos p-regulares, no centrales, $y \in \mathbf{O}^{p'}(G)$. Para tales elementos

$$|y^{\mathbf{O}^{p'}(G)}| = |\mathbf{O}^{p'}(G) : C_{\mathbf{O}^{p'}(G)}(y)| = \frac{|\mathbf{O}^{p'}(G)|}{|C_{\mathbf{O}^{p'}(G)}(y)|} = \frac{|\mathbf{O}^{p'}(G)|}{|C_G(y) \cap \mathbf{O}^{p'}(G)|}$$

multiplicando numerador y denominador por $|\mathbf{Z}(G)_{p'}|$ y aplicando la igualdad de Dedekind obtenemos

$$|y^{\mathbf{O}^{p'}(G)}| = \frac{|\mathbf{O}^{p'}(G)||\mathbf{Z}(G)_{p'}|}{|\mathbf{Z}(G)_{p'}||C_G(y) \cap \mathbf{O}^{p'}(G)|} = \frac{|\mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}|}{|C_G(y) \cap \mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}|} = \frac{|G|}{|C_G(y) \cap G|}$$

Es decir,

$$|y^{\mathbf{O}^{p'}(G)}| = \frac{|G|}{|C_G(y)|} = |y^G| = m$$

y concluimos que los elementos p-regulares de $\mathbf{O}^{p'}(G)$ tienen tamaños de clase de conjugación 1 ó m. Podemos aplicar inducción a $\mathbf{O}^{p'}(G)$ y concluir que $\mathbf{O}^{p'}(G) = PQ_0 \times S_0$, con $P \in Syl_p(G)$, $Q_0 \in Syl_q(\mathbf{O}^{p'}(G))$ para algún primo $q \neq p$, y $S_0 \leq \mathbf{Z}(\mathbf{O}^{p'}(G)) \leq \mathbf{Z}(G)$.

Como $G = \mathbf{O}^{p'}(G)\mathbf{Z}(G)_{p'}$, se tiene que $G = PQ \times A$, con $A \leq \mathbf{Z}(G)$ y $Q \in Syl_q(G)$.

Paso 10. Si $x \in G_{p'}$ no central, todo subgrupo de Sylow de $N_G(C_G(x))/C_G(x)$ es cíclico o cuaternio generalizado. Es más, si $q \neq p$ es un primo divisor del orden de este grupo cociente entonces el q-subgrupo de Sylow tiene orden q.

Sea $x \in G_{p'}$ no central y sea $W = N_G(C_G(x))/C_G(x)$. Sea Q un q-subgrupo de Sylow de W para algún primo q que divida a $|W|$ (posiblemente $q = p$). Por los supuestos iniciales del teorema existe algún primo r, distinto de p y q, que divide $|G/\mathbf{Z}(G)|$. Es decir, existe un elemento g_r de orden r en $G - \mathbf{Z}(G)$ y r divide $|C_G(g_r)| = |C_G(x)|$.

Por tanto existe un r-subgrupo de Sylow R_x de $C_G(x)$. Veamos que Q actúa como grupo de automorfismos sobre R_x, con acción $\psi : Q \longrightarrow Aut(R_x)$ tal que si $\bar{g} \in Q$ y $w \in R_x$ entonces $\psi_{\bar{g}}(w) = w^{\bar{g}} = w^g$, donde $g \in N_G(C_G(x))$ y hemos tomado barras para trabajar en W. Es fácil comprobar que

$$(w_1 w_2)^{\bar{g}} = w_1^{\bar{g}} w_2^{\bar{g}} \text{ y } (w^{\overline{g_1}})^{\overline{g_2}} = (w)^{\overline{g_1 g_2}}$$

Además la acción está bien definida por ser $\psi_{\bar{g}}(w) = w^{\bar{g}} = w^g \in R_x$, y es independiente del representante de clase elegido. Como

$$Ker(\psi) = \{\bar{g} \in Q : w^g = w, \text{ para todo } w \in R_x,\ g \in N_G(C_G(x))\}$$

$$= \{\bar{g} \in Q : g \in C_{N_G(C_G(x))}(R_x)\} \subseteq \{\bar{g} \in Q : g \in C_G(z),\, z \in R_x\}$$

$$= \{\bar{g} \in Q : g \in C_G(x)\} = \overline{C_G(x)} = \{\bar{1}\}$$

ψ es inyectiva y así Q actúa como grupo de automorfismos sobre R_x como queríamos demostrar.

Obsérvese que si $\bar{g} \in Q$ entonces $C_{R_x}(\bar{g}) = R_x \cap \mathbf{Z}(G)$. Basta probar que si $z \in C_{R_x}(\bar{g})$, entonces $z \in \mathbf{Z}(G)$. Sea $g \in N_G(C_G(x))$ tal que $\bar{g} \in Q - \{\bar{1}\}$. Supongamos que existe $z \in C_{R_x}(\bar{g}) - \mathbf{Z}(G)$. Entonces $z \in R_x \leq L_x \leq \mathbf{Z}(C_G(x))$ y y por el *Paso 1* se tiene que $C_G(z) = C_G(x)$. Como $z \in C_{R_x}(\bar{g}) = \{h \in R_x : h^{\bar{g}} = h^g = h\}$, entonces $g \in C_G(z) = C_G(x)$ y $\bar{g} = \{\bar{1}\}$.

Al ser $(|Q|, |R_x|) = 1$, la acción es coprima, y como R_x es abeliano se tiene que (véase Teorema 2.1)

$$R_x = [R_x, Q] \times C_{R_x}(Q)$$

Consideremos ahora la acción restringida de Q sobre $[R_x,\, Q]$ dada por $\psi_{\bar{q}}(w) = w^{\bar{g}} = w^g$, para todo $\bar{q} \in Q$ y $w \in [R_x,\, Q]$. La acción está bien definida y es libre de puntos fijos. Para verlo basta comprobar que si $t \in [R_x, Q] - \{1\}$ y $\bar{g} \in Q - \{\bar{1}\}$ entonces $t^{\bar{g}} \neq t$, y ningún elemento de $Q - \{\bar{1}\}$ puede fijar a t. Supongamos que $t^{\bar{g}} = t$, entonces $t \in C_{[R_x,Q]}(\bar{g}) \leq C_{R_x}(\bar{g}) = R_x \cap \mathbf{Z}(G)$. Luego $t \in \mathbf{Z}(G)$ y $t^g = t$, para todo $g \in G$. Se sigue que $t^{\bar{g}} = t$, para todo $\bar{g} \in Q$ y, por tanto, $t \in C_{R_x}(Q)$. Pero $R_x = [R_x,\, Q] \times C_{R_x}(Q)$ por lo que $[R_x,\, Q] \cap C_{R_x}(Q) = \{1\}$, lo que implica $t = 1$, contradicción. Aplicando ahora un conocido resultado (véase Teorema 2.2) se concluye que Q es cíclico o cuaternio generalizado.

Supongamos ahora que $q \neq p$ y consideremos un q-subgrupo de Sylow Q_x de $C_G(x)$. El grupo Q actúa sobre $\overline{Q}_x = Q_x/\mathbf{Z}(G)_q$, con acción $\psi_{\bar{q}}(\bar{g}) = \bar{g}^{\bar{q}} = \overline{g^q}$. Sea $M = [\overline{Q_x}]Q$ el producto semidirecto definido por esta acción. Por construcción M es q-grupo y $\overline{Q}_x \trianglelefteq M$ por lo que $\overline{Q}_x \cap \mathbf{Z}(M)$ es q-subgrupo no trivial de M y tiene elementos de orden q. Sea $\bar{t} \in \overline{Q}_x \cap \mathbf{Z}(M)$ uno de tales elementos. Podemos construir el subgrupo $T = \langle t \rangle \mathbf{Z}(G)_q \leq C_G(x)$. Entonces Q actúa sobre T con acción $\psi_{\bar{g}}(h) = h^{\bar{g}} = h^g$, para todo $\bar{g} \in Q$, $h \in T$. Además la acción es fiel, es decir $C_Q(T) = \{\bar{1}\}$, ya que como $t \in Q_x$, no central, se tiene que $C_G(t) = C_G(x)$, y si $\bar{g} \in C_Q(T)$ y $h \in T$ entonces $h^{\bar{g}} = h^g = h$, por lo que $g \in C_G(h) = C_G(x)$ y por tanto $\bar{g} \in \overline{C_G(x)} = \{\bar{1}\}$. Es más, nótese que $[T,\, Q] \subseteq \mathbf{Z}(G)_q$, puesto que al ser $t \in \mathbf{Z}(M)$ y $\bar{g} \in Q \leq M$ entonces $\overline{t^{\bar{g}}} = \overline{t^g} = \bar{t}$ y $t^g = ta$ con $a \in \mathbf{Z}(G)_q$, por lo que $t^{-1}t^g \in \mathbf{Z}(G)_q$. Por tanto, si ${t_1}^{-1}{t_1}^{\bar{g}} \in [T,\, Q]$ entonces

$${t_1}^{-1}{t_1}^{\bar{g}} = {t_1}^{-1}{t_1}^g = (t^\alpha b)^{-1}(t^g)^\alpha b^g = b^{-1}(t^{-1}t^g)^\alpha b^g \in \mathbf{Z}(G)$$

donde $b \in \mathbf{Z}(G)_q$.

Probaremos que Q es un subgrupo q-elemental, esto es, todos sus elementos son de orden q. Si $t_1 \in T$ entonces $(t_1)^q = (t^\alpha b)^q = t^{\alpha q} b^q = b^q \in \mathbf{Z}(G)$. Sea $\bar{v} \in Q$. Como $t^q \in \mathbf{Z}(G)$ y T es abeliano, entonces $[t^q, \bar{v}] = [t, \bar{v}]^q = 1$. Por tanto $t^{\bar{v}^q} = t$, para todo $t \in T$ y podemos concluir que $\bar{v}^q \in C_Q(T) = \{\bar{1}\}$. Es decir, Q es q-subgrupo elemental. Pero entonces Q no puede ser cuaternio generalizado y, según lo visto en el párrafo anterior, tiene que ser cíclico de orden q, como queríamos demostrar.

Paso 11. Para todo $x \in G_{p'}$, se tiene que $|N_G(C_G(x))/C_G(x)| = q$ para algún primo $q \neq p$.

Primero probaremos que $W = N_G(C_G(x))/C_G(x)$ es un q-grupo para algún primo q (posiblemente $q = p$). Supongamos que $|W|$ es divisible por al menos dos primos distintos. Demostraremos que existe un subgrupo U de W tal que $|U|$ es producto de dos números primos.

Por el *Paso 10*, todo subgrupo de Sylow de W es cíclico o cuaternio generalizado. Si todos los Sylows de W son cíclicos entonces por el Lema 2.7 podemos concluir que existe tal grupo U. Si algún 2-subgrupo de Sylow de W es cuaternio generalizado podemos aplicar el clásico teorema de R. Brauer y M. Suzuki (ver 45.1 de [29]) para concluir que $\mathbf{O}_{2'}(W).\langle\tau\rangle \trianglelefteq W$, donde τ es la única involución de W. Como todos los $2'$-subgrupos de Sylow de W, y por tanto los de $\mathbf{O}_{2'}(W) \lhd W$, son cíclicos, si $|\mathbf{O}_{2'}(W)|$ es divisible, como mínimo, por dos primos distintos entonces aplicando de nuevo el Lema 2.7 podemos afirmar que tal grupo U existe. Si $|\mathbf{O}_{2'}(W)|$ es divisible por un único primo, es decir, $\mathbf{O}_{2'}(W)$ es r-grupo cíclico para algún primo $r \neq 2$, entonces existe $\alpha \in \mathbf{O}_{2'}(W)$ de orden r y podemos construir el subgrupo $U = \langle\alpha\rangle\langle\tau\rangle$ de orden $2r$. Concluimos, por tanto, que en todos los casos existe un subgrupo $U \leq W$ tal que $|U| = rs$, para ciertos primos r y s, como queríamos probar.

Veamos ahora que esto nos lleva a una contradicción. Si ambos primos son distintos de p, U es de orden producto de dos primos y por tanto tiene r-complemento o s-complemento. Notar que uno de los dos subgrupos es normal en U, por los teoremas de Sylow. Concretamente si $r < s$, el s-subgrupo de Sylow es normal, y si $s < r$ entonces, el r-subgrupo de Sylow es normal. Asumiremos sin pérdida de generalidad, que el r-complemento es normal. Si uno de los primos es p, es decir, si $|U| = pr$, con $r \neq p$ entonces existe un primo $s \neq p$, r tal que s divide $|G/\mathbf{Z}(G)|$ y por tanto a $|G|$. Es decir, existe un elemento $g \in G_{p'}$ de orden s y s divide $|C_G(s)| = |C_G(x)|$. Entonces existe un s-subgrupo de Sylow S_x en $C_G(x)$ tal que $[S_x, U] \neq 1$ y razonando como en el segundo párrafo del *Paso 10*, obtenemos que U actúa como grupo de

automorfismos sobre $[S_x, U]$ con acción

$$\psi_{\bar{u}}(g) = g^{\bar{u}} = g^u \in [S_x, U]$$

Además la acción es libre de puntos fijos ya que para todo $g \in U - 1$ y $t \in [S_x, U] - 1$ se tiene que $t^{\bar{g}} \neq t$. Por tanto, aplicando por ejemplo el Lema 16.12 de [29], se obtiene que U es cíclico, y en particular U tiene r-complemento normal no trivial. Es decir, en ambos casos se concluye que U tiene r-complemento normal para algún primo $r \neq p$.

Consideramos ahora la acción de U como grupo de automorfismos de R_x dada por $\psi_{\bar{u}}(r) = r^{\bar{u}} = r^u \in R_x$, siendo R_x un r-subgrupo de Sylow abeliano del $C_G(x)$. Nótese que si $\bar{u}, \bar{v} \in U - \{\bar{1}\}$, entonces

$$C_{R_x}(\bar{u}) = C_{R_x}(\bar{v}) = R_x \cap \mathbf{Z}(G) = \mathbf{Z}(G)_r$$

por lo que aplicando el Lema 2.6, se obtiene que $\mathbf{O}_{r'}(U) = 1$. Pero U tiene r-complemento normal no trivial y obtenemos una contradicción. Por tanto, hemos demostrado que $|N_G(C_G(x))/C_G(x)|$ es potencia de un primo.

Tomemos ahora un r-subgrupo de Sylow R_x de $C_G(x)$ no central en G, para algún primo $r \neq p$. Si $t \in R_x$ es no central, entonces por el *Paso 1* se tiene que $C_G(x) = C_G(t)$. Por otro lado, si $w \in N_G(R_x)$, entonces por la misma razón, $t \in L_x$ y $C_G(t^w) = C_G(t) = C_G(x)$, de forma que $C_G(x) = C_G(t)^w = C_G(x)^w$ y $w \in N_G(C_G(x))$. Es decir, $N_G(R_x) \leq N_G(C_G(x))$. Pero como R_x no es subgrupo de Sylow de G, existe un r-subgrupo de Sylow R de G tal que $R_x \leq R$, y se sigue que $R_x < N_R(R_x)$, de donde

$$C_G(x)_r = R_x < N_R(R_x) \leq N_G(R_x) \leq N_G(C_G(x))$$

lo que implica que r divide a $|N_G(R_x)/R_x|$, y por tanto, hay elementos de orden r en el grupo cociente $W = N_G(C_G(x))/C_G(x)_r$. Es decir, r divide a $|W|$ y W no puede ser un p-grupo. Entonces W es un q grupo para un cierto $q \neq p$ y por el *Paso 10* el orden del q-grupo es exactamente q, como se quería demostrar.

Como resultado del *Paso 11* y del hecho de que todos los centralizadores de elementos p-regulares no centrales son conjugados, podemos asumir que

$$|N_G(C_G(x))/C_G(x)| = q$$

para un primo fijo $q \neq p$ y para todo $x \in G_{p'}$ no central. Por tanto, los normalizadores en G de los centralizadores de los elementos p-regulares no centrales son todos del mismo orden.

Paso 12. Podemos asumir que $\mathbf{O}_p(G) = 1$ y que $|G : N_G(C_G(x))|$ es un p-número para cada $x \in G_{p'}$ no central.

Sea $x \in G_{p'}$ no central. Para cualquier primo $r \neq p$ consideramos un r-subgrupo de Sylow R de G. Si R es central entonces $R \leq C_G(x) < N_G(C_G(x))$. Luego el primo r no divide a $|G : N_G(C_G(x))|$. Si R es abeliano no central entonces existe $y \in R - \mathbf{Z}(G)$, p'-elemento no central, tal que $R \leq C_G(y) \leq G$. Como $|C_G(y)|_r = |C_G(x)|_r = |G|_r$, r no divide $|G : C_G(x)|$. Y como $C_G(x) < N_G(C_G(x))$, el primo r tampoco divide a $|G : N_G(C_G(x)|$.

Si R no es abeliano entonces $R - \mathbf{Z}(R) \neq \{1\}$ y $R/\mathbf{Z}(R)$ es un r-grupo con centro no trivial. Luego existe $\bar{t} \in \mathbf{Z}(R/\mathbf{Z}(R)) - \{\bar{1}\}$. Sea $w \in R$, veremos que $C_R(t) = C_R(t^w) = C_R(t)^w$ y por tanto $C_R(t) \trianglelefteq R$.

Como $\bar{t} \in \mathbf{Z}(R/\mathbf{Z}(R))$ y $\bar{w} \in R/\mathbf{Z}(R)$, $[\bar{t}, \bar{w}] = \bar{1}$ por lo que $[t, w] = t^{-1}t^w \in \mathbf{Z}(R)$. Por otro lado, si $g \in C_R(t)$ entonces $t^g = t$ y

$$(t^w)^g = g^{-1}tt^{-1}t^w g = g^{-1}tgt^{-1}t^w = t^w$$

por lo que $g \in C_R(t^w)$. De manera análoga, si $g \in C_R(t^w)$ entonces

$$(t^w)^g = g^{-1}t^w g = t^w$$

Es decir,

$$(t^w)^g = g^{-1}tt^{-1}t^w g = g^{-1}tgt^{-1}t^w = t^g t^{-1}t^w = t^w$$

por lo que $t^g = t$ y $g \in C_R(t)$.

Concluimos que $C_R(t) = C_R(t^w) = C_R(t)^w$ y por tanto $C_R(t) \trianglelefteq R$. Como los centralizadores de los elementos p-regulares no centrales son todos conjugados, existe $h \in G$ tal que $C_G(t) = C_G(x)^h = C_G(x^h)$, con $x^h \in G_{p'}$ no central.

Ahora, si $g \in N_G(C_R(t))$ entonces $t^g \in C_R(t) \leq C_G(t) = C_G(x^h)$. Luego t^g es r-elemento del $C_G(x^h)$ y, aplicando el *Paso 1*, $t^g \in R_x \leq \mathbf{Z}(C_G(x^h))$. Por tanto, $C_G(x^h) \leq C_G(t^g)$, y por órdenes coinciden. Es decir

$$C_G(t) = C_G(x^h) = C_G(t^g) = C_G(t)^g = C_G(x^h)^g$$

Es decir $C_G(x^h) = C_G(x^h)^g$ y $g \in N_G(C_G(x^h))$. Concluimos que $R \leq N_G(C_R(t)) \leq N_G(C_G(x^h))$ y r no divide a $|G : N_G(C_G(x^h))|$. Como los normalizadores de los elementos p-regulares no centrales de G son del mismo orden, sus índices en G coinciden, por lo que r tampoco divide a $|G : N_G(C_G(x))|$. Obtenemos así que en todos los

casos $|G : N_G(C_G(x))|$ es p-número.

Asumiremos ahora que $\mathbf{O}_p(G) \neq \{1\}$ y consideraremos el grupo cociente $\overline{G} = G/\mathbf{O}_p(G)$. Aplicando inducción sobre el orden del grupo, veremos que en este caso el teorema se verifica. Sea $x \in G_{p'}$ y sea $\bar{y} \in C_{\overline{G}}(\bar{x})$. Entonces $\bar{x}\bar{y} = \bar{y}\bar{x}$ y $[x, y] \in \mathbf{O}_p(G)$. Por lo tanto podemos poner $x^y = xk$, con $x \in C_G(x)$, $k \in \mathbf{O}_p(G)$ y x^y un p'-elemento de $C_G(x)\mathbf{O}_p(G)$.

Como por el *Paso 1*, $C_G(x) = P_x \times L_x$, con L_x un p'-subgrupo del centralizador, y por tanto p-complemento de $C_G(x)\mathbf{O}_p(G)$, se tiene que

$$x^y \in {L_x}^h = {L_x}^{ab} = {L_x}^b$$

para algún $h = ab \in C_G(x)\mathbf{O}_p(G)$, con $a \in C_G(x)$ y $b \in \mathbf{O}_p(G)$. Obtenemos que $x^{yb^{-1}} \in L_x$ y, por el *Paso 1*,

$$C_G(x) = C_G(x^{yb^{-1}}) = C_G(x)^{yb^{-1}}$$

Por lo tanto, $yb^{-1} \in N_G(C_G(x))$, de donde $y = wb$ con $w \in N_G(C_G(x))$. Como $b \in \mathbf{O}_p(G)$ se tiene $\bar{y} = \bar{w}$, y por tanto $\bar{w} \in C_{\bar{G}}(\bar{x})$. Es decir $\bar{w}\bar{x} = \bar{x}\bar{w}$ y $[w, x] \in \mathbf{O}_p(G)$ es p-elemento.

Por otra parte $w \in N_G(C_G(x))$, por lo que $x^w \in L_x \leq C_G(x)$ y $x^{-1}x^w \in L_x$, por ser producto de p'-elementos que conmutan. Es decir $[w, x] = x^{-1}x^w$ es p'-elemento también, y por tanto $[w, x] = 1$. Es decir, $w \in C_G(x)$ y $\bar{w} \in \overline{C_G(x)}$. Pero $\bar{w} = \bar{y} \in \overline{C_G(x)}$, por lo que $C_{\overline{G}}(\bar{x}) \subseteq \overline{C_G(x)}$ y se tiene la igualdad, $C_{\overline{G}}(\bar{x}) = \overline{C_G(x)}$. Concluimos que $|\overline{G} : C_{\overline{G}}(\bar{x})| = |G : C_G(x)| = m$ y $\overline{G}$ tiene dos tamaños de clase de conjugación de elementos p-regulares. Por la hipótesis de inducción, $\overline{G}$ tiene p-complemento abeliano, de manera que G tiene p-complemento abeliano, o $\overline{G} = \overline{PQ} \times \overline{A}$ con $\overline{P} \in Syl_p(\overline{G})$, $\overline{Q} \in Syl_q(\overline{G})$ y $\overline{A} \leq \mathbf{Z}(\overline{G})$. En el primer caso llegamos a una contradicción y la demostración concluye. En el segundo caso se obtiene que G es un grupo resoluble, por serlo $\overline{G}$ y $\mathbf{O}_p(G)$, y por el *Paso 9* el resultado se sigue.

Paso 13. Para cada primo $r \neq p$, $\mathbf{O}_r(G) \subseteq \mathbf{Z}(G)$.

Sea r un primo distinto de p y supongamos que $K = \mathbf{O}_r(G)$ es no central. Por el *Paso 12*, $|G : N(C_G(x))|$ es p-número, por lo que $K \subseteq N_G(C_G(x))$, para todo $x \in G_{p'}$. Por hipótesis existen tres primos distintos que dividen $|G/\mathbf{Z}(G)|$. Es decir, existe $s \neq p,r$ tal que s divide $|G/\mathbf{Z}(G)|$ y, por el *Paso 1*, s divide $|C_G(x)/\mathbf{Z}(G)|$ también.

Por tanto, existe un s-subgrupo de Sylow S_x de $C_G(x)$, abeliano, normal y no central en G. Nótese que si $s \in S_x \subseteq C_G(x)$ y $g \in K \leq N_G(C_G(x))$ entonces s^g es s-elemento de $C_G(x)$ y por tanto K normaliza S_x y se tiene que $[S_x, K] \subseteq S_x \cap K = 1$, es decir $K \subseteq C_G(S_x) = C_G(x)$, donde la última igualdad se sigue como consecuencia del *Paso 1*. Por otro lado, si $t \in K - \mathbf{Z}(G)$, t es r-elemento no central de G, y de nuevo por el *Paso 1* se tiene que $C_G(t) = C_G(x)$. Es más, si $w \in N_G(K)$ entonces t^w es r-elemento no central y aplicando el *Paso 1*

$$C_G(t^w) = C_G(x) = C_G(t) = C_G(t)^w = C_G(x)^w$$

por lo que $w \in N_G(C_G(x))$. Pero entonces $N_G(K) = G \subseteq N_G(C_G(x))$ lo que implica que $C_G(x) \trianglelefteq G$. Pero esto no es posible ya que todos los centralizadores de elementos p-regulares no centrales de G son conjugados, y llegamos a una contradicción.

Paso 14. Conclusión.

Obsérvese primero que $\mathbf{Z}(G)_q \neq 1$. Supongamos que $\mathbf{Z}(G)_q = 1$, como q divide a m por el *Paso 11*, existe un q-subgrupo de Sylow no central Q de G, con centro no trivial. Si $g \in \mathbf{Z}(Q)$, entonces $Q \leq C_G(g) \leq G$ y $|Q| = |C_G(g)|_q = |G|_q$. Como g es un elemento p-regular no central de G, entonces $|G : C_G(g)| = m$, lo que implica que q no divide a m y llegamos a una contradicción.

Consideremos el grupo cociente $\overline{G} = G/\mathbf{Z}(G)_q$. Probaremos que $\overline{G}$ tiene dos tamaños de clase de conjugación de elementos p-regulares.

Asumiremos que $\overline{G}$ no es abeliano ya que en tal caso G sería resoluble y la demostración se termina. Si $\bar{a} \in \overline{G} - \mathbf{Z}(\overline{G})$, es fácil comprobar que $\overline{C_G(a)} \subseteq C_{\overline{G}}(\bar{a})$. Veremos por reducción al absurdo que $\overline{C_G(a)} = C_{\overline{G}}(\bar{a})$ para todo $\bar{a} \in \overline{G} - \mathbf{Z}(\overline{G})$, por lo que $|\overline{G} : C_{\overline{G}}(\bar{a})| = |G : C_G(a)| = m$ y $\overline{G}$ tiene dos tamaños de clase de conjugación de elementos p-regulares.

Supongamos entonces que existe un elemento p-regular $\bar{a} \in \overline{G}$ tal que $\overline{C_G(a)} \neq C_{\overline{G}}(\bar{a})$. Si $\overline{w} \in C_{\overline{G}}(\bar{a})$ entonces $w \in N_G(C_G(a))$, es decir, $C_{\overline{G}}(\bar{a}) \subseteq \overline{N_G(C_G(a))}$. Por el *Paso 11*, $|\overline{N_G(C_G(a))} : \overline{C_G(a)}| = |N_G(C_G(a)) : C_G(a)| = q$, con q primo. Pero como $\overline{C_G(a)} < C_{\overline{G}}(\bar{a}) \leq \overline{N_G(C_G(a))}$, se tiene que

$$|\overline{N_G(C_G(a))} : \overline{C_G(a)}| = |\overline{N_G(C_G(a))} : C_{\overline{G}}(\bar{a})||C_{\overline{G}}(\bar{a}) : \overline{C_G(a)}| = q$$

siendo q primo y $|C_{\overline{G}}(\bar{a}) : \overline{C_G(a)}| \neq 1$. Por tanto

$$|\overline{N_G(C_G(a))} : \overline{C_G(a)}| = 1$$

y $|\overline{N_G(C_G(a))}| = |\overline{C_G(a)}|$. Por el *Paso 12* se concluye que $|\overline{G} : C_{\overline{G}}(\bar{a})| = |G : N_G(C_G(a))|$ es un p-número. Aplicando ahora un conocido resultado de Kazarin (véase por ejemplo 15.7 de [29]), el subgrupo $\langle \bar{a}^{\overline{G}} \rangle$ es subgrupo normal resoluble de $\overline{G}$, lo que implica que existe algún primo r tal que $\mathbf{O}_r(\overline{G}) \neq 1$. Pero si $r = p$, llegamos a una contradicción con el *Paso 12*, y si $r \neq p$, llegamos a una contradicción con el *Paso 13*.

Concluimos por tanto que $\overline{G}$ tiene dos tamaños de clase de conjugación de elementos p-regulares, y por inducción obtenemos que $\overline{G}$ tiene p-complemento abeliano ó $\overline{G} = \overline{PQ} \times \overline{A}$, con $\overline{P} \in Syl_p(\overline{G})$, $\overline{Q} \in Syl_q(\overline{G})$ y $\overline{A} \subseteq \mathbf{Z}(\overline{G})$. En el primer caso, aplicando el Lema 2.11 se obtiene que todos los tamaños de clase de conjugación en $\overline{G_{p'}}$ son p-números. Como $|\overline{C_G(a)}| = C_{\overline{G}}(\bar{a})$ todos los tamaños de clase de conjugación en $G_{p'}$ son p-números también y, por tanto, G tiene p-complemento abeliano, lo que no puede darse. En el segundo caso se tiene como consecuencia que $\overline{G}$ es resoluble y por tanto G es resoluble, por lo que el teorema está demostrado.

Como consecuencia se tiene que si $\{1, m\}$ son los tamaños de clase de conjugación de elementos p-regulares de G y $a \in G_{p'}$, entonces

$$m = |G : C_G(a)| = |G : N_G(C_G(a))||N_G(C_G(a)) : C_G(a)| = p^a q^b$$

En particular, si $b = 0$ entonces $m = p^a$ y, por el Lema 2.11, G tiene p-complemento abeliano. Si $a = 0$ entonces $m = q^b$ y, por el Lema 2.10, tenemos que $G = P \times H = P \times Q \times A$, siendo $H = Q \times A$ un p-complemento de G y $A \in \mathbf{Z}(\overline{G})$.

Bibliografía

[1] Alemany, E., Beltrán, A., Felipe, M.J. *Finite groups with two p-regular conjugacy class lengths II.* Bulletin of the Australian Mathematical Society **79** (2009) 419-425.

[2] Arad, Z., Fisman, E. *A proof of Szep's conjecture on nonsimplicity of certain finite groups.* Journal of Algebra **108** (1987) no 2 240-354.

[3] Beltrán, A., Felipe, M. J. *Finite groups with two p-regular conjugacy class lengths.* Bulletin of the Australian Mathematical Society **67** (2003) 163-169.

[4] Beltrán, A., Felipe, M.J. *Certain relations between p-regular class sizes and the p-structure of p-solvable groups.* Journal of the Australian Mathematical Society **77** (2004) no 3 387-400.

[5] Beltrán, A., Felipe, M.J. *Prime factors of π-partial character degrees and conjugacy class sizes of π-elements.* Algebra Colloquium. **12** (2005) no 4 699-707.

[6] Beltrán, A., Felipe, M.J. *Variations on a theorem by Alan Camina on conjugacy class sizes.* Journal of Algebra. **296** (2006) 253-266.

[7] Beltrán, A., Felipe, M.J. *Some class size conditions implying solvability of finite groups.* Journal of Group Theory. **9** (2006) no 6 787-797.

[8] Beltrán, A., Felipe, M.J. *Nilpotency of p-complements and p-regular conjugacy class sizes.* Journal of Algebra. **308** (2007) no 2 641-653.

[9] Beltrán, A., Felipe, M.J. *Conjugacy classes of p-regular elements in p-solvable groups.* Proceedings Group St. Andrews. Ed. Cambridge. **1** (2007) 224-229.

[10] Beltrán, A., Felipe, M.J. *Structure of finite groups under certain arithmetical conditions on class sizes.* Journal of Algebra. **319** (2008) no 3 897-910.

[11] Beltrán, A., Felipe, M.J. *The structure of finite groups with three class sizes.* J. Group Theory. **12** (2009) no 3 539-553.

[12] Beltrán, A., Felipe, M.J. *Finite groups with four conjugacy class sizes*. Communications in Algebra. Preprint.

[13] Bianchi, M., Gillio, A., Casolo, C. *A note on conjugacy class sizes of finite groups*. Rend. Sem. Mat. Padova. **106** (2001) 255-260.

[14] Bianchi, M.G., Chillag, D., Mauri, A., Herzog, M., Scoppola, C. *Applications of a graph related to conjugacy classes of finite groups*. Arch. Math. **58** (1992) no 2 126-132.

[15] Burnside, W. *On groups of order $p^a q^b$*. Proc. Lond. Math. Soc. **2** (1904) 388-392.

[16] Camina, A.R. *Arithmetical conditions on the conjugacy class numbers of a finite group*. J. London Math. Soc. bf 2 (1972) no 5 127-132.

[17] Camina, A.R. *Finite groups of conjugate rank 2*. Nagoya Math. J. bf 53 (1974) 47-57.

[18] Camina, A.R., Camina, R.D. *Implications of conjugacy class size*. J. Group Theory **1** (1998), 257-269.

[19] Camina, A.R., Camina, R.D. *Coprime conjugacy class sizes*. Asian-Eur. J. Math., **2(2)**(2009), 183-190.

[20] Chillag, D., Herzog, M. *On the lengths of the conjugacy classes of finite groups*. J. Algebra **131** (1990), 110-125.

[21] Chillag, D., Mann, A. *Nearly odd-order and nearly real finite groups*. Common Algebra. **26** (1998) 2041-2064.

[22] Cossey, J., Wang, Y. *Remarks on the length of conjugacy classes of finite groups*. Communications in Algebra **27** (9) (1999) 4347-4353.

[23] Dolfi, S., Jabara E. *The structure of finite groups of conjugate rank 2*. Bull. London Math. Soc., **41(5)** (2009), 916-926.

[24] Dolfi, S., Pacifici, E., Sanus, L. *Finite groups with real conjugacy classes of prime size*. Israel J. Math. **175** (2010) 179-189.

[25] Felipe, M. J., Navarro, G. *Relative character correspondences in finite groups*. Canad. J. Math. **47** (1995) no 4 718-727.

[26] Fein, B., Kantor, W.M., Schacher, M. *Relative Brauer groups, II* J. Reine Angew. Math., **328** (1981) 39-57.

[27] Gorenstein, D., J.H. Walter. *On finite groups with dihedral Sylow 2-subgroups.* Illinois J. Math. **6** (1962) 553-593.

[28] Huppert, B. *Endliche Gruppen I.* Springer-Verlag. Berlín-Heidelberg-New York (1967).

[29] Huppert, B. *Character Theory of Finite Groups.* Walter de Gruyter and Co. Berlín, 1998.

[30] Ishikawa, K. *On finite p-groups which have only two conjugacy class lengths.* Israel J. Math. **129** (2002) 119-123.

[31] Ito, N. *On finite groups with given conjugate type I.* Nagoya Math. J. **6** (1953) 17-28.

[32] Ito, N. *On finite groups with given conjugate type II.* Osaka J. Math. **7** (1970) 231-251.

[33] Iwasaki, S. *On finite groups with exactly two real conjugate classes.* Arch. Math. (Basel) **33(6)** (1979) 512-517.

[34] Kazarin, L.S. *Burnside p^α-lemma.* Mathemat Notes 48 (1990), translated from Matematicheskie Zamatki **48** (1990), 45-48.

[35] Kazarin, L.S. *On groups with isolated conjugacy classes.* Izv. Vyssh. Uchebn. Zaved. Mat. **7** (1981) 40-45.

[36] Knoche, H.G. *Uber den Frobenius'schen Klassengegriff in nilpotent Grouppen.* Math. Z. **55** (1951) 71-83.

[37] Li, S. *Finite groups with exactly two class lengths of elements of prime power order.* Arch. Math (Basel) **67** (1996) no. 2 100-105.

[38] Li, S. *On the class length of elements of prime power order in finite groups.* Guangxi Sci. **6** (1999) no. 1 12-13.

[39] Liu, X., Wang, Y., Wei, H. *Notes on the length of conjugacy classes of finite groups.* J. Pure Appl. Algebra **196** (2005) no 1, 111-117.

[40] Navarro, G.,Sanus L. *Rationality and normal 2-complements.* J. Algebra **320** (2008) no 6 2451-2454.

[41] Ninomiya, Y. *Structure of p-solvable groups with three p-regular classes.* Canad. J. Math. **43** (1991) no 3 559-579.

[42] Ninomiya, Y. *Structure of p-solvable groups with three p-regular classes II.* Math. J. Okayama Univ. **35** (1993) 29-34.

[43] Ren, Y.C. *On the length of p-regular classes and the p-structure of finite groups.* Algebra Colloq. **2** (1995) no 1 3-10.

[44] Rebmann, J. *F-Gruppen.* Arch. Math. (Basel) **22** (1971) 225-230.

[45] Rose, J.S. *A course on Group Theory.* Dover First Edition. New York(1994)

[46] Robinson, J.S. *A course in the Theory of Groups.* Graduate Texts in Mathematics 80. Second Edition. Springer-Verlag. Berlin-Heidelberg-New York (1995).

[47] Sylow, M.L. *Théorèmes sur les groupes de substitutions.* Math. Ann. **5** (1872) no 4 584-594.

Notación

G, N,H,L,K	denotan siempre grupos finitos
A, X, Y	denotan siempre conjuntos finitos
$o(g)$	orden de un elemento de un grupo
$\|X\|$	número de elementos en el conjunto X
$\|G\|$	orden del grupo G
$Y \subseteq X$	Y es un subconjunto de X
$H \leq G$	H es un subgrupo de G
$H < G$	H es un subgrupo propio de G
$K \trianglelefteq G$	K es un subgrupo normal de G
gH	coclase izquierda de H en G conteniendo $g \in G$
$\|G : H\|$	el índice de H en G (donde $H \leq G$); número de coclases de H en G
$\psi : X \Longrightarrow Y$	ψ es una aplicación del conjunto X en el conjunto Y
$G_1 \cong G_2$	los grupos G_1 y G_2 son isomorfos
p	un número primo
p'	conjunto de números primos distintos de p
π	un conjunto de números primos
π'	el conjunto de números primos que no pertenecen a π
p-número	entero positivo divisible únicamente por el primo p
p'-número	entero positivo no divisible por el primo p
$\mathbb{Z}^+$	el conjunto de los números enteros positivos
(a, b)	máximo común divisor de los enteros a y b
G/K	grupo cociente de G por K (donde $K \trianglelefteq G$)
$C_G(x)$	centralizador de x en G, donde $x \in G$
$C_G(A)$	centralizador de A en G, donde $A \subseteq G$
$C_G(H)$	centralizador de H en G, donde $H \leq G$
$C_G(H/K)$	centralizador de H/K en G (donde $K \trianglelefteq G$ y $K \leq H \leq G$)
$N_G(A)$	normalizador de A en G, donde $A \subseteq G$
$N_G(H)$	normalizador de H en G, donde $H \leq G$

$\mathbf{Z}(G)$	centro de G
$O_p(G)$	p-radical de G, para un cierto primo p
$O^p(G)$	p-residual de G
F(G)	subgrupo Fitting de G
$\langle H, K \rangle$	subgrupo generado por la unión de los subgrupos H y K de G
$X \times Y$	producto cartesiano de los conjuntos X e Y
HK	subgrupo generado por el producto de los subgrupos H y K de G
$H \times K$	producto directo de los subgrupos H y K
$G_1 \times G_2 \times ... \times G_n$	producto directo de los grupos G_1, G_2, ... , G_n
$\langle X \rangle$	subgrupo de G generado por X ($\subseteq G$)
$\langle x_1, ..., x_n \rangle$	subgrupo generado por los elementos $\{x_1, ..., x_n\}$
$[g_1, g_2] = {g_1}^{-1} {g_1}^{g_2}$	conmutador de los elementos g_1 y g_2 de G
$[H, K]$	subgrupo conmutador de G, generado por los elementos $\{[h,k] : h \in H, k \in K\}$
G'	grupo derivado de G
$x^g = g^{-1}xg$	x conjugado g, donde x y g son elementos de G
x^G	clase de conjugación de x en G; es el conjunto $\{x^g \ , g \in G\}$
$K^g = g^{-1}Kg$	conjugado de K por g (donde $K \leq G$, $g \in G$)
$\lvert G : C_G(x) \rvert = \lvert x^G \rvert$	el índice del centralizador $C_G(x)$ en G, también denota el tamaño de la clase de conjugación de x en G
$G_{p'}$	conjunto de elementos p-regulares de G; es decir, elementos cuyo orden es un p'-número
$cs(G)$	conjunto de los tamaños de clase de conjugación de elementos de G
$cs_{p'}(G)$	conjunto de los tamaños de clase de conjugación de elementos de $G_{p'}$
$Stab_G(x)$	estabilizador en G de $x \in X$, donde G actúa sobre X
$Orb(x)$	la órbita de x bajo la acción de G sobre X, siendo $x \in X$
G', G'', G''',... , $G^{(n)}$	términos de la serie derivada de G
Q_8	grupo quaternio de orden 8