UNIVERSIDAD
POLITECNICA
DE VALENCIA

Clases de conjugación y grupos factorizados

Trabajo Fin de Máster
Máster en Investigación Matemática

Autor:
Víctor Manuel Ortiz Sotomayor

Dirigido por:
María José Felipe Román
Ana Martínez Pastor

Valencia, julio de 2015.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a las profesoras Ana Martínez y María José Felipe, tutoras de este proyecto, por la motivación y orientación que en todo momento me han brindado durante el desarrollo de este trabajo. Ana y María José han sabido encontrar en sus agendas el tiempo y la dedicación que esta tarea requiere.

Agradecer también a todos los docentes que me han acompañado durante este último año, afianzando mi formación como estudiante universitario.

Necesitamos unas supermatemáticas en las que las operaciones sean tan desconocidas como las cantidades sobre las que operan, y un supermatemático que no sepa qué está haciendo cuando realiza esas operaciones. Esas supermatemáticas son la teoría de grupos.

Sir Arthur Stanley Eddington

Índice general

Resumen

Un clásico problema en la Teoría de Grupos Finitos es el estudio de cómo los tamaños de las clases de conjugación influyen sobre la estructura del grupo. En las últimas décadas, numerosos investigadores han obtenido nuevos avances en esta línea. Concretamente, se han obtenido recientemente resultados interesantes a partir de la información proporcionada por los tamaños de clase de algún subconjunto de elementos del grupo tales como: elementos de orden primo, elementos reales, elementos p-regulares, etc.

Por otra parte, en los últimos años, el estudio de grupos factorizados como producto de subgrupos ha sido objeto de creciente interés. En particular, diversos autores han analizado grupos factorizados en los que diferentes familias de subgrupos de los factores satisfacen ciertas condiciones de permutabilidad (ver [4]).

En este trabajo se pretende conjugar ambas perspectivas de actualidad en la teoría de grupos. Así, en este contexto, el objetivo es analizar resultados acerca de la estructura global de un grupo factorizado a partir de los tamaños de clases de algunos de los elementos de sus factores. Una primera aproximación en esta línea puede encontrarse en [3] y [16]. En este trabajo, partiendo del análisis de dichos artículos, probaremos algunos resultados originales que hemos obtenido.

Consideramos al lector familiarizado con los conceptos y resultados básicos de la teoría general de grupos. El trabajo consta de cuatro capítulos. En el capítulo 1 vamos a recopilar algunos resultados preliminares de grupos, necesarios para el seguimiento de los resultados principales, los cuales desarrollaremos en los capítulos 2, 3 y 4. En estos resultados preliminares nos centraremos, sobre todo, en clases de grupos, clases de conjugación y productos de grupos.

A continuación, en el capítulo 2, veremos resultados relativos a la estructura de grupos factorizados con ciertos tamaños de clases de conjugación no divisibles por un número primo. En el capítulo 3, presentamos algunos resultados sobre la estructura de grupos factorizados con ciertos tamaños de clases de conjugación libres de cuadrados. Segui-

damente, en el capítulo 4, analizaremos la estructura de grupos factorizados con ciertos tamaños de clases de conjugación potencias de primos. Destacar que, en estos dos últimos capítulos, probaremos algunos resultados originales que hemos obtenido relativos a los tópicos comentados anteriormente.

Finalmente, recogemos en un apéndice algunos ejemplos de los resultados vistos en los capítulos anteriores, apoyándonos en el sistema algebraico computacional GAP, que pueden ayudarnos a entender mejor las propiedades estructurales obtenidas. El trabajo finaliza con dos secciones, en las que recogemos la bibliografía y la notación utilizada.

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

Antecedentes históricos

Este año de estudio del Máster en Investigación Matemática finaliza con el presente trabajo, el cual está enmarcado dentro de la teoría general de grupos finitos y, concretamente, en el estudio de la estructura global de un grupo factorizado a partir de los tamaños de clases de conjugación de ciertos elementos de sus factores.

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, llevadas a cabo por N.G. Abel (1802-1829) y finalmente resuelto por E. 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 mayor o igual que 5. Definió para cada ecuación de grado n un grupo, actualmente conocido como grupo de Galois de la ecuación, y demostró que solamente 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 abelianos.

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, al-

canzando 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 alemán 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 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 (euclidiana, 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, la cual 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, etc. 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 el capítulo 2. Recientemente, nuevas líneas 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.

El estudio estructural de un grupo finito que puede ser factorizado como producto de un número finito de subgrupos permutables por parejas también es de notable interés. El origen de dicha teoría puede remontarse hasta el año 1903, cuando Burnside publicó su bien conocido lema p^α; descubrió que un grupo finito no puede ser simple si se factoriza como producto de un subgrupo de Sylow y el centralizador de un elemento no trivial. Un año más tarde, utilizó este resultado para demostrar su célebre teorema $p^\alpha q^\beta$, sobre la resolubilidad de grupos finitos cuyo orden es divisible por un máximo de dos números primos, que es también un teorema sobre grupos factorizados.

Los primeros trabajos de Burnside fueron seguidos por Hall en la década 1928-1937, en una gran secuencia de trabajos que establecieron la teoría básica de los grupos finitos resolubles. Dichos trabajos determinaron la dirección en la investigación de grupos finitos resolubles durante muchos años y, probablemente, proporcionaron una buena motivación para un nuevo campo de investigación en la teoría de grupos factorizados. Descubrió que un grupo finito es resoluble si, y solo si, es el producto de subgrupos de Sylow permutables por parejas. Pero fue en un corto artículo de Itô en 1955 en el cual se puso en movimiento la teoría de productos. Él demuestra que cualquier grupo (no necesariamente finito) es metabeliano siempre que sea el producto de dos subgrupos abelianos.

Después de la aparición del teorema de Itô y motivado por los resultados de Burnside y Hall, la atención se desplazó hacia los grupos finitos que son producto de subgrupos nilpotentes, siendo conjeturado que tales grupos serían resolubles. En 1958, Wielandt lo confirma en el caso coprimo y Kegel en el caso general en 1962. El resultado de esta investigación se conoce hoy en día como el teorema de Kegel y Wielandt: todo grupo finito que se factorice como producto de dos subgrupos nilpotentes es resoluble. Sin embargo, no se sabe si el teorema de Kegel y Wielandt puede extenderse a grupos infinitos.

En el caso especial de que los factores son normales y nilpotentes, entonces el producto es nilpotente. Es un resultado bien conocido de Fitting. Sin embargo, el producto de dos subgrupos normales y superresolubles no tiene porqué ser superresoluble, ni en el caso finito.

Un camino natural de la investigación se abre cuando uno se pregunta cómo la estructura de los factores afecta a la estructura del grupo factorizado, cuando están conectados por ciertas condiciones de permutabilidad: surgen así los conceptos de productos totalmente y mutuamente permutables.

Como hemos comentado en el resumen, el objetivo principal de este trabajo es analizar resultados acerca de la estructura global de un grupo factorizado a partir de los tamaños de clase de ciertos elementos de sus factores. Por poner un ejemplo de uno de los resultados que obtendremos, partiendo de la base de que el producto de dos subgrupos normales y superresolubles puede no ser superresoluble, veremos que con ciertas condiciones de permutabilidad de los factores de un grupo factorizado y otras sobre los tamaños de clase de algunos elementos de los factores, el grupo sí que será superresoluble (ver [3] y [16]).

Capítulo 1

Resultados preliminares

Como hemos comentado en el resumen, este capítulo está destinado a realizar una recopilación de algunos resultados preliminares de grupos, necesarios para el seguimiento de los resultados principales del trabajo, los cuales desarrollaremos en los capítulos 2, 3 y 4. Concretamente, nos centraremos sobre todo en resultados sobre clases de grupos, clases de conjugación y productos de grupos.

En la mayoría de ellos omitiremos la demostración, por ser resultados estándares en la teoría general de grupos (el lector podrá hallar todos los detalles sobre sus pruebas en [8], [14], [15], [19], [20] o [21]).

Mencionar también que la notación utilizada es la estándar en este contexto. Aún así, al final de la presente memoria, dedicamos una sección exclusivamente a ello, donde el lector podrá consultar cualquier duda.

1.1. Definiciones y propiedades básicas de grupos

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

Lema 1.1.1. *Sea G un grupo finito y $U \leqslant G$ tal que $G = \bigcup_{g \in G} U^g$. Entonces $G = U$.*

Otra propiedad elemental que aparecerá en capítulos posteriores es la siguiente.

Lema 1.1.2 ([15], Corolario X.12). *Sean H, K subgrupos de un grupo finito G y supongamos que $(|G : H|, |G : K|) = 1$. Entonces $G = HK$.*

Para trabajar con p-elementos, p'-elementos y sus clases de conjugación, es imprescindible conocer la $\{p, p'\}$-factorización de un elemento cualquiera del grupo.

Lema 1.1.3 ([12], Lema 19.6). *Sea G un grupo finito, $g \in G$ y $p \in \mathbb{N}$ un número primo divisor de $|G|$. Entonces, existen dos elementos únicos g_p y $g_{p'}$ en G tales que:*

1. *g_p es p-elemento.*
2. *$g_{p'}$ es p'-elemento.*
3. *$g = g_p g_{p'} = g_{p'} g_p$.*

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

Vamos a ver ahora unas propiedades básicas del subgrupo de Frattini, las cuales nos serán de utilidad posteriormente (el lector podrá hallar todos los detalles sobre sus pruebas en [8]).

Lema 1.1.4 ([8], A - Teorema 9.2). *Sea G un grupo finito. Entonces:*

1. *Si $H \leqslant G$ tal que $G = H\Phi(G)$, entonces $G = H$.*
2. *Si $N \trianglelefteq G$ con $N \not\leqslant \Phi(G)$, entonces existe $U < G$ tal que $G = UN$.*
3. *Si $N \trianglelefteq G$ y $H \leqslant G$ tal que $N \leqslant \Phi(H)$, entonces $N \leqslant \Phi(G)$.*
4. *Si $N \trianglelefteq G$, entonces $\Phi(N) \leqslant \Phi(G)$ y $\Phi(G)N/N \leqslant \Phi(G/N)$. Es más, si $N \leqslant \Phi(G)$, entonces $\Phi(G)/N = \Phi(G/N)$.*
5. (Gaschütz) *Si $N \trianglelefteq G$ con N abeliano tal que $N \cap \Phi(G) = 1$, entonces N es complementado en G, i.e., existe $K \leqslant G$ tal que $G = KN$ con $K \cap N = 1$.*

Lema 1.1.5 ([8], A - Teorema 9.3). *Sea G un grupo finito. Entonces:*

1. *$\Phi(G)$ es nilpotente. En particular, $\Phi(G) \leqslant \mathrm{F}(G)$.*
2. *Si $N \trianglelefteq G$ con $N \leqslant \Phi(G)$, entonces $\mathrm{F}(G/N) = \mathrm{F}(G)/N$.*

En el siguiente lema, recogemos algunas propiedades básicas de conmutadores, las cuales nos serán de mucha utilidad. A lo largo de todo el trabajo, usaremos dichas propiedades sin mencionarlas.

Lema 1.1.6 ([8], A - Lema 7.4). *Sean $A, B, C \leqslant G$. Entonces:*

1. $[A, B] = [B, A] \trianglelefteq \langle A, B\rangle$.
2. $[A, B] \leqslant A$ *si, y solo si,* $B \leqslant \mathrm{N}_G(A)$.
3. *Si* A car G *y* B car G, *entonces* $[A, B]$ car G.
4. *Si* $N \trianglelefteq G$, *entonces* G/N *es abeliano si, y solo si,* $G' \leqslant N$.
5. *Si* A *y* C *son normalizados por* B, *entonces* $[AB, C] = [A, C] \cdot [B, C]$.
6. *Si* $N \trianglelefteq G$ *y* $g \in G$, *entonces* $[N, \langle g\rangle] = [N, g]$.

Pasamos ahora a recordar brevemente algunos conceptos de acciones de grupos. Dado G un grupo y X un conjunto no vacío, decimos que G **actúa (por la derecha)** sobre el conjunto X si existe una aplicación

$$\begin{array}{rccc} \varphi: & X \times G & \longrightarrow & X \\ & (x, g) & \longmapsto & x \cdot g, \end{array}$$

verificando

1. $x \cdot 1_G = x$, para todo $x \in X$.
2. $x \cdot (g_1 g_2) = (x \cdot g_1) \cdot g_2$, para todo $g_1, g_2 \in G$ y $x \in X$.

De una manera similar podemos definir la acción *por la izquierda*. En este contexto, diremos que una acción es **transitiva** si para todo $x, y \in X$, existe un $g \in G$ tal que $x \cdot g = y$. Por otro lado, diremos que la acción es **fiel** si para todo $1 \neq g \in G$, existe $x \in X$ tal que $x \cdot g \neq x$.

Recordemos que la acción de G sobre X queda completamente determinada por el siguiente homomorfismo (ver Teoremas 4.3 y 4.4 de [20]):

$$\begin{array}{rcccccc} \phi: G & \longrightarrow & \Sigma_{|X|} & & & & \\ g & \longmapsto & \phi(g): & X & \longrightarrow & X & \\ & & & x & \longmapsto & x \cdot g. & \end{array} \tag{1.1}$$

Si $\mathrm{Ker}(\varphi) = 1$ (o, equivalentemente, si la acción es fiel), por el primer teorema de isomorfía, tenemos que $G \lessapprox \Sigma_{|X|}$ y denominaremos a G **subgrupo de permutaciones** de X.

Supongamos, como caso particular, que el conjunto X anterior es ahora un grupo (lo denotaremos H a partir de ahora). En este caso, es natural requerir que para todo $g \in G$, la aplicación $\phi(g) : H \longrightarrow H$ no solo sea una permutación de H, sino que sea un automorfismo de él. Claramente, al ser ya inyectiva y suprayectiva, basta con que sea homomorfismo o, equivalentemente, que cumpla que $(h_1h_2)^g = h_1^g h_2^g$, para todo $h_1, h_2 \in H$ (notar que h^g es simple notación de acción, en este caso).

Así, diremos que G **actúa vía automorfismos** sobre H si G actúa sobre H como conjunto y, además, $(h_1h_2)^g = h_1^g h_2^g$, para todo $h_1, h_2 \in H$ y $g \in G$. Al igual que la acción de un grupo G sobre un conjunto X quedaba totalmente determinada por el homomorfismo $\varphi : G \longrightarrow \Sigma_{|X|}$, también se cumple que una acción de G vía automorfismos sobre H queda totalmente determinada por el homomorfismo $\rho : G \longrightarrow \mathrm{Aut}(H)$ (ver Teoremas 9.3 y 9.4 de [20]).

Consideremos ahora que G actúa vía automorfismos sobre H y que N, K son subgrupos de H G-invariantes (invariantes bajo la acción de G), de tal forma que $N \trianglelefteq K$. Entonces, siempre podemos considerar el homomorfismo

$$\begin{array}{rccccccc} \rho: & G & \longrightarrow & \mathrm{Aut}(K/N) & & & & \\ & g & \longmapsto & \rho(g) := \rho_g: & K/N & \longrightarrow & K/N \\ & & & & kN & \longmapsto & k^g N, \end{array}$$

para todo $k \in K$. Llamaremos a la imagen de ρ el **grupo de automorfismos inducidos por G** sobre K/N, y lo denotaremos por $\mathbf{Aut_G(K/N)}$. Notemos que, en general, $\mathrm{Aut}_G(H) \leqslant \mathrm{Aut}(H)$. Además, como $\mathrm{Ker}(\rho) = \mathrm{C}_G(K/N)$, por el primer teorema de isomorfía, tenemos que

$$G/\mathrm{C}_G(K/N) \cong \mathrm{Aut}_G(K/N).$$

Nota 1.1.7. Notemos que, en el caso particular de que tengamos $N \trianglelefteq G$, por todo lo que acabamos de ver (G siempre actúa vía automorfismos sobre él mismo), podemos asegurar que

$$G/\mathrm{C}_G(N) \cong \mathrm{Aut}_G(N).$$

Este hecho será usado en los próximos capítulos (ver Nota 3.2.4). Por otro lado, en ocasiones, la acción coprima (acción entre dos grupos de órdenes coprimos) se puede utilizar para obtener una factorización del grupo o la estructura de determinados subgrupos del grupo. El siguiente resultado, conocido como el lema de Fitting, recoge una de las propiedades de la acción coprima que utilizaremos en resultados posteriores.

Teorema 1.1.8 (Fitting - [13], Teorema 14.5). *Sea A un grupo que actúa sobre otro grupo G abeliano. Si $(|G|, |A|) = 1$, entonces*

$$G = \mathrm{C}_G(A) \times [G, A].$$

1.2. Resultados sobre clases de grupos

A lo largo de toda la memoria, vamos a trabajar con grupos que cumplen una cierta propiedad especial, como los grupos abelianos, resolubles, nilpotentes, *superresolubles*, etc. Así, destinamos esta sección a hacer un recopilatorio de las definiciones y propiedades básicas de dichos grupos. La mayoría de conceptos y resultados que vamos a ver, están extraídos de [8], donde el lector podrá profundizar más detalladamente. Mencionar que, a lo largo de toda la memoria, usaremos dichas propiedades sin referencia alguna.

Definición 1.2.1. Sea G un grupo finito. Decimos que G es **resoluble** si posee una serie subnormal con factores abelianos, i.e., si existe una serie de la forma

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_n = G,$$

donde N_i/N_{i-1} es abeliano, para todo $1 \leq i \leq n$.

Por otra parte, dado $p \in \mathbb{N}$ un número primo, decimos que G es ***p*-resoluble** si posee una serie subnormal con p-factores o p'-factores, i.e., si existe una serie de la forma

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_n = G,$$

donde N_i/N_{i-1} es p-grupo o p'-grupo, para todo $1 \leq i \leq n$.

Observemos que un grupo es p-resoluble si, y solo si, es p'-resoluble. En el siguiente lema, recogemos las propiedades más elementales de estos grupos.

Lema 1.2.2 ([8], A - Teorema 10.2). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo.*

1. *Sea $H \leqslant G$ y $N \trianglelefteq G$. Si G es p-resoluble, entonces H y G/N son también p-resolubles.*
2. *Si $N \trianglelefteq G$ con N y G/N p-resolubles, entonces G es p-resoluble.*
3. *Si $N_i \trianglelefteq G$ con G/N_i p-resoluble para $i = 1, 2$, entonces $G/(N_1 \cap N_2)$ es p-resoluble.*

4. *G es p-resoluble si, y solo si, $G/\Phi(G)$ es p-resoluble.*

5. *G es resoluble si, y solo si, G es p-resoluble para todo $p \in \mathbb{P}$ divisor de $|G|$.*

Mencionar que las cuatro primeras propiedades del resultado anterior también son válidas para grupos resolubles, como consecuencia del apartado 5. Otra propiedad que nos será útil posteriormente es la siguiente.

Lema 1.2.3 ([8], A - Teorema 10.6). *Sea G un grupo finito. Si G es resoluble o p-resoluble con $\mathrm{O}_{p'}(G) = 1$, entonces tenemos que*

$$\mathrm{F}(G)/\Phi(G) = \mathrm{Soc}(G/\Phi(G)).$$

Mencionar que los grupos p-resolubles los podemos ver como un caso particular de los grupos π-*separables*, cuando $\pi = \{p\}$.

Definición 1.2.4. Sea G un grupo finito. Dado $\pi \subseteq \mathbb{P}$, decimos que G es un **π-grupo** si $|G|$ es un π-número. Análogamente, diremos que G es un **π'-grupo** si $|G|$ es un π'-número.

Dado $\pi \subseteq \mathbb{P}$, decimos que G es **π-separable** si posee una serie subnormal con π-factores o π'-factores, i.e., si existe una serie de la forma

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_n = G,$$

donde N_i/N_{i-1} es π-grupo o π'-grupo, para todo $1 \leq i \leq n$.

Por tanto, queda claro que hablar de p-separabilidad es equivalente a hablar de p-resolubilidad y que un grupo es π-separable si, y solo si, es π'-separable.

En el siguiente resultado, recopilamos algunas propiedades de estos grupos.

Lema 1.2.5 ([15], Capítulo 3 - Sección D). *Sea G un grupo finito y sea $\pi \subseteq \mathbb{P}$.*

1. *Si $H \leqslant G$ con G π-separable, entonces H es π-separable.*

2. *Si $N \trianglelefteq G$ con G π-separable, entonces G/N es π-separable.*

3. *Si G es resoluble, entonces G es π-separable, para todo π.*

4. *Si $G > 1$ con G π-separable, entonces $\mathrm{O}_{\pi}(G) > 1$ ó $\mathrm{O}_{\pi'}(G) > 1$.*

Aprovechamos este momento para recordar la definición y las propiedades más básicas de los π-*subgrupos de Hall.*

Definición 1.2.6. Dado $\pi \subseteq \mathbb{P}$ y $H \leqslant G$, diremos que H es un **π-subgrupo de Hall** de G si $|H|$ es un π-número y $|G:H|$ es un π'-número.

Lema 1.2.7 ([8], I - Lema 3.2). *Sea $H \in \mathrm{Hall}_\pi(G)$ y $N \trianglelefteq G$. Entonces:*

1. *$H^g \in \mathrm{Hall}_\pi(G)$, para todo $g \in G$.*
2. *$HN/N \in \mathrm{Hall}_\pi(G/N)$.*
3. *$H \cap N \in \mathrm{Hall}_\pi(N)$.*

Un grupo G que posea π-subgrupos de Hall, siendo todos ellos conjugados en G y cumpliendo que cada π-subgrupo de G está contenido en un π-subgrupo de Hall de G, lo denominaremos **D_π-grupo**. Destacar que una de las propiedades más importantes de un grupo π-separable viene dada por el siguiente hecho:

Lema 1.2.8 ([19], 9.1.6). *Si un grupo finito G es π-separable, entonces G es un D_π-grupo.*

Es más, por lo visto anteriormente, si G es resoluble, entonces G es también un D_π-grupo, para todo π. Otra propiedad que nos será útil posteriormente es la siguiente.

Lema 1.2.9 ([15], Teorema 3.21). *Sea G un grupo π-separable con $\mathrm{O}_{\pi'}(G) = 1$. Entonces, tenemos que*

$$\mathrm{C}_G(\mathrm{O}_\pi(G)) \leqslant \mathrm{O}_\pi(G).$$

En el capítulo 3, veremos resultados que nos darán condiciones para que un grupo sea *p-nilpotente*.

Definición 1.2.10. Sea G un grupo finito. Dado $p \in \mathbb{N}$ un número primo, decimos que G es **p-nilpotente** si tiene p-complemento normal, es decir, si existe $N \trianglelefteq G$ con $|N|$ un p'-número tal que $G = NP$, con $P \in \mathrm{Syl}_p(G)$.

Notemos que, en el contexto de la definición anterior, también tenemos que G es el producto semidirecto del p'-radical $\mathrm{O}_{p'}(G)$ con un p-subgrupo de Sylow de G o, equivalentemente, se cumple que $\mathrm{O}^p(G) = \mathrm{O}_{p'}(G)$. Destacar también que podemos ver fácilmente que todo grupo p-nilpotente es p-resoluble.

La mayoría de las propiedades de clausura de los grupos nilpotentes se cumplen también para los grupos p-nilpotentes, como recogemos en el siguiente resultado.

Lema 1.2.11 ([8], A - Teorema 13.4). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo.*

1. *Si G es p-nilpotente, entonces también lo es cualquier subgrupo y cociente de G.*
2. *Si $N_i \trianglelefteq G$ con G/N_i p-nilpotente para $i = 1, 2$, entonces $G/(N_1 \cap N_2)$ es p-nilpotente.*
3. *Si $G/\Phi(G)$ es p-nilpotente, entonces G es p-nilpotente.*

También veremos, en el Capítulo 3, resultados que nos darán condiciones acerca de la *superresolubilidad* de un grupo. Así, pasamos a recopilar las definiciones y propiedades más elementales, las cuales hemos extraído de [5], en su mayoría.

Definición 1.2.12. Sea G un grupo finito. Decimos que G es **superresoluble** si posee una serie normal con factores cíclicos, i.e., si existe una serie de la forma

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_n = G,$$

donde $N_i \trianglelefteq G$ y N_i/N_{i-1} es cíclico, para todo $1 \leq i \leq n$.

Dado $p \in \mathbb{N}$ un número primo, decimos que G es ***p*-superresoluble** si posee una serie normal con p-factores cíclicos de orden p o p'-factores, i.e., si existe una serie de la forma

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_n = G,$$

donde $N_i \trianglelefteq G$ y N_i/N_{i-1} es cíclico de orden p o p'-grupo, para todo $1 \leq i \leq n$.

Mencionar que, equivalentemente, puede definirse un grupo superresoluble como aquel que posee una serie normal con factores cíclicos de orden primo. Queda claro que todo grupo superresoluble es resoluble pero, es más, también se cumple que todo grupo nilpotente es superresoluble.

En el siguiente teorema, reunimos las propiedades más elementales de estos grupos.

Teorema 1.2.13. *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo. Entonces:*

1. *Si $H \leqslant G$ y $N \trianglelefteq G$ con G p-superresoluble, entonces H y G/N son p-superresolubles.*
2. *El producto directo de grupos p-superresolubles es p-superresoluble.*
3. *Si $N_i \trianglelefteq G$ con G/N_i p-superresoluble para $i = 1, 2$, entonces $G/(N_1 \cap N_2)$ es p-superresoluble.*

4. *$G/\Phi(G)$ es p-superresoluble si, y solo si, G es p-superresoluble.*
5. *G es superresoluble si, y solo si, G es p-superresoluble para todo $p \in \mathbb{P}$ divisor de $|G|$.*
6. *Si $N \trianglelefteq G$ con N cíclico de orden p o p'-grupo y G/N es p-superresoluble, entonces G es p-superresoluble.*

Destacar que las cuatro primeras propiedades del resultado anterior también son ciertas para grupos superresolubles, como consecuencia del apartado 5.

Teorema 1.2.14. *Sea G un grupo finito. Entonces:*

1. *Si $N \trianglelefteq G$ con N cíclico y G/N superresoluble, entonces G es superresoluble.*
2. *Si G es superresoluble, entonces G' es nilpotente.*

Destacar que en los grupos superresolubles no se da la propiedad extensiva, es decir, no es suficiente que N y G/N sean superresolubles para que lo sea G (a diferencia de los grupos resolubles), como podíamos intuir por el apartado 1 del resultado anterior.

Ejemplo 1.2.15. Observemos el caso del grupo Σ_4: por un lado, tenemos que $|\Sigma_4/V_4| = 6$, luego Σ_4/V_4 es isomorfo a un C_6 o a Σ_3, siendo ambos superresolubles; por otro lado, V_4 también es superresoluble trivialmente. Sin embargo, Σ_4 no es superresoluble, pues la única serie normal posible es $1 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq \Sigma_4$ y V_4 no es cíclico. ■

Todos los tipos de grupos estudiados anteriormente pueden analizarse desde una perspectiva común: la teoría de *clases*. Dicha teoría estudia colecciones de grupos que verifican una cierta propiedad común, la cual es invariante por isomorfismos.

Definición 1.2.16. Una **clase de grupos** es una colección de grupos $\mathfrak{X}$ con la siguiente propiedad: si $G \in \mathfrak{X}$ y $H \cong G$, entonces $H \in \mathfrak{X}$.

Algunos ejemplos de clases de grupos son los siguientes:

- $\mathfrak{S}_p := \{G \ : \ G \text{ es } p\text{-resoluble}\}$
- $\mathfrak{N}_p := \{G \ : \ G \text{ es } p\text{-nilpotente}\}$
- $\mathfrak{U}_p := \{G \ : \ G \text{ es } p\text{-superresoluble}\}$
- $\mathfrak{A} := \{G \ : \ G \text{ es abeliano}\}$
- $\mathfrak{MA} := \{G \ : \ G/\mathrm{F}(G) \text{ es abeliano}\}$
- $\mathfrak{E}_p := \{G \ : \ G \text{ es } p\text{-elemental abeliano}\}$
- $\mathfrak{S} := \{G \ : \ G \text{ es resoluble}\}$
- $\mathfrak{N} := \{G \ : \ G \text{ es nilpotente}\}$
- $\mathfrak{U} := \{G \ : \ G \text{ es superresoluble}\}$
- $\mathfrak{P}_p := \{G \ : \ G = \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G)\}$
- $\mathfrak{P}_\pi := \{G \ : \ G = \mathrm{O}_\pi(G) \times \mathrm{O}_{\pi'}(G)\}$

Otro ejemplo de clase de grupos no tan elemental y con la que trabajaremos posteriormente es la siguiente:

$$\cdot\, \mathfrak{H}_p := \{G \,:\, |P| \leq p, \text{ con } P \in \mathrm{Syl}_p(H/K), \forall\, H/K \text{ factor principal de } G\}$$

En la literatura, a los grupos de la clase $\mathfrak{P}_\pi$ también los denominan grupos **π-descomponibles**. Notemos que la clase $\mathfrak{P}_p$ es un caso particular de la clase $\mathfrak{P}_\pi$, cuando $\pi = \{p\}$.

Por otro lado, el lector también podrá encontrar definida la clase $\mathfrak{MA}$ de la siguiente manera:

$$\cdot\, \mathfrak{MA} := \{G \,:\, \exists\, N \trianglelefteq G \text{ con } N \text{ nilpotente y } G/N \text{ abeliano}\}$$

Esto es así debido a que, formalmente, estamos hablando de un *producto de clases*. No profundizaremos sobre ello en la presente memoria, aunque el lector podrá hallar todos los detalles en [8]. Lo que sí hemos de observar es que la definición anterior es equivalente a la clase de grupos tales que $G/\mathrm{F}(G)$ es abeliano.

Como caso particular del *producto* de una clase $\mathfrak{X}$ consigo misma, tenemos los grupos G que tienen un subgrupo normal N tal que N y G/N pertenecen a $\mathfrak{X}$. En tal caso, decimos que G es **meta-$\mathfrak{X}$**. Por ejemplo, los grupos que poseen un subgrupo normal N tal que N y G/N son cíclicos, decimos que son grupos **metacíclicos**. Una propiedad importante, que aparecerá en el Capítulo 3, es la siguiente.

Teorema 1.2.17 ([19], 10.1.10). *Sea G un grupo finito. Si G tiene todos sus subgrupos de Sylow cíclicos, entonces G es metacíclico.*

Finalmente, vamos a ver el concepto de *formación* (*saturada*), el cual usaremos a menudo en los próximos capítulos.

Definición 1.2.18. Dada $\mathfrak{X}$ una clase de grupos, diremos que $\mathfrak{X}$ es una **formación** si verifica las siguientes dos condiciones:

1. Para todo grupo $G \in \mathfrak{X}$ y $N \trianglelefteq G$, se cumple que $G/N \in \mathfrak{X}$.

2. Si $N_1 \trianglelefteq G$ y $N_2 \trianglelefteq G$ tales que $G/N_1, G/N_2 \in \mathfrak{X}$, entonces $G/(N_1 \cap N_2) \in \mathfrak{X}$.

Es más, si $G/\Phi(G) \in \mathfrak{X}$ implica que $G \in \mathfrak{X}$, entonces diremos que la formación $\mathfrak{X}$ es **saturada**.

Por las propiedades vistas al principio de esta sección, queda claro que las clases $\mathfrak{S}$, $\mathfrak{S}_p$, $\mathfrak{N}_p$, $\mathfrak{U}$ y $\mathfrak{U}_p$ son ejemplos de formaciones saturadas, por citar alguna de ellas. También puede probarse, sin mucha dificultad, que las clases $\mathfrak{P}_p$ y $\mathfrak{MA}$ son formaciones saturadas o, mediante razonamientos estándares de series principales, que la clase $\mathfrak{H}_p$ es una formación. Un ejemplo de formación no saturada es la clase $\mathfrak{E}_p$ (basta con observar que $D_8/\Phi(D_8) \cong V_4$).

Trabajar con formaciones saturadas tiene muchas ventajas. Por ejemplo, si queremos ver con un argumento inductivo que un determinado grupo G está en una formación saturada y ya sabemos que los cocientes de G están en ella por inducción, podemos suponer que G tiene un único normal minimal. Efectivamente, pues si tuviera dos normales minimales distintos, su intersección sería trivial y, por tanto, G estaría en dicha formación por la propiedad 2. Además, podemos suponer que $\Phi(G) = 1$ pues, en caso contrario, $G/\Phi(G)$ estaría en la formación por inducción y, al ser saturada, G también lo estaría. Es más, en esta situación, si tenemos que G es resoluble, podemos aplicar el siguiente resultado:

Lema 1.2.19. *Si G es un grupo resoluble con $\Phi(G) = 1$ y de manera que posee un único normal minimal N, entonces $\mathrm{F}(G) = N = \mathrm{C}_G(N) = \mathrm{O}_p(G)$, para algún número primo $p \in \mathbb{N}$.*

Demostración. Al ser G resoluble, sabemos que el único normal minimal N es p-elemental abeliano para algún número primo $p \in \mathbb{N}$. Así, N es nilpotente, luego tenemos que $N \leqslant \mathrm{F}(G)$. Veamos que también se cumple que $\mathrm{F}(G) \leqslant \mathrm{C}_G(N)$. Sabemos que

$$\mathrm{Z}(\mathrm{F}(G)) \text{ car } \mathrm{F}(G) \trianglelefteq G,$$

luego $\mathrm{Z}(\mathrm{F}(G)) \trianglelefteq G$ y, en consecuencia, $N \cap \mathrm{Z}(\mathrm{F}(G)) \trianglelefteq G$. Por minimalidad de N, concluimos que $N \cap \mathrm{Z}(\mathrm{F}(G)) = 1$ ó N. El primer caso queda descartado por ser $\mathrm{F}(G)$ nilpotente y $N \trianglelefteq \mathrm{F}(G)$. Así, deducimos que $N \leqslant \mathrm{Z}(\mathrm{F}(G))$ y, por tanto, que $\mathrm{F}(G) \leqslant \mathrm{C}_G(N)$.

Veamos que $C := \mathrm{C}_G(N) = N$, con lo que concluiremos que $N = \mathrm{F}(G) = \mathrm{C}_G(N)$. Tenemos que $N \nleqslant \Phi(G)$ luego, necesariamente, existe $M <\cdot\, G$ tal que $N \nleqslant M$. Luego $M_G = 1$ pues, en caso contrario, $N \leqslant M_G \leqslant M$ y sería una contradicción. Así, tenemos que

$$M \leqslant MN \leqslant G,$$

y por maximalidad de M en G, concluimos que $G = MN$. Pero, al ser N abeliano, tenemos que $N \leqslant C$ y, por la identidad de Dedekind, deducimos que

$$C = C \cap G = C \cap MN = N(C \cap M). \tag{1.2}$$

Pero $C \cap M = 1$ porque $C \cap M \leqslant M$, $M_G = 1$ y $C \cap M \trianglelefteq MN = G$ ya que es centralizado por N y normalizado por M, por ser $C = \mathrm{C}_G(N)$ normal en G, ya que $N \trianglelefteq G$. Concluimos por (1.2) que $C = N$. Finalmente, está claro que $\mathrm{O}_p(G) \leqslant \mathrm{F}(G) = N$ y $N \leqslant \mathrm{O}_p(G)$ al ser N p-elemental abeliano. Esto finaliza la prueba. □

Nota 1.2.20. Por tanto, en un argumento inductivo, si queremos ver que un determinado grupo G está en una formación saturada y ya sabemos que los cocientes de G están en dicha formación saturada por inducción, entonces podemos asumir que G tiene un único subgrupo N normal minimal y que $\Phi(G) = 1$. Además, si G es resoluble, podemos afirmar que $N = \mathrm{F}(G) = \mathrm{C}_G(N) = \mathrm{O}_p(G)$. Este razonamiento será utilizado con mucha frecuencia en los próximos capítulos.

1.3. Resultados sobre clases de conjugación

Como hemos comentado en el resumen, uno de los objetivos del trabajo es conocer la estructura de un grupo a partir de cierta información sobre los tamaños de clase de algunos elementos. En muchas demostraciones, trabajaremos por inducción y en cierto momento necesitaremos afirmar que algún subgrupo normal del grupo hereda las hipótesis del enunciado. En esos momentos, resulta de mucha utilidad el siguiente resultado.

Lema 1.3.1. *Sea G un grupo finito con $N \trianglelefteq G$, $n \in N$ y $g \in G$. Entonces:*

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

$$\mathrm{C}_G(xy) = \mathrm{C}_G(x) \cap \mathrm{C}_G(y).$$

Demostración. 1. Como $N \trianglelefteq G$ y $\mathrm{C}_G(n) \leqslant G$, tenemos que $N\mathrm{C}_G(n) \leqslant G$. Aplicando el teorema de Lagrange sobre la transitividad de índices junto al segundo teorema de isomorfía, podemos ver que

$$\left|n^N\right| = |N : \mathrm{C}_N(n)| = |N : \mathrm{C}_G(n) \cap N| = |N\mathrm{C}_G(n) : \mathrm{C}_G(n)| \;\big|\; |G : \mathrm{C}_G(n)| = \left|n^G\right|,$$

con lo que queda probado el primer apartado.

2. Veamos en primer lugar que $\mathrm{C}_G(g)N/N \leqslant \mathrm{C}_{G/N}(gN)$. Sea $hN \in \mathrm{C}_G(g)N/N$. Entonces $h \in \mathrm{C}_G(g)N$ y, por tanto, existirán $n_1 \in N$ y $g_1 \in \mathrm{C}_G(g)$ tales que $h = g_1 n_1$. Luego $hN = (g_1 n_1)N = (g_1 N)(n_1 N) = g_1 N$, pues $n_1 \in N$.

Además, tenemos que

$$(hN)(gN) = (g_1 N)(gN) = (g_1 g)N = (gg_1)N = (gN)(g_1 N) = (gN)(hN),$$

donde la tercera igualdad se da debido a que $g_1 \in \mathrm{C}_G(g)$. Concluimos que $hN \in \mathrm{C}_{G/N}(gN)$, tal y como queríamos ver.

Así, aplicando el teorema de Lagrange sobre la transitividad de índices, tenemos que

$$\begin{aligned} \left|(gN)^{G/N}\right| &= \left|G/N : \mathrm{C}_{G/N}(gN)\right| \,\big|\, |G/N : \mathrm{C}_G(g)N/N| \\ &= |G : \mathrm{C}_G(g)N| \,\big|\, |G : \mathrm{C}_G(g)| = \left|g^G\right|, \end{aligned}$$

con lo que queda probado el apartado 2.

3. La inclusión $\mathrm{C}_G(x) \cap \mathrm{C}_G(y) \leqslant \mathrm{C}_G(xy)$ es clara. Veamos que también se da la contraria.

Sea $w \in \mathrm{C}_G(xy)$ y supongamos que $r := \mathrm{o}(x)$ y $s := \mathrm{o}(y)$. Entonces $(xy)^w = xy$ y, elevando la ecuación a $\mathrm{o}(y)$, tenemos que $((xy)^w)^s = (xy)^s$. Pero

$$((xy)^w)^s = ((xy)^s)^w = w^{-1}x^s y^s w,$$

ya que x e y conmutan. Así pues, necesariamente tenemos que $(xy)^s = w^{-1}x^s y^s w$, de donde obtenemos que

$$w^{-1}x^s w = x^s, \tag{1.3}$$

pues $\mathrm{o}(y) = s$. De manera análoga, elevando ahora la ecuación a $\mathrm{o}(x)$, obtenemos que

$$w^{-1}y^r w = y^r. \tag{1.4}$$

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

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

De igual forma, obtenemos que $(y^r)^a = y$. Elevando ahora la ecuación (1.3) a b, obtenemos que $(w^{-1}x^s w)^b = (x^s)^b$. Pero, teniendo en cuenta que $(w^{-1}x^s w)^b = w^{-1}(x^s)^b w$ y que acabamos de ver que $x = (x^s)^b$, deducimos que $w^{-1}xw = x$, luego $w \in \mathrm{C}_G(x)$.

De manera totalmente análoga, al elevar la ecuación (1.4) a a, obtenemos que $w \in \mathrm{C}_G(y)$ y, por tanto, $w \in \mathrm{C}_G(x) \cap \mathrm{C}_G(y)$. □

El siguiente resultado nos será de utilidad en los próximos capítulos.

Lema 1.3.2 (Wielandt). *Sea G un grupo finito, $p \in \mathbb{N}$ un número primo y $x \in G$. Si el orden de x y $\left|x^G\right|$ son potencias de p, entonces $x \in \mathrm{O}_p(G)$.*

Demostración. Sea $x \in G$ tal que $\mathrm{o}(x)$ y $\left|x^G\right|$ son potencias de p. Sea $P \in \mathrm{Syl}_p(G)$ tal que $x \in P$. Como $\left|x^G\right| = |G : \mathrm{C}_G(x)|$ es una potencia de p y p no divide a $|G : P|$, por el Lema 1.1.2, tenemos que $G = P\mathrm{C}_G(x)$.

Así, tenemos que

$$\langle x^G \rangle = \langle x^{P\mathrm{C}_G(x)} \rangle = \langle x^P \rangle \leqslant P,$$

pues $x \in P$. Además, como $\langle x^G \rangle \trianglelefteq G$, concluimos que $x \in \langle x^G \rangle \leqslant \mathrm{O}_p(G)$. □

En el siguiente resultado, Kazarin extiende, usando teoría modular de representaciones, el célebre teorema de Burnside sobre la no simplicidad de grupos con tamaños de clase que son potencias de números primos.

Teorema 1.3.3 (Kazarin - [13], Teorema 15.7). *Sea G un grupo finito. Supongamos que existe $1 \neq g \in G$ tal que $\left|g^G\right|$ es potencia de un número primo $p \in \mathbb{N}$. Entonces, $\langle g^G \rangle$ es un subgrupo normal y resoluble de G.*

1.4. Resultados sobre productos de grupos

Esta sección está destinada a hacer un recopilatorio de algunos resultados sobre grupos factorizados como producto de subgrupos que satisfacen ciertas condiciones de permutabilidad. La mayoría de ellos han sido extraídos de [4], donde el lector podrá profundizar más detalladamente.

En el estudio estructural de los grupos factorizados es interesante saber qué subgrupos heredarán la factorización del grupo. Formalicemos en una apropiada definición los subgrupos con esta propiedad.

Definición 1.4.1. Dado un grupo $G = G_1G_2 \cdots G_r$ factorizado como el producto de los subgrupos $G_1, G_2, \ldots, G_r$, diremos que un subgrupo S de G es **prefactorizado** (con respecto a esta factorización) si $S = (S \cap G_1)(S \cap G_2) \cdots (S \cap G_r)$ o, equivalentemente, si todo $s \in S$ puede ser escrito como $s = s_1s_2 \cdots s_r$, con $s_i \in S \cap G_i$ para todo $1 \leq i \leq r$.

El primer resultado que vamos a ver nos dice que en cualquier grupo factorizado como producto de dos subgrupos cualesquiera, siempre existe un p-subgrupo de Sylow prefactorizado, para cada número primo $p \in \mathbb{N}$ divisor del orden del grupo.

Lema 1.4.2. *Sea $G = AB$ el producto de los subgrupos A y B. Entonces, para cada número primo $p \in \mathbb{N}$ divisor del orden de G, existe $P \in \mathrm{Syl}_p(G)$ prefactorizado de la forma $P = (P \cap A)(P \cap B)$, donde $P \cap A \in \mathrm{Syl}_p(A)$ y $P \cap B \in \mathrm{Syl}_p(B)$.*

Demostración. Sea $P_A \in \mathrm{Syl}_p(A)$ y $P_B \in \mathrm{Syl}_p(B)$. Sea también $P_G \in \mathrm{Syl}_p(G)$ tal que $P_A \leqslant P_G$. Luego existe $g \in G$ tal que $P_B \leqslant P_G^g$.

Así, tenemos que $P_A \leqslant P_G \cap A \leqslant A$ y, como $P_A \in \mathrm{Syl}_p(A)$, concluimos que $P_A = P_G \cap A$. Análogamente, también tenemos que $P_B = P_G^g \cap B$.

Pero, como $g \in G = AB$, existen $a \in A$ y $b \in B$ tales que $g = ab$. Por tanto, conjugando con a la igualdad $P_A = P_G \cap A$, tenemos que

$$P_A^a = (P_G \cap A)^a = P_G^a \cap A \in \mathrm{Syl}_p(A),$$

pues P_A^a vuelve a ser un p-subgrupo de Sylow de A. Análogamente, conjugando con b^{-1} la igualdad $P_B = P_G^g \cap B$, llegamos a que

$$P_B^{b^{-1}} = (P_G^{ab} \cap B)^{b^{-1}} = P_G^a \cap B \in \mathrm{Syl}_p(B),$$

ya que $P_B^{b^{-1}}$ vuelve a ser un p-subgrupo de Sylow de B. Definiendo $P := P_G^a \in \mathrm{Syl}_p(G)$, ya tenemos que existe un p-subgrupo de Sylow de G tal que $P \cap A \in \mathrm{Syl}_p(A)$ y $P \cap B \in \mathrm{Syl}_p(B)$. Solo nos queda ver que $P = (P \cap A)(P \cap B)$.

Claramente, tenemos que $(P \cap A)(P \cap B) \subseteq P$, luego $|(P \cap A)(P \cap B)| \leq |P|$. Además, $P \cap A \cap B$ es un p-grupo contenido en $A \cap B$, luego $|P \cap A \cap B| \leq |A \cap B|_p$. Así, tenemos que

$$\begin{aligned} |P| &= |G|_p = \frac{|A|_p \cdot |B|_p}{|A \cap B|_p} = \frac{|P \cap A| \cdot |P \cap B|}{|A \cap B|_p} \\ &\leq \frac{|P \cap A| \cdot |P \cap B|}{|P \cap A \cap B|} = |(P \cap A)(P \cap B)|\,. \end{aligned}$$

Concluimos que $P = (P \cap A)(P \cap B)$ y queda finalizada la demostración. □

Mencionar que el resultado anterior es cierto también para π-subgrupos de Hall, bajo la hipótesis de que G, A y B sean D_π-grupos, con una demostración totalmente análoga a la anterior (ver [1], Lema 1.3.2).

Lema 1.4.3. *Sea $\pi \subseteq \mathbb{P}$ y sea $G = AB$ un grupo finito, producto de los subgrupos A y B. Si A, B y G son D_π-grupos, entonces existe $H \in \mathrm{Hall}_\pi(G)$ tal que $H = (H \cap A)(H \cap B)$ con $H \cap A \in \mathrm{Hall}_\pi(A)$ y $H \cap B \in \mathrm{Hall}_\pi(B)$.*

Notemos que, en el resultado anterior, no hemos necesitado ninguna condición de permutabilidad sobre los factores. Sin embargo, para extenderlo a un grupo G que sea producto de un número arbitrario de subgrupos es necesario añadir una hipótesis de permutabilidad entre los factores, llamada permutabilidad *mutua*, la cual nos aparecerá con frecuencia de aquí en adelante.

Definición 1.4.4. Dados dos subgrupos A y B de un grupo G, diremos que A y B son **mutuamente permutables** si A permuta con todo subgrupo de B y B permuta con todo subgrupo de A. Es decir, $AX = XA$ y $BY = YB$, para todo $X \leqslant B$ e $Y \leqslant A$.

Si $G = AB$ con A y B mutuamente permutables, diremos que G es el **producto mutuamente permutable** de A y B.

Más general, si $G = G_1G_2 \cdots G_r$ con G_i y G_j mutuamente permutables, para todo $i, j \in \{1, 2, \ldots, r\}$, diremos que G es el **producto mutuamente permutable por parejas** (o **dos a dos**) de los subgrupos $G_1, G_2, \ldots, G_r$.

Recordemos también que, dado un grupo G, decimos que un subgrupo H es **permutable** en G si H permuta con todo subgrupo de G. Notemos que si tenemos A y B dos subgrupos permutables en G, en particular, son mutuamente permutables.

Como comentábamos antes de la definición anterior, si añadimos la hipótesis de que los factores de la factorización de G son mutuamente permutables por parejas, se puede extender el Lema 1.4.2 y el Lema 1.4.3 a un producto de un número arbitrario de factores.

Teorema 1.4.5. *Sea G el producto mutuamente permutable por parejas de los subgrupos $G_1, G_2, \ldots, G_r$. Entonces:*

1. *Para cada número primo $p \in \mathbb{N}$ divisor de $|G|$, existe $P \in \mathrm{Syl}_p(G)$ tal que P es prefactorizado, es decir, $P = (P \cap G_1)(P \cap G_2) \cdots (P \cap G_r)$ con $P \cap G_i \in \mathrm{Syl}_p(G_i)$, para todo $1 \leq i \leq r$.*

2. *Si además G es π-separable, para cada conjunto de números primos π divisores de $|G|$, existe $H \in \mathrm{Hall}_\pi(G)$ tal que $H = (H \cap G_1)(H \cap G_2) \cdots (H \cap G_r)$ con $H \cap G_i \in \mathrm{Hall}_\pi(G_i)$, para todo $1 \leq i \leq r$.*

DEMOSTRACIÓN. Basta con ver la prueba del apartado 2, pues el primer apartado será consecuencia directa. Notemos que la condición de la π-separabilidad de G garantiza que G es un D_π-grupo (y, por tanto, todos sus subgrupos también, pues la π-separabilidad es heredada), pero no es necesaria para el apartado 1.

Trabajaremos por inducción sobre r. Supongamos $r > 1$ y que el resultado cierto hasta $r-1$. Consideremos el producto $G_1G_2\cdots G_{r-1}$. Entonces, por hipótesis de inducción, existe $T \in \mathrm{Hall}_\pi(G_1G_2\cdots G_{r-1})$ tal que

$$T = (T\cap G_1)(T\cap G_2)\cdots(T\cap G_{r-1}),$$

con $T\cap G_i \in \mathrm{Hall}_\pi(G_i)$, para todo $1 \leq i \leq r-1$.

En el siguiente paso es donde es fundamental el uso de la permutabilidad mutua. Notemos que, al ser el producto de los factores mutuamente permutables por parejas, tenemos que

$$\begin{aligned} TG_r &= (T\cap G_1)(T\cap G_2)\cdots(T\cap G_{r-2})(T\cap G_{r-1})G_r \\ &= (T\cap G_1)(T\cap G_2)\cdots(T\cap G_{r-2})G_r(T\cap G_{r-1}) \\ &\vdots \\ &= G_r(T\cap G_1)(T\cap G_2)\cdots(T\cap G_{r-2})(T\cap G_{r-1}) = G_rT, \end{aligned}$$

donde hemos usado que cada $T\cap G_i \leqslant G_i$, que es mutuamente permutable con G_r.

Luego $TG_r \leqslant G$. Sea $H \in \mathrm{Hall}_\pi(TG_r)$ tal que $T \leqslant H$. Entonces, tenemos que

$$H = H\cap TG_r = T(H\cap G_r) = (T\cap G_1)(T\cap G_2)\cdots(T\cap G_{r-1})(H\cap G_r),$$

y $T\cap G_i \leqslant H\cap G_i$ con $T\cap G_i \in \mathrm{Hall}_\pi(G_i)$, para todo $1 \leq i \leq r-1$.

Como $|H\cap G_i|$ divide a $|H|$ (que es un π-número) para todo i, tenemos que $T\cap G_i = H\cap G_i \in \mathrm{Hall}_\pi(G_i)$, para todo $1 \leq i \leq r-1$. Solo queda ver que $H\cap G_r \in \mathrm{Hall}_\pi(G_r)$ y que $H \in \mathrm{Hall}_\pi(G)$ para finalizar la prueba.

Notemos que

$$\begin{aligned} |TG_r : H| &= |TG_r : T(H\cap G_r)| = |TG_r(H\cap G_r) : T(H\cap G_r)| \\ &= \frac{\cancel{|T(H\cap G_r)|}\cdot|G_r|}{|T(H\cap G_r)\cap G_r|\cdot\cancel{|T(H\cap G_r)|}} = |G_r : H\cap G_r|, \end{aligned}$$

ya que, por la identidad de Dedekind, tenemos que

$$T(H\cap G_r)\cap G_r = (H\cap G_r)(T\cap G_r) = H\cap G_r.$$

Luego, como $|G_r : H \cap G_r| = |TG_r : H|$ (el cual es un π'-número), ya tenemos que $H \cap G_r \in \mathrm{Hall}_\pi(G_r)$. Si tuviéramos dos factores solo, por un argumento elemental de índices, tendríamos que $|G : H|$ divide a $|G_1 : (H \cap G_1)| \cdot |G_2 : (H \cap G_2)|$. Razonando recursivamente de este modo, llegamos a que

$$|G : H| = |G_1 G_2 \cdots G_r : (H \cap G_1)(H \cap G_2) \cdots (H \cap G_r)|$$

divide a $|G_1 : (H \cap G_1)| \cdot |G_2 : (H \cap G_2)| \cdots |G_r : (H \cap G_r)|$, el cual es π'-número luego, necesariamente, $|G : H|$ también debe serlo. Esto finaliza la prueba. □

Notemos que, el resultado anterior, también es cierto si cambiamos en el apartado 2 la hipótesis de π-separabilidad de G por la resolubilidad de los G_i, para todo $1 \leq i \leq r$, tal y como puede se puede ver en la Proposición 4.1.45 de [4]. Destacar que la demostración es totalmente análoga, pues dichas hipótesis son utilizadas solamente para garantizar que G y sus subgrupos son D_π-grupos.

El siguiente resultado es particularmente útil en un argumento inductivo, cuando estemos trabajando con cocientes de un grupo.

Lema 1.4.6 ([4], Lema 4.1.10). *Sea G el producto mutuamente permutable de los subgrupos A y B y $N \trianglelefteq G$. Entonces, tenemos que G/N es el producto mutuamente permutable de los subgrupos AN/N y BN/N.*

Demostración. Sea $X/N \leqslant BN/N$. Veamos que AN/N permuta con X/N. Como $X/N \leqslant BN/N$, tenemos que $N \trianglelefteq X \leqslant BN$ y, por la identidad de Dedekind, deducimos que $X = X \cap BN = N(X \cap B)$.

Por hipótesis, A y B son mutuamente permutables y tenemos que $X \cap B \leqslant B$, luego $A(X \cap B) = (X \cap B)A$. Además, como $N \trianglelefteq G$, también se cumple que $AN = NA$ y $(X \cap B)N = N(X \cap B)$. Así, usando todos estos argumentos, tenemos que

$$AX = AN(X \cap B) = A(X \cap B)N = (X \cap B)AN = (X \cap B)NA = XA.$$

Luego

$$(X/N) \cdot (AN/N) = XAN/N = AXN/N = ANX/N = (AN/N) \cdot (X/N),$$

con lo que hemos visto que AN/N permuta con X/N, para todo $X/N \leqslant BN/N$. Un razonamiento totalmente análogo sirve para ver que BN/N permuta con todo subgrupo de AN/N también. Luego AN/N y BN/N son mutuamente permutables y queda finalizada la demostración. □

Se puede ver sin dificultad, como corolario del resultado anterior, que dicha propiedad se puede extender a un producto de n subgrupos mutuamente permutables dos a dos.

Corolario 1.4.7 ([4], Corolario 4.1.11). *Sea G el producto mutuamente permutable por parejas de los subgrupos $G_1, G_2, \ldots, G_r$ y $N \trianglelefteq G$. Entonces G/N es el producto mutuamente permutable por parejas de los subgrupos $G_1N/N, G_2N/N, \ldots, G_rN/N$*

El siguiente resultado nos da información sobre los subgrupos de un producto mutuamente permutable.

Lema 1.4.8 ([4], Lema 4.1.21). *Sea G el producto mutuamente permutable de los subgrupos A y B. Entonces:*

1. *Si $U \leqslant G$, entonces $(U \cap A)(U \cap B)$ es un subgrupo de G y $U \cap A$ y $U \cap B$ son mutuamente permutables.*
2. *Si $N \trianglelefteq G$, entonces $(N \cap A)(N \cap B)$ es un subgrupo normal de G.*

Demostración. 1. Sea $X \leqslant U \cap A$. Así, $X \leqslant U$ y $X \leqslant A$ y, al ser A y B mutuamente permutables, tenemos que $XB = BX$. Entonces, por la identidad de Dedekind, tenemos que

$$X(U \cap B) = U \cap XB = U \cap BX = (U \cap B)X.$$

Así, X permuta con $U \cap B$, para todo $X \leqslant U \cap A$. En particular, tomando $X = U \cap A$, tenemos que $(U \cap A)(U \cap B) = (U \cap B)(U \cap A)$, por lo que $(U \cap A)(U \cap B)$ es un subgrupo de G.

Un razonamiento totalmente análogo sirve para ver que $U \cap A$ permuta con todo subgrupo de $U \cap B$, lo cual finaliza la prueba de 1.

2. Sea $N \trianglelefteq G$. Entonces, por la identidad de Dedekind, tenemos que

$$N \cap A(N \cap B) = (N \cap A)(N \cap B) = N \cap (N \cap A)B.$$

Así, al ser $N \trianglelefteq G$ y A y B mutuamente permutables, tenemos que A normaliza a N y a $A(N \cap B)$. Análogamente, B normaliza a N y a $B(N \cap A)$. Luego $AB = G$ normaliza a $(N \cap A)(N \cap B)$, lo cual finaliza la demostración. □

Mencionar que el resultado anterior se puede extender fácilmente a un grupo G que sea el producto de un número arbitrario de subgrupos mutuamente permutables dos a dos.

Corolario 1.4.9 ([4], Corolario 4.1.22). *Sea G el producto mutuamente permutable por parejas de los subgrupos $G_1, G_2, \ldots, G_r$. Entonces:*

1. *Si $U \leqslant G$, entonces $(U \cap G_1)(U \cap G_2)\cdots(U \cap G_r) \leqslant G$, el cual es el producto mutuamente permutable por parejas de los subgrupos $U \cap G_1, U \cap G_2, \ldots, U \cap G_r$.*
2. *Si $N \trianglelefteq G$, entonces $(N \cap G_1)(N \cap G_2)\cdots(N \cap G_r)$ es un subgrupo normal de G.*

En muchas ocasiones, cuando estemos trabajando con un grupo G que sea el producto mutuamente permutable por parejas de un número finito de subgrupos, necesitaremos un subgrupo normal minimal de G contenido dentro de uno de los factores. Si la factorización de G consta solo de dos factores, no tendremos ningún problema, como vamos a ver a continuación. Sin embargo, si consta de más de 3 factores, solo es cierto en el caso de que dicho normal minimal sea no abeliano.

Teorema 1.4.10 ([4], Teorema 4.3.8). *Sea G el producto mutuamente permutable por parejas de los subgrupos $G_1, G_2, \ldots, G_r$. Si N es un subgrupo normal minimal no abeliano de G, entonces existe $i \in \{1, 2, \ldots, r\}$ tal que $N \leqslant G_i$.*

Teorema 1.4.11 ([4], Teorema 4.3.11). *Sea G un grupo no trivial, el cual es el producto mutuamente permutable de los subgrupos A y B. Entonces, tenemos que $A_G B_G \neq 1$.*

Sus pruebas no son para nada elementales, tal y como se puede ver en [4]. No se sabe si este último resultado se puede extender a un producto arbitrario de factores mutuamente permutables dos a dos, esto es, si algún factor de un producto mutuamente permutable por parejas contiene un subgrupo normal minimal del grupo. Lo que sí es cierto, por el Teorema 1.4.10, es que se puede extender a r factores arbitrarios si el grupo contiene un normal minimal no abeliano.

Capítulo 2

Grupos factorizados y tamaños de clases de conjugación no divisibles por un primo

2.1. Introducción

Una de las cuestiones que han sido ampliamente estudiadas es qué puede decirse sobre de la estructura de un grupo G, si se conoce alguna información acerca de la estructura aritmética de $\left|x^G\right|$ para algunos elementos $x \in G$. En algunos artículos se han dado respuestas (véase, por ejemplo [3], [6], [7], [16] o [17]).

En 1990, Chillag y Herzog caracterizaron (ver [6]), con una prueba bastante elemental, la estructura de los grupos donde todo elemento tiene tamaño de clase no divisible por p.

Teorema 2.1.1 ([6], Proposición 4). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo. Entonces, p no divide a $\left|x^G\right|$ para todo $x \in G$ si, y solo si, G es p-descomponible con p-subgrupo de Sylow central, es decir,*

$$G = \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G),$$

con $\mathrm{O}_p(G) \leqslant \mathrm{Z}(G)$.

En 1995, Y. Ren (ver [18]) comprobó que si se restringían las hipótesis del resultado anterior a solamente p'-elementos, seguía siendo necesario y suficiente para que el grupo fuese p-descomponible.

Diez años después, Liu, Wang y Wei vieron (ver [16], Teorema 5) que el resultado anterior de Y. Ren era también válido si se consideraban solamente p'-elementos de orden

potencia de primo. Para probarlo, usaron un resultado de Fein, Kantor y Schacher ([9], Teorema 1), que utiliza la clasificación de los grupos finitos simples.

Finalmente, en 2012, Ballester-Bolinches, Cossey y Li (ver [3]) vieron que el resultado anterior de Liu, Wang y Wei se puede extender a un grupo factorizado como un producto de un número arbitrario de subgrupos mutuamente permutables por parejas.

Teorema A ([3], Teorema 1.1). *Sea G el producto mutuamente permutable por parejas de los subgrupos $G_1, G_2, \ldots, G_r$ y sea $p \in \mathbb{N}$ un número primo. Entonces:*

1. *p no divide a $\left|x^G\right|$, para todo p'-elemento de orden potencia de primo $x \in \bigcup_{i=1}^{r} G_i$ si, y solo si, $G = \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G)$.*
2. *p no divide a $\left|x^G\right|$, para todo elemento $x \in \bigcup_{i=1}^{r} G_i$ si, y solo si, $G = \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G)$ con $\mathrm{O}_p(G)$ abeliano.*

Notar que este resultado generaliza a los mencionados anteriormente cuando se considera la factorización trivial $G = G_1 = G_2 = \cdots = G_r$.

En la siguiente sección, probaremos algunos de los resultados aquí citados.

2.2. Resultados centrales

Como hemos comentado en la introducción, la estructura de un grupo con tamaños de clases de conjugación no divisibles por p, para todo p'-elemento del grupo, es bastante concreta:

Teorema 2.2.1 ([18]). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo divisor de $|G|$. Entonces, p no divide a $\left|x^G\right|$ para todo p'-elemento $x \in G$ si, y solo si, G es p-descomponible, i.e.,*

$$G = \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G).$$

Demostración. Supongamos que G es p-descomponible. Notemos que, en esta situación, $\mathrm{O}_p(G)$ es el único p-subgrupo de Sylow de G. Sea $h \in G$ un p'-elemento. Entonces, está claro que $h \in \mathrm{O}_{p'}(G)$, pues $\mathrm{O}_{p'}(G)$ es el único p'-subgrupo de Hall de G. Si tomamos ahora $g \in \mathrm{O}_p(G)$, entonces tenemos que $[g, h] = 1$, para todo $g \in G$. Luego $\mathrm{O}_p(G) \leqslant \mathrm{C}_G(h) \leqslant G$. Concluimos que $|G : \mathrm{C}_G(h)| = \left|h^G\right|$ divide a $|G : \mathrm{O}_p(G)|$, el cual es p'-número (pues $\mathrm{O}_p(G) \in \mathrm{Syl}_p(G)$), siendo esto válido para todo p'-elemento $h \in G$.

Veamos ahora la implicación directa. Sea $g \in G$ un p'-elemento de G. Entonces, por hipótesis, $\left|g^G\right| = |G : \mathrm{C}_G(g)|$ es un p'-número. Como p divide a $|G|$, necesariamente tenemos que $\mathrm{C}_G(g)$ contiene a un p-Sylow de G, esto es, existe $P \in \mathrm{Syl}_p(G)$ tal que $P \leqslant \mathrm{C}_G(g)$. Luego $g \in \mathrm{C}_G(P)$.

Por otra parte, si $x \in G$ entonces, por el Lema 1.1.3, $x = x_p x_{p'}$ con x_p la p-parte de x y $x_{p'}$ la p'-parte de x. Por lo que acabamos de ver, existe $t \in G$ tal que $P^t \leqslant \mathrm{C}_G(x_{p'}) \leqslant G$. Luego

$$x_{p'} \in \mathrm{C}_G(P^t). \tag{2.1}$$

Además, como $P^t \in \mathrm{Syl}_p(G)$, tenemos que $P^t \in \mathrm{Syl}_p(\mathrm{C}_G(x_{p'}))$. También sabemos que x_p y $x_{p'}$ conmutan, luego $x_p \in \mathrm{C}_G(x_{p'})$. Al ser x_p un p-elemento de $\mathrm{C}_G(x_{p'})$, existirá $a \in \mathrm{C}_G(x_{p'})$ tal que $x_p \in (P^t)^a = P^{ta}$.

Pero $a \in \mathrm{C}_G(x_{p'})$ luego, fijándonos en la ecuación (2.1), tenemos que

$$x_{p'} = x_{p'}^a \in \mathrm{C}_{G^a}((P^t)^a) = \mathrm{C}_G(P^{ta}).$$

Así, $x = x_p x_{p'} \in P^{ta}\mathrm{C}_G(P^{ta}) = (P\mathrm{C}_G(P))^{ta}$. Pero esto lo hemos hecho para $x \in G$ cualquiera, luego

$$G \subseteq \bigcup_{h \in G} (P\mathrm{C}_G(P))^h \subseteq G,$$

de donde deducimos que $G = \bigcup_{h \in G} (P\mathrm{C}_G(P))^h$. Por el Lema 1.1.1, concluimos que $G = P\mathrm{C}_G(P)$. Por tanto, tenemos que $P \trianglelefteq G$ y, así, $P = \mathrm{O}_p(G)$. Aplicando el teorema de Schur-Zassenhaus, tenemos que P es complementado en G, es decir, existe $H \leqslant G$ tal que $G = PH$ con $P \cap H = 1$. Deducimos que, necesariamente, H debe ser un p'-grupo pues, por el segundo teorema de isomorfía, tenemos que

$$H = H/(P \cap H) \cong PH/P = G/P,$$

luego $|H| = |G/P|$ que es un p'-número.

Además, notemos que si $y \in G$ es un p'-elemento entonces, por hipótesis, $\left|y^G\right|$ es un p'-número, luego $P = \mathrm{O}_p(G) \leqslant \mathrm{C}_G(y)$ y, consecuentemente, $y \in \mathrm{C}_G(P)$. Luego $\mathrm{C}_G(P)$ contiene a todos los p'-elementos de G. Como H era un p'-grupo, concluimos que $H \leqslant \mathrm{C}_G(P)$ y, por tanto, $H \trianglelefteq PH = G$. Luego $H \leqslant \mathrm{O}_{p'}(G)$.

Como tenemos que $G = PH$ con $P \cap H = 1$ y $P \trianglelefteq G$ y $H \trianglelefteq G$, concluimos que

$$G = P \times H = \mathrm{O}_p(G) \times H \leqslant \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G) \leqslant G,$$

lo cual finaliza la demostración. □

Señalar que, en la demostración anterior, las técnicas utilizadas han sido bastante elementales. Sin embargo, en la prueba del próximo teorema, vamos a tener que usar la clasificación de los grupos finitos simples.

Esto es así debido a que, en ocasiones, cuando aparecen hipótesis únicamente sobre los p'-elementos de un grupo de orden potencia de primo, las pruebas de los resultados se pueden complicar mucho, pues se pierde información global del grupo, siendo necesario el uso de la clasificación.

Enunciemos el siguiente resultado de Fein, Kantor y Schacher (ver [9]), que es una consecuencia de la clasificación de los grupos finitos simples, el cual usaremos posteriormente.

Teorema 2.2.2 ([9], Teorema 1). *Sea G un grupo de permutaciones transitivo sobre un conjunto Ω con $|\Omega| > 1$. Entonces, existe un número primo $p \in \mathbb{N}$ y un p-elemento $g \in G$ tal que g actúa sobre Ω libre de puntos fijos, i.e.,*

$$\alpha \cdot g \neq \alpha, \quad \forall\, \alpha \in \Omega.$$

Como ya dijimos en la sección anterior, Liu, Wang y Wei (ver [16], Teorema 5) comprobaron que el Teorema 2.2.1 era también válido si se consideraban solamente p'-elementos de orden potencia de primo.

Teorema 2.2.3 ([16], Teorema 5). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo divisor de $|G|$. Entonces, p no divide a $\left|x^G\right|$ para todo p'-elemento $x \in G$ de orden potencia de primo si, y solo si, G es p-descomponible, i.e.,*

$$G = \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G).$$

Demostración. Si G es p-descomponible, basta con aplicar el Teorema 2.2.1. Supongamos ahora que p no divide a $\left|x^G\right|$ para todo p'-elemento $x \in G$ de orden potencia de primo. Veamos, en primer lugar, que G tiene un único $P \in \mathrm{Syl}_p(G)$, esto es, que $P \trianglelefteq G$. Sea $\Omega := \mathrm{Syl}_p(G)$. Podemos suponer que $|\Omega| > 1$ y consideremos la acción por conjugación de G sobre Ω dada por el siguiente homomorfismo:

$$\begin{array}{rcl} \gamma : G & \longrightarrow & \Sigma_{|\Omega|} \\ g & \longmapsto & \gamma(g) := \gamma_g : \begin{array}{rcl} \Omega & \longrightarrow & \Omega \\ P & \longmapsto & \gamma_g(P) := P^g, \end{array} \end{array}$$

con $P \in \Omega$. Entonces G actúa transitivamente sobre Ω pues dados $P^{g_1}, P^{g_2} \in \Omega$, siempre existe $g_1^{-1}g_2 \in G$ tal que $(P^{g_1})^{g_1^{-1}g_2} = P^{g_2}$.

Claramente, tenemos que $K := \mathrm{Ker}(\gamma) = \bigcap_{P\in\Omega} \mathrm{N}_G(P)$. Luego γ induce la acción por conjugación de $\overline{G} := G/K$ sobre Ω dada por el siguiente homomorfismo:

$$\begin{array}{rcl} \varphi : \overline{G} & \longrightarrow & \Sigma_{|\Omega|} \\ \overline{g} & \longmapsto & \varphi(\overline{g}) := \varphi_{\overline{g}} : \begin{array}{ccc} \Omega & \longrightarrow & \Omega \\ P & \longmapsto & \varphi_{\overline{g}}(P) := P^g, \end{array} \end{array}$$

donde $\overline{g} := gK$. Observemos que la acción dada por φ está bien definida pues, dados $\overline{a}, \overline{b} \in \overline{G}$ tales que $\overline{a} = \overline{b}$, entonces $ab^{-1} \in K$. Así, $P^{ab^{-1}} = P$, para todo $P \in \Omega$. Luego $P^a = P^b$ para todo $P \in \Omega$, lo cual implica que $\varphi_{\overline{a}} = \varphi_{\overline{b}}$ y, por tanto, está bien definida.

Además, la acción es transitiva pues lo era la acción dada por γ. Es más, $\overline{G}$ actúa como grupo de permutaciones sobre Ω trivialmente. Así, estamos en condiciones de aplicar el Teorema 2.2.2 y podemos afirmar que existe un número primo $r \in \mathbb{N}$ y un r-elemento $\overline{g} \in \overline{G}$ tal que $\overline{g}$ actúa sobre Ω libre de puntos fijos.

Ahora, por el Lema 1.1.3, descomponemos g en su r-parte y su r'-parte, i.e., $g = g_r g_{r'}$. Así, si definimos $\overline{g_r} := g_r K$ y $\overline{g_{r'}} := g_{r'} K$, tenemos que

$$\overline{g} = gK = (g_r g_{r'})K = (g_r K)(g_{r'} K) = \overline{g_r} \cdot \overline{g_{r'}}.$$

Al ser $\overline{g}$ un r-elemento, necesariamente $\overline{g_{r'}} = 1$. Luego $\overline{g} = \overline{g_r}$, donde $g_r \in G$ es un r-elemento. Como $\overline{g}$ actúa sobre Ω libre de puntos fijos y $\overline{g} = \overline{g_r}$, tenemos que $P^{g_r} \neq P$ para todo $P \in \Omega$. Así, $P \nleqslant \mathrm{C}_G(g_r)$ para todo $P \in \Omega$, luego p divide a $\left|g_r^G\right|$ con g_r un r-elemento de G.

Necesariamente, concluimos que $r = p$ pues, en caso contrario, tendríamos una contradicción con las hipótesis del enunciado. Pero si $r = p$, entonces g_r es un p-elemento de G, luego $g_r \in P$, para algún $P \in \Omega$. Deducimos que $P^{g_r} = P$, lo cual vuelve a ser una contradicción pues $\overline{g} = \overline{g_r}$ actuaba sobre Ω libre de puntos fijos.

Deducimos que, necesariamente, $|\Omega| = 1$. Así, tenemos que $P \trianglelefteq G$ y, por tanto, $P = \mathrm{O}_p(G)$. Al ser $P \in \mathrm{Syl}_p(G)$, existe un p'-subgrupo H de G tal que $G = PH$ con $P \cap H = 1$. Así, solo nos falta ver que $H \trianglelefteq G$ para que formen un producto directo y, por tanto, tendremos que $H \leqslant \mathrm{O}_{p'}(G)$, con lo que habremos finalizado.

Sea $h \in H$ (luego es p'-elemento) de orden potencia de primo. Por hipótesis, tenemos que p no divide a $\left|h^G\right|$, luego $P = \mathrm{O}_p(G) \leqslant \mathrm{C}_G(h)$. Por tanto, tenemos que $h \in \mathrm{C}_G(P)$. Gracias al Lema 1.1.3, tenemos que cualquier elemento de H lo podemos descomponer como producto de elementos en H de orden potencia de primo y, por lo que acabamos de ver, todos estarán en $\mathrm{C}_G(P)$. Entonces, concluimos que cualquier elemento de H estará en $\mathrm{C}_G(P)$ y, por tanto, tenemos que $H \leqslant \mathrm{C}_G(P)$.

Así, $H \trianglelefteq HP = G$. Esto finaliza la demostración, pues tenemos que

$$G = P \times H = \mathrm{O}_p(G) \times H \leqslant \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G) \leqslant G. \qquad \square$$

El último objetivo de este capítulo es ver que el resultado anterior se puede extender a un grupo factorizado como producto de un número arbitrario de subgrupos mutuamente permutables por parejas, es decir, ver la prueba del Teorema A.

Teorema A ([3], Teorema 1.1). *Sea G el producto mutuamente permutable por parejas de los subgrupos $G_1, G_2, \ldots, G_r$ y sea $p \in \mathbb{N}$ un número primo. Entonces:*

1. *p no divide a $\left|x^G\right|$, para todo p'-elemento de orden potencia de primo $x \in \bigcup_{i=1}^{r} G_i$ si, y solo si, $G = \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G)$.*
2. *p no divide a $\left|x^G\right|$, para todo elemento $x \in \bigcup_{i=1}^{r} G_i$ si, y solo si, $G = \mathrm{O}_p(G) \times \mathrm{O}_{p'}(G)$ con $\mathrm{O}_p(G)$ abeliano.*

Demostración. 1. Si G es p-descomponible, basta con aplicar el Teorema 2.2.3. Por tanto, veamos la implicación directa. Supongamos falso el teorema y sea G un contraejemplo minimal. Sea $N \trianglelefteq G$ y veamos que $\overline{G} := G/N$ hereda las hipótesis del teorema. Por el Corolario 1.4.7, tenemos que G/N es el producto mutuamente permutable por parejas de los subgrupos $G_1N/N, G_2N/N, \ldots, G_rN/N$. Ahora, consideremos un p'-elemento de orden potencia de primo $\overline{g} := gN \in \bigcup_{i=1}^{r} G_iN/N$ (tomaremos $\mathrm{o}(\overline{g}) = q^n$, con $q \neq p$ y $n \in \mathbb{Z}^+$). Claramente, podemos considerar que $g \in G_i$, para algún i. Al ser $\overline{g}$ un q-elemento (con $q \neq p$), por el Lema 1.1.3, podemos suponer que g es un q-elemento también. Así, por hipótesis, p no divide a $\left|g^G\right|$. Pero, por el Lema 1.3.1 (2), $\left|\overline{g}^{\overline{G}}\right|$ divide a $\left|g^G\right|$.

Por tanto, los cocientes de G heredan las hipótesis y, como la clase de los grupos p-descomponibles es una formación, podemos suponer que G posee un único normal minimal N. Además, por minimalidad de G, tenemos que

$$G/N = \mathrm{O}_p(G/N) \times \mathrm{O}_{p'}(G/N). \tag{2.2}$$

Definamos $Q/N := \mathrm{O}_{p'}(G/N)$ y $PN/N := \mathrm{O}_p(G/N)$ con $P \in \mathrm{Syl}_p(G)$ ya que, al ser G/N p-descomponible, tenemos que $\mathrm{O}_p(G/N) \in \mathrm{Syl}_p(G/N)$. Así, tenemos que $G = PNQ$, con $Q \trianglelefteq G$ y $PN \trianglelefteq G$.

Supongamos que N no es abeliano. Entonces, por el Teorema 1.4.10, tenemos que existe $j \in \{1, 2, \ldots, r\}$ tal que $N \leqslant G_j$. Como N es un normal minimal no abeliano, no puede ser un p-grupo. Así, debe existir $n \in N \leqslant G_j$ un p'-elemento de orden potencia de primo. Entonces, por hipótesis, tenemos que p no divide a $\left|n^G\right|$. Pero, por el Lema 1.3.1 (1), $\left|n^N\right|$ divide a $\left|n^G\right|$, luego p no divide tampoco a $\left|n^N\right|$, para todo p'-elemento de orden potencia de primo $n \in N$. Así, por el Teorema 2.2.3, tenemos que

$$N = \mathrm{O}_p(N) \times \mathrm{O}_{p'}(N). \tag{2.3}$$

Pero, por otra parte, tenemos que $\mathrm{O}_p(N)$ car $N \cdot \trianglelefteq G$. Por minimalidad de N en G, deducimos que $\mathrm{O}_p(N) = 1$ ó N. Como N no puede ser un p-grupo, concluimos que $\mathrm{O}_p(N) = 1$ y, por (2.3), que $N = \mathrm{O}_{p'}(N)$.

Está claro que todo p'-elemento de PN está en N. Sea $y \in PN$ un p'-elemento de orden potencia de primo. Por lo que acabamos de ver, $y \in N \leqslant G_j$ luego, por hipótesis, tenemos que p no divide a $\left|y^G\right|$. Pero $PN \trianglelefteq G$ por (2.2), luego $\left|y^{PN}\right|$ divide a $\left|y^G\right|$ y, por tanto, p no divide a $\left|y^{PN}\right|$, para todo p'-elemento de orden potencia de primo $y \in PN$. Así, nuevamente por el Teorema 2.2.3, tenemos que

$$PN = \mathrm{O}_p(PN) \times \mathrm{O}_{p'}(PN).$$

Pero, al ser $N \trianglelefteq G$ un p'-grupo, necesariamente tenemos que $N = \mathrm{O}_{p'}(PN)$. Luego, por el segundo teorema de isomorfía, tenemos que

$$\mathrm{O}_p(PN) \cong PN/\mathrm{O}_{p'}(PN) = PN/N \cong P/(P \cap N) = P,$$

pues P y N son de órdenes coprimos. Así, concluimos que

$$P = \mathrm{O}_p(PN) \text{ car } PN \trianglelefteq G,$$

luego $P \trianglelefteq G$. Al ser N el único normal minimal de G, tenemos que $N \leqslant P$, lo que obliga a que $N = 1$ (pues N es p'-grupo) y tendríamos una contradicción.

Así, podemos suponer que N es abeliano. De hecho, al ser además $N \cdot \trianglelefteq G$, podemos suponer que N es q-elemental abeliano, para algún número primo $q \in \mathbb{N}$ divisor de $|G|$.

Supongamos, en primer lugar, que $q = p$ y, por tanto, que N es un p-grupo. Así, al ser $Q/N = \mathrm{O}_{p'}(G/N)$ un p'-grupo, tenemos que $Q = NT$ con $T \cap N = 1$ y T un p'-grupo. Como teníamos que $G = PNQ$ y $Q = NT$ con N un p-grupo normal en G, está claro que $G = PT$.

Teníamos que T era un p'-grupo, pero también vemos que

$$|G : T| = \frac{|PT|}{|T|} = |P|,$$

luego $T \in \mathrm{Hall}_{p'}(G)$. Pero observamos que $1 \trianglelefteq N \trianglelefteq Q \trianglelefteq G$, donde N es p-grupo, Q/N es p'-grupo y G/Q es p-grupo (pues $G/Q = PQ/Q \cong P$). Luego G es p'-separable y, por el Teorema 1.4.5 (2), podemos suponer que T es prefactorizado (si fuese el prefactorizado T^g con cierto $g \in G$, entonces $G = PT = PT^g$ y definiríamos $T := T^g$), luego

$$T = (T \cap G_1) \cdots (T \cap G_r).$$

Sea $x \in T \cap G_i \leqslant G_i$ un p'-elemento de orden potencia de primo (existe pues $T \cap G_i$ es un p'-grupo). Entonces, por hipótesis, tenemos que p no divide a $\left|x^G\right| = |G : \mathrm{C}_G(x)|$. Luego $\mathrm{C}_G(x)$ debe contener algún p-subgrupo de Sylow de G pero, como $P = PN \trianglelefteq G$, deducimos que $P \leqslant \mathrm{C}_G(x)$ y, por tanto, que $x \in \mathrm{C}_G(P)$, para todo p'-elemento de orden potencia de primo $x \in T \cap G_i$.

Escojamos $y \in T$. Entonces, tenemos que $y = y_1 y_2 \cdots y_r$ donde $y_i \in T \cap G_i$ son p'-elementos. Por el Lema 1.1.3, tenemos que cada y_i se puede descomponer como producto de elementos de órdenes potencias de primos, donde cada uno de ellos será, en particular, un p'-elemento de orden potencia de primo contenido en $T \cap G_i$. Así, todos ellos estarán en $\mathrm{C}_G(P)$ y, por tanto, tenemos que $y \in \mathrm{C}_G(P)$, para todo $y \in T$. Concluimos que $T \leqslant \mathrm{C}_G(P)$. Por tanto, juntando este último dato junto con lo que ya teníamos, obtenemos que

$$G = PT = P \times T,$$

lo cual es una contradicción, pues G era un contraejemplo.

Así, podemos suponer que N es p'-grupo. Sea $U := PN \trianglelefteq G$. Claramente, por el Teorema 1.4.5 (1), podemos suponer que P es prefactorizado, es decir, que

$$P = (P \cap G_1) \cdots (P \cap G_r),$$

pues $PN = (PN)^g = P^g N$, para todo $g \in G$. Así, por el Corolario 1.4.9 (2), tenemos que

$$(U \cap G_1)(U \cap G_2) \cdots (U \cap G_r) \trianglelefteq G.$$

Por unicidad de N como normal minimal de G, tenemos que

$$N \leqslant (U \cap G_1)(U \cap G_2) \cdots (U \cap G_r),$$

pero además, como $P \leqslant U$, observamos que

$$P = (P \cap G_1) \cdots (P \cap G_r) \leqslant (U \cap G_1)(U \cap G_2) \cdots (U \cap G_r).$$

Luego $U = PN \leqslant (U \cap G_1)(U \cap G_2) \cdots (U \cap G_r) \leqslant U$. Deducimos que

$$U = (U \cap G_1)(U \cap G_2) \cdots (U \cap G_r) \trianglelefteq G.$$

Supongamos que $U < G$. Sea $x \in U \cap G_i \leqslant G_i$ un p'-elemento de orden potencia de primo. Entonces, por hipótesis, tenemos que p no divide a $\left|x^G\right|$. Pero, por el Lema 1.3.1 (1), p tampoco divide a $\left|x^U\right|$. Así, U cumple las hipotesis del teorema y, por minimalidad de G, tenemos necesariamente que

$$U = P \times N = \mathrm{O}_p(U) \times \mathrm{O}_{p'}(U).$$

Concluimos que $P = \mathrm{O}_p(U)$ car $U \trianglelefteq G$, luego $P \trianglelefteq G$ lo cual es una contradicción, pues tendríamos que $N \leqslant P$ con N un p'-grupo. Así, podemos suponer que

$$G = U = PN,$$

con $P \in \mathrm{Syl}_p(G)$, N un p'-grupo normal en G y, por tanto, $P \cap N = 1$. Veamos que $P \trianglelefteq G$ y tendremos la contradicción final.

Notemos que, en el caso en el que estamos, tenemos que G es p'-separable. Efectivamente, pues podemos construir la serie $1 \trianglelefteq N \trianglelefteq PN = G$ de forma que N es un p'-grupo y $G/N \cong P$ es un p-grupo.

Así, tenemos que $N \in \mathrm{Hall}_{p'}(G)$ y $N \trianglelefteq G$ luego, por el Teorema 1.4.5 (2), tenemos que

$$N = (N \cap G_1)(N \cap G_2) \cdots (N \cap G_r).$$

Sea $n_i \in N \cap G_i \leqslant N$. Entonces, al ser N un q-grupo con $q \neq p$, tenemos que n_i es un p'-elemento de orden potencia de primo. Así, por hipótesis, tenemos que p no divide a $\left|n_i^G\right|$. Deducimos que debe existir $P^g \leqslant \mathrm{C}_G(n_i)$, con $P^g \in \mathrm{Syl}_p(G)$. Además, como N es abeliano, tenemos que $N \leqslant \mathrm{C}_G(n_i)$.

Concluimos que $G = PN = P^g N \leqslant \mathrm{C}_G(n_i)$ y, por tanto, $n_i \in \mathrm{Z}(G)$. Como un elemento cualquiera $n \in N$ lo podemos descomponer como $n = n_1 n_2 \cdots n_r$ con $n_i \in N \cap G_i$, tenemos que $n \in \mathrm{Z}(G)$, luego $N \leqslant \mathrm{Z}(G)$. Esto implica que $[P, N] = 1$ y, por tanto, hemos llegado a la contradicción final. Esto finaliza la prueba del apartado 1.

2. Comencemos con la implicación directa. Por el apartado 1, solo queda ver que $\mathrm{O}_p(G)$ es abeliano. Al ser G p-descomponible, tenemos que el único p-subgrupo de Sylow de G es $\mathrm{O}_p(G)$ y, por el Teorema 1.4.5 (1), sabemos que es prefactorizado. Tomemos $x \in \mathrm{O}_p(G) \cap G_i \leqslant G_i$, para algún $i \in \{1, 2, \ldots, r\}$. Entonces, por hipótesis, tenemos que

p no divide a $\left|x^G\right| = |G : \mathrm{C}_G(x)|$. Por tanto, deducimos que $\mathrm{O}_p(G) \leqslant \mathrm{C}_G(x)$, pues es el único p-subgrupo de Sylow de G. Así, $x \in \mathrm{C}_G(\mathrm{O}_p(G))$, para todo $x \in \mathrm{O}_p(G) \cap G_i$ y para todo $i \in \{1, 2, \ldots, r\}$. Concluimos que

$$\mathrm{O}_p(G) = (\mathrm{O}_p(G) \cap G_1)(\mathrm{O}_p(G) \cap G_2) \cdots (\mathrm{O}_p(G) \cap G_r) \leqslant \mathrm{C}_G(\mathrm{O}_p(G)),$$

luego es abeliano.

Para ver la implicación recíproca consideramos $x \in G_i$ con $i \in \{1, 2, \ldots, r\}$. Como tenemos que G es p-descomponible y $\mathrm{O}_p(G)$ es abeliano, deducimos que $\mathrm{O}_p(G) \leqslant \mathrm{Z}(G)$. Luego el único p-subgrupo de Sylow de G es central. Así, tenemos que

$$\mathrm{O}_p(G) \leqslant \mathrm{Z}(G) \leqslant \mathrm{C}_G(x),$$

para todo $x \in G_i$. Luego $\left|x^G\right|$ es p'-número (pues $\mathrm{C}_G(x)$ contiene al único p-subgrupo de Sylow de G), para todo $x \in G_i$. Esto finaliza la prueba del teorema. □

Capítulo 3

Grupos factorizados y tamaños de clases de conjugación libres de cuadrados

Recordamos que el objetivo de este capítulo es probar diversos resultados sobre la estructura de un grupo factorizado suponiendo que ciertos elementos de los factores tienen tamaños de clase libres de cuadrados.

3.1. Introducción

En 1990, usando el teorema de la clasificación de grupos finitos simples, Chillag y Herzog (ver [6]) demostraron el siguiente resultado:

Teorema 3.1.1 ([6], Proposición 5). *Si 4 no divide a $\left|x^G\right|$ para todo $x \in G$, entonces G es resoluble.*

En 1999, Cossey y Wang (ver [7]) generalizaron el resultado anterior. No solo vieron que se podía ampliar a primos al cuadrado distintos de 2, sino que se podía sacar información adicional sobre el grupo, como la p-nilpotencia. Mencionar que, en la prueba, no usaron el teorema de clasificación de los grupos finitos simples.

Teorema 3.1.2 ([7], Teorema 1). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo tal que $(p-1, |G|) = 1$. Si p^2 no divide a $\left|x^G\right|$ para cualquier $x \in G$, entonces G es resoluble, p-nilpotente y $G/\mathrm{O}_p(G)$ tiene p-subgrupos de Sylow de orden a lo sumo p.*

Ya en 2005, sin usar el teorema de la clasificación, Liu, Wang y Wei (ver [16]) generalizaron el Teorema 3.1.2, restringiendo las hipótesis, por un lado, a p'-elementos y, por otro lado, a elementos de orden potencia de primo.

Teorema 3.1.3 ([16], Teorema 6). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo cumpliendo que $(p-1, |G|) = 1$. Si p^2 no divide a $\left|x^G\right|$ para cualquier p'-elemento $x \in G$, entonces G es resoluble, p-nilpotente y los p-subgrupos de Sylow de $G/\mathrm{O}_p(G)$ son de orden a lo sumo p.*

Teorema 3.1.4 ([16], Teorema 7). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo cumpliendo que $(p-1, |G|) = 1$. Si p^2 no divide a $\left|x^G\right|$ para cualquier elemento $x \in G$ de orden potencia de primo, entonces G es resoluble, p-nilpotente y P' es trivial o elemental abeliano, para P un p-subgrupo de Sylow de G.*

En 2013, Qian y Wang (ver [17]) generalizaron los dos teoremas anteriores, considerando conjuntamente ambas condiciones. Para ello, usaron el Teorema 2.2.2, el cual vimos que es consecuencia de la clasificación de los grupos finitos simples.

Teorema 3.1.5 ([17], Teorema A). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo cumpliendo que $(p-1, |G|) = 1$. Si p^2 no divide a $\left|x^G\right|$ para cualquier p'-elemento $x \in G$ de orden potencia de primo, entonces G es resoluble, p-nilpotente y los p-subgrupos de Sylow de $G/\mathrm{O}_p(G)$ son elementales abelianos.*

Como veremos en el Ejemplo A.2.1 y en el Ejemplo A.2.2 del Apéndice A, con estas condiciones del resultado de Qian y Wang, no se pueden obtener las propiedades adicionales que obtienen Liu, Wang y Wei en los Teoremas 3.1.3 y 3.1.4.

Uno de los objetivos de este capítulo es probar, utilizando también la clasificación, el siguiente resultado original que generaliza al teorema anterior a través de productos mutuamente permutables. Es más, como veremos en los Ejemplos A.2.4 y A.2.5 del Apéndice A, puede llegar a ser más económico que el resultado anterior, computacionalmente hablando.

Teorema B. *Sea $G = AB$ el producto mutuamente permutable de los subgrupos A y B y $p \in \mathbb{N}$ un número primo cumpliendo que $(p-1, |G|) = 1$. Si p^2 no divide a $\left|x^G\right|$ para cualquier p'-elemento $x \in A \cup B$ de orden potencia de primo, entonces tenemos que:*

1. *G es resoluble.*
2. *G es p-nilpotente.*
3. *Los p-subgrupos de Sylow de $G/\mathrm{O}_p(G)$ son elementales abelianos.*

Por otro lado, Ballester-Bolinches, Cossey y Li también probaron (ver [3]) el siguiente resultado para productos mutuamente permutables que, en particular, proporciona una condición suficiente para que un grupo p-resoluble sea p-superresoluble.

Teorema C ([3], Teorema 1.3). *Sea G el producto mutuamente permutable de los subgrupos A y B. Supongamos que para todo p'-elemento $x \in A \cup B$, $\left|x^G\right|$ no es divisible por p^2. Entonces, el orden de los p-subgrupos de Sylow de todo factor principal de G es a lo sumo p. En particular, si G es p-resoluble, tenemos que G es p-superresoluble.*

En la siguiente sección veremos la prueba de este resultado, que también usa la clasificación de los grupos finitos simples, y daremos una generalización de la segunda afirmación para p'-elementos de orden potencia de primo, evitando el uso de la clasificación.

Teorema D. *Sea G el producto mutuamente permutable de los subgrupos A y B. Supongamos que para todo p'-elemento $x \in A \cup B$ de orden potencia de primo, $\left|x^G\right|$ no es divisible por p^2. Entonces, si G es p-resoluble, tenemos que G es p-superresoluble.*

Mencionar que, actualmente, estamos trabajando en una posible generalización completa del Teorema C y hemos obtenido algunos resultados parciales en este sentido.

A continuación, recopilamos algunos resultados conocidos que proporcionan condiciones para que un grupo sea superresoluble. En 1999, Cossey y Wang (ver [7]) obtuvieron el siguiente teorema.

Teorema 3.1.6 ([7], Teorema 2). *Sea G un grupo finito y supongamos que $\left|x^G\right|$ es libre de cuadrados para todo elemento de G. Entonces, tenemos que G es superresoluble y $G/\mathrm{F}(G)$ y G' son cíclicos de órdenes libres de cuadrados.*

Ya en 2005, Liu, Wang y Wei (ver [16]) generalizan la superresolubilidad del resultado anterior considerando, por un lado, elementos de orden potencia de primo y, por otro lado, un producto de dos factores permutables en el grupo.

Teorema 3.1.7 ([16], Lema 8). *Sea G un grupo finito y supongamos que $\left|x^G\right|$ es libre de cuadrados, para todo elemento de orden potencia de primo $x \in G$. Entonces, G es superresoluble.*

Teorema 3.1.8 ([16], Teorema 10). *Sea $G = AB$ con A, B subgrupos de G. Si A y B son permutables en G y $\left|x^G\right|$ es libre de cuadrados, para todo elemento $x \in A \cup B$, entonces G es superresoluble.*

Además, extendieron el primero de ellos para un producto de dos subgrupos normales en el grupo.

Teorema 3.1.9 ([16], Proposición 9). *Sea $G = AB$ con A, B subgrupos de G. Si $A \trianglelefteq G$ y $B \trianglelefteq G$ con $\left|x^G\right|$ libre de cuadrados, para todo elemento $x \in A \cup B$ de orden potencia de primo, entonces G es superresoluble.*

Finalmente, en 2012, Ballester-Bolinches, Cossey y Li (ver [3]) generalizaron el Teorema 3.1.8 para p'-elementos y considerando un producto mutuamente permutable.

Teorema 3.1.10 ([3], Corolario 1.5). *Sea G el producto mutuamente permutable de los subgrupos A y B. Supongamos que para todo número primo $p \in \mathbb{N}$ divisor de $|G|$ y para todo p'-elemento $x \in A \cup B$, $\left|x^G\right|$ no es divisible por p^2. Entonces, tenemos que G es superresoluble.*

Cerraremos este capítulo probando una generalización del Teorema 3.1.10 para p'-elementos de orden potencia de primo de los factores.

Teorema E. *Sea G el producto mutuamente permutable de los subgrupos A y B. Supongamos que para todo número primo $p \in \mathbb{N}$ divisor de $|G|$ y para todo p'-elemento $x \in A \cup B$ de orden potencia de primo, $\left|x^G\right|$ no es divisible por p^2. Entonces, tenemos que G es superresoluble.*

Por último, destacar que estos resultados serán presentados en el Tercer Congreso de Jóvenes Investigadores de la RSME (ver [10]).

3.2. Resultados centrales

Comencemos la sección viendo la demostración del Teorema B. Obtendremos las mismas conclusiones que obtuvieron Qian y Wang en el Teorema 3.1.5, pero trabajando con un grupo factorizado como producto de dos subgrupos mutuamente permutables. Recalcar también que, en el Apéndice A, veremos ejemplos para ver el alcance de las hipótesis que se manejan.

Aunque las técnicas que vamos a usar son muy similares a las que usaron Qian y Wang, los subgrupos normales de un grupo factorizado como producto de subgrupos mutuamente permutables no tienen porqué ser, ni siquiera, factorizados (ver Lema 1.4.8).

Esto supone un problema a la hora de aplicar una posible inducción. Nosotros, como veremos, hemos solventado dicho inconveniente.

Antes de probar dicho resultado, veamos algunos lemas que facilitarán la demostración en su debido momento. Destacar que el primero de ellos usa la clasificación de los grupos finitos simples.

Lema 3.2.1 ([17], Lema 2.1). *Supongamos que G es un grupo simple y no abeliano. Entonces, existe un número primo $p \in \mathbb{N}$ $(p \neq 2)$ y un p-elemento en G tal que su clase de conjugación es divisible por 4.*

Demostración. Supongamos, por reducción al absurdo, que 4 no divide a $\left|x^G\right|$ para todo p-elemento $x \in G$ con $p \neq 2$. Al ser G simple y no abeliano por hipótesis, tenemos que el orden de G es par necesariamente.

Sea $P \in \mathrm{Syl}_2(G)$. P es nilpotente, luego $\mathrm{Z}(P) > 1$. Así, por el teorema de Cauchy, existe $1 \neq g \in \mathrm{Z}(P)$ tal que $\mathrm{o}(g) = 2$. Si ahora definimos

$$\Omega \coloneqq g^G = \{g^t \ : \ t \in G\},$$

veamos que G actúa (por conjugación) como grupo de permutaciones transitivo sobre Ω (notemos que $|\Omega| > 1$, pues en caso contrario, $1 \neq g \in \mathrm{Z}(G) = 1$, que sería una contradicción). En efecto, tenemos que:

1. Si tomamos $h \in G$ y $g^t \in \Omega$ (con $t \in G$), tenemos que $g^t \cdot h = (g^t)^h = g^{th} \in \Omega$.

2. Consideremos el homomorfismo $\phi : G \longrightarrow \Sigma_{|\Omega|}$ asociado a la acción (ver (1.1)). Al ser G simple por hipótesis y $\mathrm{Ker}(\phi) \trianglelefteq G$, concluimos que $\mathrm{Ker}(\phi) = 1$ y, por tanto, $G \lessapprox \Sigma_{|\Omega|}$ (si $G = \mathrm{Ker}(\phi)$, entonces $1 \neq g \in \mathrm{Z}(G) = 1$, que sería una contradicción).

3. Dados $\alpha \coloneqq g^{t_1}, \beta \coloneqq g^{t_2} \in \Omega$ (con $t_1, t_2 \in G$), siempre podemos tomar $t_1^{-1}t_2 \in G$ para que $\alpha^{t_1^{-1}t_2} = \beta$, luego la acción es transitiva.

Aplicando el Teorema 2.2.2, existe un primo $q \in \mathbb{N}$ y un q-elemento $a \in G$ que actúa sobre Ω libre de puntos fijos.

Si $q = 2$, entonces a es un 2-elemento, luego $a \in P^b$ para algún $b \in G$. Además, teníamos que $g \in \mathrm{Z}(P)$, luego $g^b \in \mathrm{Z}(P^b)$. Así tenemos que $g^b a = a g^b$, lo que implica que $(g^b)^a = g^b$, lo cual es una contradicción pues a actúa sobre Ω libre de puntos fijos.

Luego, obligatoriamente, tenemos que $q \neq 2$. Sea $K \coloneqq a^G$. Vamos a ver que $|K| = 2m$ con m impar. Si suponemos que $|K|$ es impar, tenemos que $|K| = \left|a^G\right| = |G : \mathrm{C}_G(a)|$ es

impar. Pero como el orden de G era par, necesariamente, debe existir $P^c \leqslant \mathrm{C}_G(a)$ para algún $c \in G$. Así,

$$g^c \in P^c \leqslant \mathrm{C}_G(a),$$

luego $(g^c)^a = g^c$, lo cual es una contradicción pues a actúa sobre Ω libre de puntos fijos. Luego $|K| = \left|a^G\right| = 2m$ con m impar, pues estamos suponiendo, por hipótesis, que 4 no divide a $\left|x^G\right|$ para todo p-elemento $x \in G$ con $p \neq 2$.

Recordar que $\mathrm{o}(g) = 2$, luego $\langle g \rangle \cong C_2$. Vamos a ver que $\langle g \rangle$ actúa sobre K como grupo de permutaciones y libre de puntos fijos (notemos que $|K| = 2m > 1$). En efecto:

1. Sea $u \in \langle g \rangle$ y $v := a^{g_1} \in K = a^G$, con $g_1 \in G$. Entonces $v^u = (a^{g_1})^u = a^{g_1 u} \in a^G = K$, luego $\langle g \rangle$ actúa por conjugación sobre K.

2. Consideremos el homomorfismo $\varphi : \langle g \rangle \longrightarrow \Sigma_{|K|}$ asociado a esta acción (ver (1.1)). Al ser $\langle g \rangle \cong C_2$, tenemos que $\mathrm{Ker}(\varphi) = 1$ (si $\langle g \rangle = \mathrm{Ker}(\varphi)$, entonces $a^g = a$, lo cual implica que $g^a = g$ que es una contradicción, pues a actúa sobre Ω libre de puntos fijos). Por tanto, $\langle g \rangle \lessapprox \Sigma_{|K|}$.

3. Si $\langle g \rangle$ no actuase libre de puntos fijos sobre K, existiría $a^{g_2} \in K$ (con $g_2 \in G$) tal que $(a^{g_2})^g = a^{g_2}$, lo que implicaría que $(g^{g_2^{-1}})^a = g^{g_2^{-1}}$, contradiciendo de nuevo que a actúa sobre Ω libre de puntos fijos.

Así, tenemos que $\langle g \rangle \lessapprox \Sigma_{|K|}$ y además:

$$\begin{array}{rcll} g : K & \longrightarrow & K & \text{(biyectiva)} \\ x & \longmapsto & x^g \neq x & \text{(pues actúa libre de puntos fijos)} \\ x^g & \longmapsto & x^{g^2} = x & \text{(pues o(g)=2)} \\ y & \longmapsto & y^g & \\ y^g & \longmapsto & y & \\ \vdots & \vdots & \vdots & \end{array}$$

Luego g se puede ver como producto de m transposiciones en $\Sigma_{|K|}$, ya que $|K| = 2m$. Concluimos que g es una permutación impar en $\Sigma_{|K|}$.

Pero, al igual que G actuaba sobre $\Omega = g^G$ como grupo de permutaciones, también actúa sobre $K = a^G$ como grupo de permutaciones, luego $g \in G \lessapprox \Sigma_{|K|}$. Como $A_{|K|} \trianglelefteq \Sigma_{|K|}$, entonces tenemos que $G \cap A_{|K|} \trianglelefteq G$, con G simple por hipótesis.

Si $G \cap A_{|K|} = G$, entonces $G \leqslant A_{|K|}$, pero $g \in G$ era permutación impar, lo cual es una contradicción pues $A_{|K|}$ solamente contiene permutaciones pares.

Luego, necesariamente, tenemos que $G \cap A_{|K|} = 1$. Entonces, en G no hay permutaciones pares, salvo el elemento neutro. Además, $|G|$ es par y mayor estricto que 2 pues, si fuese 2, sería abeliano en contra de nuestras hipótesis.

Pero si no hay permutaciones pares, si tomamos $1 \neq h_1 \in G$, $1 \neq h_2 \in G$ con $h_1 \neq h_2$, entonces $h_1 h_2 \in G$ es permutación par, luego $h_1 h_2 = 1$ y $h_1 = h_2^{-1}$.

Esto implica que, necesariamente, G tiene solamente 3 elementos. Efectivamente, si existiese $h_3 \in G$ con $h_3 \neq h_1$ y $h_3 \neq h_2$, entonces $h_3 h_2 = 1$ por la misma razón que antes. Así, $h_3 = h_2^{-1}$, luego $h_3 = h_1$ y tendríamos una contradicción.

Luego $G \cong C_3$, lo cual también es una contradicción pues sería abeliano. Esto finaliza la demostración. □

Lema 3.2.2 ([17], Teorema A). *Sea G un grupo finito y $p \in \mathbb{N}$ un número primo tal que $(p-1, |G|) = 1$. Si p^2 no divide a $\left|x^G\right|$ para todo p'-elemento $x \in G$ de orden potencia de primo, entonces G es resoluble.*

Demostración. Claramente, podemos suponer que G no es abeliano. Si G es simple, estamos en condiciones de aplicar el Lema 3.2.1. Así, existe un número primo $q \in \mathbb{N}$ ($q \neq 2$) y un q-elemento en G tal que su clase de conjugación es divisible por 4. Pero tomando $p = 2$ en las hipótesis de nuestro teorema, también tenemos que 4 no divide a $\left|x^G\right|$ para todo $2'$-elemento $x \in G$ de orden potencia de primo, lo cual es una contradicción. Luego $p \neq 2$ y, por tanto, $p - 1$ es par. Pero teníamos que G era simple y no abeliano luego, necesariamente, tenemos que $|G|$ es par. Esto contradice nuestra hipótesis de que $(p-1, |G|) = 1$.

Así, podemos suponer que G no es simple. Trabajaremos por inducción sobre el orden de G. Al ser G no simple, existe un subgrupo $1 < N < G$ tal que $N \trianglelefteq G$. Luego $|N| < |G|$ y, por tanto, N cumple la hipótesis de que $(p-1, |N|) = 1$ para el primo p que tenemos fijado, pues $|N|$ divide a $|G|$.

Por otro lado, si N fuese p-grupo, sería resoluble, luego nos limitamos al caso de que N sea p'-grupo. Así, debe existir al menos un p'-elemento $x \in N$ ($\leqslant G$) de orden potencia de primo. Luego, por hipótesis del teorema, p^2 no divide a $\left|x^G\right|$. Pero, por el Lema 1.3.1 (1), $\left|x^N\right|$ divide a $\left|x^G\right|$ y, por tanto, p^2 tampoco divide a $\left|x^N\right|$, para cualquier p'-elemento $x \in N$ de orden potencia de primo. Así pues, se cumplen las hipótesis de nuestro teorema y, aplicando inducción, tenemos que N es resoluble.

Ahora vamos a ver un razonamiento parecido para afirmar que el grupo cociente $\overline{G} := G/N$ es también resoluble. Como $|G| = \left|\overline{G}\right| \cdot |N|$, tenemos que $\left|\overline{G}\right|$ divide a $|G|$ y, por tanto, $\overline{G}$ hereda la hipótesis de que $(p-1, \left|\overline{G}\right|) = 1$ para el primo p que tenemos

fijado.

Además, claramente tenemos que $\overline{G}$ hereda también la hipótesis de que p^2 no divide a $\left|\overline{g}^{\overline{G}}\right|$ para cualquier $\overline{g} \in \overline{G}$ p'-elemento de orden potencia de primo.

Así pues, se cumplen las hipótesis de nuestro teorema y, aplicando inducción, tenemos que $\overline{G}$ es resoluble. Finalmente, aplicando la propiedad extensiva de los grupos resolubles, concluimos que G es resoluble. □

Por fin estamos preparados para demostrar el primero de los resultados originales de este capítulo.

Teorema B. *Sea $G = AB$ el producto mutuamente permutable de los subgrupos A y B y $p \in \mathbb{N}$ un número primo cumpliendo que $(p-1, |G|) = 1$. Si p^2 no divide a $\left|x^G\right|$ para cualquier p'-elemento $x \in A \cup B$ de orden potencia de primo, entonces tenemos que:*

1. *G es resoluble.*
2. *G es p-nilpotente.*
3. *Los p-subgrupos de Sylow de $G/\mathrm{O}_p(G)$ son elementales abelianos.*

Demostración. 1. Veamos que G es resoluble por inducción. Por el Teorema 1.4.11, tenemos que $A_G \neq 1$ o $B_G \neq 1$. Supongamos que $A_G \neq 1$. Entonces, existe $1 < M \trianglelefteq G$ tal que $M \leqslant A$. Si $M = G = A$ entonces, por el Lema 3.2.2, concluiríamos que G es resoluble. Luego podemos suponer que $M < G$. Vamos a ver que $\overline{G} := G/M$ hereda todas las hipótesis del enunciado y, por tanto, será resoluble por inducción. Tenemos que

$$\overline{G} = G/M = (A/M) \cdot (BM/M)\,,$$

que es el producto mutuamente permutable de los subgrupos A/M y BM/M por el Lema 1.4.6. Además, como $\left|\overline{G}\right|$ divide a $|G|$, claramente tenemos que $(p-1, \left|\overline{G}\right|) = 1$ para el primo p que tenemos fijado. Además, podemos afirmar que $\overline{G}$ hereda la hipótesis de que p^2 no divide a $\left|\overline{x}^{\overline{G}}\right|$, para cualquier p'-elemento $\overline{x} \in A/M \cup BM/M$ de orden potencia de primo.

Así, se heredan las hipótesis para $\overline{G}$ y, por hipótesis de inducción, tenemos que $\overline{G}$ es resoluble. Solo falta ver que M también lo es y aplicar la propiedad extensiva de los grupos resolubles. Pero $M \leqslant A$ luego, para todo p'-elemento $x \in M$ de orden potencia de primo, p^2 no divide a $\left|x^G\right|$ y, por el Lema 1.3.1 (1), tampoco divide a $\left|x^M\right|$. Así, M sería resoluble por el Lema 3.2.2. Esto finaliza la prueba del apartado 1.

2. Veamos que G es p-nilpotente. Claramente, podemos suponer que G no es simple pues, en caso contrario, sería simple y abeliano y, por tanto, cíclico de orden primo. Luego suponemos que G no es simple y trabajaremos por inducción sobre $|G|$. Hemos visto en el apartado 1 que los cocientes de G heredan las hipótesis del teorema y, por tanto, son p-nilpotentes. Además, como la clase de los grupos p-nilpotentes es una formación saturada y G resoluble por el apartado 1, por la Nota 1.2.20, podemos suponer que existe un único $N \cdot \trianglelefteq G$ tal que $N \not\leqslant \Phi(G)$ y $N = \mathrm{F}(G) = \mathrm{C}_G(N) = \mathrm{O}_r(G)$, para algún número primo $r \in \mathbb{N}$.

Nuevamente, por el Teorema 1.4.11, tenemos que $A_G \neq 1$ o $B_G \neq 1$. Supongamos que $A_G \neq 1$. Entonces, por unicidad de N como normal minimal de G, tenemos que $N \leqslant A_G \leqslant A$. Denotamos $\overline{G} := G/N$, el cual es p-nilpotente por inducción.

Si $r \neq p$, entonces tenemos que N es un p'-grupo. Sea $P \in \mathrm{Syl}_p(G)$. Entonces, tenemos que $\overline{P} := PN/N \in \mathrm{Syl}_p(\overline{G})$. Así, como $\overline{G}$ es p-nilpotente, existe $\overline{H} := H/N$ p-complemento normal tal que

$$\overline{G} = \overline{H} \cdot \overline{P},$$

con $\overline{H} \trianglelefteq \overline{G}$ (luego $H \trianglelefteq G$) y $\left|\overline{H}\right|$ es un p'-número. Luego

$$G/N = (H/N) \cdot (PN/N).$$

Así, $G = HPN = HNP = HP$ ya que $N \leqslant H$. Al ser $H \trianglelefteq G$ y p'-grupo (pues $\overline{H}$ y N también lo son), concluimos que G es p-nilpotente, tal y como queríamos probar.

Por tanto, suponemos que $r = p$ y que N es p-grupo. $\overline{G}$ es el producto mutuamente permutable de los subgrupos A/N y BN/N, por el Lema 1.4.6. Así, por el Teorema 1.4.11, tenemos que existe $E/N \cdot \trianglelefteq G/N$ tal que $E/N \leqslant A/N$ o $E/N \leqslant BN/N$.

En el primer caso llegamos a que $E \trianglelefteq G$ con $E \leqslant A$, luego E verifica las hipótesis del enunciado. En el segundo caso, llegaríamos a que $E \leqslant BN$ y, como $N \leqslant E$ y estamos suponiendo que $N \leqslant A$, por la identidad de Dedekind, tenemos que

$$E = E \cap BN = N(E \cap B) \leqslant (E \cap A)(E \cap B) \leqslant E.$$

Así, $E = (E \cap A)(E \cap B)$ y, por el Lema 1.4.8, ambos factores son mutuamente permutables. Además, E verifica las demás hipótesis del enunciado trivialmente. Luego, en ambos casos, llegamos a que E verifica las hipótesis del teorema.

Si $E < G$, entonces sería p-nilpotente por inducción. Pero $E/N \cdot \trianglelefteq G/N$ y G/N verificaba las hipótesis luego, por el apartado 1, G/N es resoluble y, por tanto, E/N es q-elemental abeliano para algún primo $q \in \mathbb{N}$. Notemos que $q \neq p$ pues, si $q = p$,

al ser N un p-grupo, E debería ser p-grupo también y, como $E \trianglelefteq G$, concluiríamos que $E \leqslant \mathrm{O}_p(G) = N$, luego $E/N = 1$, que es una contradicción pues E/N es normal minimal de G/N.

Como E es p-nilpotente y E/N es un q-grupo, tenemos que $E = QN$ con $Q \in \mathrm{Syl}_q(E)$ y $Q \trianglelefteq E$. Luego Q car $E \trianglelefteq G$ y, por tanto, $Q \trianglelefteq G$ con Q un q-grupo. Así, $Q \leqslant \mathrm{O}_q(G) = 1$ pues $N = \mathrm{O}_p(G) = \mathrm{F}(G)$. Esto nos lleva a que $E = N$, lo cual es una contradicción, pues E/N era normal minimal de G/N.

Así, podemos suponer que $E = G$. Entonces, por ser E/N q-elemental abeliano, si tomamos $Q \in \mathrm{Syl}_q(G)$, por el Lema 1.1.2, tenemos que

$$G = E = QN = Q\mathrm{O}_p(G), \tag{3.1}$$

siendo $Q \cong G/N$ abeliano. Por el Lema 1.4.2, podemos suponer que

$$Q = (Q \cap A)(Q \cap B) \in \mathrm{Syl}_q(G).$$

Además, también podemos suponer que $Q \cap A \neq 1$ o que $Q \cap B \neq 1$ pues, en caso contrario, $G = N = \mathrm{O}_p(G)$ sería un p-grupo y, por tanto, p-nilpotente.

Supongamos que $Q \cap B \neq 1$. Sea $1 \neq x \in Q \cap B$ y sea $E_1 := \langle x \rangle N \trianglelefteq QN = G$ (pues $N \leqslant \langle x \rangle N$ y $\langle x \rangle \trianglelefteq Q$ ya que Q es abeliano). Entonces, como estamos suponiendo que $N \leqslant A$, tenemos que $N \leqslant A \cap E_1$ y $\langle x \rangle \leqslant B \cap E_1$. Luego

$$E_1 = \langle x \rangle N \leqslant (B \cap E_1)(A \cap E_1) \leqslant E_1,$$

de donde deducimos que $E_1 = (E_1 \cap A)(E_1 \cap B)$, siendo el producto mutuamente permutable por el Lema 1.4.8. Concluimos que E_1 verifica las hipótesis del teorema.

Si $Q \cap B = 1$, entonces $Q = Q \cap A \neq 1$, de donde deducimos que $Q \leqslant A$. Además, como estamos suponiendo que $N \leqslant A$, tendríamos que $G = QN \leqslant A$, luego $G = A$. Sea $1 \neq x \in Q$ y sea $E_1 := \langle x \rangle N \trianglelefteq QN = G$ (pues $N \leqslant \langle x \rangle N$ y $\langle x \rangle \trianglelefteq Q$ ya que Q es abeliano). Por tanto, también tenemos que E_1 verifica las hipótesis, pues $E_1 \trianglelefteq G$ y $E_1 \leqslant A$.

En cualquiera de los dos casos, si $E_1 < G$, tenemos que E_1 es p-nilpotente por inducción. Así, tenemos que $E_1 = \langle x \rangle N$ con $N \in \mathrm{Syl}_p(E_1)$ y $\langle x \rangle \in \mathrm{Syl}_q(E_1)$ con $\langle x \rangle \trianglelefteq E_1$. Luego

$$\langle x \rangle \text{ car } E_1 \trianglelefteq G,$$

de donde deducimos que $\langle x \rangle \trianglelefteq G$. Así, tenemos que $\langle x \rangle \leqslant \mathrm{O}_q(G) = 1$, lo cual es una contradicción pues $x \neq 1$. Luego $G = E_1 = N\langle x \rangle$ con x un q-elemento. Así, tenemos que

$\langle x\rangle$ actúa coprimamente sobre N (que es abeliano) luego, por el Teorema 1.1.8, tenemos que

$$N = [N, \langle x\rangle] \times \mathrm{C}_N(\langle x\rangle). \tag{3.2}$$

Notemos que $\mathrm{C}_N(\langle x\rangle) = \mathrm{C}_N(x)$. Además, tenemos que $\mathrm{C}_N(x) \trianglelefteq G = N\langle x\rangle$, ya que $\mathrm{C}_N(x) \trianglelefteq N$ (por (3.2)) y $\mathrm{C}_N(x)$ es normalizado por $\langle x\rangle$. Como $\mathrm{C}_N(x) \leqslant N$, por minimalidad de N, concluimos que $\mathrm{C}_N(x) = 1$ ó N. Si $\mathrm{C}_N(x) = N$, entonces $x \in \mathrm{C}_G(N) = N$, lo cual es una contradicción al ser N un p-grupo y $x \neq 1$ un q-elemento. Luego, necesariamente, concluimos que $\mathrm{C}_N(x) = 1$. Así, como $G = N\langle x\rangle$, por la identidad de Dedekind, tenemos que

$$\mathrm{C}_G(x) = \mathrm{C}_G(x) \cap G = \mathrm{C}_G(x) \cap N\langle x\rangle = \langle x\rangle(\mathrm{C}_G(x) \cap N) = \langle x\rangle \mathrm{C}_N(x) = \langle x\rangle.$$

Como $x \in G$ es un p'-elemento de orden potencia de primo, por hipótesis, tenemos que

$$p^2 \nmid \left|x^G\right| = |G : \mathrm{C}_G(x)| = |N\langle x\rangle : \langle x\rangle| = \frac{|N| \cdot \cancel{|\langle x\rangle|}}{|N \cap \langle x\rangle| \cdot \cancel{|\langle x\rangle|}} = |N|\,,$$

ya que $N \cap \langle x\rangle = 1$, al ser N y $\langle x\rangle$ de órdenes coprimos. Al ser N un p-grupo, necesariamente, tenemos que $|N| = p$ y $N \cong C_p$. Pero, por el segundo teorema de isomorfía, tenemos que

$$\langle x\rangle = \langle x\rangle/(N \cap \langle x\rangle) \cong N\langle x\rangle/N = G/N = \mathrm{N}_G(N)/\mathrm{C}_G(N) \lessapprox \mathrm{Aut}(N) \cong C_{p-1}.$$

Luego $|\langle x\rangle|$ divide a $p-1$ y también divide a $|G|$, lo cual es una contradicción con la hipótesis de que $(p-1, |G|) = 1$. Esto finaliza la prueba del apartado 2.

3. Para finalizar, veamos que los p-subgrupos de Sylow de $G/\mathrm{O}_p(G)$ son elementales abelianos. Como todos son conjugados, basta con ver que existe algún $P/\mathrm{O}_p(G) \in \mathrm{Syl}_p(G/\mathrm{O}_p(G))$ elemental abeliano. Razonaremos por inducción en el orden de G.

Supongamos que $\mathrm{O}_p(G) \neq 1$. Sea $\overline{G} := G/\mathrm{O}_p(G)$. $\overline{G}$ hereda las hipótesis del enunciado luego, por inducción, tenemos que los p-subgrupos de Sylow de $\overline{G}/\mathrm{O}_p(\overline{G})$ son elementales abelianos. Pero $\mathrm{O}_p(\overline{G}) = 1$, lo que prueba la tesis en este caso. Así pues, podemos suponer que $\mathrm{O}_p(G) = 1$. Luego solo tenemos que ver que un p-subgrupo de Sylow de G es elemental abeliano. Ahora bien, como $\mathrm{O}_p(G) = 1$, tenemos que $\mathrm{F}(G) \leqslant \mathrm{O}_{p'}(G)$. Concluimos que $\mathrm{F}(G)$ es p'-grupo y, como $\Phi(G) \leqslant \mathrm{F}(G)$ siempre, necesariamente $\Phi(G)$ debe ser un p'-grupo también.

Supongamos que $\Phi(G) > 1$. Sea $\tilde{G} := G/\Phi(G)$. Entonces, por hipótesis de inducción, los p-subgrupos de Sylow de $\tilde{G}/\mathrm{O}_p(\tilde{G})$ son elementales abelianos. Pero, como

$\mathrm{F}(G)/\Phi(G) = \mathrm{F}(\tilde{G})$ y estamos suponiendo que $\mathrm{O}_p(G) = 1$, deducimos que $\mathrm{O}_p(\tilde{G}) = 1$. Por tanto, tenemos que $\tilde{G}/\mathrm{O}_p(\tilde{G}) = \tilde{G} = G/\Phi(G)$. Así, podemos elegir un p-subgrupo de Sylow de la forma $P\Phi(G)/\Phi(G)$, con $P \in \mathrm{Syl}_p(G)$. Finalmente, por el segundo teorema de isomorfía, tenemos que

$$P\Phi(G)/\Phi(G) \cong P/(P \cap \Phi(G)) = P,$$

pues $P \in \mathrm{Syl}_p(G)$ y $\Phi(G)$ es un p'-grupo. Concluimos que P es elemental abeliano, con lo que queda finalizada la prueba en este caso.

Así, podemos suponer que $\Phi(G) = 1$. Entonces, tenemos que $\mathrm{O}_p(G) = \Phi(G) = 1$. Claramente, podemos suponer que G no es simple pues, en caso contrario, sería isomorfo a un cíclico de orden primo. Por el Lema 1.4.11, podemos escoger $N \cdot \trianglelefteq G$ tal que $N \leqslant A$. Al ser G resoluble, N es q-elemental abeliano para algún número primo $q \in \mathbb{N}$ (con $q \neq p$ pues, en caso contrario, $1 < N \leqslant \mathrm{O}_p(G) = 1$, lo cual sería una contradicción). Además, $N \cap \Phi(G) = 1$ pues $\Phi(G) = 1$. Así, estamos en condiciones de aplicar el apartado 5 del Lema 1.1.4 y podemos afirmar que existe S complemento de N en G, esto es, $G = SN$ con $S \cap N = 1$.

Si $\mathrm{O}_p(S) = 1$, aplicándole la hipótesis de inducción a $\hat{G} := G/N$, los p-subgrupos de Sylow de $\hat{G}/\mathrm{O}_p(\hat{G})$ son elementales abelianos. Pero, por el segundo teorema de isomorfía, tenemos que

$$\hat{G} = G/N = SN/N \cong S/(S \cap N) = S,$$

pues $S \cap N = 1$. Luego $\mathrm{O}_p(\hat{G}) \cong \mathrm{O}_p(S) = 1$ y, por tanto, los p-subgrupos de Sylow de $\hat{G} = G/N$ son elementales abelianos. Es decir, podemos elegir $PN/N \in \mathrm{Syl}_p(G/N)$ que sea elemental abeliano, con $P \in \mathrm{Syl}_p(G)$. Pero, nuevamente por el segundo teorema de isomorfía, tenemos que

$$PN/N \cong P/(P \cap N) = P,$$

pues P es p-grupo y N es p'-grupo. Esto finaliza la prueba en este caso. Así, podemos suponer que $\mathrm{O}_p(S) > 1$. Sea $P \in \mathrm{Syl}_p(S)$ (notemos que, como $|G : S| = |N|$ es un p'-número, realmente P es un p-subgrupo de Sylow de G). Así, tenemos que

$$1 < \mathrm{O}_p(S) \trianglelefteq P,$$

pues $\mathrm{O}_p(S) \trianglelefteq S$ y $P \leqslant S$. Además, P es nilpotente, luego $\mathrm{O}_p(S) \cap \mathrm{Z}(P) \neq 1$.

Luego podemos considerar $Z \cdot \trianglelefteq \mathrm{O}_p(S) \cap \mathrm{Z}(P)$. Al ser $\mathrm{O}_p(S) \cap \mathrm{Z}(P)$ un p-grupo, Z es p-elemental abeliano. Veamos que $Z \leqslant \mathrm{Z}(S)$. Teníamos que G es p-nilpotente por el apartado 2 y, como $S \leqslant G$, S también es p-nilpotente. Luego $S = PT_1$ con $T_1 \trianglelefteq S$ y $|T_1|$

un p'-número. Como $\mathrm{O}_p(S)$ y T_1 son ambos normales en S, concluimos que

$$[T_1, \mathrm{O}_p(S)] \leqslant T_1 \cap \mathrm{O}_p(S) = 1,$$

pues T_1 es p'-grupo. Así, como $Z \leqslant \mathrm{O}_p(S) \cap \mathrm{Z}(P) \leqslant \mathrm{O}_p(S)$, tenemos que

$$[Z, T_1] \leqslant [\mathrm{O}_p(S), T_1] = 1.$$

Como $Z \leqslant \mathrm{Z}(P)$ y $S = PT_1$, concluimos que $Z \leqslant \mathrm{Z}(S)$, para todo $Z \cdot \trianglelefteq \mathrm{O}_p(S) \cap \mathrm{Z}(P)$.

Veamos ahora que $\mathrm{C}_N(Z) \trianglelefteq G = SN$. Por un lado, tenemos que $\mathrm{C}_N(Z) \trianglelefteq N$ pues N es abeliano. Por otro lado, $\mathrm{C}_N(Z) = \mathrm{C}_G(Z) \cap N$ es normalizado por S, pues $Z \leqslant \mathrm{Z}(S)$. Por tanto, $\mathrm{C}_N(Z) \trianglelefteq SN = G$. Pero $\mathrm{C}_N(Z) \leqslant N \cdot \trianglelefteq G$ luego, por minimalidad de N, distinguimos dos casos.

Si $\mathrm{C}_N(Z) = N$, entonces $Z \leqslant \mathrm{Z}(N)$ y ya teníamos que $Z \leqslant \mathrm{Z}(S)$, luego $Z \leqslant \mathrm{Z}(G)$ (pues $G = SN$). Esto implica que $Z \trianglelefteq G$. Pero, por otro lado, vimos que Z era p-grupo. Concluimos que $Z \leqslant \mathrm{O}_p(G) = 1$, lo cual es una contradicción. Así, tenemos que $\mathrm{C}_N(Z) = 1$, para todo $Z \cdot \trianglelefteq \mathrm{O}_p(S) \cap \mathrm{Z}(P)$. Como $N > 1$ era q-elemental abeliano para algún número primo $q \neq p$, podemos considerar un q-elemento $1 \neq x \in N \leqslant A$.

Sea $P_0 \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Entonces, existe un $g \in G$ tal que $P_0 \leqslant P^g$, pues $P \in \mathrm{Syl}_p(G)$. Definimos $M := P_0^{g^{-1}}$ y $n := x^{g^{-1}}$. Entonces, tenemos que $M \leqslant P$ y que $M \in \mathrm{Syl}_p(\mathrm{C}_G(n))$, pues $P_0 \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Así,

$$M \leqslant P \cap \mathrm{C}_G(n) = \mathrm{C}_P(n).$$

Además, $\mathrm{C}_P(n) \leqslant P \in \mathrm{Syl}_p(G)$, luego $\mathrm{C}_P(n)$ es un p-grupo. Por otro lado, teníamos que $M \in \mathrm{Syl}_p(\mathrm{C}_G(n))$. Juntando estos argumentos junto a que

$$M \leqslant \mathrm{C}_P(n) \leqslant \mathrm{C}_G(n),$$

llegamos a que $M = \mathrm{C}_P(n)$. Tenemos un p'-elemento $x \in N \leqslant A$ de orden potencia de primo luego, por hipótesis del enunciado del teorema, tenemos que

$$p^2 \nmid \left|x^G\right| = \left|n^G\right| = |G : \mathrm{C}_G(n)| = \frac{|G|}{|\mathrm{C}_G(n)|}.$$

En particular,

$$p^2 \nmid \left|n^G\right|_p = \frac{|G|_p}{|\mathrm{C}_G(n)|_p} = \frac{|P|}{|M|} = |P : M|,$$

pues $P \in \mathrm{Syl}_p(G)$ y $M \in \mathrm{Syl}_p(\mathrm{C}_G(n))$. Al ser ambos p-grupos, necesariamente $|P : M|$ es una potencia de p, la cual no es divisible por p^2, luego tenemos dos casos: $|P : M| = 1$ ó p.

Si $|P:M|=1$, entonces $P=M=\mathrm{C}_P(n)$. Luego n conmuta con todo P. Como vimos que $Z \leqslant \mathrm{Z}(P)$, en particular, n conmuta con todo Z. Concluimos que $n \in \mathrm{C}_N(Z)=1$, lo cual es una contradicción pues habíamos elegido $n \neq 1$. Luego $|P:M|=p$. Así, tenemos que $M<P$, el cual es nilpotente, luego $M<\mathrm{N}_P(M) \leqslant P$. Necesariamente $P=\mathrm{N}_P(M)$, luego $M \trianglelefteq P$. Veamos que $M \cap Z=1$. Tenemos que

$$M \cap Z \leqslant Z \cdot \trianglelefteq \mathrm{Z}(P) \cap \mathrm{O}_p(S) \leqslant \mathrm{Z}(P),$$

con $\mathrm{Z}(P)$ abeliano. Así, tenemos que $M \cap Z \trianglelefteq \mathrm{Z}(P) \cap \mathrm{O}_p(S)$. Por minimalidad de Z, tenemos dos casos.

Si $M \cap Z = Z$, tendríamos que $Z \leqslant M = \mathrm{C}_P(n)$. Por un razonamiento análogo que hemos hecho anteriormente, concluiríamos que $n \in \mathrm{C}_N(Z)=1$, lo cual sería una contradicción. Así, podemos suponer que $M \cap Z=1$. Además, tenemos que $M<MZ \leqslant P$, pues $Z \leqslant \mathrm{Z}(P)$. Como el índice de P sobre M era p, concluimos que $ZM=P$.

Así, tenemos que $P=Z \times M$ pues $ZM=P$, $M \trianglelefteq P$, $Z \leqslant \mathrm{Z}(P)$ y $M \cap Z=1$. Solo nos queda ver que M es también p-elemental abeliano para finalizar la demostración. Por la identidad de Dedekind, tenemos que

$$\mathrm{Z}(P)=\mathrm{Z}(P) \cap P=\mathrm{Z}(P) \cap MZ=Z(\mathrm{Z}(P) \cap M),$$

pues $Z \leqslant \mathrm{Z}(P)$. Consecuentemente, usando otra vez la identidad de Dedekind, obtenemos que

$$\mathrm{Z}(P) \cap \mathrm{O}_p(S)=\mathrm{O}_p(S) \cap Z(\mathrm{Z}(P) \cap M)=Z(\mathrm{Z}(P) \cap M \cap \mathrm{O}_p(S)), \tag{3.3}$$

ya que $Z \leqslant \mathrm{O}_p(S)$.

Supongamos que $\mathrm{Z}(P) \cap M \cap \mathrm{O}_p(S) \neq 1$. Entonces, como $\mathrm{Z}(P) \cap M \cap \mathrm{O}_p(S) \trianglelefteq \mathrm{O}_p(S) \cap \mathrm{Z}(P)$ (ya que $M \trianglelefteq P$), podríamos tomar $Z_1 \cdot \trianglelefteq \mathrm{O}_p(S) \cap \mathrm{Z}(P)$ tal que $Z_1 \leqslant \mathrm{Z}(P) \cap M \cap \mathrm{O}_p(S) \leqslant M$. Pero vimos que $\mathrm{C}_N(Z_1)=1$, pues se cumplía para todo normal minimal de $\mathrm{O}_p(S) \cap \mathrm{Z}(P)$. Así, tenemos que $Z_1 \leqslant M=\mathrm{C}_P(n)$, luego $n \in \mathrm{C}_N(Z_1)=1$, lo cual es una contradicción.

Luego podemos suponer que $\mathrm{Z}(P) \cap M \cap \mathrm{O}_p(S)=1$ y, por (3.3), tenemos que $Z=\mathrm{Z}(P) \cap \mathrm{O}_p(S)$. Por otro lado, nuevamente por la identidad de Dedekind, tenemos que

$$\mathrm{O}_p(S)=\mathrm{O}_p(S) \cap P=\mathrm{O}_p(S) \cap MZ=Z(\mathrm{O}_p(S) \cap M). \tag{3.4}$$

Si $\mathrm{O}_p(S) \cap M \neq 1$ entonces, como $\mathrm{O}_p(S) \cap M \trianglelefteq P$ (pues $\mathrm{O}_p(S) \trianglelefteq S$ y $P \leqslant S$, luego $\mathrm{O}_p(S)$ es normalizado por P) y P es un p-grupo, concluiríamos que $\mathrm{O}_p(S) \cap M \cap \mathrm{Z}(P) \neq 1$, lo cual es una contradicción. Luego podemos suponer que $\mathrm{O}_p(S) \cap M=1$ y, por (3.4),

que $Z = \mathrm{O}_p(S)$. Sea $T/N := \mathrm{O}_p(G/N)$. Entonces, tenemos que $T \trianglelefteq G = NS$. Así, por la identidad de Dedekind, obtenemos que

$$T = T \cap G = T \cap NS = N(T \cap S), \tag{3.5}$$

ya que $N \leqslant T$. Definiendo $K := T \cap S \trianglelefteq S$, por (3.5) y por el segundo teorema de isomorfía, tenemos que

$$T/N = NK/N \cong K/(K \cap N) = K,$$

pues $K \cap N \leqslant S \cap N = 1$. Luego K es isomorfo a T/N, que es un p-grupo. Concluimos que $K \leqslant \mathrm{O}_p(S) = Z$. Por otra parte, tenemos que

$$\mathrm{O}_p(S)N/N \cong \mathrm{O}_p(S)/(\mathrm{O}_p(S) \cap N) = \mathrm{O}_p(S),$$

donde $\mathrm{O}_p(S) \cap N = 1$ pues son de órdenes coprimos. Luego $\mathrm{O}_p(S)N/N$ es un p-grupo. Además, $\mathrm{O}_p(S)N \trianglelefteq G$ pues $G = NS$ y $N \leqslant N\mathrm{O}_p(S)$. Concluimos que

$$\mathrm{O}_p(G/N) = T/N = KN/N \leqslant ZN/N = \mathrm{O}_p(S)N/N \leqslant \mathrm{O}_p(G/N),$$

pues acabamos de ver que $K \leqslant Z$ y que $ZN/N \leqslant \mathrm{O}_p(G/N)$. Luego $\mathrm{O}_p(G/N) = ZN/N$.

Por último, tenemos que $(PN/N)/(ZN/N) \in \mathrm{Syl}_p(\hat{G}/\mathrm{O}_p(\hat{G}))$ es p-elemental abeliano por inducción sobre $\hat{G} = G/N$. Pero, usando los teoremas de isomorfía, junto a que $Z \leqslant P$, que $P \cap N = 1$ (por ser de órdenes coprimos), que $M \cap Z = 1$ y la identidad de Dedekind, obtenemos que

$$\begin{aligned}(PN/N)/(ZN/N) &\cong PN/ZN = P(ZN)/ZN \cong P/(P \cap ZN)\\ &= P/(Z(P \cap N)) = P/Z = MZ/Z\\ &\cong M/(M \cap Z) = M.\end{aligned}$$

Esto finaliza la prueba. □

Mencionar que el Teorema 3.1.5 fue nuestro punto de partida. Observemos que podemos obtener dicho resultado como un simple corolario del resultado anterior cuando $G = A = B$. Recalcar también que, en el Apéndice A, mostraremos ejemplos sobre algunas ventajas computacionales del resultado anterior y veremos que la hipótesis de que $(p-1, |G|) = 1$ no es superflua (ver Ejemplos A.2.3, A.2.4 y A.2.5).

Nuestro próximo objetivo, en este capítulo, es ver la demostración del Teorema C. Para ello, necesitamos ver unos lemas previos.

Teorema 3.2.3 ([8], A - Teorema 13.6). *Sea G un grupo finito y A un grupo que actúa vía automorfismos sobre G. Sea H/K un factor de composición de G A-invariante. Si H/K no es resoluble, supongamos además que* $\mathrm{Inn}(G) \leqslant \mathrm{Aut}_A(G)$.

1. *Si H/K no es resoluble, entonces $\mathrm{Aut}_A(H/K)$ posee un único normal minimal, el cual es A-isomorfo a H/K.*
2. *Si H/K es resoluble, entonces H/K es p-elemental abeliano para algún número primo $p \in \mathbb{N}$, siendo $\mathrm{O}_p(\mathrm{Aut}_A(H/K)) = 1$.*

En particular, si $p \in \mathbb{N}$ es un número primo divisor de $|H/K|$, en ambos casos tenemos que

$$\mathrm{O}_p(\mathrm{Aut}_A(H/K)) = 1.$$

Nota 3.2.4. En el caso particular de que tengamos $N \cdot \trianglelefteq G$, tenemos que N es un G-factor de composición y se cumple trivialmente que $\mathrm{Inn}(G) \leqslant \mathrm{Aut}_G(G)$ (de hecho, se da la igualdad en este caso). Así, por el teorema anterior, podemos asegurar que si $p \in \mathbb{N}$ es un número primo divisor de $|N|$, entonces $\mathrm{O}_p(\mathrm{Aut}_G(N)) = 1$ y, por la Nota 1.1.7, deducimos que

$$\mathrm{O}_p(G/\mathrm{C}_G(N)) = 1.$$

Este hecho nos será útil posteriormente. Por otro lado, el siguiente resultado que vamos a probar nos da información sobre la estructura de un grupo que actúa fielmente, bajo ciertas condiciones, sobre otro abeliano.

Lema 3.2.5 ([3], Lema 2.4). *Sea $p \in \mathbb{N}$ un número primo y Q un p'-grupo que actúa fielmente sobre N p-elemental abeliano, con $|[N, x]| = p$ para todo $1 \neq x \in Q$. Entonces, tenemos que Q es cíclico.*

Demostración. Supongamos falso el resultado y trabajemos por contraejemplo minimal, de tal manera que elegimos N y Q que no verifiquen el teorema con $|N| + |Q|$ minimal. Notemos que, entonces, N no puede ser cíclico. Efectivamente pues, en caso contrario, teniendo en cuenta que $\mathrm{C}_Q(N) = 1$ (por ser la acción fiel), tendríamos que

$$Q = \mathrm{N}_Q(N)/\mathrm{C}_Q(N) \lessapprox \mathrm{Aut}(N) \cong \mathrm{Aut}(C_p) \cong C_{p-1},$$

pues si suponemos que N es cíclico, al ser p-elemental abeliano por hipótesis, necesariamente tenemos que $N \cong C_p$. Esto supone una contradicción, pues estamos suponiendo que Q no es cíclico.

Así, podemos suponer que N no es cíclico. Claramente, las hipótesis del teorema son heredadas para los subgrupos de Q. Como Q no es cíclico, tenemos que $Q = \langle a_1, a_2, \ldots, a_i \rangle$ con $i \geq 2$.

Sea $Q_0 = \langle a_1, a_2 \rangle$. Entonces, tenemos que $Q_0 \leqslant Q$, luego cumple el teorema por minimalidad de Q. Pero $Q_0 = \langle a_1, a_2 \rangle$ no es cíclico, por tanto tendríamos un contraejemplo de orden inferior al de Q.

Así, podemos suponer que $Q = Q_0 = \langle a, b \rangle$. Como Q actúa coprimamente sobre N abeliano, por el Teorema 1.1.8, tenemos que

$$N = [N, Q] \times \mathrm{C}_N(Q).$$

Supongamos que $\mathrm{C}_N(Q) > 1$. Entonces, tenemos que

$$[x, N] = [x, [N, Q]\mathrm{C}_N(Q)] = [x, [N, Q]] \cdot [x, \mathrm{C}_N(Q)] = [x, [N, Q]],$$

ya que $\mathrm{C}_N(Q)$ normaliza a $[N, Q]$ y centraliza a $x \in Q$. Luego $|[x, [N, Q]]| = |[x, N]| = p$, para todo $1 \neq x \in Q$.

Así, teniendo en cuenta lo anterior junto al hecho de que Q también actúa fielmente sobre $[N, Q]$ (notar que $[N, Q]$ es normalizado por Q), el cual es p-elemental abeliano también (por ser subgrupo de N), llegamos a que Q es cíclico, por minimalidad de N (tenemos que $|[N, Q]| < |N|$, pues estamos suponiendo que $\mathrm{C}_N(Q) > 1$), lo cual es una contradicción.

Luego podemos suponer que $N = [N, Q]$. Veamos que $\mathrm{C}_N(a)$ y $\mathrm{C}_N(b)$ son subgrupos maximales de N (notemos que $\mathrm{C}_N(a), \mathrm{C}_N(b) < N$, pues en caso contrario tendríamos que $[a, N] = 1$ ó $[b, N] = 1$, en contradicción con las hipótesis). Supongamos que existe M tal que $\mathrm{C}_N(a) < M \leqslant N$. Como $\langle a \rangle$ actúa coprimamente sobre N abeliano, nuevamente por el lema de Fitting tenemos que

$$N = [\langle a \rangle, N] \times \mathrm{C}_N(\langle a \rangle).$$

Pero $\mathrm{C}_N(\langle a \rangle) = \mathrm{C}_N(a)$ y $[\langle a \rangle, N] = [a, N]$ pues $N \trianglelefteq Q$. Así, tenemos que

$$N = [a, N] \times \mathrm{C}_N(a), \tag{3.6}$$

donde $|[a, N]| = p$, por hipótesis. Deducimos que $|N : \mathrm{C}_N(a)| = |[a, N]| = p$ pero, como estamos suponiendo que $\mathrm{C}_N(a) < M \leqslant N$, necesariamente tenemos que $M = N$. Por tanto, $\mathrm{C}_N(a) <\cdot\, N$. Un razonamiento análogo sirve para ver que $\mathrm{C}_N(b) <\cdot\, N$. Además, tenemos que

$$\mathrm{C}_N(a) \cap \mathrm{C}_N(b) \leqslant \mathrm{C}_N(Q) = 1,$$

con $\mathrm{C}_N(a) \neq \mathrm{C}_N(b)$ (en caso contrario, tendríamos por (3.6) y la ecuación anterior que $|N| = |[a, N]| = p$ y, por tanto, N sería cíclico, lo cual es una contradicción).

Así, observamos que

$$\mathrm{C}_N(a) < \mathrm{C}_N(a) \times \mathrm{C}_N(b) \leqslant N,$$

donde el primer contenido es estricto debido a que $\mathrm{C}_N(a) \neq \mathrm{C}_N(b)$ junto a que $\mathrm{C}_N(a) \cap \mathrm{C}_N(b) = 1$. Por maximalidad de $\mathrm{C}_N(a)$ en N, concluimos que

$$N = \mathrm{C}_N(a) \times \mathrm{C}_N(b).$$

Veamos ahora que $[a, b] = 1$. Para ello, observamos primeramente que

$$\mathrm{C}_N(a) \times \mathrm{C}_N(b) = N = N^{b^{-1}} = (\mathrm{C}_N(a) \times \mathrm{C}_N(b))^{b^{-1}} = \mathrm{C}_N(a)^{b^{-1}} \times \mathrm{C}_N(b),$$

de donde concluimos que $\mathrm{C}_N(a)^{b^{-1}} = \mathrm{C}_N(a)$. Así, si elegimos $n \in \mathrm{C}_N(a)$, tenemos que

$$n^{[a,b]} = n^{a^{-1}b^{-1}ab} = n^{b^{-1}ab} = (n^{b^{-1}})^{ab} = (n^{b^{-1}})^{b} = n,$$

donde la segunda igualdad se da debido a que $n \in \mathrm{C}_N(a)$ y la cuarta se da porque si $n \in \mathrm{C}_N(a)$, entonces $n^{b^{-1}} \in \mathrm{C}_N(a)^{b^{-1}} = \mathrm{C}_N(a)$. Por tanto, $[a, b]$ centraliza a todo elemento de $\mathrm{C}_N(a)$. Un razonamiento análogo sirve para ver que $[a, b]$ también centraliza a todo elemento de $\mathrm{C}_N(b)$, por lo que concluimos que $[a, b]$ centraliza a todo elemento de N y, por tanto, $[a, b] \in \mathrm{C}_Q(N) = 1$.

Así, tenemos que $Q = \langle a, b \rangle$ es abeliano. Notemos que $\mathrm{C}_N(ab) < \cdot\, N$, por un razonamiento totalmente análogo al visto anteriormente (observar que si $ab = 1$, entonces $a = b^{-1}$ y, por tanto, $Q = \langle a, b \rangle$ sería cíclico, lo cual es una contradicción).

Elijamos $n \in \mathrm{C}_N(ab)$. Entonces, operando en pasos, tenemos que

$$\begin{array}{ll} (1) \quad n^{-1}abn = ab, & (2) \quad n^{-1}ann^{-1}bn = ab, \\ (3) \quad a^{-1}n^{-1}an = bn^{-1}b^{-1}n, & (4) \quad [a, n] = [b^{-1}, n]. \end{array} \tag{3.7}$$

Pero, en particular, $n \in N = \mathrm{C}_N(a) \times \mathrm{C}_N(b)$, luego $n = c_a c_b$ con $c_a \in \mathrm{C}_N(a)$ y $c_b \in \mathrm{C}_N(b)$. Por un lado, vemos que

$$[a, n] = [a, c_a c_b] = [a, c_b] = (c_b^{-1})^a c_b \in \mathrm{C}_N(b),$$

pues $(c_b^{-1})^a \in \mathrm{C}_N(b)^a = \mathrm{C}_N(b^a) = \mathrm{C}_N(b)$ al ser Q abeliano. Pero, por otro lado, tenemos que

$$[b^{-1}, n] = [b^{-1}, c_a c_b] = [b^{-1}, c_b c_a] = [b^{-1}, c_a] = (c_a^{-1})^{b^{-1}} c_a \in \mathrm{C}_N(a),$$

pues $(c_a^{-1})^{b^{-1}} \in \mathrm{C}_N(a)^{b^{-1}} = \mathrm{C}_N(a)$ al ser Q abeliano y $c_a c_b = c_b c_a$, por formar $\mathrm{C}_N(a)$ y $\mathrm{C}_N(b)$ un producto directo. Por (3.7), concluimos que $[a,n] = [b^{-1},n] \in \mathrm{C}_N(a) \cap \mathrm{C}_N(b) = 1$, por lo que $n \in \mathrm{C}_N(a) \cap \mathrm{C}_N(b^{-1}) = \mathrm{C}_N(a) \cap \mathrm{C}_N(b) = 1$. Deducimos que $1 = \mathrm{C}_N(ab) < \cdot N$.

Fijándonos en que $\mathrm{C}_N(ab) = 1 < [ab,N]$ (pues $|[ab,N]| = p$, por las hipótesis) y en que $[ab,N] \leqslant N$ (pues $N^{ab} = N$), por maximalidad de $\mathrm{C}_N(ab)$ en N, tenemos que $N = [ab,N]$ y, por tanto, N sería cíclico. Esta contradicción completa la demostración.□

En la prueba del siguiente resultado es necesario el uso de la clasificación de los grupos finitos simples, además de la teoría de caracteres.

Lema 3.2.6 ([6], Proposición 3). *Sea $p \in \mathbb{N}$ un número primo. Si p divide a $|\mathrm{C}_G(x)|$, para todo $x \in G$, entonces G no es simple y no abeliano.*

Mencionar que, actualmente, estamos trabajando en una posible generalización del lema anterior para elementos de orden potencia de primo, con el objetivo de generalizar el Teorema C. En este contexto, hemos obtenido algún caso particular como, por ejemplo, cuando p es el mayor número primo que divide a $|G|$.

Estamos ya en disposición de probar el Teorema C. Destacar que, a continuación de éste, generalizaremos directamente su segunda afirmación para p'-elementos de orden potencia de primo, evitando el uso de la clasificación.

Teorema C ([3], Teorema 1.3). *Sea G el producto mutuamente permutable de los subgrupos A y B. Supongamos que para todo p'-elemento $x \in A \cup B$, $\left|x^G\right|$ no es divisible por p^2. Entonces, el orden de los p-subgrupos de Sylow de todo factor principal de G es a lo sumo p. En particular, si G es p-resoluble, tenemos que G es p-superresoluble.*

Demostración. Supongamos falso el teorema y sea G un contraejemplo minimal. Claramente, las hipótesis del teorema son heredadas por los cocientes de G. Además, la clase $\mathfrak{H}_p$ de los grupos que cumplen que todos sus factores principales tienen p-subgrupos de Sylow de orden a lo sumo p es una formación. Por todo esto, podemos asumir que existe un único $N \cdot \trianglelefteq G$ (ver Nota 1.2.20) tal que $N \leqslant A$ o $N \leqslant B$ (por el Teorema 1.4.11), que los factores principales de G/N tienen p-subgrupos de Sylow de orden a lo sumo p y que los p-subgrupos de Sylow de N tienen orden al menos p^2. Supongamos que N no es resoluble. Entonces, tenemos que

$$N \cong N_1 \times N_2 \times \cdots \times N_t, \tag{3.8}$$

con N_i isomorfos entre sí, simples y no abelianos, para todo $1 \leq i \leq t$.

Si p dividiese a $|\mathrm{C}_{N_i}(x_i)|$ para todo $x_i \in N_i$ entonces, por el Lema 3.2.6, tendríamos que N_i no es simple y no abeliano, lo cual es una contradicción. Así, tenemos que, para cada i, existe $x_i \in N_i$ tal que p no divide a $|\mathrm{C}_{N_i}(x_i)|$. Luego $\mathrm{C}_{N_i}(x_i)$ es un p'-grupo, para todo i.

Sea $x = x_1 x_2 \cdots x_t \in N$, con $x_i \in N_i$. Como cada $x_j \in \mathrm{C}_{N_j}(x_j)$ trivialmente, tenemos que todos los x_i son p'-elementos. Por tanto, x es un p'-elemento contenido en A o B. Así, por hipótesis, sabemos que p^2 no divide a $\left|x^G\right|$ y, por el Lema 1.3.1 (1), tampoco divide a $\left|x^N\right|$. Pero, por (3.8), vemos que

$$\mathrm{C}_N(x) = \mathrm{C}_{N_1}(x_1) \times \mathrm{C}_{N_2}(x_2) \times \cdots \times \mathrm{C}_{N_t}(x_t).$$

Como cada factor directo es un p'-grupo, concluimos que $\mathrm{C}_N(x)$ es un p'-grupo también. Como p^2 no divide a $\left|x^N\right| = |N : \mathrm{C}_N(x)|$, tenemos que $|N|_p \leq p$, lo cual es una contradicción.

Luego podemos asumir que N es resoluble y, por tanto, q-elemental abeliano para algún número primo $q \in \mathbb{N}$. Si $q \neq p$, entonces los p-subgrupos de Sylow de N tendrían orden menor o igual que p, lo cual es una contradicción. Así, tenemos que N es un p-grupo abeliano. Además, podemos asumirlo no central, pues si $N \leqslant \mathrm{Z}(G)$, entonces N sería cíclico y volveríamos a tener la misma contradicción.

Sea $K := \mathrm{C}_G(N) \trianglelefteq G$ y tomemos $Z/K \cdot \trianglelefteq G/K$ tal que $Z/K \leqslant AK/K$, el cual sabemos que existe por el Teorema 1.4.11. Si Z/K fuese p-grupo entonces, por la Nota 3.2.4, tendríamos que

$$Z/K \leqslant \mathrm{O}_p(G/K) = 1,$$

lo cual es una contradicción. Así, podemos asumir que Z/K no es p-grupo.

Sea $1 \neq \overline{x} := xK \in Z/K \leqslant AK/K$ (luego $x \notin K$) un p'-elemento. Podemos escoger $x \in A$ que sea p'-elemento. Así, tenemos que $\langle x \rangle$ actúa coprimamente sobre N abeliano luego, por el Teorema 1.1.8, obtenemos que

$$N = [N, \langle x \rangle] \times \mathrm{C}_N(\langle x \rangle) = [N, x] \times \mathrm{C}_N(x),$$

pues $N \trianglelefteq G$. Además, notemos que $\mathrm{C}_N(x) \neq N$, pues $x \notin K$. Ahora, observando que

$$|N : \mathrm{C}_N(x)| = |N : \mathrm{C}_G(x) \cap N| = |N\mathrm{C}_G(x) : \mathrm{C}_G(x)| \;\big|\; |G : \mathrm{C}_G(x)|,$$

deducimos que

$$|[N, x]| = \frac{|N|}{|\mathrm{C}_N(x)|} = |N : \mathrm{C}_N(x)| \;\big|\; |G : \mathrm{C}_G(x)| = \left|x^G\right|.$$

Pero como, por hipótesis, tenemos que p^2 no divide a $\left|x^G\right|$, concluimos que $|[N,x]| = p$ (pues $[N,x]$ es p-grupo, al ser $[N,x] \leqslant N$ y $\mathrm{C}_N(x) \neq N$).

Observemos que $[N,x] = [N,\overline{x}]$ luego, si tomamos $\overline{Q} := QK/K \in \mathrm{Syl}_q(Z/K)$ con $q \neq p$, tenemos que $|[N,\overline{x}]| = p$, para todo $1 \neq \overline{x} \in \overline{Q}$. Además, $\overline{Q}$ actúa fielmente sobre N p-elemental abeliano. Así, se cumplen las hipótesis del Lema 3.2.5 y podemos afirmar que $\overline{Q}$ es cíclico para todo $\overline{Q} \in \mathrm{Syl}_q(Z/K)$.

Por otro lado, cualquier cociente de G hereda las hipótesis del teorema y, por tanto, verifica la tesis. Así, si tomamos un p-subgrupo de Sylow de Z/K, tenemos que es cíclico (pues Z/K es normal minimal de G/K, luego sus p-subgrupos de Sylow tienen orden a lo sumo p). Por tanto, por el Teorema 1.2.17, tenemos que Z/K es metacíclico y, como consecuencia, es resoluble. Así, tenemos que

$$(Z/K)' \text{ car } Z/K \trianglelefteq G/K,$$

luego $(Z/K)' \trianglelefteq G/K$ y, por minimalidad de Z/K, concluimos que $(Z/K)' = 1$ (pues $(Z/K)' < Z/K$, al ser Z/K resoluble). Deducimos que Z/K es abeliano y, por tanto, es producto directo de sus subgrupos de Sylow, los cuales son cíclicos y de órdenes coprimos. Concluimos pues que Z/K es cíclico.

Pero Z/K es normal minimal de G/K, además de ser cíclico, luego es q-elemental abeliano para algún número primo $q \in \mathbb{N}$ ($q \neq p$, pues Z/K no era p-grupo). Necesariamente, deducimos que

$$\langle xK \rangle = Z/K \cong C_q,$$

con $x \notin K$ y $\mathrm{o}(xK) = q$. Luego podemos asumir que $x \in Z$ es un q-elemento, con $q \neq p$. Así, tenemos que $\langle x \rangle$ actúa coprimamente sobre N abeliano luego, por el Teorema 1.1.8, tenemos que

$$N = [N,x] \times \mathrm{C}_N(x), \tag{3.9}$$

con $N \neq \mathrm{C}_N(x)$ (pues $x \notin K$). Como hemos visto anteriormente, podemos afirmar que $|[N,x]| = p$. Pero, como $K \leqslant K\langle x \rangle \leqslant Z$, concluimos que $Z = K\langle x \rangle$, pues $|Z/K| = q$ y $x \notin K$. Así, al ser $Z = K\langle x \rangle$, deducimos que $\mathrm{C}_N(Z) = \mathrm{C}_N(x)$.

Pero $\mathrm{C}_N(Z) \trianglelefteq G$ y $\mathrm{C}_N(Z) \leqslant N$, luego tenemos que $\mathrm{C}_N(x) = 1$ ó N. El segundo caso queda descartado, pues $x \notin K$. Esto implica que $\mathrm{C}_N(x) = 1$ y, por (3.9), tenemos que $|N| = p$. Esta contradicción finaliza la prueba del teorema. □

Como hemos comentado anteriormente, vamos a ver que podemos generalizar, de forma elemental, la segunda afirmación del resultado anterior para p'-elementos de orden potencia de primo.

Teorema D. *Sea G el producto mutuamente permutable de los subgrupos A y B. Supongamos que para todo p'-elemento $x \in A \cup B$ de orden potencia de primo, $\left|x^G\right|$ no es divisible por p^2. Entonces, si G es p-resoluble, tenemos que G es p-superresoluble.*

DEMOSTRACIÓN. Lo probraremos por inducción sobre $|G|$. Notemos que G no puede ser simple ya que, en caso contrario, al ser G p-resoluble por hipótesis, G sería p'-grupo (en ese caso ya estaría, pues sería p-superresoluble trivialmente) o p-grupo. Si fuese un p-grupo simple, entonces sería isomorfo a un cíclico de orden p y, por tanto, p-superresoluble.

Así, asumimos que G no es simple. Como vimos que la clase de los grupos p-superresolubles es una formación saturada y tenemos que los cocientes de G heredan las hipótesis del teorema (luego verifican la tesis), por la Nota 1.2.20, podemos asumir que existe un único $N \cdot \trianglelefteq G$ ($N < G$, pues G no es simple) y que $\Phi(G) = 1$. Por tanto, al ser G p-resoluble, por unicidad de N como normal minimal de G, tenemos dos casos: que N sea p-grupo o p'-grupo. Si N fuese p'-grupo, al verificar la tesis del teorema G/N por inducción, ya tendríamos que G es p-superresoluble.

Así, podemos asumir que N es un p-grupo y, por ser normal minimal de G, es p-elemental abeliano. Como teníamos que $\Phi(G) = 1$ y G es p-resoluble con $\mathrm{O}_{p'}(G) = 1$ (si fuese $\mathrm{O}_{p'}(G) > 1$, tendríamos que $N \leqslant \mathrm{O}_{p'}(G)$, por unicidad de N como normal minimal de G, lo cual sería una contradicción), por el Lema 1.2.3, podemos afirmar que $\mathrm{F}(G) = \mathrm{Socle}(G) = N$. Además, $\mathrm{O}_p(G) \leqslant \mathrm{F}(G) = N$ y, por otro lado, tenemos que $N \leqslant \mathrm{O}_p(G)$, por ser N un p-grupo normal de G. Es más, $N \leqslant \mathrm{C}_G(N)$, por ser N abeliano y, por el Lema 1.2.9, tenemos que

$$\mathrm{C}_G(N) = \mathrm{C}_G(\mathrm{O}_p(G)) \leqslant \mathrm{O}_p(G) = N,$$

con lo que concluimos que

$$N = \mathrm{O}_p(G) = \mathrm{F}(G) = \mathrm{C}_G(N) = \mathrm{Socle}(G).$$

Sea $Z/N \cdot \trianglelefteq G/N$ tal que $Z/N \leqslant AN/N$ o $Z/N \leqslant BN/N$ (sabemos que existe por el Teorema 1.4.11). Supongamos que $Z/N \leqslant AN/N$. Así, por la identidad de Dedekind, tenemos que

$$Z = Z \cap AN = N(Z \cap A). \tag{3.10}$$

Claramente, al ser Z/N normal minimal de G/N p-resoluble, tenemos que Z/N es p-grupo o p'-grupo. El primer caso queda descartado, pues en caso contrario tendríamos que

$$Z/N \leqslant \mathrm{O}_p(G/N) = \mathrm{O}_p(G/\mathrm{O}_p(G)) = 1,$$

lo cual es una contradicción. Así, podemos asumir que Z/N es un p'-grupo. Sea $Q \in \mathrm{Syl}_q(A \cap Z)$, con $q \neq p$. Entonces, por (3.10) (N es p-grupo), tenemos que $Q \in \mathrm{Syl}_q(Z)$, luego

$$Q = Q/(Q \cap N) \cong QN/N \in \mathrm{Syl}_q(Z/N).$$

Así, al ser Q isomorfo a un subgrupo de Z/N (el cual actúa fielmente sobre N, pues $N = \mathrm{C}_G(N)$), tenemos que Q actúa fielmente sobre N, el cual es p-elemental abeliano. Sea $1 \neq a \in Q \leqslant A \cap Z \leqslant A$. Entonces, tenemos que $\langle a \rangle$ actúa coprimamente sobre N abeliano luego, por el Teorema 1.1.8, concluimos que

$$N = [N, \langle a \rangle] \times \mathrm{C}_N(\langle a \rangle) = [N, a] \times \mathrm{C}_N(a), \tag{3.11}$$

pues $N \trianglelefteq G$. Por hipótesis, tenemos que p^2 no divide a $\left|a^G\right| = |G : \mathrm{C}_G(a)|$ pero tenemos que $|N : \mathrm{C}_N(a)|$ divide a $|G : \mathrm{C}_G(a)|$, luego p^2 no divide a $\frac{|N|}{|\mathrm{C}_N(a)|} = |[N, a]|$ (por (3.11)). Como $[N, a] \leqslant N$, deducimos que $[N, a]$ es un p-grupo también, luego $|[N, a]| = 1$ ó p.

Claramente, el primer caso no se puede dar pues, si se diese, entonces $N = \mathrm{C}_N(a)$ por (3.11), luego $a \in \mathrm{C}_G(N) = N$ y es una contradicción, al ser N un p-grupo y a un p'-elemento no trivial. Por tanto, tenemos que $|[N, a]| = p$, para todo $1 \neq a \in Q$, el cual actúa fielmente sobre N p-elemental abeliano. Por el Lema 3.2.5, deducimos que Q es cíclico, para todo $Q \cong QN/N \in \mathrm{Syl}_q(Z/N)$. Así, Z/N tiene todos sus subgrupos de Sylow cíclicos y, por el Teorema 1.2.17, Z/N es metacíclico.

Por un razonamiento visto con anterioridad, podemos concluir que que Z/N es cíclico. Pero Z/N es normal minimal de G/N, además de ser cíclico, luego es q-elemental abeliano para algún número primo $q \in \mathbb{N}$ ($q \neq p$, pues Z/N no era p-grupo). Necesariamente, deducimos que

$$\langle xN \rangle = Z/N \cong C_q,$$

con $x \notin N$ y $\mathrm{o}(xN) = q$. Podemos asumir que $x \in Z$ es un q-elemento con $q \neq p$. De hecho, por (3.10), tenemos que $x \in A \cap Z$, pues N es p-grupo. Así, tenemos que $\langle x \rangle$ actúa coprimamente sobre N abeliano luego, por el Teorema 1.1.8, tenemos que

$$N = [N, x] \times \mathrm{C}_N(x). \tag{3.12}$$

Por un razonamiento ya visto anteriormente, podemos afirmar que $|[N, x]| = p$. Pero, como $N \leqslant N\langle x \rangle \leqslant Z$, concluimos que $Z = N\langle x \rangle$, pues $|Z/N| = q$ y $x \notin N$. Así, al ser $Z = N\langle x \rangle$ con N abeliano, deducimos que $\mathrm{C}_N(Z) = \mathrm{C}_N(x)$.

Pero $\mathrm{C}_N(Z) \trianglelefteq G$ y $\mathrm{C}_N(Z) \leqslant N$, luego tenemos que $\mathrm{C}_N(x) = 1$ ó N. El segundo caso queda descartado, pues $x \notin N = \mathrm{C}_G(N)$. Esto implica que $\mathrm{C}_N(x) = 1$ y, por (3.12),

tenemos que $|N| = p$. Así, como G/N verificaba la tesis del teorema por inducción, tenemos que G/N es p-superresoluble con N cíclico de orden p, luego G es p-superresoluble. Esto finaliza la prueba. □

Finalizamos este capítulo con una consecuencia de los Teoremas B y D.

Teorema E. *Sea G el producto mutuamente permutable de los subgrupos A y B. Supongamos que para todo número primo $p \in \mathbb{N}$ y para todo p'-elemento $x \in A \cup B$ de orden potencia de primo, $\left|x^G\right|$ no es divisible por p^2. Entonces, tenemos que G es superresoluble.*

Demostración. Tomemos $p \in \mathbb{N}$ el menor número primo que divide a $|G|$. Entonces, está claro que $(p-1, |G|) = 1$. Así, estamos en condiciones de aplicar el Teorema B y, por tanto, podemos afirmar que G es resoluble. Luego G es p-resoluble para todo $p \in \mathbb{N}$ divisor de $|G|$. Aplicando el Teorema D, deducimos que G es p-superresoluble para todo $p \in \mathbb{N}$ divisor de $|G|$. Esto implica que G es superresoluble. □

Observemos que podemos obtener el Corolario 3.1.10 como consecuencia directa de nuestro último resultado.

Capítulo 4

Grupos factorizados y tamaños de clases de conjugación potencias de primos

Recordemos que el objetivo de este capítulo es probar diversos resultados sobre la estructura de un grupo factorizado, pero esta vez suponiendo que los tamaños de clase de ciertos elementos de los factores son potencias de primos.

4.1. Introducción

En 1953, R. Baer (ver [2]) caracterizó todos los grupos finitos tales que todo elemento de orden potencia de primo de G tiene tamaño de clase potencia de primo.

Teorema 4.1.1 ([2], Teorema). *Sea G un grupo finito. Entonces, todo elemento de orden potencia de primo de G tiene tamaño de clase potencia de primo si, y solo si, G es el producto directo de los grupos $G_1, G_2, \ldots, G_n$, cumpliendo las siguientes condiciones:*

1. *G_i y G_j son de órdenes coprimos, para $i \neq j$.*
2. *Si G_i no es un p-grupo, entonces $|G_i|$ es divisible exactamente por dos primos distintos, siendo sus subgrupos de Sylow abelianos.*

En 1990, Chillag y Herzog (ver [6]) vieron qué información estructural adicional se podía obtener si se consideraba que los tamaños de clase eran potencias de primos para todo elemento de G.

Teorema 4.1.2 ([6], Teorema 2). *Sea G un grupo finito. Entonces, $\left|x^G\right|$ es potencia de primo para todo $x \in G$ si, y solo si, G es nilpotente con a lo sumo un subgrupo de Sylow no abeliano o*

$$G = A \times P\mathrm{O}_q(G),$$

siendo A un $\{p,q\}'$-subgrupo abeliano de G, $P \in \mathrm{Syl}_p(G)$ no normal en G y $P \cap P^g = \mathrm{O}_p(G)$, para cada $g \in G \setminus \mathrm{N}_G(P)$.

Actualmente, estamos trabajando en una posible extensión de ambos teoremas a grupos factorizados como producto de dos subgrupos. De hecho, como la prueba que dio Baer del Teorema 4.1.1 es bastante complicada, estamos intentando encontrar una demostración alternativa más sencilla y que se extienda a grupos factorizados. En esta línea, hemos obtenido el siguiente resultado original, el cual probaremos en la siguiente sección.

Teorema F. *Sea $G = AB$ un grupo finito. Supongamos que para todo elemento $x \in A \cup B$ de orden potencia de primo, $\left|x^G\right|$ es potencia de primo. Entonces, tenemos que $G \in \mathfrak{MA}$, es decir, $G/\mathrm{F}(G)$ es abeliano.*

Observemos que no hemos necesitado ninguna condición de permutabilidad sobre los factores, a diferencia de otros resultados de capítulos anteriores.

Por otro lado, antes de probar el Teorema 4.1.2, Chillag y Herzog vieron (ver [6]) qué información estructural se podía obtener, no solamente si los tamaños de clase eran potencias de primos, sino si eran todos potencias de un mismo número primo $p \in \mathbb{N}$.

Teorema 4.1.3 ([6], Observación (3)). *Sea G un grupo finito. Entonces, $\left|x^G\right|$ es potencia de un mismo número primo $p \in \mathbb{N}$ para todo elemento $x \in G$ si, y solo si, G es p-descomponible con $\mathrm{O}_{p'}(G)$ abeliano.*

Siguiendo en la línea de intentar generalizar el Teorema 4.1.1, hemos generalizado el Teorema 4.1.3, obteniendo el siguiente resultado original, el cual es el segundo objetivo del presente capítulo.

Teorema G. *Sea $G = AB$ un grupo finito. Entonces, $\left|x^G\right|$ es potencia de un mismo número primo $p \in \mathbb{N}$ para todo elemento $x \in A \cup B$ de orden potencia de primo si, y solo si, G es p-descomponible con $\mathrm{O}_{p'}(G)$ abeliano.*

Notemos que, en el contexto de los tres teoremas anteriores, un factor directo es abeliano si, y solo si, es central. Si nos fijamos en el Teorema 2.1.1, en estas hipótesis, se

vislumbra en cierto modo cómo la estructura aritmética de $\left|x^G\right|$ afecta a la centralidad de los factores directos de un grupo p-descomponible.

Destacar que, actualmente, también estamos trabajando en una posible generalización del Teorema G, considerando tamaños de clase π-números, para todo elemento de orden potencia de primo de los factores. De tener éxito, generalizaríamos el siguiente resultado de Chillag y Herzog:

Teorema 4.1.4 ([6], Observación (4)). *Sea G un grupo finito. Entonces, $\left|x^G\right|$ es un π-número para todo elemento $x \in G$ si, y solo si,*

$$G = G_1 \times G_2,$$

con G_1 un π-grupo y G_2 un π'-grupo abeliano.

Por último, mencionar que siguiendo la línea de una posible generalización del Teorema 4.1.1, hemos obtenido otros resultados originales, que suponen un avance en la consecución de nuestro objetivo, los cuales no incluímos en la presente memoria por extensión. Algunos de estos resultados serán presentados en el Tercer Congreso de Jóvenes Investigadores de la RSME (ver [10]).

4.2. Resultados centrales

El primer objetivo de esta sección es ver la prueba del siguiente resultado.

Teorema F. *Sea $G = AB$ un grupo finito. Supongamos que para todo elemento $x \in A \cup B$ de orden potencia de primo, $\left|x^G\right|$ es potencia de primo. Entonces, tenemos que $G \in \mathfrak{MA}$, es decir, $G/\mathrm{F}(G)$ es abeliano.*

Demostración. Primeramente, veamos que G es resoluble por inducción sobre $|G|$. Sea $p \in \mathbb{N}$ un número primo tal que p divide a $|A|$. Entonces, por el teorema de Cauchy, existe $1 \neq x \in A$ tal que $\mathrm{o}(x) = p$. Por hipótesis, tenemos que $\left|x^G\right|$ es potencia de primo. Entonces, por el Teorema 1.3.3, tenemos que $H := \langle x^G \rangle$ es un subgrupo normal y resoluble de G.

Notemos que $H > 1$, pues $1 \neq x \in H$. Si $H = G$, entonces ya tendríamos que G es resoluble. Así, podemos suponer que $H < G$. Sea $\overline{G} := G/H = (AH/H)(BH/H)$. $\overline{G}$ hereda la hipótesis de que todo elemento de $AH/H \cup BH/H$ de orden potencia de primo tiene tamaño de clase potencia de primo. Por tanto, por hipótesis de inducción, tenemos

que $\overline{G}$ es resoluble. Aplicando la propiedad extensiva de los grupos resolubles, tenemos que G es resoluble.

Veamos ahora que $G/\mathrm{F}(G)$ es abeliano. Claramente, al ser ya G resoluble, podemos suponer que G no es simple. Sea G un contraejemplo minimal. Como los cocientes de G heredan las hipótesis del teorema y vimos que la clase $\mathfrak{MA}$ es una formación saturada, al ser G resoluble, por la Nota 1.2.20, podemos suponer que $\Phi(G) = 1$ y que existe un único $N \cdot \trianglelefteq G$ tal que

$$N = \mathrm{O}_p(G) = \mathrm{F}(G) = \mathrm{C}_G(N),$$

con $p \in \mathbb{N}$ un número primo divisor de $|G|$. Así, por el apartado 5 del Lema 1.1.4, tenemos que existe $T \leqslant G$ tal que $G = TN$ con $T \cap N = 1$. Veamos que T es un p'-grupo o, equivalentemente, que $N \in \mathrm{Syl}_p(G)$ y, por tanto, tendremos que $T \in \mathrm{Hall}_{p'}(G)$.

Por el Lema 1.4.2, sabemos que existe $P \in \mathrm{Syl}_p(G)$ tal que $P = (P \cap A)(P \cap B)$. Sea $a \in A \cap P$. Entonces, por hipótesis, tenemos que $\left|a^G\right|$ es potencia de primo. Ahora, distinguimos dos casos. Si $\left|a^G\right|$ es un p-número, por el Lema 1.3.2, tenemos que $a \in \mathrm{O}_p(G)$. Por otro lado, si $\left|a^G\right|$ es un p'-número, tenemos que $\mathrm{C}_G(a)$ contiene a algún p-subgrupo de Sylow de G, el cual contiene a $N = \mathrm{O}_p(G)$ y, por tanto, $a \in \mathrm{C}_G(\mathrm{O}_p(G)) = \mathrm{C}_G(N) = N = \mathrm{O}_p(G)$. Así, concluimos que $P \cap A \leqslant N$. Análogamente, podemos ver que $P \cap B \leqslant N$. Deducimos que $P = N$ y, por tanto, que $N \in \mathrm{Syl}_p(G)$.

Por tanto, tenemos que $T \in \mathrm{Hall}_{p'}(G)$. Por el Lema 1.4.3, podemos suponer que $T = (T \cap A)(T \cap B)$. Nuevamente por el Lema 1.4.2, podemos considerar $R \in \mathrm{Syl}_r(T)$ prefactorizado, donde $r \neq p$, $r \in \mathbb{P}$. Así, tenemos que

$$R = (R \cap T \cap A)(R \cap T \cap B) = (R \cap A)(R \cap B).$$

Sea $1 \neq x \in R \cap A$. Sabemos, por hipótesis, que $\left|x^G\right|$ es potencia de primo. Si $\left|x^G\right|$ es potencia de un primo distinto de p, por un razonamiento visto anteriormente concluiríamos que $x \in N$, lo cual es una contradicción, pues x es p'-elemento no trivial y N es un p-grupo. Por tanto, tenemos que $\left|x^G\right|$ es una potencia de p. Así, sabemos que existe un p'-subgrupo de Hall de G contenido en $\mathrm{C}_G(x)$, es decir, existe $g \in G$ tal que $T^g \leqslant \mathrm{C}_G(x)$. Pero, como $G = TN$, podemos suponer que $g := n \in N$. Por tanto, tenemos que

$$x \in \mathrm{C}_G(T^n) = \mathrm{C}_G(T)^n = \{n^{-1}cn \ : \ c \in \mathrm{C}_G(T)\} \subseteq N\mathrm{C}_G(T)N = N\mathrm{C}_G(T),$$

pues $N \trianglelefteq G$. Luego $R \cap A \subseteq N\mathrm{C}_G(T)$. Análogamente, podemos ver que $R \cap B \subseteq N\mathrm{C}_G(T)$ y, por tanto, $R \subseteq N\mathrm{C}_G(T)$. Notemos que podemos repetir el mismo argumento para todo

número primo $r \in \mathbb{N}$ divisor de $|T|$. Ahora, consideremos

$$M \coloneqq \langle R \in \mathrm{Syl}_r(T) \ : \ R \text{ es prefactorizado, con } r \Big| \ |T| \rangle \leqslant T.$$

Por lo que acabamos de ver, tenemos que $M \leqslant N\mathrm{C}_G(T)$. Veamos que M es abeliano. Tenemos que

$$[M, M] \leqslant [M, N\mathrm{C}_G(T)] = [M, \mathrm{C}_G(T)] \cdot [M, N] = [M, N] \leqslant N,$$

pues M es centralizado por $\mathrm{C}_G(T)$ y N es normalizado por M y $\mathrm{C}_G(T)$. Así, vemos que

$$[MN/N, MN/N] = [M, M]N/N = 1,$$

luego MN/N es abeliano. Pero $MN/N \cong M/(M \cap N) = M$, pues M y N son de órdenes coprimos. Esto implica que M es abeliano y, por tanto, producto directo de sus subgrupos de Sylow. Pero todo subgrupo de Sylow de M lo es de T y, por tanto,

$$|M| = \prod_{r \in \pi(T)} |R| = |T|\,,$$

con lo que concluimos que $M = T$ es abeliano. Finalmente, por el segundo teorema de isomorfía, tenemos que

$$G/N = TN/N \cong T/(T \cap N) = T,$$

el cual es abeliano, luego $G' \leqslant N = \mathrm{F}(G)$ y, por tanto, $G/\mathrm{F}(G)$ es abeliano. Esto finaliza la prueba. □

Finalizamos este capítulo viendo la prueba del Teorema G.

Teorema G. *Sea $G = AB$ un grupo finito. Entonces, $\left|x^G\right|$ es potencia de un mismo número primo $p \in \mathbb{N}$ para todo elemento $x \in A \cup B$ de orden potencia de primo si, y solo si, G es p-descomponible con $\mathrm{O}_{p'}(G)$ abeliano.*

Demostración. Supongamos que G es p-descomponible con $\mathrm{O}_{p'}(G)$ abeliano. Sea $x \in G$ de orden potencia de primo. Si $\mathrm{o}(x)$ es un p-número, entonces $x \in \mathrm{O}_p(G)$, pues es el único p-subgrupo de Sylow de G. Por tanto, tenemos que

$$\mathrm{O}_{p'}(G) \leqslant \mathrm{C}_G(x) \leqslant G,$$

pues $[\mathrm{O}_p(G), \mathrm{O}_{p'}(G)] = 1$. Luego $\left|x^G\right| = |G : \mathrm{C}_G(x)|$ divide a $\left|G : \mathrm{O}_{p'}(G)\right| = |\mathrm{O}_p(G)|$, el cual es un p-número. Por otro lado, si $\mathrm{o}(x)$ es un p'-número de orden potencia de primo,

entonces $x \in Q \in \mathrm{Syl}_q(G)$, con $q \neq p$. Necesariamente, tenemos que $x \in Q \leqslant \mathrm{O}_{p'}(G)$. Por tanto, tenemos que

$$\mathrm{O}_{p'}(G) \leqslant \mathrm{C}_G(\mathrm{O}_{p'}(G)) \leqslant \mathrm{C}_G(x) \leqslant G,$$

por ser $\mathrm{O}_{p'}(G)$ abeliano. Luego $\left|x^G\right|$ también es un p-número.

Veamos ahora la implicación directa. Por el Lema 1.4.2, podemos escoger $P \in \mathrm{Syl}_p(G)$ tal que $P = (P \cap A)(P \cap B)$. Veamos que $P \trianglelefteq G$. Sea $a \in A \cap P$. Entonces, por hipótesis, tenemos que $\left|a^G\right|$ es un p-número. Así, por el Lema 1.3.2, tenemos que $a \in \mathrm{O}_p(G)$. Por tanto, tenemos que $A \cap P \leqslant \mathrm{O}_p(G)$. Análogamente, tenemos que $B \cap P \leqslant \mathrm{O}_p(G)$. Luego $P = \mathrm{O}_p(G)$. Por tanto, tenemos que G es p'-separable. Así, sabemos que G posee p'-subgrupos de Hall.

Sea $H \in \mathrm{Hall}_{p'}(G)$. Veamos que H es abeliano por inducción sobre $|G|$. Si $\mathrm{O}_p(G) \neq 1$, por inducción sobre $\overline{G} := G/\mathrm{O}_p(G)$, tenemos que todos los p'-subgrupos de Hall de $\overline{G}$ son abelianos y, en particular, $\overline{H} := H\mathrm{O}_p(G)/\mathrm{O}_p(G) \in \mathrm{Hall}_{p'}(\overline{G})$ también lo es. Pero $H\mathrm{O}_p(G)/\mathrm{O}_p(G) \cong H$, luego H es abeliano.

Así, podemos suponer que $\mathrm{O}_p(G) = 1$ y, por tanto, que G es un p'-grupo. Por tanto, tenemos que ver que G es abeliano. Como para todo elemento $x \in A \cup B$ de orden potencia de primo, tenemos que $\left|x^G\right|$ es un p-número, necesariamente tenemos que $\left|x^G\right| = 1$, pues $\left|x^G\right|$ divide a $|G|$ que es un p'-número. Por tanto, todo elemento de orden potencia de primo de $A \cup B$ pertenece a $\mathrm{Z}(G)$. Por ser G resoluble por el Teorema F, tenemos que A y B se pueden expresar como producto de sus subgrupos de Sylow. Teniendo en cuenta que todo elemento de un subgrupo de Sylow de A o B pertenece a $\mathrm{Z}(G)$, podemos concluir que $A \leqslant \mathrm{Z}(G)$ y que $B \leqslant \mathrm{Z}(G)$. Por tanto, como $G = AB$, tenemos que $G = \mathrm{Z}(G)$.

Solo nos queda ver que $[H, \mathrm{O}_p(G)] = 1$ para finalizar la prueba, pues ya tenemos que $G = \mathrm{O}_p(G)H$ con $\mathrm{O}_p(G) \cap H = 1$, $\mathrm{O}_p(G) \trianglelefteq G$ y H abeliano. Trabajaremos por inducción sobre $|G|$. Sabemos que los cocientes de G heredan las hipótesis del teorema y, como vimos que la clase $\mathfrak{P}_p$ de los grupos p-descomponibles era una formación saturada y ya tenemos que G es resoluble, por la Nota 1.2.20, podemos asumir que existe un único $N \cdot \trianglelefteq G$ con

$$N = \mathrm{F}(G) = \mathrm{O}_r(G) = \mathrm{C}_G(N),$$

donde $r \in \mathbb{P}$. Si $r \neq p$, entonces $\mathrm{O}_p(G) = 1$ y, por tanto, se cumpliría trivialmente que $[H, \mathrm{O}_p(G)] = 1$. Luego podemos asumir que $r = p$ y, en consecuencia, que $N = \mathrm{O}_p(G) \in \mathrm{Syl}_p(G)$.

Al ser N el único p-subgrupo de Sylow de G, es prefactorizado, esto es, $N = \mathrm{O}_p(G) = (\mathrm{O}_p(G) \cap A)(\mathrm{O}_p(G) \cap B)$. Sea $y \in \mathrm{O}_p(G) \cap A$. Entonces, por hipótesis, tenemos que

$\left|y^G\right|$ es un p-número. Pero, por otro lado, como $y \in \mathrm{O}_p(G) = N$, tenemos que $N = \mathrm{C}_G(N) \leqslant \mathrm{C}_G(y) \leqslant G$, luego $\left|y^G\right| = |G : \mathrm{C}_G(y)|$ divide a $|G : N|$, el cual es un p'-número. Concluimos que $\left|y^G\right| = 1$ y, por tanto, tenemos que $y \in \mathrm{Z}(G)$. Notemos que el mismo razonamiento sirve para elementos de $\mathrm{O}_p(G) \cap B$, por lo que deducimos que $\mathrm{O}_p(G) \leqslant \mathrm{Z}(G)$ y, por tanto, tenemos que $[H, \mathrm{O}_p(G)] = 1$. Esto finaliza la prueba. $\square$

Apéndice A

Ejemplos con GAP

A.1. Introducción

El programa GAP, que significa, Groups, Algorithms and Programming, es un sistema libre, abierto y extensible para el cálculo en álgebra discreta abstracta. Esto quiere decir que el programa puede distribuirse libremente y que el código es abierto para que se pueda examinar y cambiar. El término extensible significa que el usuario puede escribir sus programas en GAP y utilizarlos como bibliotecas que forman parte del sistema.

El proyecto GAP empezó en noviembre de 1985, bajo la dirección del profesor Joachim Neubuser, en el Lehrstuhl D fur Mathematik, RWTH-Aechen. Desde su jubilación en 1997, la coordinación del proyecto GAP, ahora convertido en un proyecto internacional, se lleva a cabo en St. Andrews (Escocia).

GAP es un sistema interactivo. Ejecuta continuamente un bucle de lectura, evaluación y escritura. Esto quiere decir que cada vez que escribimos una expresión, ésta es leída por GAP, evaluada y, entonces, se muestra el resultado. Podemos escribir funciones o incluso programas enteros que contienen muchas funciones e instrucciones, y probarlas sin abandonar el programa.

Las aplicaciones más importantes y significativas de dicho programa son en Teoría de Grupos. Los grupos se pueden introducir en GAP de varias maneras, en función de la representación que tengamos. Una de las maneras más fáciles de introducir grupos es como grupos de permutaciones, ya que las permutaciones son objetos fáciles de manejar en GAP. También es posible trabajar con grupos de matrices y con grupos finitamente presentados por generadores y relaciones.

También tiene incorporada información sobre muchos grupos en sus librerías: algunos

grupos básicos (cíclicos, diédricos, grupos de matrices clásicos, los grupos de permutaciones transitivos de grado a lo sumo 30, ciertos grupos de orden *pequeño* (conocidos como `SmallGroups`), algunos grupos finitos perfectos de orden a lo sumo 106, grupos de permutaciones de orden menor que 100, los subgrupos irreducibles resolubles de $GL(n,p)$ para $n > 1$ y $p^n < 256$), ...

El programa lleva incorporadas algunas funciones básicas que nos permiten conocer por ejemplo: el orden del grupo, las clases de conjugación y sus tamaños, los subgrupos normales, el *core* de un subgrupo, el centro, la clausura normal, el subgrupo derivado, los subgrupos de Sylow, la resolubilidad, la longitud de la serie derivada, representaciones irreducibles, ...

El programa GAP se distribuye libremente en código fuente. Esto significa que puede ser compilado en multitud de plataformas y sistemas operativos. A pesar de que el programa puede ser compilado con los sistemas comerciales de ventanas más habituales del mercado, se obtienen los mejores resultados con sistemas del tipo Unix, como Linux. La página web `http://www.gap-system.org/` (ver [11]) contiene contiene más información sobre el programa GAP, soporte técnico, grupos de usuarios, manuales, cómo descargar el programa, actualizaciones y paquetes adicionales.

Este software ha sido de vital importancia para el desarrollo del presente trabajo. Concretamente hemos trabajado con la versión 4.4.12, pues es (de momento) la única versión disponible para trabajar con una interfaz más cómoda en el entorno Windows. Dicha interfaz es el programa GGAP, el cual también es gratuito (`http://ggap.sourceforge.net/index.html`).

Nos ha servido de herramienta para obtener, como mostraremos en el presente capítulo, ejemplos de grupos *pequeños* que satisfacen los resultados que hemos obtenido en los capítulos anteriores. Nos referimos a *pequeños* porque nos hemos centrado en los grupos de la librería `SmallGroups`.

La librería `SmallGroups` contiene todos los grupos con ciertos órdenes *pequeños*. La palabra *pequeño* viene dada porque la librería contiene grupos cuyo orden es menor que una cierta cota o cuya factorización en primos es pequeña, en cierto sentido. Los grupos se clasifican según sus órdenes y se enumeran salvo isomorfismo. Actualmente, la librería contiene los siguientes grupos:

1. Los grupos de orden menor o igual que 2000, excepto 1024 (**423.164.062 grupos**).
2. Los grupos de orden libre de cubos y menor o igual que 50.000 (**395.703 grupos**).
3. Los grupos de orden p^7, para los primos $p = 3, 5, 7$ y 11 (**907.489 grupos**).

4. Los grupos de orden p^n, con $n \leq 6$, para "todos" los primos.

5. Los grupos de orden $q^n p$, donde q^n divide a $2^8, 3^6, 5^5$ o 7^4 y p es un primo arbitrario distinto de q.

6. Los grupos de orden libre de cuadrados.

7. Los grupos cuyo orden es factorizable en, como máximo, 3 primos.

A.2. Códigos y ejemplos

Tal y como mencionamos después del Teorema 3.1.5 veamos que, bajo las hipótesis de dicho teorema, no se cumple que "los p-subgrupos de Sylow de $G/\mathrm{O}_p(G)$ tienen orden a lo sumo p" ni que "P' es trivial o elemental abeliano", tal y como afirman los Teoremas 3.1.3 y 3.1.4. Para ello, mostramos a continuación contraejemplos para ambas afirmaciones.

Ejemplo A.2.1. Sea $p = 2$ que cumple trivialmente que $(p-1, |G|) = 1$, para cualquier grupo G. Tomemos $G := D_6 \times D_{10}$. Veamos que G cumple las hipótesis del Teorema 3.1.5:

```
gap> G:=DirectProduct(DihedralGroup(6),DihedralGroup(10));
<pc group of size 60 with 4 generators>
gap> O2:=PCore(G, 2);
Group([  ])
gap> Filtered(Elements(G), x-> (IsPrimePowerInt(Order(x))=true
> or Order(x)=1) and (Order(x) mod 2) > 0);
[ <identity> of ..., f2, f4, f2^2, f4^2, f4^3, f4^4 ]
gap> List([1..Length(last)], y-> Size(ConjugacyClass(G, last[y])));
[ 1, 2, 2, 2, 2, 2, 2 ]
```

Como podemos observar, G cumple las condiciones del teorema pues, todo $2'$-elemento de orden potencia de primo cumple que 4 no divide al tamaño de su clase de conjugación. Sin embargo, los 2-subgrupos de Sylow de $G/\mathrm{O}_2(G)$ son los 2-subgrupos de Sylow de G, pues $\mathrm{O}_2(G) = 1$, y tienen orden 4. ■

Ejemplo A.2.2. Volvemos a tomar $p = 2$ el cual, para cualquier grupo G, cumple trivialmente que $(p-1, |G|) = 1$. Elegimos un 2-grupo que no tenga subgrupo derivado

abeliano ni trivial. Por tanto, buscamos un 2-grupo con longitud de serie derivada mayor o igual que 3.

Además, al ser un 2-grupo, cumplirá las condiciones del Teorema 3.1.5 trivialmente, pues el único $2'$-elemento de orden potencia de primo será el elemento neutro, el cual tiene tamaño de clase no divisible por 4.

```
gap> First(AllSmallGroups(8), x-> DerivedLength(x)>2);
fail
gap> First(AllSmallGroups(16), x-> DerivedLength(x)>2);
fail
gap> First(AllSmallGroups(32), x-> DerivedLength(x)>2);
fail
gap> First(AllSmallGroups(64), x-> DerivedLength(x)>2);
fail
gap> G:=First(AllSmallGroups(128), x-> DerivedLength(x)>2);
<pc group of size 128 with 7 generators>
gap> StructureDescription(G);
"((C4 : C8) : C2) : C2"
gap> IsAbelian(DerivedSubgroup(G));
false
gap> IsTrivial(DerivedSubgroup(G));
false
gap> Filtered(Elements(G), x-> (IsPrimePowerInt(Order(x))=true
> or Order(x)=1)  and (Order(x) mod 2) > 0);
[ <identity> of ... ]
```

Como podemos observar, el primer 2-grupo que cumple tal condición es un grupo definido por productos semidirectos de la forma $[[[C_4]C_8]C_2]C_2$. ■

En el siguiente ejemplo mostramos que la hipótesis de que $(p-1, |G|) = 1$ del Teorema B no es superflua.

Ejemplo A.2.3. Vamos a tomar $G := \Sigma_5$, que tiene orden 120, el cual es un producto mutuamente permutable trivial. Tomaremos $p = 3$, por lo que $(2, 120) = 2 \neq 1$. Veamos que 9 no divide a ningún tamaño de clase de cualquier $3'$-elemento de orden potencia de primo pero, sin embargo, G no es resoluble.

```
gap> G:=SymmetricGroup(5);;
> L1:=Filtered(Elements(G), x-> IsPrimePowerInt(Order(x))=true and
> (Order(x) mod 3)>0);;
```

```
> L2:=List([1..Length(L1)], x-> Size(ConjugacyClass(G, L1[x])));;
> L3:=Filtered(L2, x-> Size(Union(DivisorsInt(x), [9]))>Size(
> DivisorsInt(x)));;
> if Length(L2)=Length(L3) then;
>       Print("true");
> else;
>       Print("false");
> fi;
true
```

Por tanto, hemos comprobado que la hipótesis de que $(p-1, |G|) = 1$ no es superflua.■

A partir de la versión 4.7.4 de GAP, viene instalado el paquete `PERMUT`, el cual es obra de A. Ballester-Bolinches, E. Cosme-Llópez y R. Esteban-Romero. Es un paquete para trabajar con la permutabilidad en grupos. Incluye funciones para ver qué subgrupos poseen ciertas propiedades de permutabilidad como, por ejemplo, la permutabilidad mutua, la cual hemos trabajado con asiduidad en la presente memoria.

Como hemos comentado en la sección anterior, la interfaz GGAP no permite de momento trabajar con otras versiones superiores a la 4.4.12. Por tanto, a fin de mantener la comodidad de manejo de dicha interfaz, decidimos programar algoritmos que nos permitieran ver dichas propiedades de permutabilidad que necesitábamos.

A continuación, mostramos los algoritmos obtenidos y, posteriormente, veremos ejemplos de los resultados originales que hemos obtenido en capítulos anteriores.

El primer problema que nos encontramos fue que, en GGAP, no funcionaba el comando `AllSubgroups()`, el cual devuelve todos los subgrupos de un grupo dado. Por tanto, creamos una función que nos determinará todos los subgrupos.

```
gap> AllSubgroups := function(g)
>       local C;
>       if Size(g) = 1 then;
>               return [g];
>               break;
>       fi;
>       C := ConjugacyClassesSubgroups(LatticeSubgroups(g));
>       return Union(List([1..Size(C)],i-> List([1..Size
> (Elements(C[i]))], j->Elements(C[i])[j])));
>       end;
function( g ) ... end
gap> G:=SymmetricGroup(3);;
```

```
> AllSubgroups(G);
[ Group(()), Group([ (2,3) ]), Group([ (1,3,2), (1,2) ]),
Group([ (1,2) ]), Group([ (1,2,3) ]), Group([ (1,3) ]) ]
```

Simplemente hemos buscado en el retículo de subgrupos, aquellos que son conjugados y hemos extraído los elementos de cada clase de conjugación.

La siguiente función encuentra los subgrupos de un grupo G que permutan con un subgrupo H fijado. Notemos que algunos son triviales, como G, el subgrupo trivial, los subgrupos normales de G y los que estén contenidos o contengan a H.

```
gap> SubPermut := function(g, h)
>       if Size(h) = 1 then;
>               return AllSubgroups(g);
>       else;
>               return Filtered(AllSubgroups(g), x->
> Elements(Union(List([1..Size(Elements(h))], y->
> List([1..Size(Elements(x))], k->Elements(h)[y]* Elements(x)[k])))) =
> Elements(Group(Union(GeneratorsOfGroup(h), GeneratorsOfGroup(x)))));
>       fi;
>       end;
function( g, h ) ... end
gap> G:=SymmetricGroup(3);;
> SubPermut(G, Group((1,2)));
[ Group(()), Group([ (1,3,2), (1,2) ]), Group([ (1,2) ]),
Group([ (1,2,3) ]) ]
```

Notemos que no requieren que H sea subgrupo de G, pero está implícito que ambos deben ser subgrupos de un mismo grupo común. Es decir, ambos grupos deben ser introducidos en GAP del mismo modo. Esto está implícito en cada uno de los siguientes programas.

La siguiente función determina si un subgrupo H de un grupo G es permutable en G (esto es, si permuta con todo subgrupo de G). Notemos que si $H \trianglelefteq G$, es permutable trivialmente, luego distinguiremos ese caso definiendo una nueva función que nos permita saber si el subgrupo es permutable pero no normal en el grupo. Posteriormente, comprobaremos dichas funciones con algunos subgrupos de Σ_3 y Σ_4.

```
gap> IsPermutable := function(g, h)
>       if SubPermut(g,h)=AllSubgroups(g) then;
>               return true;
```

```
>       else;
>               return false;
>       fi;
>       end;
function( g, h ) ... end
gap> IsPermutableAndNotNormal := function(g, h)
>       if SubPermut(g,h)=AllSubgroups(g) then;
>               if IsNormal(g, h)=false then;
>                       return true;
>               else;
>                       return false;
>               fi;
>       else;
>               return false;
>       fi;
>       end;
function( g, h ) ... end
gap> G:=SymmetricGroup(3);;
> IsPermutable(G, Group((1,2)));
false
gap> IsPermutable(G, Group((1,2,3))); # es un subgrupo normal
true
gap> H:=SymmetricGroup(4);;
> IsPermutable(H, Group([ (1,4)(2,3), (1,3)(2,4) ])); # es normal
true
gap> IsPermutable(H, Group((1,2,3)));
false
```

Las próximas funciones calculan todos los subgrupos permutables de un grupo G y los permutables pero no normales. Posteriormente, presentamos algunos ejemplos en los que aplicaremos dichas funciones.

```
gap> PermutableSubgroups := function(g);
>       return Filtered(AllSubgroups(g), x->IsPermutable(g, x) = true);
>       end;
function( g ) ... end
gap> PermutableSubgroupsNotNormal := function(g);
>       return Filtered(AllSubgroups(g), x->
> IsPermutableAndNotNormal(g, x) = true);
>       end;
function( g ) ... end
gap> G:=SymmetricGroup(3);;
> PermutableSubgroups(G);
```

```
[ Group(()), Group([ (1,3,2), (1,2) ]), Group([ (1,2,3) ]) ]
gap> PermutableSubgroupsNotNormal(G);
[  ]
gap> H:=SymmetricGroup(4);;
> PermutableSubgroups(H);
> PermutableSubgroupsNotNormal(H);
[ Group([ (1,3)(2,4), (1,4)(2,3), (2,4,3), (1,2) ]),
  Group([ (1,3)(2,4), (1,4)(2,3), (2,4,3) ]),
  Group([ (1,4)(2,3), (1,3)(2,4) ]) ]
[  ]
# Todos son normales
# No hay subgrupos permutables no normales en S3 ni en S4
# Ejemplo no trivial:
gap> g1:=SmallGroup(16,6);
> StructureDescription(g1);
<pc group of size 16 with 4 generators>
"C8 : C2"
gap> PermutableSubgroupsNotNormal(g1);
[ Group([ f2 ]), Group([ f2*f4 ]) ]
```

Queremos crear ahora una función que, dado dos subgrupos de un grupo, nos diga si son o no mutuamente permutables. Así mismo, definimos una nueva función para comprobar si son mutuamente permutables pero no normales en el grupo. Notemos que aquí ya sí que vamos a pedir que ambos sean subgrupos, aunque seguiría estando implícito. Aplicaremos dichas funciones a ciertos subgrupos de Σ_3 y Σ_4.

```
gap> AreMutuallyPermutableSubgroups := function(g, h, k)
>       if (IsSubgroup(g, h)=true and IsSubgroup(g, k)=true) then;
>               if (IsPermutable(k,h)=true and IsPermutable(h, k)=
> true) then;
>                       return true;
>               else;
>                       return false;
>               fi;
>       else;
>               Print("Error: no son ambos subgrupos de G");
>       fi;
>       end;
function( g, h, k ) ... end
gap> AreMutuallyPermutableNotNormalSubgroups := function(g, h, k)
>       if (IsSubgroup(g, h)=true and IsSubgroup(g, k)=true) then;
>               if (AreMutuallyPermutableSubgroups(g,h,k)=true and
```

```
> IsNormal(g,h)=false and IsNormal(g,k)=false) then;
>                         return true;
>                 else;
>                         return false;
>                 fi;
>         else;
>                 Print("Error: no son ambos subgrupos de G");
>         fi;
>         end;
function( g, h, k ) ... end
gap> G:=SymmetricGroup(4);;
> H:=AlternatingGroup(4);;
> K:=Subgroup(G,[(1,2,3,4),(1,3)]);;
> AreMutuallyPermutableSubgroups(G, K, H);
true
gap> AreMutuallyPermutableSubgroups(SymmetricGroup(3),
> Group((1,2,3)), Group((1,2)));
true
gap> AreMutuallyPermutableNotNormalSubgroups(G, H, K);
false
gap> AreMutuallyPermutableNotNormalSubgroups(SymmetricGroup(3),
> Group((1,2,3)), Group((1,2)));
false
```

Ahora, creamos un programa que, dado un grupo, nos encuentre subgrupos mutuamente permutables con uno dado y subgrupos mutuamente permutables no normales con dicho subgrupo prefijado. Comprobaremos de nuevo con el grupo Σ_4.

```
gap> SubgroupsMutuallyPermutable := function(g, h)
>         return Filtered(AllSubgroups(g), x->
> AreMutuallyPermutableSubgroups(g, x, h)=true);
>         end;
function( g, h ) ... end
gap> SubgroupsMutuallyPermutableNotNormal := function(g, h)
>         if IsNormal(g, h)=true then;
>                 Print("Error: es un subgrupo normal");
>         else;
>                 return Filtered(AllSubgroups(g), x->
> AreMutuallyPermutableNotNormalSubgroups(g, x, h)=true);
>         fi;
>         end;
function( g, h ) ... end
gap> G:=SymmetricGroup(4);;
```

```
> K:=Subgroup(G,[(1,2,3,4),(1,3)]);;
> SubgroupsMutuallyPermutable(G, K);
[ Group(()), Group([ (1,3)(2,4), (1,4)(2,3), (2,4,3) ]),
  Group([ (1,4)(2,3), (1,2)(3,4), (1,3) ]),
  Group([ (1,3)(2,4), (2,4) ]), Group([ (1,4)(2,3), (1,3)(2,4) ]),
  Group([ (1,3)(2,4), (1,4,3,2) ]), Group([ (1,3)(2,4) ]) ]
gap> SubgroupsMutuallyPermutableNotNormal(G, K);
[ Group([ (1,4)(2,3), (1,2)(3,4), (1,3) ]),
  Group([ (1,3)(2,4), (2,4) ]), Group([ (1,3)(2,4), (1,4,3,2) ]),
  Group([ (1,3)(2,4) ]) ]
```

Finalmente, queremos crear dos funciones: una que encuentre una factorización de un grupo G como producto de dos subgrupos mutuamente permutables no triviales y otra en la que los factores del grupo no sean normales. Mostramos varios ejemplos de las funciones definidas.

```
gap> ProductOfMutuallyPermutableSubgroupsNotTrivial := function(g)
>       local L, a, b, s, sol, v;
>       sol := [];
>       L := AllSubgroups(g);
>       for i in [1..Length(L)] do;
>               v := [];
>               if (Size(L[i]) > 1 and Size(L[i])<Size(g)) then;
>                       a:= SubgroupsMutuallyPermutable(g, L[i]);
>                       b:=Filtered(a, x-> Size(x)<Size(g));
>                       s:=Filtered(b, x->
> Size(Group(Union(GeneratorsOfGroup(L[i]), GeneratorsOfGroup(x))))
> =Size(g));
>                       if Length(s)>0 then;
>                               Add(v, L[i]);
>                               if Size(sol)=0 or
> Size(Intersection(Set(Flat(sol)), Set([L[i]])))=0 then;
>                                       for x in [1..Length(s)] do;
>                                               Add(v, s[x]);
>                                       od;
>                                       Add(sol, v);
>                               else;
>                                       for x in [1..Length(s)] do;
>                                               if Size(
> Intersection(Set(Flat(TransposedMat(sol)[1])), Set([s[x]])))=0 then;
>                                                 Add(v,s[x]);
>                                               fi;
>                                       od;
```

```
>                                         if Size(v)>1 then;
>                                                 Add(sol, v);
>                                         fi;
>                                 fi;
>                         fi;
>                 fi;
>         od;
>         return sol;
>         end;
function( g ) ... end
gap> ProductOfMutuallyPermutableSubgroupsNotTrivialAndNotNormal :=
> function(g)
>         local L, a, s, sol, v;
>         sol := [];
>         L := Filtered(AllSubgroups(g), x-> IsNormal(g, x)=false);
>         for i in [1..Length(L)] do;
>                 v := [];
>                 a:=SubgroupsMutuallyPermutableNotNormal(g, L[i]);
>                 s:=Filtered(a, x-> Size(Group(Union(
> GeneratorsOfGroup(L[i]), GeneratorsOfGroup(x))))=Size(g));
>                 if Length(s)>0 then;
>                         Add(v, L[i]);
>                         if Size(sol)=0 or Size(Intersection(Set(
> Flat(sol)), Set([L[i]])))=0 then;
>                                 for x in [1..Length(s)] do;
>                                         Add(v, s[x]);
>                                 od;
>                                 Add(sol, v);
>                         else;
>                                 for x in [1..Length(s)] do;
>                                         if Size(Intersection(Set(
> Flat(TransposedMat(sol)[1])), Set([s[x]])))=0 then;
>                                                 Add(v, s[x]);
>                                         fi;
>                                 od;
>                                 if Size(v)>1 then;
>                                         Add(sol, v);
>                                 fi;
>                         fi;
>                 fi;
>         od;
>         return sol;
>         end;
function( g ) ... end
```

```
gap> g:=SymmetricGroup(3);
Sym( [ 1 .. 3 ] )
gap> ProductOfMutuallyPermutableSubgroupsNotTrivial(g);
[ [ Group([ (2,3) ]), Group([ (1,2,3) ]) ],
  [ Group([ (1,2) ]), Group([ (1,2,3) ]) ],
  [ Group([ (1,2,3) ]), Group([ (1,3) ]) ] ]
gap> ProductOfMutuallyPermutableSubgroupsNotTrivialAndNotNormal(g);
[  ]
gap> G:= SmallGroup(16, 3);
<pc group of size 16 with 4 generators>
gap> StructureDescription(G);
"(C4 x C2) : C2"
gap> ProductOfMutuallyPermutableSubgroupsNotTrivialAndNotNormal(G);
[ [ Group([ f1, f4 ]), Group([ f1*f2, f3*f4 ]),
 Group([ f1*f2*f3, f3*f4 ]) ],
  [ Group([ f1*f3, f4 ]), Group([ f1*f2, f3*f4 ]),
  Group([ f1*f2*f3, f3*f4 ]) ] ]
```

Comentamos brevemente estas funciones y los resultados obtenidos. La primera función filtra, de los subgrupos de G, los que son no triviales y tienen "pareja", es decir, existe otro subgrupo de G tal que ambos son mutuamente permutables y el orden del producto de ambos es igual al orden de G. El programa devuelve una lista de listas, es decir, listas donde el primer elemento es un subgrupo fijo, siendo los que le siguen en su misma lista posibles parejas para él. Como podemos observar en el ejemplo de Σ_3, no se repiten parejas en las listas.

Por ejemplo, en el grupo $[C_4 \times C_2]C_2$ que acabamos de ver, el subgrupo `Group([ f1, f4 ])` tiene dos posibles parejas: `Group([ f1*f2, f3*f4 ])` y, por otro lado, `Group([ f1*f2*f3, f3*f4 ])`. Luego tenemos dos posibles productos mutuamente permutables no triviales para dicho grupo, donde ninguno de los factores es normal.

Veamos un programa que nos dirá si un determinado grupo cumple las hipótesis del Teorema 3.1.5. Así mismo, comprobaremos dicha función con el grupo $C_5 \times [C_9]C_3$ y con el número primo 5, viendo además el número de $5'$-elementos de orden potencia de primo y sus tamaños de clase.

```
gap> VerificaHipotesisTeoB := function(g, p)
>       local L1, L2, L3;
>       if IsPrime(p)=false then;
>               Print("Error: p no es primo");
>       else;
>               if Gcd(Size(g), p)=1 then;
```

```
>                         Print("Error: p no divide a |G|");
>                 else;
>                         if Gcd(p-1, Order(g)) > 1 then;
>                                 Print("Error: no se cumple que
> (p-1, |G|)=1");
>                         else;
>                                 L1:=Filtered(Elements(g), x->
> IsPrimePowerInt(Order(x))=true  and (Order(x) mod p)>0);
>                                 L2:=List([1..Length(L1)], x->
> Size(ConjugacyClass(g, L1[x])));
>                                 L3:=Filtered(L2, x-> Size(Union(
> DivisorsInt(x), [p^2]))>Size(DivisorsInt(x)));
>                                 if Length(L2)=Length(L3) then;
>                                         return true;
>                                 else;
>                                         return false;
>                                 fi;
>                         fi;
>                 fi;
>         fi;
>         end;
function( g ) ... end
gap> G2 := SmallGroup(135, 4);
<pc group of size 135 with 4 generators>
gap> StructureDescription(G2);
> VerificaHipotesisTeoB(G2, 5);
"C5 x (C9 : C3)"
true
gap> L1:=Filtered(Elements(G2), x-> IsPrimePowerInt(Order(x))=true
> and Order(x) mod 5>0);;
> Size(L1);
> List([1..Length(L1)], x-> Size(ConjugacyClass(G2, L1[x])));
26
[ 3, 3, 1, 3, 3, 3, 3, 3, 1, 3, 3, 3, 3, 3, 3, 3, 3,
 3, 3, 3, 3, 3, 3, 3, 3, 3 ]
```

En el siguiente ejemplo mostramos que nuestro Teorema B no solo generaliza al Teorema 3.1.5, sino que puede ser más económico que él, computacionalmente hablando.

Ejemplo A.2.4. Acabamos de ver que el grupo `G2` del ejemplo anterior tiene 26 elementos de orden potencia de primo y no divisible por 5. Vamos a ver que podemos encontrar una factorización de `G2`, como un producto mutuamente permutable, de manera que tengamos menos elementos para comprobar si sus tamaños de clase cumplen las

condiciones.

```
gap> VerificaHipotesisProductoTeoB := function(g, h, k, p)
>       local L11, L12, L21, L22, L31, L32;
>       if IsPrime(p)=false then;
>               Print("Error: p no es primo");
>       else;
>               if Size(Intersection(DivisorsInt(Order(g)), [p]))
> =0 then;
>                       Print("Error: p no divide a |G|");
>               else;
>                       if Gcd(p-1, Order(g)) > 1 then;
>                               Print("Error: no se cumple que
> (p-1, |G|)=1");
>                       else;
>                               L11:=Filtered(Elements(h), x->
> IsPrimePowerInt(Order(x))=true  and Order(x) mod p>0);
>                               L12:=Filtered(Elements(k), x->
> IsPrimePowerInt(Order(x))=true  and Order(x) mod p>0);
>                               L21:=List([1..Length(L11)], x->
> Size(ConjugacyClass(g, L11[x])));
>                               L22:=List([1..Length(L12)], x->
> Size(ConjugacyClass(g, L12[x])));
>                               L31:=Filtered(L21, x-> Size(Union(
> DivisorsInt(x), [p^2]))>Size(DivisorsInt(x)));
>                               L32:=Filtered(L22, x-> Size(Union(
> DivisorsInt(x), [p^2]))>Size(DivisorsInt(x)));
>                               if Length(L22)=Length(L32) and
> Length(L21)=Length(L31) then;
>                                       return true;
>                               else;
>                                       return false;
>                               fi;
>                       fi;
>               fi;
>       fi;
>       end;
function( g ) ... end
gap> G2 := SmallGroup(135, 4);;
> f1:=GeneratorsOfGroup(G2)[1];;
> f2:=GeneratorsOfGroup(G2)[2];;
> f3:=GeneratorsOfGroup(G2)[3];;
> f4:=GeneratorsOfGroup(G2)[4];;
> H2:=Group(f2);;
> K2:=Group(f1,f3,f4);;
```

```
> StructureDescription(H2);
> StructureDescription(K2);
> Intersection(H2, K2);
"C3"
"C45"
Group([  ])
gap> AreMutuallyPermutableSubgroups(H2,K2);
> IsNormal(G2, H2);
> IsNormal(G2,K2);
true
false
true
gap> VerificaHipotesisProductoTeoB(G2, H2, K2, 5);
true
gap> L2:=Filtered(Elements(H2), x-> IsPrimePowerInt(Order(x))=true
> and Order(x) mod 5>0);;
> Size(L2);
2
gap> L3:=Filtered(Elements(K2), x-> IsPrimePowerInt(Order(x))=true
> and Order(x) mod 5>0);;
> Size(L3);
8
```

Como podemos ver, el programa solo ha tenido que comprobar si 10 elementos cumplen las condiciones del Teorema B, es decir, el número de elementos se ha reducido a menos de la mitad. ■

Ejemplo A.2.5. Veamos un grupo G que no cumple las condiciones del Teorema 3.1.5 pero, sin embargo, existe una factorización para la cual sí podemos aplicarle el Teorema B.

```
gap> G3:=SmallGroup(36, 10);
<pc group of size 36 with 4 generators>
gap> StructureDescription(G3);
> VerificaHipotesisTeoB(G3, 2);
"S3 x S3"
false
gap> ProductOfMutuallyPermutableSubgroupsNotTrivialAndNot
> Normal(G3);
[ [ Group([ f1, f3 ]), Group([ f2, f4 ]), Group([ f2*f3, f4 ]),
      Group([ f2*f3^2, f4 ]) ],
[ Group([ f1*f4, f3 ]), Group([ f2, f4 ]), Group([ f2*f3, f4 ]),
```

```
      Group([ f2*f3^2, f4 ]) ],
[ Group([ f1*f4^2, f3 ]), Group([ f2, f4 ]), Group([ f2*f3, f4 ]),
      Group([ f2*f3^2, f4 ]) ] ]
gap> f1:=GeneratorsOfGroup(G3)[1];;
> f2:=GeneratorsOfGroup(G3)[2];;
> f3:=GeneratorsOfGroup(G3)[3];;
> f4:=GeneratorsOfGroup(G3)[4];;
> Order(Group([ f1, f3 ]))*Order(Group([ f2, f4 ]));
> Order(Intersection(Group([ f1, f3 ]), Group([ f2, f4 ])));
36
1
gap> AreMutuallyPermutableSubgroups(G3, Group([ f1, f3 ]),
> Group([ f2, f4 ]));
true
gap> VerificaHipotesisProductoTeoB(G3, Group([ f1, f3 ]),
> Group([ f2, f4 ]), 2);
true
```

Por tanto, queda de manifiesto otra ventaja más de nuestro Teorema B. ■

Bibliografía

[1] B. Amberg, S. Franciosi y F. de Giovanni. *Products of groups.* Oxford University Press Inc., 1992.

[2] R. Baer. Group elements of prime power index. *Trans. Amer. Math. Soc.*, 75:20–47, 1953.

[3] A. Ballester-Bolinches, J. Cossey y Y. Li. Mutually permutable products and conjugacy classes. *Monatsh Math*, 170:305–310, 2013.

[4] A. Ballester-Bolinches, R. Esteban-Romero y M. Asaad. *Products of finite groups.* De Gruyter, 2010.

[5] H.G. Bray y M. Weinstein. *Between nilpotent and solvable.* Polygonal, 1982.

[6] D. Chillag y M. Herzog. On the length of the conjugacy classes of finite groups. *J. Algebra*, 131:110–125, 1990.

[7] J. Cossey y Y. Wang. Remarks on the length of conjugacy classes of finite groups. *Communications in Algebra*, 27:4347–4353, 1999.

[8] K. Doerk y T. Hawkes. *Finite Soluble Groups.* De Gruyter, 1992.

[9] B. Fein, W. M. Kantor y M. Schacher. Relative Brauer groups II. *J. Reine Angew. Math.*, 328:39–57, 1981.

[10] M.J. Felipe-Román, A. Martínez-Pastor y V.M. Ortiz-Sotomayor. *Clases de conjugación y grupos factorizados.* Tercer Congreso de Jóvenes Investigadores de la RSME, Universidad de Murcia, 7-11 de septiembre de 2015.

[11] GAP. Groups, Algorithms and Programming - a System for Computational Discrete Algebra. `http://www.gap-system.org/`, Versión 4.4.12, 2008.

[12] B. Huppert. *Endliche Gruppen I.* Springer-Verlag, 1967.

[13] B. Huppert. *Character Theory of Finite Groups.* De Gruyter, 1998.

[14] I.M. Isaacs. *Algebra: A Graduate Course.* Brooks/Cole Publishing Company, 1994.

[15] I.M. Isaacs. *Finite Group Theory.* American Mathematical Society, 2008.

[16] X. Liu, Y. Wang y H. Wei. Notes on the length of conjugacy clases of finite groups. *J. Pure and Applied Algebra*, 196:111–117, 2005.

[17] G. Qian y Y. Wang. On conjugacy class sizes and character degrees of finite groups. *Journal of Algebra and Its Applications*, 13:1350100 (9 pages), 2014.

[18] Y. Ren. On the length of p-regular classes and the p-structure of finite groups. *Algebra Colloq.*, 2:3–10, 1995.

[19] Derek J.S. Robinson. *A Course in the Theory of Groups.* Springer-Verlag, 1996.

[20] J.S. Rose. *A course on Group Theory.* Cambridge University Press, 1978.

[21] W.R. Scott. *Group Theory.* Dover, 1987.

Notación

$G, H, N, M, \ldots$	grupos finitos
$X, Y, \Omega, \ldots$	conjuntos finitos
$A \setminus B$	diferencia conjuntista entre A y B, esto es, el conjunto $\{x \in A : x \notin B\}$
$A \cap B$	intersección de los conjuntos A y B
$A \cup B$	unión de los conjuntos A y B
$\|G\|$	orden del grupo G
$\|X\|$	número de elementos del conjunto X
$\pi(X)$	conjunto de números primos divisores de $\|X\|$
p	un número primo
p'	conjunto de números primos distintos de p
π	conjunto de números primos
π'	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
π-número	entero positivo tal que todo número primo que lo divide pertenece a π
π'-número	entero positivo tal que todo número primo que lo divide no pertenece a π
p-elemento	elemento de un grupo cuyo orden es un p-número
p'-elemento	elemento de un grupo cuyo orden es un p'-número
$\|G\|_p$	mayor potencia de p que divide a $\|G\|$

(a, b)	máximo común divisor de los enteros a y b
$a \mid b$	a divide a b
$a \nmid b$	a no divide a b
$\mathrm{o}(g)$	orden del elemento g de un grupo
$x^g = g^{-1}xg$	x conjugado g
x^G	clase de conjugación de x en G, esto es, el conjunto $\{x^g \ : \ g \in G\}$
$H \leqslant G$	H es un subgrupo de G
$H \not\leqslant G$	H no es un subgrupo de G
$H < G$	H es un subgrupo propio de G
$X \subseteq Y$	X es un subconjunto de Y
$N \operatorname{car} G$	N es un subgrupo característico de G
$N \cdot \trianglelefteq G$	N es un subgrupo normal minimal de G
$N \trianglelefteq G$	N es un subgrupo normal de G
$M <\cdot G$	M es un subgrupo maximal de G
gH	coclase izquierda de H en G, donde $g \in G$ y $H \leqslant G$
G/N	grupo cociente de G sobre N (donde $N \trianglelefteq G$)
$\lvert G : H \rvert$	índice de H en G (donde $H \leq G$); número de coclases de H en G
$G \cong H$	los grupos G y H son isomorfos
$H \lessapprox G$	H es isomorfo a un subgrupo de G
$H^g = g^{-1}Hg$	conjugado de H por g (donde $H \leqslant G$ y $g \in G$)
H^G	conjugado de H por G, esto es, el conjunto $\{H^g \ : \ g \in G\}$
$H_G = \bigcap_{g \in G} H^g$	*core* en G de H, esto es, el mayor subgrupo normal de G contenido en H
$G \times H$	producto directo de los grupos G y H
$[G]\, H$	producto semidirecto de los grupos G y H, donde $G \trianglelefteq H$
$\langle x_1, \ldots, x_n \rangle$	subgrupo generado por los elementos $\{x_1, \ldots, x_n\}$
$[g_1, g_2] = g_1^{-1} g_1^{g_2}$	conmutador de los elementos $g_1, g_2 \in G$
$[H, K]$	conmutador de los grupos H y K, i.e., $\langle [h, k] \ : \ h \in H, \ k \in K \rangle$
G'	subgrupo derivado de G, esto es, $[G, G]$

$\mathrm{Inn}(G)$	grupo de automorfismos internos de G
$\mathrm{Aut}(G)$	grupo de automorfismos de G
$\mathrm{C}_G(x)$	centralizador en G de x
$\mathrm{C}_G(H)$	centralizador en G de H
$\mathrm{N}_G(H)$	normalizador en G de H
$\mathrm{O}_p(G)$	p-radical de G, con p un número primo
$\mathrm{O}_{p'}(G)$	p'-radical de G, con p' conjunto de números primos, divisores de $\lvert G\rvert$, distintos de p
$\mathrm{O}_\pi(G)$	π-radical de G, con π un conjunto de números primos, divisores de $\lvert G\rvert$
$\mathrm{O}_{\pi'}(G)$	π'-radical de G, con π' conjunto de números primos, divisores de $\lvert G\rvert$, que no pertenecen a π
$\mathrm{O}^p(G)$	p-residual de G, con p un número primo
$\Phi(G)$	subgrupo de Frattini de G
$\mathrm{F}(G)$	subgrupo de Fitting de G
$\mathrm{Soc}(G)$	*socle* de G, esto es, el producto de todos los normales minimales de G
$\mathrm{Syl}_p(G)$	conjunto de p-subgrupos de Sylow de G
$\mathrm{Hall}_\pi(G)$	conjunto de π-subgrupos de Hall de G
$\mathrm{Z}(G)$	centro de G
A_n	grupo alternado de orden $\frac{n!}{2}$
D_n	grupo diédrico de orden n
Σ_n	grupo simétrico de orden $n!$
C_p	grupo cíclico de orden p
V_4	4-grupo de Klein
$\mathrm{Ker}(\phi)$	núcleo de la aplicación ϕ
$\mathbb{P}$	conjunto de todos los números primos