UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

Grupos finitos y extensiones cíclicas.

Autor/es

Miguel Herreros Gaona

Director/es

MARÍA DEL PILAR BENITO CLAVIJO

Facultad

Facultad de Ciencia y Tecnología

Titulación

Grado en Matemáticas

Departamento

MATEMÁTICAS Y COMPUTACIÓN

Curso académico

2021-22

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

Facultad de Ciencia y Tecnología

Trabajo de Fin de Grado

Grado en Matemáticas

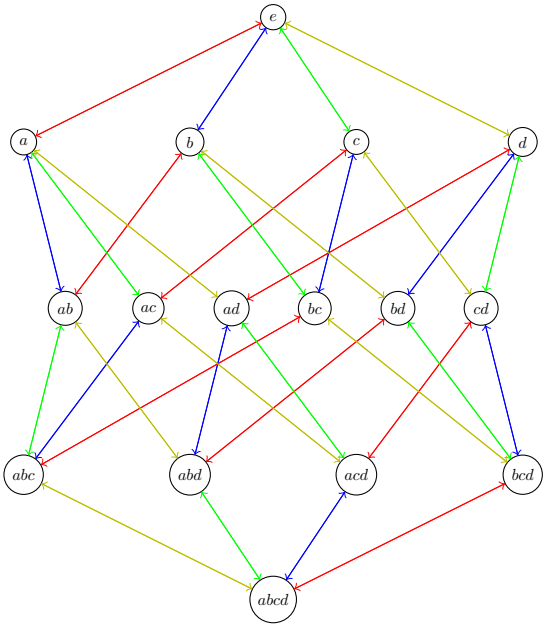
Grupos finitos y extensiones cíclicas

Grupos finitos y extensiones cíclicas

Finite groups and cyclic extensions

Realizado por: Miguel Herreros Gaona

Tutelado por: María del Pilar Benito Clavijo



Curso 2021-2022

Resumen

¿Cómo se construyen grupos nuevos a partir de otros más sencillos? La respuesta general es muy complicada, pues no solo depende de qué grupos estés utilizando como bloques básicos sino también de cómo los "pegas" para formarlos. En este Trabajo de Fin de Grado daremos dos técnicas que nos permitirán clasificar todos los grupos finitos de orden menor o igual que dieciséis construyéndolos como productos semidirectos o extensiones cíclicas de otros más sencillos, sin necesidad de usar los Teoremas de Sylow o el Teorema de Clasificación de Grupos Abelianos Finitamente Generados. Para ello, el trabajo está dividido en tres capítulos, el primero consistirá en una introducción histórica a la teoría de grupos, haciendo especial hincapié en los resultados que conciernen a los grupos finitos, junto con una breve muestra de algunos grupos básicos que usaremos más adelante. El segundo contiene los conceptos y resultados básicos que usaremos en el tercer capítulo para dar la clasificación.

Abstract

How do we make new groups using simpler ones? The general answer is quite difficult indeed, since not only depends on the groups we use as basic blocks but also on how you "glue" them. In this End of Degree Project we will give two techniques that will allow us to classify all finite groups of order lesser than or equal than sixteen, constructing them as semidirect products or cyclic extensions of simpler groups, without using Sylow's Theorems or the Fundamental Theorem of Finitely Generated Abelian Groups. This project will be divided in three chapters, the first one will consist in a summary of the History of group theory, emphasizing the results concerning finite groups, alongside a small sample of some basic groups that we will be using further on. The second one will consist in basic concepts and results that we will use in the third chapter for the classification.

Índice general

Capítulo 1

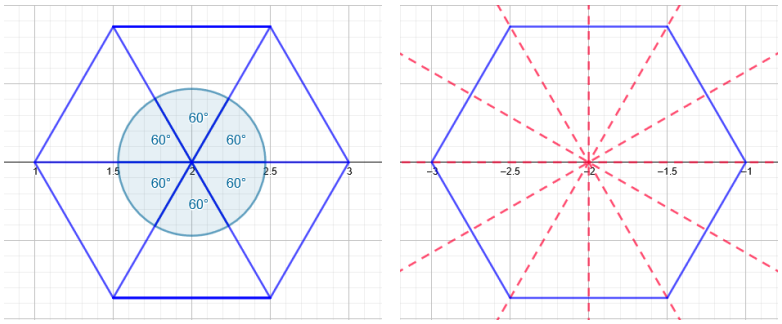
Grupos

Antes de iniciar la clasificación de grupos de orden pequeño conviene responder a unas cuantas preguntas previas para motivar dicha clasificación como qué es un grupo, por qué este objeto es relevante y dónde encontramos sus orígenes. Empecemos por la definición.

Definición 1.1. Un grupo grupo G es un conjunto con una operación binaria, $\cdot : G \times G \to G$, a la que generalmente llamamos producto y que denotaremos mediante la yuxtaposición de dos elementos, xy. El producto debe ser asociativo, es decir, dados $x, y, z \in G$, $(xy)z = x(yz)$. En G debe haber un elemento distinguido e, al que se dice *neutro*, tal que $xe = ex = x$ para todo elemento x de G. Además, para cada elemento $x \in G$ existe un elemento x^{-1}, llamado *inverso de* x, que cumple que $xx^{-1} = x^{-1}x = e$.

Nota: Aunque en este trabajo usaremos la notación multiplicativa, en el estudio de los grupos abelianos es costumbre usar la notación aditiva, en la que a la operación binaria se dice suma y se denota $+$. El neutro y el inverso, llamado opuesto, se escriben como 0 y $-x$.

La Teoría de Grupos es muy importante para las matemáticas debido a que, a grandes rasgos, estudia la simetría, no necesariamente geométrica, de muy diversas estructuras. Consideremos por ejemplo el polinomio $z^n - 1$. Sus raíces van a ser los complejos en forma polar $x^k = e^{\frac{2\pi k\, i}{n}}$ para todo $k = 0, \ldots, n-1$. Se tiene que el conjunto de dichas raíces $C_n = \left\{x^k | k = 0, \ldots, n-1\right\}$ posee estructura de grupo. En efecto, usando propiedades básicas de números complejos, es facil comprobar que se cumplen las tres propiedades de la definición teniendo en cuenta que $e^{\frac{2\pi(k+n)\, i}{n}} = e^{\frac{2\pi k\, i}{n}}$. Si nos fijamos, la notación que hemos usado para esta familia no es casual, pues todos los elementos son las potencias sucesivas de uno fijo al que hemos llamado x. Los grupos que cumplen esta propiedad son muy importantes dentro de la teoría de grupos y se dicen *grupos cíclicos*. Otra familia de grupos muy común aparece de forma natural cuando tratamos de analizar las simetrías de un n-ágono regular. Como se puede observar en la Figura 1.1, en el caso del hexágono



(a) Rotaciones (b) Reflexiones

Figura 1.1: Simetrías de un hexágono regular

regular hay doce simetrías, seis rotaciones y seis reflexiones. Si consideramos el conjunto de las simetrías con la operación composición, es evidente que las seis rotaciones poseen estructura de grupo cíclico de seis elementos generado por la rotación de ángulo $\frac{2\pi}{6}$. Con un poco más de maña, es fácil comprobar que, fijada una reflexión τ, el resto aparecen al componer τ con cada una de las seis rotaciones. De este modo tan visual llegamos al grupo diédrico $D_6 = \left\{Id = \sigma^0, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4, \tau\sigma^5\right\}$.

Sin embargo, la historia de la teoría de grupos empieza más de un siglo antes de la primera definición formal (Weber, von Dyck, 1882)[1] y de las primeras clasificaciones de los mismos. Además sus orígenes recorren diversas áreas de las matemáticas aparentemente distintas pero en las que subyacía la idea de invarianza de algún objeto bajo una serie de transformaciones, ya sea la permutación de las raíces de $x^n - 1$ o bien las simetrías de una figura. Esta idea, tras diversos pasos de abstracción y de forma paralela a la exigencia de formalismo en las matemáticas, dio lugar al concepto de grupo. A continuación haremos un resumen de la evolución de la teoría de grupos basándonos en las referencias [3] y [9] y en la línea del tiempo establecida en [7]. Cerraremos el capítulo con algunos comentarios sobre el Problema de Burnside [6], la clasificación de grupos simples [1] y una sección que ilustrará los principales grupos que usaremos a lo largo del trabajo y mostrará lo compleja que resulta la clasificación de los grupos finitos en general [2].

1.1. Evolución de la teoría

La teoría de grupos principalmente surgió de tres fuentes: la teoría de números, el álgebra clásica (teoría de ecuaciones algebraicas) y la geometría (y el análisis).

En teoría de números, los primeros pasos se dan de la mano de Euler que, en 1758 prueba que cada desplazamiento de un cuerpo rígido se puede expresar como composición de una rotación y una traslación[2]. Pionero en la moderna aproximación de la aritmética modular, sus aportaciones en este campo son importantes en la evolución de la teoría.

[1] La noción abstracta de grupo se desarrolla gradualmente, como veremos en la evolución de la teoría.
[2] Introduce la noción de *ángulo de Euler*, que los físicos siguen usando en la actualidad

(a) Leonhard Euler (b) Carl Friedrich Gauss

Figura 1.2: Euler (1707-1783) y Gauss (1777-1855)

Como muestra tenemos siguiente resultado que introduce la noción de la función que lleva su nombre, φ de Euler, y que proporciona el número de generadores del cíclico C_n:[3]

Teorema de Euler (1763): Si a y n son coprimos positivos, $a^{\varphi(n)} \equiv 1$ módulo n.

El trabajo de unificación en teoría de números lo realiza Gauss en sus *Disquisitiones Arithmeticae* (1798)[4] en el que aparecen los enteros modulares $\mathbb{Z}_n$ (versión natural de los cíclicos) ejemplos fundamentales y básicos de grupo aditivos abelianos finitos. En el caso particular $n = p$ primo, Gauss observa que los elementos no nulos de $\mathbb{Z}_p$ son potencias de un único elemento (grupo cíclico) y que el conjunto tiene un número de generadores igual a $\varphi(p-1)$. Este tratado incluye también, en relación con la noción de grupo, el estudio de las formas cuadráticas binarias (expresiones de la forma $ax^2 + bxy + cy^2$ con $a, b, c \in \mathbb{Z}$) demostrando que su composición es asociativa y que tanto el neutro como, dada una forma, su inversa, existen.

En la segunda mitad del siglo XVIII, las principales cuestiones abiertas del álgebra radicaban en las ecuaciones polinómicas, concretamente en la existencia de las raíces y formas prácticas de calcularlas. En 1770, Lagrange publicó *Réflexions sur la résolution algébrique des équations* un trabajo que trata el problema de la resolución de la ecuación de grado cinco, pues ya se sabía cómo resolver las ecuaciones polinómicas de hasta cuarto grado mediante radicales. Analizando varios métodos para resolver cúbicas y cuárticas se da cuenta que la idea básica era reducir tales ecuaciones a una auxiliar un grado menor que la original, llamada resolvente. Lagrange intenta generalizar tales razonamientos para grado n arbitrario de la siguiente forma, dado un polinomio $f(x)$, construye una función racional $R(x_1, x_2, \ldots, x_n)$ usando las raíces (x_i) y los coeficientes de $f(x)$. Si $y_1, y_2, \ldots, y_k$ son los diferentes valores que toma R cuando se consideran todas las permutaciones de las raíces $x_1, x_2, \ldots, x_n$, la resolvente de $f(x)$ viene dada por $g(x) = (x - y_1)(x - y_2)\ldots(x - y_k)$. Por ejemplo si $f(x)$ fuera una cuártica con raíces x_1, x_2, x_3 y x_4 y consideramos $R(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$, resulta que toma 3 valores

[3] El Teorema de Euler es una generalización del conocido como Pequeño Teorema de Fermat. Basta considerar $n = p$ primo sabiendo que $\varphi(n)$ denota el número de números primos con n y menores que n.

[4] Gauss lo escribe con 21 años y se publica en Leipzig en 1801.

(a) Joseph-Louis Lagrange (b) Paolo Ruffini

Figura 1.3: Lagrange (1736-1813) y Ruffini (1765-1822)

distintos al hacer las permutaciones, obteniendo así que la resolvente tiene grado 3. Sin embargo, al intentar aplicar este análisis a la ecuación de grado cinco, se encuentra con que el grado de la resolvente es 6. Aunque Lagrange no llega a resolver el problema de la quíntica, su trabajo fue el primero en relacionar las soluciones de una ecuación polinómica y las permutaciones de sus raíces. Así, la noción de grupo (como grupo de permutaciones) está implícita en sus resultados. Basándose en el trabajo de Lagrange, Paolo Ruffini publica en 1799 *Teoria generale delle equazioni: in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grad superiore al quarto* donde se trata la irresolubilidad de la ecuación de grado cinco y que pone los cimientos de la relación entre las permutaciones de las raíces y la resolubilidad de las ecuaciones algebraicas. Su estudio sobre el problema de irresolubilidad era incompleto y, en 1826, Abel[5] lo cierra probando que no se pueden resolver por radicales las ecuaciones polinómicas generales de grado mayor o igual que cinco. Sin embargo, este resultado no dice qué polinomios concretos son los que admiten una solución mediante radicales. En sus últimos años de vida, Abel[6] estuvo trabajando en el problema de dar una caracterización para tales polinomios. Agustin-Louis Cauchy es una figura clave en el desarrollo de esta nueva teoría de las permutaciones. Sobre este tema, entre 1815 y 1944 publica dos trabajos[7]. En el primero estudia las permutaciones de raíces de polinomios con el objeto de encontrar fórmulas algebraicas que le permitieran resolver dichas ecuaciones. La madured alcanzada en sus estudios sobre permutaciones le permite elaborar la memoria de 1844 en la que trata esta teoría como una disciplina propia, desconectada de las raíces del álgebra clásica, en la que además introdujo la notación y diversos conceptos que aún a día de hoy seguimos usando[8]. Uno de los resultados más

[5] *Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen* (1826).

[6] Desgraciadamente Abel fallece en 1829, con apenas 27 años de edad, antes de encontrarla.

[7] *Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manieres possibles les quantités qu'elle renferme* (1815) y *Mémoire sur les arrangements que l'on peut former avec des lettres données, et sur les permutations ou substitutionsa l'aide desquelles on passe d'un arrangementa un autre* (1844)

[8] Define el concepto de grupo de permutaciones, introduce la notación cíclica, habla de la identidad como


(a) Niels Henrik Abel


(b) A. Louis Cauchy

Figura 1.4: Abel (1802-1829) y Cauchy (1789-1857)

conocidos aparece en dicha memoria es el llamado Teorema de Cauchy:

> Teorema de Cauchy (1844): Si p es un número primo divisor del orden de un grupo, el grupo contiene un subgrupo de orden p.

Hay que puntualizar que sus resultados fueron enunciados y probados en el contexto de grupos de permutaciones.

En 1846, Liouville publica *Sur les conditions de résolubilité des équations par radicaux*, trabajo de un joven matemático llamado Évariste Galois[9]. En él, Galois expone que lo más importante a la hora de encontrar una solución algebraica de una ecuación era la estructura subyacente al grupo de permutaciones asociado a dicha ecuación. Introduce también los conceptos de lo que hoy conocemos como subgrupos normales y grupos resolubles y los usa con gran efecto para la resolubilidad de ecuaciones. El salto de abstracción en teoría de grupos llegó en 1854 [10] de la mano de Cayley que introduce la primera definición formal de grupo en los siguientes términos:

> A set of symbols $1, \alpha, \beta, \ldots$, all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group. These symbols are not in general convertible (commutative) but associative, it follows that if the entire group is multiplied by any one of the symbols, either as further or nearer factor (left or right), the effect is simply to reproduce the group (...) These symbols are not ingeneral convertible [commutative], but are associative.

---

permutación. Incluso aparece en sus resultados la idea de producto de dos grupos. Entre otros resultados, demuestra que toda permutación es producto de 3-ciclos y calcula subgrupos de los grupos simétricos hasta orden 6.

[9]Galois fue un matemático y activista político francés. Abiertamente republicano, en medio de la Revolución de Julio (1830), fue expulsado de la *École Normale* con 18 años por sus opiniones políticas, aunque siguió estudiando álgebra por su cuenta. En 1831 Poisson le pidió que le mandara su trabajo sobre ecuaciones polinómicas, pero tras una valoración negativa del mismo, Galois dejó de publicar sus artículos, simplemente mandándole su investigación a un amigo mediante cartas hasta el propio día de su muerte, el 30 de mayo de 1832; motivo por el cual su trabajo fue desconocido hasta que Liouville lo publicó.

[10]El trabajo en el que se recoge la definición es *On the theory of groups, as depending on the symbolic equation* $\zeta^n = 1$.(1854)


(a) Évariste Galois

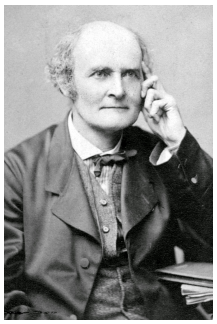

(b) Arthur Cayley

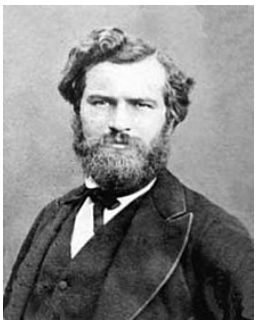
Figura 1.5: Galois (1811-1832) y Cayley (1821-1895)

Esta definición, en apariencia simple bajo los estándares actuales, permite a Cayley presentar los cuaternios, las matrices, las permutaciones y las formas cuadráticas de Gauss bajo el mismo prisma. También demuestra que dado uno de esos grupos abstractos, es decir, sin verlo como un grupo de permutaciones, se podía construir una tabla definiendo su multiplicación y que hay una correspondencia biyectiva entre ese grupo y un grupo de permutaciones, resultado conocido hoy como *Teorema de Cayley.*

Los resultados dados por Galois, Cauchy, Cayley y otros son presentados de forma unificada en 1870 por Jordan en *Traité des substitutions et des équations algébriques* [11]. En este tratado se formaliza la intuición que tenía Galois de los grupos resolubles, se introducen las nociones de homomorfismo e isomorfismo y de serie de composición y se prueba una parte del teorema de Jordan-Hölder que establece que este tipo de series, para un mismo grupo, tienen la misma longitud y la familia de factores simples es única salvo orden e isomorfismos. La otra parte de este resultado sería probada por Hölder en 1889. Además Jordan termina de demostrar el teorema de Cayley estableciendo que esa biyección entre un grupo y un cierto grupo de permutaciones es un homomorfismo. Este tratado de 1870 marca un antes y un después en el tratamiento de la teoría de grupos. En 1872 Sylow, basándose en el trabajo de Galois, publica *Théoremes sur les groupes de substitutions* un artículo de importancia suma en la teoría de estructura de los grupos finitos. De acuerdo con [9, Capítulo 8], en el trabajo aparecen las demostraciones completas de ocho teoremas, una parte de los cuales son conocidos hoy como Teoremas de Sylow (Teoremas I y II):

> Teorema I: Si p^α es la mayor potencia del primo p que aparece en el orden grupo, este grupo posee un subgrupo de orden p^α. Además, si el normalizador del subgrupo en el grupo tiene orden $p^\alpha m$, el orden del grupo es $p^\alpha m(pr+1)$.
>
> Teorema II: Un grupo contiene exactamente $pr+1$ subgupos de orden p^α. Se obtienen por transformación de uno de ellos por *sustituciones* [paso de una permutación a otra] del grupo.

[11] De acuerdo con H. Wussing, "The work represents a review of the whole of contemporary mathematics from the standpoint of the occurrence of group-theoretic thinking in permutation-theoretic form"(en *The Genesis of the Abstract Group Concept, M.I.T. Press, 1984*).


(a) Camille Jordan


(b) Ludwig Sylow

Figura 1.6: Jordan (1838-1922) y Sylow (1832-1918)

Como corolario, Sylow establece que

> Si el orden del grupo de Galois de una ecuación algebraica es una potencia de un primo, la ecuación es resoluble por radicales.

Sylow prueba estos resultados para grupos de permutaciones y, en 1887, Frobenius se da cuenta que todo grupo finito se puede representar como grupo de permutaciones de sus propios elementos y que las demostraciones de Sylow son válidas para grupos abstractos[12].

En cuanto a la geometría (y el análisis), la figura más importante es, sin duda alguna, Felix Klein que establece en 1872 el conocido como Programa Erlangen[13] en el que defiende que la teoría de grupos y la idea de simetría es el mejor camino para organizar el conocimiento geométrico. El objetivo era el estudio de la geometría mediante invariantes bajo diversos grupos de transformaciones. Klein, reconoce la similitud de su trabajo con los grupos de permutaciones y la teoría de Galois con la diferencia de que los grupos en la teoría de Galois son finitos y actúan sobre un conjunto discreto mientras que en su trabajo, son grupos finitos que actúan sobre variedades continuas. El Programa Erlangen (sigue vigente) sirvió para dar visibilidad a las aplicaciones de la teoría de grupos en otras áreas de las matemáticas y para la extensión de los grupos finitos vistos como grupos de permutaciones a grupos infinitos vistos como grupos de transformaciones. Wussing (The Genesis of the abstract group concept) atribuye a Klein la siguiente defensa de la teoría de grupos,

> *Group theory appears as a distinct discipline throughout the whole of modern mathematics. It permeates the most varied areas as an ordering and classifying principle.*

El mayor exponente en el estudio de grupos de transformaciones fue Sophus Lie. En 1874, inspirado por la teoría de Galois y por el Programa Erlangen, trató de formular una teoría equivalente a la de Galois para ecuaciones algebraicas para las ecuaciones diferenciales

[12]Siguiendo a Weber, Frobenius da una definición de grupo abstracto mediante cuatro postulados que usa para establecer los Teoremas de Sylow.

[13]Vergleichende Betrachtungen über neuere geometrische Forschungen: Programm zum Eintritt in die philosophische Facultät und den Senat der k. Friedrich-Alexanders-Universität zu Erlangen.

(a) Felix Klein (b) Sophus Lie

Figura 1.7: Klein (1849-1925) y Sophus Lie (1842-1899)

(*Über Gruppen von transformationen*). Su trabajo fue importante en el desarrollo de los grupos continuos y para principios de la década de 1880 consiguió dar una clasificación de los mismos. En su honor, a las variedades diferenciales que además tienen estructura de grupo y que cumplen que tanto el producto como la inversión son continuas se les llaman grupos de Lie. Además sentó las bases para que matemáticos como Picard o Vessiot llegaran a obtener una teoría de Galois diferencial.

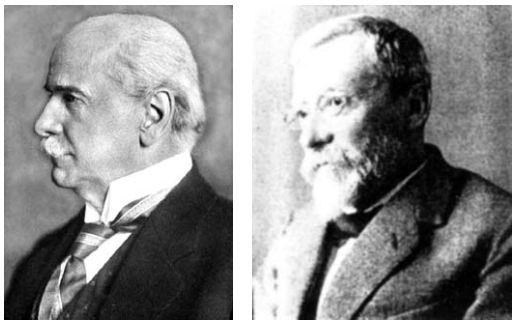
Y llegamos a la moderna definición de grupo (finito) dada por Weber en 1882 en un artículo[14] conjunto con Dedekind sobre formas cuadráticas:

> Un sistema G de elementos arbitrarios $\theta_1, \theta_2, \ldots, \theta_h$ se llama grupo de grado h si satisface:
>
> 1. Mediante alguna norma designada como composición o multiplicación, de dos elementos cualesquiera de un sistema se obtiene un nuevo elemento del mismo sistema.
> 2. Siempre se cumple que $(\theta_r\theta_s)\theta_t = \theta_r(\theta_s\theta_t)$.
> 3. De $\theta\theta_s = \theta\theta_t$ se sigue que $\theta_s = \theta_t$.

La definición tanto para grupos finitos como infinitos la da, el mismo año, von Dyck en *Gruppentheoretische Studien* (1882), donde defiende la utilidad de presentar los grupos mediante generadores y relaciones.

El desarrollo en la teoría de grupos de finales del siglo xix vino de la mano de Otto Hölder, cuando en 1892 publicó *Die einfachen Gruppen im ersten und zweiten Hundert der Ordnungszahlen*. Este trabajo expone que todos los grupos simples[15] que había hasta orden 200, eran conocidos. En 1893, introduce técnicas para clasificar grupos de orden producto de dos o tres primos y bajas potencias (*Die Gruppen der Ordnungen* p^3, pq^2, pqr, p^4). Estos y otros trabajos conducen a la edición de dos textos *Lehrbuch der Algebra* (Weber, 1896) y *Theory of groups of finite order* (Burnside, 1897), que unificaron toda la teoría

[14] Theorie der algebraischen Functionen einer Veränderlichen (Richard Dedekind y Heinrich Weber).
[15] Un grupo se dice simple si no posee subgrupos normales propios.



(a) Walther von Dyck (b) Otto Hölder

Figura 1.8: von Dyck (1856-1934) y Hölder (1859-1937)

de grupos hasta la fecha y sirvieron como base para el desarrollo de la misma durante el siglo xx.

En 1902 Burnside plantea un problema[16] que influenciaría el desarrollo de la teoría de grupos combinatoria.

> **Definición 1.2.** Dado un grupo G y un elemento $g \in G$, llamaremos *orden de* g, y lo denotaremos mediante $|g|$, al menor número natural $n \in \mathbb{N}$ tal que $g^n = e$. Si no existe tal número, diremos que el orden de g es infinito. Los grupos en los que todos sus elementos son de orden finito se dicen *grupos periódicos*. Un grupo periódico en el que el conjunto de órdenes de sus elementos está acotado, se dice *periódico con exponente acotado*.

Las definiciones previas nos permite establecer

> Problema General de Burnside (1902): Todo grupo periódico finitamente generado es necesariamente finito.

Soluciones del problema en formas débiles fueron dados por Burnside[17] en 1905 y Schur[18] en 1911. Los resultados iniciales apuntaban a que el Problema de Burnside iba a ser cierto, pero en 1964 Golod y Shafarevich dieron un contraejemplo en el caso general.[19]

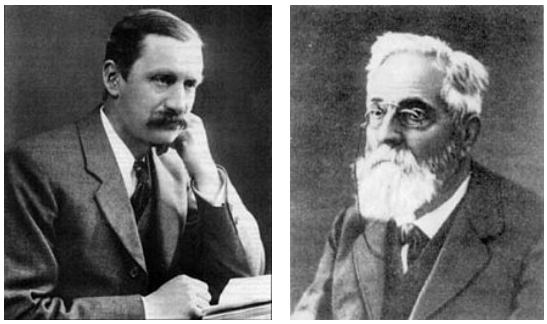
En esta primera mitad del siglo xx también se produjeron grandes avances tanto en grupos continuos como en grupos finitos. En el caso de los continuos, se formalizó el concepto de grupo topológico, Hermann Weyl (1885-1955) estableció entre 1923 y 1938 una teoría sobre los grupos compactos (grupos topológicos que como espacios topológicos son

[16] *On an unsettled question in the theory of discontinuous groups*, Quart. J. Pure and Appl Math. 33 (1902), 230-238.

[17] Todo subgrupo periódico de $GL(n, \mathbb{C})$ con exponente acotado es finito. (*On Criteria for the Finiteness of the Order of a Group of linear Substituions*, Proceedings of the London Mathematical Society, vol 2 (1), 1905, 435-440).

[18] Todo subgrupo periódico de $GL(n, \mathbb{C})$ es finito. (*Uber Gruppen periodischer substitutionen*, Sitzungsber. Preuss. Akad. Wiss, vol 619627 (4), 1911).

[19] *On the class field tower*, Izv. Akad. Nauk SSSR. Ser. Mat, 1964



(a) William Burnside (b) Heinrich M. Weber

Figura 1.9: Burnside (1852-1927) y Weber (1842-1913)

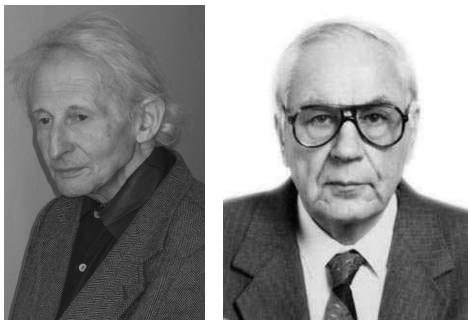
compactos) y Élie Cartan dio una clasificación de las álgebras de Lie semisimples, estructura algebraica muy relacionada con los grupos de Lie. Los grupos finitos, por otro lado, vieron el nacimiento de la teoría de carácteres por parte de Frobenius y una generalización de los teoremas de Sylow debida a Phillip Hall. El mayor avance en la teoría de grupos finitos comenzó a mediados de siglo con el trabajo de diversos matemáticos, como los ya mencionados Frobenius y Hall o bien Richard Brauer y K. A. Fowler, que dio comienzo a la clasificación de los grupos simples finitos. La prueba de la clasificación de ntales grupos se alargó hasta 2004 con los resultados de Aschbacher y Smith sobre *quasithin groups*[20]. En esta clasificación participaron grandes matemáticos como John Horton Conway, que desgraciadamente murió el 11 de abril de 2020 debido a complicaciones con el Covid-19 o Jaques Tits y John G. Thopmson, ganadores del premio Abel [21] de 2008 *por sus logros en álgebra profunda y, en particular, por dar forma a la teoría moderna de grupos.* El teorema de clasificación de grupos simples es facil de enunciar:

> Los grupos simples finitos están, salvo isomorfismos, en una de las siguientes categorías: grupos de orden primo, grupos alternados, grupos de tipo Lie o bien uno de los 26 grupos esporádicos,

pero es dificil de entender por la longitud y complejidad de su prueba. Su demostración ocupa unas 15.000 páginas que son suma de varios cientos de artículos publicados por más de 100 autores entre 1955 y 2004. Solamente la clasificación de los *quasithin groups*, último eslabón, dada Aschbacher y Smith ocupa 1221 páginas. De acuerdo con los notices de la AMS [1], el análisis de los de grupos finitos implica la solución de dos problemas:

[20]The classification of quasithin groups, Math. Surveys Monog., AMS, volumes 111 and 112 (2004).

[21]El artículo "Europeos y americanos comparten un prestigioso premio de matemáticas" (Servicio de Información Comunitario sobre Investigación y Desarrollo, CORDIS, 28/03/08) hace una síntesis de los avances alcanzados en la teoría de grupos y su vinculación con las simetrías. En referencia al premio Abel 2008, este artículo dice: " (...) Los logros de John Thompson y Jacques Tits tienen una influencia profunda y extraordinaria", declaró el Comité Abel en su mención."Se complementan recíprocamente y, en conjunto, constituyen la columna vertebral de la moderna teoría de grupos."



(a) Evgenii S. Golod (b) Igor Shafarevich

Figura 1.10: Golod (1935-2018) y Shafarevich (1923-2017)

I. Problema de clasificación: Determinar todos los grupos simples finitos.

II. Problema de Extensión: Dados dos grupos X e Y, determinar todas las extensiones de X por Y, es decir, dar todos los grupos salvo isomorfismo G con un subgrupo normal H tales que $H \cong X$ y $G/H \cong Y$.

De acuerdo con Aschbacher y Smith, si el primer problema ha sido duro, el segundo lo es mucho más (tratable en casos especiales). En este trabajo ilustraremos el Problema de Extensión en el caso de extensiones cíclicas para obtener, de forma unificada, la clasificación de los grupos de orden 16. En las notas históricas de [10], Wild afirma que Hölder inicia la teoría de extensiones de grupos en 1895.

1.2. Ejemplos, imágenes y cifras.

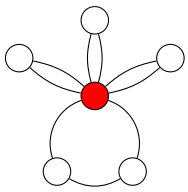


Figura 1.11: Grafo cíclico de D_3.

En este sección pretendemos dar vida a los grupos finitos, mostrando diversos ejemplos de los mismos, algunas representaciones gráficas y viendo algunos datos que muestran la envergadura del problema de la clasificación de los grupos finitos. Como hemos visto previamente en la introducción, dos de las familias más comunes en la teoría de grupos finitos son los grupos cíclicos de orden n, C_n y los diédricos, D_n. Definimos los grupos cíclicos como los grupos generados por un único elemento g, esto es, aquellos grupos tales que todos sus elementos son potencia del generador g, como hemos visto en el caso de las n-raíces de la unidad. Dado que $|C_n| = n$, para que g genere los n elementos del grupo, necesariamente $|g| = n$, lo cual nos lleva a que $g^i = g^j$ si y solamente si $i \equiv j$ (mód n), dándonos así la presentación habitual, $C_n = \langle g \rangle = \{g^i \,|\, i \in \mathbb{Z}\} = \{g^i \,|\, i = 0, 1, \ldots, n-1\}$. En el caso de los diédricos D_n, si los vemos como los grupos de simetrías que actúan sobre un n-ágono, podemos ver que dada una reflexión $\tau \in D_n$ sobre un eje dado y una rotación $\sigma \in D_n$, como hemos visto anteriormente, D_n va a estar generado por σ y τ con $|\sigma| = n$ y $|\tau| = 2$.

Sin embargo no basta con fijar eso, también nos tenemos que dar cuenta que estos grupos no son, en general, abelianos, de hecho lo que ocurre es que, si aplicamos la rotación σ e inmediatamente después la reflexión τ, nos va a quedar el mismo resultado que si hubiéramos aplicado primero τ y después la rotación inversa $\sigma^{-1} = \sigma^{n-1}$, luego a la hora de denotar D_n, a los generadores σ y τ, añadimos las relaciones anteriores, quedándonos $D_n = \langle \sigma, \tau \,|\, |\sigma| = n,\, |\tau| = 2,\, \tau\sigma = \sigma^{-1}\tau \rangle$. Otra familia de grupos importantes es la familia de los grupos cuaternio generalizados Q_{4n}, con n una potencia de 2 mayor o igual a 2. El más pequeño de estos, Q_8 representa a la unidad $e = 1$ y a los tres cuaterniones básicos i, j, k con la propia multiplicación heredada de los cuaterniones y viene presentado mediante $Q_8 = \langle i, j, k \,|\, i^2 = j^2 = k^2 = ijk = -1,\, (-1)^2 = 1 \rangle = \{\pm 1, \pm i, \pm j, \pm k\}$. Aunque esta es la forma más habitual de presentarlo debido a su relación con los cuaterniones, como $ij = k$, realmente con solo dos generadores nos basta, dándonos lugar a la presentación $Q_8 = \langle i, j \,|\, i^4 = j^4 = 1,\, i^2 = j^2,\, ji = (-i)j \rangle$. Además, esta presentación es la que nos permite generalizar a los $Q_{4n} = \langle a, b \,|\, a^{2n} = b^4 = e,\, a^n = b^2,\, bab^{-1} = a^{-1} \rangle$, con n una potencia de 2 mayor o igual a 2. Cabe mencionar que si no restringimos que n sea una potencia de 2, a los grupos de la forma Q_{4n} se les denomina grupos dicíclicos. También aparecen con bastante frecuencia los grupos alternados A_n que se definen como el conjunto de todas las permutaciones pares de un conjunto de cardinal n y los A_n con $n \geq 5$ constituyen una de las familias dadas por el Teorema de Clasificación de los Grupos Simples Finitos. Concretamente el A_5 es el grupo simple no abeliano y el grupo no resoluble de menor orden que existe, con 60 elementos. En este trabajo usaremos también una familia

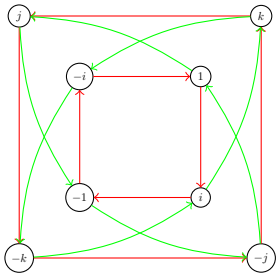


Figura 1.12: Grafo de Cayley de Q_8

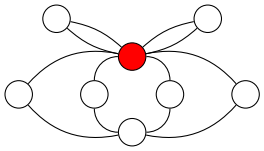


Figura 1.13: Grafo cíclico de K_8.

Orden	Número	Orden	Número
2^{10}	49487365422	$2^8 \cdot 7$	1083553
$2^9 \cdot 3$	408641062	$2^7 \cdot 3 \cdot 5$	241004
2^9	10494213	$2^7 \cdot 3^2$	157877
$2^8 \cdot 5$	1116461	2^8	56092
$2^8 \cdot 3$	1090265	$2^6 \cdot 3^3$	47937

Cuadro 1.1: Número de grupos de diversos órdenes.

que constituye una generalización del 4-grupo de Klein, K_4, el grupo de orden 4 en el que todos sus elementos no triviales son de orden 2. Estos K_{2n}, son grupos abelianos de orden $2n$ que definimos como el producto cartesiano de C_n por C_2, es decir $K_{2n} = C_n \times C_2$.

Por último haremos un pequeño comentario en relación al número de grupos salvo isomorfismo que hay dado un determinado orden, pues cuantos más grupos hay, más difícil resulta clasificarlos. Este trabajo lo inició Cayley dando una clasificación de los grupos de orden 4, 6, 8 y 12 y fue avanzando con resultados más generales como por ejemplo los de E. Netto [22] y Hölder, que determinaron, respectivamente, los grupos de orden p^2 y pq y los grupos de orden p^3, p^2q, pqr, y p^4. Históricamente, este trabajo involucraba muchas cuentas y pruebas por casos hechas a mano, lo cual provocó que muchas de estas clasificaciones tuvieran algún error, tal y como cuentan Besche, Eick y O'Brien [2]. En este artículo cuentan además que el principal problema no radica en dar una lista completa [23] de grupos de un determinado orden, sino en demostrar que no hay dos grupos en la lista que sean isomorfos. En 1993, László Pyber fue capaz de dar una cota superior al número de grupos, mostrando que, si denotamos por $f(n)$ al número de grupos salvo isomorfismo de orden n, entonces $f(n) \leq n^{(2/27+o(1))\mu(n)^2}$, donde $\mu(n)$ es el mayor exponente en la factorización en primos de n. En base a esta cota, cabría esperarse que cuanto más alto tenga un exponente, más grupos salvo isomorfismo habrá y por tanto, más complicada será hacer la clasificación; y, en efecto si tenemos en cuenta que hay 14 grupos de orden 16, 267 de orden 64 y nos fijamos en la tabla 1.1, en la que Besche et al. representaron los diez órdenes hasta 2000 con mayor número de grupos, vemos que el número de grupos crece exponencialmente conforme vamos tomando potencias sucesivas de 2, hasta llegar a los 49 487 365 422 grupos de orden 1024 que, para hacernos una idea de la magnitud de ese número, M. Wild comenta [10] que, si nos repartiéramos todos esos grupos entre todas las personas del mundo, tendríamos aproximadamente 7 grupos para cada uno.

[22] *Substitutionentheorie und ihre Anwendung auf die Algebra* (1882).

[23] En el sentido de que haya al menos un representante de cada clase de isomorfismo.

Capítulo 2

Preliminares

En este Capítulo estableceremos las definiciones, notaciones y resultados que serán usados para la clasificación de grupos de orden pequeño. El texto de referencia es [5]. La Sección 2.1 introduce los básicos en grupos (notaciones, definiciones y resultados clásicos) necesarios para el seguimiento del trabajo. En la Sección 2.2 se han unificado, reorganizado y probado los resultados necesarios y que son el hilo conductor de las clasificaciones del Capítulo 3.

En general, emplearemos la letra G para denotar un grupo arbitrario y $|G|$ representará su número de elementos que, en el caso finito será un natural $n \geq 1$ y en el no finito, escribiremos como $|G| = \infty$. Los elementos de G los denotaremos con letras minúsculas del abecedario (con frecuencia usaremos g, h, x, y, a, b); la letra e (el número 0 si el grupo es aditivo) la reservamos para el elemento neutro de G y g^{-1} denota el inverso si hablamos de grupos multiplicativos ($-g$ para grupos aditivos). Recordamos que la definición de grupo y el orden de un elemento, que hemos denotado usando también la doble barra $|g|$, ya han sido introducidos en el Capítulo 1, donde también hemos presentado la mayor parte de los grupos finitos que necesitaremos para nuestra clasificación: cíclicos, diédricos y simétricos.

El grupo G se dice *conmutativo o abeliano* si su poducto es conmutativo, esto es: $xy = yx$ para todo $x, y \in G$. Dado un entero positivo m, la expresión x^m representará el producto m veces del elemento x si $m \geq 1$ y $x^0 = e$. Escribiremos $x^{-m} = (x^{-1})^m$ para el producto m veces del inverso. Observamos que $x^{-m} = (x^m)^{-1}$. La existencia de inversos y la asociatividad nos permiten usar leyes cancelativas a derecha (si $yx = zx$, entonces $y = z$) e izquierda (si $xy = xz$, entonces $y = z$). Si denotamos por l_x, r_x las multiplicaciones a derecha e izquierda por el elemento x, las leyes cancelativas equivalen a afirmar que l_x y r_x son inyectivas; añadiendo la existencia de inversos, podemos afirmar que son biyectivas.

2.1. Conceptos y notaciones

En cualquier estructura algebraica es común considerar los subconjuntos para los que la operación binaria es cerrada y contienen los inversos de cualquiera de sus elementos. Tales conjuntos en grupos se dicen *subgrupos* y se denotan con el símbolo $\leq$. El criterio

que determina en un solo paso si un subconjunto no vacío H de G es subgrupo:

$$H \leq G \text{ si y solo si } \quad xy^{-1} \in H \ \forall x, y \in H. \tag{2.1}$$

Una de las formas de encontrar subgrupos de G es mediante generación por subconjuntos:

Definición 2.1. Dado un subconjunto no vacío S de G, el *subgrupo generado por S en G* es el conjunto de elementos de la forma:

$$\langle S \rangle = \{s_1^{m_1} s_2^{m_2} \cdots s_r^{m_r} : r \in \mathbb{N}, s_i \in S, m_i \in \mathbb{Z}\}. \tag{2.2}$$

Un subgrupo H se dice finitamente generado si $H = \langle S \rangle$ y S es finito.

Ejemplo 2.1. *Los grupos finitos son todos finitamente generados. En el caso de los cíclicos C_n su generador es cualquier elemento de orden n. Los diédricos D_n se pueden generar usando la rotación σ de ángulo $\frac{2\pi}{n}$ (orden n) y una cualquiera de sus reflexiones, τ (orden 2). De este modo tenemos $D_n = \langle \sigma, \tau \rangle$ y, como la relación entre ambas simetrías es $\tau\sigma = \sigma^{-1}\tau$, de acuerdo con* (2.2) *tenemos que:*

$$D_n = \{\sigma^r \tau^p : r = 0, \ldots n-1, p = 0, 1\}. \tag{2.3}$$

El concepto de coclase e índice nos lleva al primer resultado simple pero profundo en este capítulo, el Teorema de Lagrange.

Definición 2.2. Dado un subgupo H de G, para cada $x \in G$, llamaremos *coclase* a izquierda (a derecha) del elemento x respecto del subgrupo H al conjunto

$$xH = \{xh : h \in H\} (Hx = \{hx : h \in H\}), \tag{2.4}$$

El subgrupo H define en G la relación de equivalencia entre elementos: x e y relacionados sii $xH = yH$ sii $y^{-1}x \in H$. El número de clases de equivalencia de la relación anterior se dice *índice del subgrupo H en G* y se denota en la forma $[G : H]$.

Teorema 2.1 (Teorema de Lagrange)**.** *Si H es un subgrupo de un grupo finito G, entonces las coclases de G tienen exactamente $|H|$ elementos y $|G| = [G : H] \cdot |H|$.*[1]

Nota: La primera consecuencia elemental del Teorema de Lagrange es que, como $|g| = \langle g \rangle$ para cualquier elemento $g \in G$, tenemos que el orden de un elemento siempre divide al orden del grupo que lo contiene.

---

[1] En sus Disquisitiones Arithmeticae (1801), Carl F. Gauss demostró el Teorema de Lagrange para el caso concreto del grupo multiplicativo de los enteros modulares distintos de 0 módulo p, con p primo. En 1844 Augustin-Louis Cauchy lo probó para el grupo simétrico S_n y Camille Jordan lo demostró de forma general para cualquier grupo de permutaciones en 1861.

Las aplicaciones entre dos grupos $\varphi\colon G \to G'$ tales que $\varphi(xy) = \varphi(x)\varphi(y)$ se dicen *homomorfismos de grupos* y si son biyectivas, isomorfismos. El concepto de imagen $Im\,\varphi$ como aplicación y de núcleo, $ker\,\varphi = \{x \in G : \varphi(x) = e_{G'}\}$ proporcionan subgrupos de G' y G respectivamente. Si φ es isomorfismo y $G = G'$, φ se dice *automorfismo de* G. El conjunto de todos los automorfismos es un grupo con la composición que denotaremos en la forma:

$$Aut(G) = \{\varphi : G \to G : \varphi \text{ isomorfismo}\} \tag{2.5}$$

El grupo simétrico $S_n = Perm([n])$ aparece como grupo de aplicaciones biyectivas, llamadas permutaciones, del conjunto de $[n] = \{1, \ldots, n\}$. Si consideramos cualquier conjunto S (finito o no) y sus aplicaciones biyectivas, llegamos al grupo general de permutaciones $Perm(S)$ y al siguiente resultado [2]

Teorema 2.2 (Teorema de Cayley, 1854)**.** *Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones. En particular, si* $|G| = n$*,* G *es isomorfo a un subgrupo del grupo simétrico* S_n*.*

Demostración. La aplicación $\Omega : G\colon \to Perm(G)$ dada por $x \mapsto l_x$ es un homomorfismo de grupos inyectiva. Su restricción al conjunto imagen nos da el isomorfismo. □

Desde la noción de coclase llegamos a los subgrupos normales y la estructura cociente.

Definición 2.3. Un subgrupo N se dice normal en G, y escribiremos $N \trianglelefteq G$, si $Nx = xN$ (equivalentemente, $xNx^{-1} = N$) para todo $x \in G$. En este caso, el conjunto de coclases

$$G/N = \{xN : x \in G\} \tag{2.6}$$

con la operación $(xN)(yN) = (xy)N$ es un grupo llamado grupo cociente de G por N.

Nota: El conjunto $Z(G) = \{z \in G : zx = xz\ \forall x \in G\}$, llamado centro de G es subgrupo normal. Sus subgrupos también lo son. Además, todos los subgrupos de índice 2 son normales. En efecto, un subgrupo N de índice 2 de G, determina dos coclases en G: xN y N. Observamos que $Nx \cap N = \emptyset$, luego $Nx = xN$ puesto que G es unión disjunta de coclases y los conjuntos $xN = l_x(N)$ y $Nx = r_x(N)$ tienen igual cardinal.

Un resultado importante asociado al grupo cociente es el conocido como el Teorema de Correspondencia, que nos permitirá relacionar ciertos subgrupos normales de G con subgrupos normales del cociente G/N.

[2] W. Burnside, en su libro "Theory of groups of finite order"(1911), afirma que el resultado lo prueba C. Jordan en 1870. Pero en 1980, Eric Nummela (*Cayley's Theorem for Topological Groups*, Amer. Math. Monthly 87 (3): 202-203, 1980) dice que Arthur Cayley demostró en 1854 que la correspondencia en el teorema es biyectiva, pero que no probó que fuera homomorfismo.

Teorema 2.3 (Teorema de Correspondencia)**.** *Sea G un grupo y $N \trianglelefteq G$. Entonces existe una correspondencia biyectiva entre los subgrupos de G que contienen a N y los subgrupos de G/N. Esta biyección lleva subgrupos normales que contienen a N de G a subgrupos normales del cociente.*

Como se ha visto en el Capítulo 1, a lo largo de la historia los grupos se veían, no como estructuras independientes, sino como transformaciones que actuaban sobre un conjunto, como por ejemplo cuando Galois trataba las permutaciones de las raíces de polinomios. Esta idea es lo que hoy en día conocemos como acciones de grupos. La noción de acción permite alcanzar importantes resultados estructurales en Teoría de Grupos.

Definición 2.4. Una acción de grupo de un grupo G sobre un conjunto X es una aplicación $\cdot\colon G \times X \to X$ de tal forma que cumple:

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

Si existe una acción de grupo entre G y X, diremos que G actúa en X.

La acción de G sobre X determina la relación de equivalencia:

$$x \sim y \text{ si y solo si } \text{ existe } y = g \cdot x \text{ para algun } g \in G, \tag{2.7}$$

cuyas clases de equivalencia se dice órbitas y las denotaremos como $orb(x) = \{g \cdot x |\, g \in G\}$. El estabilizador de un elemento $x \in X$ se define como $stab_G(x) = \{g \in G | g \cdot x = x\}$ y es un subgrupo de G. Ambos conceptos están relacionados por el llamado Teorema Órbita-Estabilizador, que usaremos con frecuencia.

Teorema 2.4 (Teorema Órbita-Estabilizador)**.** *Sea X un conjunto finito, G grupo y $\rho\colon G \times X \to X$ un acción de G sobre X. Entonces $|orb_G(x)| = [G : stab_G(x)]$.*

Como aplicación de la noción de acción y este teorema se puede dar una demostración del resultado establecido por Cauchy en 1844:

Teorema 2.5 (Teorema de Cauchy)**.** *Sean G un grupo de orden n y p primo divisor de n. Entonces existe un elemento $x \in G$ tal que $|x| = p$.*

Demostración. Consideremos el conjunto

$$X = \{(x_1, x_2, \ldots, x_p) \in G^p |\, x_1 x_2 \cdots x_p = e\}\,. \tag{2.8}$$

Notemos que las $p-1$ primeras coordenadas de un elemento $x \in X$ se pueden elegir de forma arbitraria, mientras que x_p viene completamente determinada por las anteriores, con lo cual $|X| = n^{p-1}$. Consideremos ahora el grupo cíclico de orden p, $C_p = \langle c \rangle$ que actúa sobre X mediante $c \cdot (x_1, x_2, \ldots, x_p) = (x_2, x_3, \ldots, x_p, x_1)$. Por el Teorema Órbita-Estabilizador, el número de elementos de cada órbita divide a p, luego o bien 1 o bien p, por ser p primo. Denotemos por r el número de órbitas de un elemento y por s el número

de órbitas de p elementos, entonces tenemos que $|X| = n^{p-1} = r + sp$. Como p divide a n (y por tanto a n^{p-1}), entonces necesariamente dividirá a r. Sea $e_X = (e, e, \cdots, e)$, es evidente que $orb(e_X) = \{e_X\}$, con lo que $r \neq 0$ y por tanto hay al menos p elementos cuya órbita tiene solo un elemento. Tomemos uno de esos elementos a_X distinto de e_X, este elemento será de la forma $a_X = (a, a, \cdots, a)$ con $a \in G$ pero como $a_X \in X$, tenemos que $a^p = e$ y por tanto $|a|\,|p$. Como $a \neq e$, tenemos que $|a| = p$. □

De entre todas las acciones, a lo largo del trabajo usaremos la acción por conjugación y resultados estructurales derivados de la misma.

Definición 2.5. Para un grupo G, la aplicación τ es una acción llamada *acción por conjugación* de G sobre sí mismo:

$$\begin{aligned} \tau \colon G \times G &\to G \\ (g, x) &\mapsto \tau_g(x) := gxg^{-1}. \end{aligned}$$

Sus órbitas se dicen clases de conjugación, denotadas en el trabajo mediante $Cl(x)$). Los estabilizadores son los conocidos centralizadores de elementos y que se denomtan como $C_G(x)$. A los automorfismos $\tau_g(x)$ les llamaremos *automorfismos internos de G*.

Nota: A lo largo de la memoria, usaremos de forma indistinta las notaciones τ_g (si la acción se denota como τ) o t_g para denotar la conjugación por el elemento g.

Cuando se aplica el Teorema Órbita-Estabilizador se llega a un resultado que relaciona el orden de G, el de su centro, $Z(G)$, y con los índices de los distintos centralizadores.

Corolario 2.5.1 (Ecuación de clases)**.** *Sea G un grupo finito y $\tau_g(x) = g^{-1}xg$ la acción por conjugación de G. Si $\{x_1, \ldots, x_r\}$ es un conjunto de representantes de las clases de conjugación de cardinal mayor que* 1*. Entonces se tiene que:*

$$|G| = |Z(g)| + \sum_{i=1}^{r} [G : C_G(g_i)]. \tag{2.9}$$

Demostración. El resultado se sigue de que G es la unión disjunta de clases de conjugación, de que $Z(G)$ es la unión de las clases de conjugación de tamaño 1 y del Teorema 2.4. □

Una de las formas más habituales de obtener grupos nuevos usando otros conocidos es la construccion conocida como producto semidirecto. Para ello supongamos que tenemos un grupo G con dos subgrupos $N \trianglelefteq G$ y $H \leqslant G$ de tal forma que $G = NH$ y $N \cap H = \{e\}$. Además, *el grupo cociente G/N es isomorfo al subgrupo H*. Como $G = NH$, podemos expresar cada elemento $g \in G$ de la forma $g = nh$ con $n \in N$, $h \in H$. Además, usando $N \cap H = \{e\}$, la descomposición como producto es única. En efecto, supongamos que $g = n_1h_1 = n_2h_2$ con $n_1, n_2 \in N$ y $h_1, h_2 \in H$. Esto nos lleva a que $n_2^{-1}n_1 = h_2h_1^{-1}$,

que es un elemento de $N \cap H = \{e\}$. Por tanto, $n_1 = n_2$ y $h_1 = h_2$. Además, dados $n_1h_1, n_2h_2 \in NH$, su producto $(n_1h_1)(n_2h_2) \in G$, lo podemos ver también como un elemento de NH gracias a que N es normal: $(n_1h_1)(n_2h_2) = n_1\left(h_1n_2h_1^{-1}\right)h_1h_2$. En este caso decimos que G es un *producto semidirecto interno* de N y H. Este concepto nos lleva a plantear la posibilidad de a partir de dos grupos N y H (arbitrarios), construir un nuevo grupo G de tal forma que se cumplan las condiciones anteriores.

Definición 2.6 (Producto semidirecto externo)**.** Sean N y H grupos, $Aut(N)$ el grupo de automorfismos de N y $\phi\colon H \to Aut(N), h \mapsto \phi_h$, un homomorfismo de grupos. Llamaremos *producto semidirecto externo de N y H con respecto a ϕ* y lo denotaremos mediante $N \rtimes_\phi H$ al par $(G, *)$ donde $G = N \times H$ y $*$ es la operación binaria definida por la expresión: $(n_1, h_1) * (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2)$.

Es sencillo probar que $G = N \rtimes_\phi H$ es un grupo para el que $H \cong \{e_N\} \times H \leqslant G$, $N \cong N \times \{e_H\} \trianglelefteq G$ y $(\{e_N\} \times H) \cap (N \times \{e_H\}) = \{(e_N, e_H)\}$. Por analogía con el producto semidirecto interno, y siempre que no de lugar a confusión, se suele denotar (n, h) como nh, (e_N, h) como h, (n, e_H) como n y (e_N, e_H) como e. Con este acuerdo de notación, $hnh^{-1} = \phi_h(n)$. Así, mientras que en los productos semidirectos internos, partimos de dos subgrupos, uno de ellos normal, sobre el que el otro actúa por conjugación, en los externos usando dos grupos, N y H, se construye un tercero, G, de tal forma que $H \leqslant G$, $N \trianglelefteq G$ y la forma en la que H actúa por conjugación sobre N la determina el homomorfismo ϕ.

Nota: El producto semidirecto es un caso particular del Problema de Extensión expuesto en el primer capítulo. Extendemos usando N y H de modo que $G/N \cong H$. En este caso se impone que $N \cap H = \{e\}$ y la extensión viene dada por una acción, el homomorfismo ϕ, ya que $Aut(N)$ es un subgrupo de $Perm(N)$. El papel de ϕ es muy importante, ya que define el producto marcando la forma en que los elementos de H y N se pueden intercambiar ($hn = \phi_h(n)h$).

De esta forma disponemos de varias formas de extender N a través de H, tantas como homomorfismos ϕ, si bien las extensiones pueden dar lugar a grupos isomorfos. Un caso especial ocurre cuando $\phi(h) = Id_N$ para todo $h \in H$, pues entonces tenemos que $(n_1, h_1) * (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2) = (n_1n_2, h_1h_2)$. A este caso en el que producto ocurre componente a componente se le dice *producto directo externo*. Su análogo, el llamado producto *producto directo interno*, se define en la forma: un grupo G y dos subgrupos $H, N \trianglelefteq G$ tales que $G = NH$ y $N \cap H = \{e\}$. La normalidad de ambos subgrupos y el hecho de que $H \cap N = \{e\}$ hace que los elementos de H y N conmuten. En efecto, si $h \in H$ y $n \in N$, el producto $nhn^{-1}h^{-1}$ lo podemos ver de dos formas distintas. Usando asociatividad, $nhn^{-1}h^{-1} = n(hn^{-1}h^{-1}) = (nhn^{-1})h^{-1}$. La normalidad de N y H nos llevan a $nhn^{-1}h^{-1} \in N \cap H = \{e\}$ y por tanto $nh = hn$.

2.2. Hechos básicos

Desde los preliminares de la sección previa, vamos a establecer una serie de lemas que nos permitirán obtener la clasificación de los grupos de orden ≤ 16 en el siguiente capítulo evitando el uso del Teorema de Clasificación de grupos abelianos finitamente generados y los llamados Teoremas de Sylow. Los resultados hacen referencia a estructura de grupos de orden producto de dos primos y al cálculo de automorfismos y nos permitirán obtener la clasificación usando productos semidirectos y las llamadas extensiones cíclicas que introduciremos en el siguiente capítulo.

Lema 2.1. *Los grupos de orden primo son cíclicos y únicos salvo isomorfismo.*

Demostración. Sea G grupo de orden p primo. Por el Teorema de Cauchy 2.5 existe $g \in G$ de orden p. Entonces $\{e\} \neq \langle g \rangle \leqslant G$. Ahora bien, debido al Teorema de Lagrange 2.1, tenemos que el orden de $\langle g \rangle$ divide al orden de G, es decir, o bien $| < g > | = 1$ o bien $| < g > | = p$. Como $\{e\} \neq \langle g \rangle$, entonces $|\langle g \rangle| = p$, luego $G = \langle g \rangle = \left\{g^k : i = 0, \ldots, p-1\right\}$. Ahora sea otro grupo cíclico del mismo orden, $H =< h >= \{h^k : i = 0, \ldots, p-1\}$. Consideremos la aplicación $f \colon G \to H, \quad g^i \mapsto h^i$ con $i = 0, 1, \ldots, p-1$. Esta aplicación es claramente biyectiva y homomorfismo de grupos. En efecto,

$$f\left(g^i \cdot g^j\right) = f\left(g^{i+j}\right) = h^{i+j} = h^i \cdot h^j = f\left(g^i\right) \cdot f\left(g^j\right).$$

Por tanto G y H son isomorfos. □

Lema 2.2. *Dos elementos conjugados son del mismo orden.*

Demostración. Sea G grupo y sean $x, y \in G$ con $|x| = n$ y $\left|yxy^{-1}\right| = m$. Como

$$\begin{aligned}\left(yxy^{-1}\right)^n &= \left(yxy^{-1}\right)\left(yxy^{-1}\right)\ldots\left(yxy^{-1}\right) = yx\left(y^{-1}y\right)xy^{-1}\ldots yx\left(y^{-1}y\right)xy^{-1} \\ &= yx^n y^{-1} = yy^{-1} = e,\end{aligned}$$

tenemos que m divide a n ya que el orden de un elemento es mínimo. De forma análoga se ve que n divide a m, pues

$$e = \left(yxy^{-1}\right)^m = yx^m y^{-1} \implies y = yx^m \implies e = x^m.$$

Por tanto $n = |x| = m = \left|yxy^{-1}\right|$. □

Lema 2.3. *Sea G grupo y $Z(G)$ su centro. Si $G/Z(G)$ es cíclico entonces G es abeliano.*

Demostración. Si $G/Z(G)$ es cíclico, existe algún $x \in G$ tal que $G/Z(G) = \langle x\, Z(G)\rangle$. Así, dado $g \in G$, existe $n \in \mathbb{Z}$ tal que $g\, Z(G) = x^n\, Z(G)$. Por la relación de equivalencia del cociente, $z = (x^n)^{-1} g \in Z(G)$, con lo que $g = x^n z$ para algún $z \in Z(G)$. Usando el párrafo anterior, cualquier par g_1, g_2 de elementos de G, descomponen como $g_1 = x^{n_1} z_1$ y $g_2 = x^{n_2} z_2$, $n_i \in \mathbb{Z}$ y z_i. Esto permite comprobar fácilmente que G es abeliano:

$$g_1 g_2 = x^{n_1} z_1 x^{n_2} z_2 \underset{z_1 \in Z(G)}{=} x^{n_1+n_2} z_2 z_1 \underset{z_2 \in Z(G)}{=} x^{n_2} z_2 x^{n_1} z_1 = g_2 g_1.$$

□

Lema 2.4. *Sea G grupo y sean S, T subgrupos de G. Entonces $ST \leqslant G$ si y solo si $ST = TS$.*

Demostración. Supongamos que $ST \leqslant G$. Sea $xy \in ST$, como ST es un subgrupo, tenemos que existirá $g = ab \in ST$ de tal forma que $xy = g^{-1}$. Ahora bien, esto nos lleva a que $xy = g^{-1} = (ab)^{-1} = b^{-1}a^{-1} \in TS$, luego $ST \subset TS$. Por otra parte, sea $yx \in TS$. Tenemos que $x^{-1}y^{-1} \in ST$, pues S y T son subgrupos de G. Como ST es subgrupo, tenemos que $\left(x^{-1}y^{-1}\right)^{-1} \in ST$, luego $yx \in ST$ y por tanto, $TS \subset ST$. Con lo que $ST = TS$. Por otro lado, si suponemos que $ST = TS$ tomemos $xy, ab \in ST$. Entonces $(xy)(ab)^{-1} = xyb^{-1}a^{-1}$. Como $y^{-1}b \in T$ y $a^{-1} \in S$, tenemos que $yb^{-1}a^{-1} \in TS$ y como $ST = TS$, existirá un $cd \in ST$ tal que $cd = yb^{-1}a^{-1}$, luego $(xy)(ab)^{-1} = xyb^{-1}a^{-1} = xcd \in ST$, pues $xc \in S$ y $d \in T$. Luego $ST \leqslant G$. □

Nota: Recordemos que dados dos subconjuntos S y T de G, definimos el subconjunto producto $ST := \{xy |\, x \in S \text{ e } y \in T\}$.

Lema 2.5. *Si todo elemento de G es de orden 2 excepto e, entonces G es abeliano. Además, si $G \neq \{e\}$ es finito y tiene n generadores distintos, entonces $G \cong C_2^n$.*

Demostración. Sean $x, y \in G$ tal que $x, y \neq e$, luego tanto x como y son de orden 2.

$$xy = (yy)(xy)(xx) = y(yx)(yx)x = y(yx)^2x = yx.$$

Ya que, o bien $yx = e$, en cuyo caso $(yx)^2 = e^2 = e$ o bien $yx \neq e$, en cuyo caso, por hipótesis tenemos que $|yx| = 2$ luego $(yx)^2 = e$. Para probar que $G \cong (C_2)^n$ empecemos notando que el orden de G es una potencia de dos. En efecto, si existiera algún p primo impar tal que $p |\, |G|$, por el Teorema de Cauchy tendríamos que existiría un elemento de orden p, lo cual contradice las hipótesis. Luego $|G| = 2^n$ para algún $n \in \mathbb{N}$. Tomemos $x_1 \in G$ tal que $|x_1| = 2$ y definimos $H_1 = \langle x_1 \rangle \leqslant G$. Si $|G| = 2$, entonces $G \cong H_1 \cong C_2$; si no, podemos tomar $x_2 \in G$ también de orden 2 de forma que $x_2 \notin H_1$. Como $H_1 \cap \langle x_2 \rangle = \{e\}$, tenemos que $H_2 = H_1 \langle x_2 \rangle \cong C_2 \times C_2$ y tenemos que $H_2 \leqslant G$ (pues $H_1 \langle x_2 \rangle = \langle x_2 \rangle H_1$ y podemos aplicar el Lema 2.4) y que $|H_2| = 2^2$, luego existe un $x_3 \in G$ de tal forma que $x_3 \notin H_2$ y podemos repetir el proceso. De esta forma, podremos definir de forma recursiva $H_k = H_{k-1} \langle x_k \rangle$ mientras que $|H_{k-1}| < |G|$. Además, estos H_k cumplen que $|H_k| = 2^k$, $H_k = H_{k-1} \langle x_k \rangle \cong (C_2)^{k-1} \times C_2$ y $H_k \leqslant G$. Por último, notemos que $H_n \cong (C_2)^n$ y que $|H_n| = 2^n = |G|$. Luego $G = H_n \cong (C_2)^n$. □

Lema 2.6. *Si p es primo, el número de elementos de orden p en un grupo finito G es múltiplo de $p - 1$.*

Demostración. El resultado es claro si p no divide a $|G|$ pues no puede tener elementos de orden p. En otro caso, por el teorema de Cauchy, tomamos $x \in G$ con $|x| = p$. Entonces el subgrupo G, $\langle x \rangle = \left\{e, x, x^2, \ldots, x^{p-1}\right\}$ nos da $p - 1$ elementos de orden p (el orden de un elemento divide al orden del grupo). Si no hubiera más elementos de orden p ya estaría. Si

existe $y \in G$ tal que el orden de y es igual a p e $y \notin \langle x \rangle$, entonces $\langle y \rangle = \{e, y, y^2, \ldots, y^{p-1}\}$ y $\langle x \rangle \cap \langle y \rangle = \{e\}$ (el orden de un subgrupo divide al orden del grupo). De esta forma, dado que G es finito, podemos conseguir una colección finita, $x_1, x_2, \ldots x_n \in G$, todos de orden p, de forma que los subgrupos $\langle x_i \rangle$ tienen dos a dos intersección trivial y cada uno aporta $p-1$ elementos de orden p. □

Lema 2.7. *Si G es un grupo de orden p^m con p primo y $m > 1$, entonces el centro de G, $Z(G)$, es no trivial.*

Demostración. Si $Z(G) = \{e\}$, en la ecuación de clases (2.9) observamos que cada término del sumatorio es divisible por p. Entonces $p^m = |G| \equiv 1(\text{mód } p)$, una contradicción. Por tanto $Z(G) \neq \{e\}$. □

Lema 2.8. *Si G es un grupo no abeliano de orden pq con p y q primos distintos, entonces $Z(G) = \{e\}$.*

Demostración. Como $Z(G) \leq G$, por el Teorema de Lagrange, $|Z(G)| = 1$, p, q o pq. Ahora bien, si $|Z(G)| = pq$, $G = Z(G)$ es abeliano, luego descartamos este caso. Si $|Z(G)| = p$ ó q, entonces $|G/Z(G)| = q$ ó p. En cualquiera de los casos, por el Lema 2.3, G sería abeliano, lo cual es una contradicción. Con lo que $|Z(G)| = 1$ y por tanto $Z(G) = \{e\}$. □

Lema 2.9. *Sea G un grupo no abeliano de orden pq con p y q primos distintos. Entonces el número de elementos de orden p en G es un múltiplo de q.*

Demostración. Por el Lema 2.8 $Z(G) = \{e\}$. Usando el Teorema de Cauchy, podemos tomar $x \in G$ tal que $|x| = p$. El elemento x no es central, luego $C_G(x) \neq G$. Como x está en su centralizador, por el Teorema de Lagrange, $p \,|\, |C_G(x)|$, luego $|C_G(x)| = p$. Usando el Teorema Órbita-Estabilizador, $|Cl(x)| = [G : C_G(x)] = q$. Recordar que los elementos de la clase de conjungación $Cl(x)$ tienen orden p de acuerdo con Lema 2.2. Es decir, los elementos de orden p están en clases de conjugación de orden q por lo tanto el número de elementos de orden p es múltiplo de q. □

Lema 2.10. *Supongamos que G es un grupo no abeliano de orden $2n$ con $n = 4, 6$ o un primo impar. Supongamos además que existen $x, y \in G$ tales que $x^n = y^2 = e$ y, en los casos $n = 4, 6$, que $y \notin \langle x \rangle$. Entonces $G \cong D_n$, siendo D_n el grupo diédrico de orden $2n$.*

Demostración. Observamos que $y \notin \langle x \rangle$, $n = 2, 3$, equivale a $y \neq x^2$ o $y \neq x^3$. Consideremos $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$, todos estos elementos distintos ya que $|x| = n$. Sea el conjunto $\{y, xy, x^2y, \ldots, x^{n-1}y\}$; sus elementos son distintos pues r_y es biyectiva. Ambos conjuntos o son disjuntos o coinciden, y este último caso solo se puede dar si $y \in \langle x \rangle$, en cuyo caso, como y es de orden 2, n tiene que ser par por el Teorema de Lagrange. Luego $n = 4, 6$ y sus únicos elementos de orden 2 son x^2 o x^3, situación descartada por las hipótesis. De esta forma obtenemos que $G = \{e, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}$, ya que tenemos $2n$ elementos distintos. Además como

$$|G : \langle x \rangle| = \frac{|G|}{|\langle x \rangle|} = \frac{2n}{n} = 2,$$

entonces $\langle x\rangle \trianglelefteq G$. Con lo cual, existe $m \in \{1, 2, \ldots, n-1\}$ tal que $yxy^{-1} = x^m$. Ahora bien, $yxy^{-1} = x$ implica $yx = xy$, y G es no abeliano, luego $2 \leq m \leq n-1$. Ahora:

$$x = y^2xy^{-2} = y\,(yxy{-}1)\,y^{-1} = yx^my^{-1} = x^{m^2} \text{ luego}$$
$$m^2 \equiv 1\ (mod\, n) \iff n \mid m^2 - 1 = (m+1)(m-1).$$

Por tanto, si n es un primo impar, $n|m^2-1$, luego o bien $n|(m+1)$ o bien $n|(m-1)$ y como $1 < m \leq n-11$, necesariamente $m = n-1$. En el caso de que $n = 4$, entonces $2 \leq m \leq 3$ y $m^2 \equiv 1\,(\text{mod } 4)$, con lo que $m = n-1 = 3$. Por último, en el caso de que $n = 6$, $2 \leq m \leq 5$ y $m^2 \equiv 1\,(\text{mod } 6)$, con lo que $m = n-1 = 5$. En todos los casos, $G = \left\langle x, y | x^n = y^2 = e,\ yxy^{-1} = x^{n-1}\right\rangle \cong D_n$. □

Lema 2.11. *Si G es un grupo de orden $2p$ con p primo impar, o bien G es cíclico o bien es diédrico.*

Demostración. Por el Teorema de Cauchy existen dos elementos distintos, pues p es primo impar, $x, y \in G$ de órdenes p y 2, luego $x^p = y^2 = e$. Además, por el Teorema de Lagrange, $\langle x\rangle \cap \langle y\rangle = \{e\}$. Si G es abeliano, $(xy)^{2p} = x^py^2 = e$ y como $(xy)^p = y \neq e \neq (xy)^2 = x^2$, este elemento tiene orden $2p$, luego $G = \langle xy\rangle \cong C_{2p}$. Si G no es abeliano, como $\langle x\rangle \cap \langle y\rangle = \{e\}$, se cumplen las hipótesis del Lema 2.10 y $G \cong D_p$. □

Terminamos la sección con dos resultados de cálculo de de subgrupos de índice 2 en grupos de orden 16 y de algunos grupos de automorfismos. Recordemos que los subgrupos de índice dos son siempre normales y serán fundamentales en las extensiones, tanto para las dadas por productos semidirectos, como para las cíclicas.

Lema 2.12. *Si G es un grupo de orden 16 y no isomorfo a $C_2^4 = C_2 \times C_2 \times C_2 \times C_2$ entonces G contiene un subgrupo normal isomorfo a C_8 o K_8.*

Demostración. Cualquier subgrupo de orden 8 en uno de orden 16 es normal por tener índice 2, así es que basta con encontrar un cíclico o un $K_8 = C_4 \times C_2$. Si hay en G un elemento x de orden 8, ya tenemos que $\langle x\rangle \cong C_8$. Así que supongamos que G no tiene elementos de orden 8. Entonces, los elementos de distintos del neutro tienen orden 2 ó 4 y, como G no es isomorfoa C_2^4, usando el Lema 2.5, G tiene elementos de orden 4. Además por el Lema 2.7, $Z(G) \neq \{e\}$, luego existe $z \in Z(G)$ de orden 2. Llamamos $H =< z >$, que es subgrupo normal de G, y consideramos dos casos:

- Si existiera un elemento x de orden 4 tal que $x^2 \neq z$ entonces $\langle x\rangle \cap H = \{e\}$ y llegamos al producto semidirecto $\langle x, z\rangle = \langle x\rangle\, H$ pues H es normal. Como además $xz = zx$ ya que $z \in Z(G)$, el producto va a ser directo, luego $K_8 \cong \langle x\rangle \times H \cong \langle x\rangle\, H$.
- Supongamos por el contrario que todo elemento x de orden 4 cumple que $x^2 = z$. Entonces todo elemento del cociente G/H tendrá orden menor o igual que 2 ya que, dado un elemento $x \in G$ de orden 4, el elemento xH en el cociente cumple que $(xH)^2 = x^2H = zH = H$. Por el Lema 2.5 concluímos que G/H es abeliano. Ahora, si $x \in G$ de orden 4, para todo elemento y tenemos que $yxy^{-1} \in xH$. En efecto:

$$yxy^{-1}H = yHxHy^{-1}H \underset{G/H \text{ abeliano}}{=} yHy^{-1}HxH = yy^{-1}xH = xH.$$

Esto nos lleva a que $Cl(x) \subseteq xH$, luego $|Cl(x)| \leq 2 = |xH|$. Por el Teorema Órbita-Estabilizador tenemos que $|C_G(x)| \geq 8$. De aquí se sigue que existe $y \in C_G(x) \setminus \langle x \rangle$. Si $|y| = 2$, entonces $\langle x \rangle \cap \langle y \rangle = \{e\}$ y, como x e y conmutan, $\langle x, y \rangle = \langle x \rangle \langle y \rangle \cong \langle x \rangle \times \langle y \rangle \cong K_8$. Por el contrario, si $|y| = 4$, por hipótesis tenemos que $y^2 = z$ de donde se sigue, junto a que $y \in C_G(x)$, que $(xy)^2 = x^2y^2 = z^2 = e$ y por tanto $|xy| \leq 2$. Concretamente, $|xy| = 2$ ya que $xy = e$ implica $y = x^{-1} \in \langle x \rangle$ lo cual es imposible pues $y \notin \langle x \rangle$. Esta última afirmación también obliga a que $xy \notin \langle x \rangle$. Así que $\langle x \rangle \cap \langle xy \rangle = \{e\}$ y, como $x, xy \in C_G(x)$ ambos elementos conmutan nos encontramos en las condiciones de un producto directo y por tanto $\langle x, xy \rangle \cong K_8$.

□

Definir homomorfismos de grupos finitamente generados se reduce a definir las imágenes de los generadores de tal manera que se respeten las relaciones de productos entre ellos. Teniendo en cuenta que para cualquier homomorfismo φ se cumple que $\varphi(e) = e$,

- la relación $xx^{-1} = x^{-1}x = e$ nos lleva a $\varphi(x^{-1}) = \varphi(x)^{-1}$, y
- de $x^n = e$ concluimos que $\varphi(x)^n = e$. En particular, $|\varphi(x)|$ debe dividir a $|x|$.

Los automorfismos de un grupo G no son fáciles de obtener, pero las consideraciones previas restringen las posibilidades de cálculo. De hecho, si $\varphi \in Aut(G)$, $|\varphi(x)| = |x|$. Además, estos subgrupos, salvo isomorfismos, son subgrupos del grupo de $Perm(G)$. En el caso de grupos cíclicos tenemos que:

Lema 2.13. *Para cualquier entero $n \geq 2$, $Aut(C_n)$ es isomorfo al grupo de la unidades $\mathbb{Z}_n^\times = \{a + n\mathbb{Z} : m.c.d.(a, n) = 1\}$ del anillo de enteros modulares $\mathbb{Z}_n$.*

Demostración. Como $C_n = \langle g \rangle$ con g elemento de orden n, un automorfismo φ de C_n está completamente determinado por $\varphi(g)$ que debe ser un elemento de orden n. Los elementos de orden n de C_n son de la forma g^k donde $m.c.d.(k, n) = 1$. Esta condición determina de forma completa las unidades de $\mathbb{Z}_n$. Ahora, una aplicación de la forma $\varphi_s \colon g \mapsto g^s$ es homomorfismo C_n y todos los homomorfismos son así. Serán isomorfismos si y solo si $\langle g^s \rangle = \langle g \rangle$, lo que equivale a que $|g^s| = n$. Finalmente la aplicación $\tau : \mathbb{Z}_n^\times \to Aut(C_n)$ donde $\tau(a) = \varphi_a$ nos da el isomorfismo deseado. □

Para uso posterior, necesitamos conocer los grupos de automorfismos de D_3, C_8 y $K_8 = C_4 \times C_2$. Daremos sus elementos, los órdenes de los mismos, una presentación como grupo de permutaciones (nos informará sobre los elementos que fijan) y sus clases de conjugación. También concluiremos su estructura salvo isomorfismos. La completa información aparece en las Tablas 2.2,2.1 y 2.3.

Lema 2.14. *Los grupos de automorfismos de C_8, D_3 y K_8 son isomorfos a K_4, D_3 y D_4 respectivamente.*

Demostración. De acuerdo con el Lema 2.13 y su demostración, los posibles automorfismos de C_8 son los que vienen dados en la Tabla 2.1. Además, es inmediato comprobar que el

orden de φ es menor o igual que 2 para todo $\varphi \in Aut(C_8)$, luego como $Aut(C_8)$ es un grupo de orden 4 y todos sus elementos distintos del neutro son de orden 2, tenemos que $Aut(C_8) \cong K_4$ usando el Lema 2.5.

El grupo $Aut(D_3)$ lo vamos a construir mediante imágenes de generadores. Sean $a, b \in D_3$ tales que $|a| = 3$ y $|b| = 2$. Al igual que antes, todos los automorfismos tienen que llevar elementos a elementos del mismo orden, lo cual nos limita las posibles opciones a las de la Tabla 2.2 como máximo. Para ver que son automorfismos, consideremos φ_2 y φ_3. La extensión $\varphi_k(a^ib^j) = \varphi_k(a^i)\varphi_k(b^j)$ proporcionan los homomorfismos. Basta con comprobar que son inyectivos para concluir que son automorfismos. Sean $(a^ib^j), (a^kb^l) \in D_3$ (notemos que, en particular $0 \leq i, k \leq 2$ y $0 \leq j, l \leq 1$). Por un lado, si suponemos que $\varphi_2(a^ib^j) = a^{2i}b^j = a^{2k}b^l = \varphi_2(a^kb^l)$, tenemos que $a^{2(i-k)} = b^{l-j}$ y ambas partes de la igualdad son iguales a e. Esto nos lleva a que $b^{l-j} = e$, y por tanto $b^l = b^j$, y a que $3|(i-k)$, luego $a^{i-k} = e$ y $a^i = a^k$. Así $a^ib^j = a^kb^l$ y φ_2 es inyectiva, lo que implica automorfismo (conjunto inicial y final de orden 6). De igual forma, si suponemos que $\varphi_3(a^ib^j) = a^{i+j}b^j = a^{k+l}b^l = \varphi_3(a^kb^l)$, como $l, j = 0, 1$, de nuevo $a^{i+j-k-l} = b^{l-j}$ y ambas partes de la igualdad son iguales a e. Esto nos lleva a que $b^{l-j} = e$ luego $b^l = b^j$. Con lo que $a^{i+j-k-l} = a^{i-k} = e$, por tanto $a^i = a^k$ y concluimos que $a^ib^j = a^kb^l$ y por tanto φ_3 es inyectiva. Tenemos que $\varphi_3^2(a) = a$ y $\varphi_3^2(b) = a^2b$, luego $\varphi_5 = \varphi_3^2$. Por otra parte, $\varphi_3 \circ \varphi_2(a) = a^2$ y $\varphi_3 \circ \varphi_2(b) = ab$, luego $\varphi_4 = \varphi_3 \circ \varphi_2$. Por último, $\varphi_3^2 \circ \varphi_2(a) = a^2$ y $\varphi_3^2 \circ \varphi_2(b) = a^2b$, de donde $\varphi_6 = \varphi_3^2 \circ \varphi_2$. Como la composición de automorfismos también lo es, las seis lo son y proporcionan todos los automorfismos de D_3. Usando el Lema 2.11 con $p = 3$, concluimos $Aut(D_3) \cong D_3$.

Por último, el caso $Aut(K_8)$ procederemos de forma similar al caso anterior. Tenemos que $K_8 = \langle x, y \rangle$ con x de orden 4 e y de orden 2, esta vez no solo tenemos que exigir que las imágenes de los generadores sean del mismo orden, sino que además tenemos que exigir que $\psi(y) \neq \psi(x^2)$, pues $y \neq x^2$. Imponer esta condición limita los automorfismos a, como mucho, los descritos en la Tabla 2.3. Falta ver que todas las opciones son válidas. Empezamos probando que ψ_5 y ψ_6 lo son. En efecto, sean $x^iy^j, x^ky^l \in K_8$. Comprobemos que son inyectivas. Supongamos que $\psi_5(x^iy^j) = x^iy^{i+j} = x^ky^{k+l} = \psi_5(x^ky^l)$. Tenemos entonces que $x^{i-k} = y^{k+l-i-j} = e$, pues $\langle x \rangle \cap \langle y \rangle = \{e\}$. Así que, $x^i = x^k$ y por tanto $i \equiv k$ (mód 4), lo cual implica que $i - k \equiv 0$ (mód 2), luego tenemos que $y^{j-l} = y^{k-i} = e$, es decir, $y^j = y^l$. Con lo que concluimos que $x^iy^j = x^ky^l$, por tanto ψ_5 es inyectiva y por tanto automorfismo. Supongamos ahora que $\psi_6(x^iy^j) = x^iy^ix^{2j}y^j = x^{i+2j}y^{i+j} = x^{k+2l}y^{k+l} = x^ky^kx^{2l}y^l = \psi_6(x^ky^l)$, tenemos que $x^{i+2j-k-2l} = y^{k+l-i-j} = e$. Esto nos dice que $x^{i-k} = (x^2)^{l-j}$ y que $y^{k-i} = y^{j-l}$. Notemos que $j, l \in \{0, 1\}$. Supongamos que $j \neq l$, entonces tenemos que $j - l = \pm 1$. Supongamos sin pérdida de generalidad que $j - l = 1$. Entonces $x^{i-k} = x^{-2} = x^2$, de donde sacamos que $x^i = x^{k+2}$ y por tanto $i = k + 2 + 4n$ con $n \in \mathbb{N}$. Sin embargo, $y^{k-i} = y^{-2-4n} = e \neq y = y^{j-l}$, con lo cual llegamos a una contradicción y deducimos que $j = l$. Esto nos lleva directamente a que $y^j = y^l$ y además, tenemos que $x^{k-i} = e$, luego $x^i = x^k$. Por tanto, $x^iy^j = x^ky^l$, así que ψ_5 es inyectiva, luego es automorfismo. Es facil ver que $\psi_6^2 = \psi_3$ y $\psi_6^3 = \psi_8$. Además $\psi_6\psi_5 = \psi_4$, $\psi_6^2\psi_5 = \psi_7$ y $\psi_6^3\psi_5 = \psi_2$ de donde los elementos de la Tabla 2.3 son todos los automorfismos de K_8 y, como se cumplen las hipótesis del Lema 2.10 para $n = 4$, el grupo es isomorfo a D_4. $\square$

Nota: Incluimos en las tablas una columna con las clases de conjungación y otra en la que vemos los automorfismos como una permutación para identificar rápidamente sus elementos fijos. Esta información la usaremos más adelante. En la tabla 2.2, a cada $a^i b^j$ le asignamos la etiqueta $i+3j$; en 2.1, a cada x^i, le asignamos la etiqueta i; y por último, en 2.3, a cada $x^i y^j$ le asignamos la etiqueta $i+4j$. Además resaltaremos en rojo las combinaciones necesarias para el trabajo posterior.

$Aut(C_8) \cong K_4$	$\varphi(x)$	$\lvert\varphi\rvert$	$\varphi \in S_8$	$Cl(\varphi_i)$
$\varphi_1 = id$	x	1	(0)(1)(2)(3)(4)(5)(6)(7)	$\{\varphi_1\}$
φ_2	x^3	2	(0)(1 3)(2 6)(4)(5 7)	$\{\varphi_2\}$
φ_3	x^5	2	(0)(1 5)(2)(3 7)(4)(6)	$\{\varphi_3\}$
φ_4	x^7	2	(0)(1 7)(2 6)(3 5)(4)	$\{\varphi_4\}$

Cuadro 2.1: Grupo de automorfismos de C_8

$Aut(D_3) \cong D_3$	$\varphi(a)$	$\varphi(b)$	$\lvert\varphi\rvert$	$\varphi \in S_6$	$Cl(\varphi_i)$
$\varphi_1 = id$	a	b	1	(0)	$\{\varphi_1\}$
φ_2	a^2	b	2	(0)(12)(3)(45)	$\{\varphi_2, \varphi_4, \varphi_6\}$
φ_3	a	ab	3	(0)(1)(2)(345)	$\{\varphi_3, \varphi_5\}$
φ_4	a^2	ab	2	(0)(12)(34)(5)	$\{\varphi_2, \varphi_4, \varphi_6\}$
φ_5	a	a^2b	3	(0)(1)(2)(354)	$\{\varphi_3, \varphi_5\}$
φ_6	a^2	a^2b	2	(0)(12)(35)(4)	$\{\varphi_2, \varphi_4, \varphi_6\}$

Cuadro 2.2: Grupo de automorfismos de D_3

$Aut(K_8) \cong D_4$	$\psi(x)$	$\psi(y)$	$\lvert\psi\rvert$	$\psi \in S_8$	$Cl(\psi_i)$
$\psi_1 = id$	x	y	1	(0)(1)(2)(3)(4)(5)(6)(7)	$\{\psi_1\}$
ψ_2	x	x^2y	2	(0)(1)(2)(3)(46)(57)	$\{\psi_2, \psi_4\}$
ψ_3	x^3	y	2	(0)(13)(2)(4)(57)(6)	$\{\psi_3\}$
ψ_4	x^3	x^2y	2	(0)(13)(2)(46)(5)(7)	$\{\psi_2, \psi_4\}$
ψ_5	xy	y	2	(0)(15)(2)(37)(4)(6)	$\{\psi_5, \psi_7\}$
ψ_6	xy	x^2y	4	(0)(1537)(2)(46)	$\{\psi_6, \psi_8\}$
ψ_7	x^3y	y	2	(0)(17)(2)(35)(4)(6)	$\{\psi_5, \psi_7\}$
ψ_8	x^3y	x^2y	4	(0)(1745)(2)(46)	$\{\psi_6, \psi_8\}$

Cuadro 2.3: Grupo de automorfismos de K_8

Capítulo 3

Grupos de orden menor o igual que 16

El Capítulo 2 proporciona las herramientas suficeintes para describir los grupos hasta orden 16. En la Sección 3.1 de este capítulo final, se clasifican los de orden ≤ 15. El procedimiento de clasificación general es la descomposición en productos semidirectos. El caso más laborioso, los grupos de orden 12, aparece al final de la sección y para ello seguiremos indicaciones del artículo de 2016 *Classifying groups of small order* [8] de Gerard Thompson. Cerraremos el capítulo con la clasificación de los grupos de orden 16 en La sección 3.2. La técnica se basa en el uso de la noción de extensión cíclica, tal y como establece Marcel M. Wolfgang Wild en *The Groups of Order Sixteen Made Easy* [10].

3.1. Orden menor o igual que 15

En esta sección probaremos que los grupos de orden menor o igual que 15 son los descritos en el Teorema 3.1. La clasificación sigue el esquema de la factorización del orden del grupo en producto de primos que permite localizar patrones en su estructura.

Teorema 3.1. *Salvo isomorfismos, los grupos de orden menor o igual que* 15*, están en uno de los siguientes listados:*

a) Cíclicos, C_n *con* $1 \leq n \leq 15$.

b) Producto directo de cíclicos, $C_2 \times C_2 \times C_2$, $C_2 \times C_2$, $C_2 \times C_6$ *y* $C_3 \times C_3$.

c) Diédricos, D_n *con* $3 \leq n \leq 7$.

d) Cuaternio Q_8*, alternado* A_4 *y dicíclico* Q_{12}.

Los grupos de los apartados c) y d) son todos no abelianos.

Para la prueba del resultado, iremos agrupando en varias categorías dependiendo de la factorización del orden en primos.

• **Orden primo:** Loas posibilidades en este caso son $|G| = 2, 3, 5, 7, 11, 13$. Debido al Lema 2.1, la única opción para estos grupos de orden primo es que sean cíclicos.

• **Orden 4:** Si el grupo tiene un elemento de orden 4, es isomorfo a C_4. En otro caso, por el Teorema de Cauchy, todos los elementos del grupo G, distintos del neutro, son de orden dos. La única posibilidad es $C_2 \times C_2$ de acuerdo con el Lema 2.5.

• **Orden $2p$, p primo impar:** Los posibles órdenes son $6, 10, 14$ y, usando el Lema 2.11, llegamos a que ó bien G es cíclico o uno de los diédricos D_3, D_5, D_7.

• **Orden 9:** Aplicando el Lema 2.7 tenemos que $Z(G) \neq \{e\}$ y, por el Teorema de Lagrange, $|Z(G)| = 3$ ó $Z(G) = G$. Si suponemos $|Z(G)| = 3$, G no es abeliano, pero $G/Z(G)$ es de orden 3 luego cíclico y el Lema 2.3 nos dice que G es abeliano, contradicción. Por tanto G es abeliano y, si tiene un elemento de orden 9, es isomorfo a C_9. En otro caso, todos los elementos distintos de e son de orden 3. Tomamos uno de ellos x, el subgrupo cíclico $H = \langle x \rangle$ y un elemento y de G que no esté en H. Entonces $H \cap \langle x \rangle = e$ y, como ambos subgrupos son normales, $\langle H, y \rangle = H\langle y \rangle$ es un subgrupo de orden 9 de G. Así G es producto directo interno de dos subgrupos de orden 3, luego isomorfo a $C_3 \times C_3$.

• **Orden 15:** Probaremos que todos los grupos de este orden son abelianos por reducción al absurdo. Supongamos que G es no abeliano y, por tanto que no hay elementos de orden 15. Ahora bien, sea n_3 el número de elementos de orden 3 en G. Por el Lema 2.9, n_3 es múltiplo de 5; mientras que por el Lema 2.6 n_3 es múltiplo de 2. Luego n_3 es múltiplo de 10. Por el mismo razonamiento, si n_5 es el número de elementos de orden 5 llegamos a que n_5 es múltiplo de 3 y de 4, luego es múltiplo de 12. Todo esto implica que existen números enteros positivos a, b tales que $n_3 = 10a$ y $n_5 = 12b$. Luego,

$$|G| = n_1 + n_3 + n_5 + n_{15} = 1 + 10a + 12b = 15$$

Ahora bien, es evidente que no existen tales enteros positivos, luego llegamos a una contradicción, luego G es abeliano. Por el Teorema de Cauchy 2.5, existen elementos $x, y \in G$ de orden 3 y 5 y $\langle x \rangle \cap \langle y \rangle = \{e\}$ por Lagrange. Como G es abeliano, $(xy)^{15} = x^{15}y^{15} = e$ y $(xy)^3 = x^3y^3 \neq e \neq (xy)^5$. El orden de xy, divisor de 15, no es 3 ni 5, luego es 15 y $G = \langle xy \rangle \cong C_{15}$.

• **Orden 8:** Empecemos suponiendo que G es abeliano. Si G tiene un elemento de orden 8, entonces $G \cong C_8$, mientras que si suponemos que todo elemento de G distinto de e es de orden 2, por el Lema 2.5, tendremos que $G \cong (C_2)^3$. En cualquier otro caso tendremos que los elementos de G distintos de e serán orden 4 y de orden 2. Tomemos ahora un $x \in G$ elemento de orden 4. Podemos tomar un elemento de orden 2 $y \in G$ de tal forma que $y \neq x^2$. En efecto, si suponemos que el único elemento de orden 2 es x^2, tomemos un $y \in G \setminus \langle x \rangle$, entonces tenemos que $x^3y \in G \setminus \langle x \rangle$ es de orden 4 y sin embargo, $(x^3y)^2 = x^6y^2 = x^2y^2 = x^2x^2 = x^4 = e$. Con lo cual existe un $y \in G$ de tal forma que $y \neq x^2$ y que y sea de orden 2. Con lo que nos encontramos en las condiciones de un producto directo y por tanto $G = \langle x \rangle \times \langle y \rangle \cong C_4 \times C_2$. De ahora en adelante, supongamos que G es no abeliano. Notemos que $D_4 = \langle \sigma, \tau \,|\, \sigma^4 = \tau^2 = e,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$ es claramente un grupo no abeliano de orden 8, veamos ahora si existe algún otro grupo

no abeliano de orden 8. Sea $G \ncong D_4$, por el Lema 2.5, existe $x \in G$ tal que $|x| = 4$. Supongamos que existe $y \in G$ tal que $y^2 = e$ y que $y \notin < x >$, entonces, en virtud del Lema 2.10, $G \cong D_4$. Absurdo. Luego todos los elementos que no están en $< x >$ son de orden 4. Elegimos $y \notin < x >$, luego $|y^2| = 2$ y como el único elemento de orden 2 en G es $x^2 \in \langle x \rangle$, tenemos que $y^2 = x^2$. Además, $z := x^2 \in Z(G)$ pues por el Lema 2.2, $|yzy^{-1}| = |z| = 2$ luego $Cl(z) = \{z\}$ y la Ecuación de Clases nos asegura que z es central.Notemos también que $< x >$ es de índice 2, luego subgrupo normal y dado $y \notin < x >$ tenemos que $G = \langle x \rangle \sqcup \langle x \rangle y = \left\{e, x, x^2, x^3, y, xy, x^2y, x^3y\right\}$ y además,

$$yxy^{-1} = \begin{cases} x \\ x^{-1} \end{cases}, \text{ pero como } G \text{ es no abeliano, } yxy^{-1} = x^{-1}$$

Si llamamos 1 a e, -1 a x^2, i a x, $-i$ a x^3, j a y, $-j$ a y^3, k a xy y $-k$ a x^3y, tenemos que

$$G = \{\pm 1, \pm i, \pm j, \pm k\}$$

Con $|i| = |j| = |k| = 4$, $l^{-1} = -l$, $\forall l \in \{i, j, k\}$ y $i^2 = j^2 = k^2 = -1$, luego $G \cong Q_8$.

• **Orden 12:**. Supongamos que G es abeliano. Si G tiene un elemento de orden 12 tenemos que $G \cong C_{12}$. Supongamos ahora que G no tiene elementos de orden 12. Por el Teorema de Cauchy, tenemos que existe $x \in G$ de orden 3. Como $\langle x \rangle \trianglelefteq G$, consideremos el cociente $G/\langle x \rangle$; tenemos que $|G/\langle x \rangle| = 4$, con lo que tenemos dos opciones, o bien $G/\langle x \rangle \cong C_4$ o bien $G/\langle x \rangle \cong K_4$. En el primer caso, existe $y \in G \setminus \langle x \rangle$ tal que $G/\langle x \rangle = \left\{y^i \langle x \rangle \,|\, i = 0, 1, 2, 3\right\}$. Como $|y| \neq 12$, necesariamente $|y| = 4$. Pero el Teorema de Lagrange garantiza que $\langle y \rangle \cap \langle x \rangle = \{e\}$ lo que nos lleva a que $o(xy) = 12$: $(xy)^{12} = e$ y $(xy)^4 \neq e \neq (xy)^3$, imposible pues hemos supuesto que en G no hay elementos de orden 12. Por tanto, $G/\langle x \rangle \cong K_4$, luego existen $y, z \in G \setminus \langle x \rangle$ tales que $G/\langle x \rangle = \{e\langle x \rangle, y\langle x \rangle, z\langle x \rangle, yz\langle x \rangle\}$. Como $y, z \notin \langle x \rangle$, $y^2, z^2 \in \langle x \rangle$ y G no tiene elementos de orden 12, tenemos que y y z son o bien de orden 6, o bien de orden 2. Podemos suponer sin pérdida de generalidad que ambos son de orden 2, pues si fueran de orden 6, y^3 y z^3 serían de orden 2 y serían distintos entre sí, pues si fuesen iguales tendríamos que $y\langle x \rangle = y^3\langle x \rangle = z^3\langle x \rangle = z\langle x \rangle$, lo cual es imposible. Notemos entonces que $|xy| = 6$, $z \notin \langle xy \rangle$, $\langle xy \rangle \trianglelefteq G$ y $\langle z \rangle \trianglelefteq G$, luego nos encontramos en las condiciones de un producto directo interno y por tanto $G \cong C_6 \times C_2$.

Supongamos en lo que sigue que G es no abeliano. Entonces tenemos que $|Z(G)| \neq 12$. Además si $|Z(G)| = 6, 4$ implica $|G/Z(G)| = 2, 3$ respectivamente, luego $G/Z(G)$ cíclico, y por el Lema 2.3 concluiríamos que G es abeliano, así que podemos descartar ambos casos. Si suponemos que $|Z(G)| = 3$, entonces por la Ecuación de Clases tenemos que tiene que existir al menos una órbita de 3 elementos para que la paridad se mantenga, $|G| = 1 + 1 + 1 + 3 + \cdots$. Ahora bien, sea x un elemento en dicha órbita, entonces $|stab_G(x)| = 4$. Pero como $Z(G) \leqslant stab_G(x)$, llegaríamos a la conclusión de que $3|4$, lo cual es claramente falso. Así que o bien $|Z(G)| = 1$ o bien $|Z(G)| = 2$. Supongamos que $Z(G) = \{e, z\}$, con $z^2 = e$. Como hemos supuesto que G no es abeliano, la única opción es que $G/Z(G) = D_3$. Por el Teorema de Cauchy existe un elemento de orden 3 que propociona $\overline{N}$ subgrupo cíclico y normal (tiene índice 2) de $G/Z(G)$. Usando el Teorema

de Correspondencia, tenemos que $\overline{N}$ genera un subgrupo que contiene a $Z(G)$ y es de orden 6. Luego su índice 2 y, por tanto, $N \trianglelefteq G$. Como $Z(N) \neq \{e\}$, ya que al menos $z \in Z(N)$, por el Lema 2.8 tenemos que N es abeliano, luego es cíclico. Describimos $N = \langle x \rangle$ y, como $[G : N] = 2$, existe $y \in G$ tal que $y \notin N$ y $G = N \cup yN$ (dos clases). Además $y^2 \in N$ ya que el crupo cociente G/N tiene orden 2. Por otro lado, como $Z(G) \leqslant N$ y x^3 es el único elemento de N de orden 2 tenemos que $Z(G) = \left\{e, x^3\right\}$. Esto es relevante porque junto al hecho de que y^2 esté tanto en $\langle x \rangle$ como en $\langle y \rangle$, por tanto y^2 conmuta con x e y. Pero como $G = \langle x, y \rangle = \langle x \rangle \langle y \rangle$, pues N es normal, y^2 conmuta con todo elemento de G, es decir, que y^2 está en $Z(G)$, lo cual nos limita las opciones de y^2 a dos, o bien $y^2 = e$ o bien $y^2 = x^3$. Si $y^2 = e$, nos encontramos en las condiciones del Lema 2.10 y entonces $G \cong D_6$. Si por el contrario suponemos que $y^2 = x^3$, nos falta ver cómo conmutan x e y. Tenemos que $G = \langle x \rangle \langle y \rangle = \left\{e, x, x^2, x^3, x^4, x^5, y, xy, x^2y, x^3y, x^4y, x^5y\right\}$. Como $y \notin \langle x \rangle$, tenemos que $yx \notin \langle x \rangle$ y, evidentemente, $y \neq yx$. Como hemos supuesto que G es no abeliano, tenemos que $yx \neq xy$. Por otro lado, si suponemos que $yx = x^3y$, como $x^3 \in Z(G)$, de $yx = yx^3$ llegamos a $x = x^3$ lo cual es imposible dado que $|x| = 6$. En el caso de $yx = x^2y$, notemos que $(yx)^2 = yx(yx) = x^2y(yx) = x^2y^2x = x^6 = e$ y como $yx \neq x^3$, nos encontramos en las condiciones del Lema 2.10 y entonces $G \cong D_6$. Para descartar el caso $yx = x^4y$, nos fijamos otra vez en $(yx)^2 = x^4y^2x = x^8 = x^2$, luego $\left|(yx)^2\right| = 3$ y $(yx)^6 = e$, es decir que $\left((yx)^3\right)^2 = e$ y por tanto $\left|(yx)^3\right| = 2$. Además tenemos que $(yx)^3 = (yx)x^2 = yx^3 \neq e$. Observamos que $(yx)^3 \neq x^3$, luego también nos encontramos en las condiciones del Lema 2.10. Así que si queremos evitar que $G \cong D_6$, necesitamos que $y^2 = x^3$ y $yx = x^5y$, lo cual nos lleva a que $G = \langle x, y | x^6 = y^4 = e,\ y^2 = x^3,\ yxy^{-1} = x^{-1} \rangle$; que es la presentación habitual del grupo dicíclico de orden 12, luego $G \cong Q_{12}$

Supongamos ahora que $|Z(G)| = 1$, una vez más, para respetar la paridad en la ecuación de clases, G tiene que tener clases de conjugación de orden 3, dando así los siguientes casos:

- **Caso 1:** $12 = 1 + 3 + 2 + 2 + 2 + 2$
- **Caso 2:** $12 = 1 + 3 + 2 + 2 + 4$
- **Caso 3:** $12 = 1 + 3 + 3 + 3 + 2$
- **Caso 4:** $12 = 1 + 3 + 4 + 4$

En los 3 primeros casos tomamos un $x \in G$ cuya clase de conjugación sea de orden 2. Entonces $|C_G(x)| = 6$, $C_G(x)$ tiene índice 2 y por tanto $C_G(x) \trianglelefteq G$. Si $C_G(x)$ fuera abeliano, entonces podemos suponer que $|x| = 6$ y $C_G(x) = \langle x \rangle$; luego podemos escribir $G = \langle x \rangle \cup \langle x \rangle y$ con $y \notin \langle x \rangle$ y $y^2 \in \langle x \rangle$. Como hemos visto antes $y^2 \in Z(G)$, luego $x^6 = y^2 = e$ e $y \neq x^3$, así que por el Lema 2.10, $G \cong D_6$. Lo cual no tiene sentido ya que, como hemos visto antes, $|Z(D_6)| = 2$. Por otro lado, si $C_G(x)$ no fuera abeliano, entonces $C_G(x) \cong D_3$. De la misma forma, gracias a la normalidad y a que el índice de $C_G(x)$ en G es 2, tenemos que $G = D_3 \cup D_3y$, con $y \notin D_3$ e $y^2 \in D_3$. Estudiemos ahora qué pasa según el orden de y^2.

- **Caso 1:** $\left|y^2\right| = 3$. Entonces, $|y| = 3$ ó 6. Si el orden de y es 6, tenemos un subgrupo cíclico de orden 6 normal y por tanto volvemos al caso anterior. Por el contrario, si el orden de y es 3 notemos entonces que $\langle y \rangle = \left\langle y^2 \right\rangle \leqslant C_G(x)$, lo cual implica que y está en $C_G(x)$ llegando así a una contradicción.

- **Caso 2:** $\left|y^2\right| = 2$. Para esto, notemos que dado que $C_G(x) \cong D_3$, $|x| = 3$ ó 2. Si $|x| =$

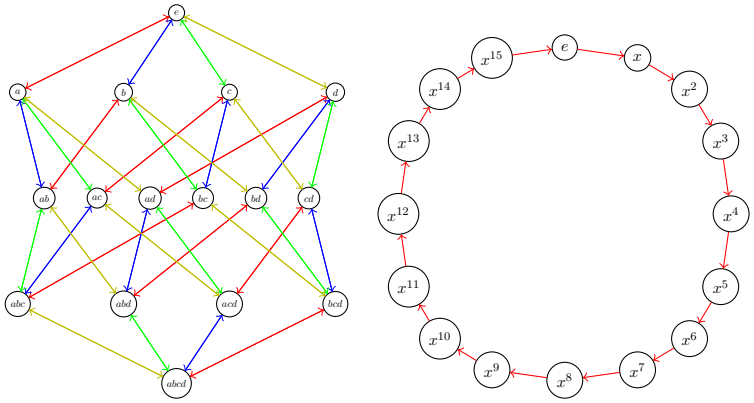
3 nos encontramos en las hipótesis de un producto semidirecto entre $\langle x \rangle$ y $\langle y^2 \rangle$. Como además $xy^2 = y^2x$, concretamente es un producto directo, luego $\langle x, y^2 \rangle = C_6 \trianglelefteq G$ y al igual que antes, llegamos a una contradicción. Por el contrario, si suponemos que $|x| = 2$ y en $D_3 \cong C_G(x)$ los tres elementos de orden dos son conjugados llegaríamos a que $Cl(x)$ tendría tres elementos, lo cual es imposible ya que estamos suponiendo que x es un elemento cuya clase de conjugación tiene dos elementos.

- **Caso 3:** $y^2 = e$. En este caso nos encontramos en las hipótesis de un producto semidirecto y $G \cong D_3 \rtimes_\varphi C_2$. Con o bien $\varphi = id$, en cuyo caso será un producto directo, o bien $\varphi \in Aut(D_3)$ de orden 2. Supongamos ahora que $D_3 = \langle a, b | a^3 = b^2 = e,\ bab^{-1} = a^2 \rangle$ y $C_2 = \langle y \rangle$, entonces tenemos los automorfismos establecidos por la tabla 2.2. Ahora bien, en el caso de $G = D_3 \times C_2$, notemos que $|(a, y)| = 6$. Además $|(b, e)| = 2$ y $(a, y)^3 = (e, y) \neq (b, e)$. Luego nos encontramos en las hipótesis del Lema 2.10 y $G \cong D_6$, lo cual es una contradicción ya que, como se ha visto antes, $|Z(D_6)| = 2$. En los otros tres casos restantes se sigue un razonamiento completamente análogo, por lo que simplemente vamos a indicar los elementos escogidos para aplicar el Lema 2.10 en cada caso. Si $G = D_3 \rtimes_{\varphi_2} C_2$, entonces tomamos como elemento de orden 6 a aby y como elemento de orden 2 a b. Si $G = D_3 \rtimes_{\varphi_4} C_2$, entonces tomamos como elemento de orden 6 a by y como elemento de orden 2 a b. Por último, si $G = D_3 \rtimes_{\varphi_6} C_2$, entonces tomamos como elemento de orden 6 a by y como elemento de orden 2 a b. Por tanto, este caso tampoco se da

Consideramos entonces el caso $12 = 1 + 3 + 4 + 4$. Notemos que para cualquier x en una clase de conjugación de cardinal 4, como $x \in C_G(x)$, por el Teorema de Lagrange, $|\langle x \rangle| \,|C_G(x)| = 3$, luego $|x| = 3$. Por otro lado, los elementos de la clase de cardinal 3 pueden tener orden 2 o 4 (todos con el mismo orden por ser conjugados), ya que su estabilizador tendrá orden 4. Si todos son de orden 4 e y es uno de ellos, como $C_G(y)$ es un grupo, $y^2 \in C_G(y)$, pero y^2 tiene orden 2 y no hay clases de conjugación de elementos de orden 2. Con lo que llegamos a la conclusión de que los elementos de la clase de cardinal 3 son todos de orden 2 y que no hay elementos de orden 6. Sean $x, y \in G$ elementos de orden 2 y 3, respectivamente. Entonces yxy^2 e y^2xy son elementos de orden 2 al ser conjugados de x. Estudiemos ahora dos posibilidades, que alguno de estos elementos sean iguales o que sean distintos. Es fácil comprobar que si hay dos iguales, entonces $xy = yx$ y por tanto el subgrupo $\langle x, y \rangle = \langle xy \rangle$ tiene orden 6, lo cual es imposible pues no hay elementos de orden 6 en G. Con lo que llegamos a la conclusión de que los 3 son distintos y $Cl(x) = \{x, yxy^2, y^2xy\}$. Como hemos encontrado los 3 elementos de orden 2 de G, el resto de elementos distintos de e son de orden 3 y vienen dados en dos clases de conjugación de 4 elementos cada una, así que a continuación probaremos que $Cl(y) = \{y, xy, yx, xyx\}$ y que $Cl(y^2) = \{y^2, xy^2, y^2x, xy^2x\}$, pues una vez que lo tengamos, ya tendremos todos los elementos de G. Empecemos notando que el hecho de que xy e yx sean de orden 3 nos lleva a que $(xy)^2 = (xy)^{-1} = y^2x$ y a que $(yx)^2 = (yx)^{-1} = xy^2$. También tenemos que xyx y xy^2x son elementos de orden 3, por ser conjugados de y y de y^2, respectivamente. Además, es inmediato comprobar que yx y xy son conjugados, pues $yx = x(yx)x$. Por otro lado, que $yxyx = xy^2$ nos lleva a que $y(xyx)y^2 = xy^2y^2 = xy$, luego tenemos que

$g \in G$	$\phi(g) \in A_4$	$g \in G$	$\phi(g) \in A_4$	$g \in G$	$\phi(g) \in A_4$
e	1	y	(123)	y^2	(132)
x	(12)(34)	xy	(243)	xy^2	(143)
yxy^2	(14)(23)	yx	(134)	y^2x	(234)
y^2xy	(13)(24)	xyx	(142)	xy^2x	(124)

Cuadro 3.1: Isomorfismo entre G y A_4



(a) $G_0 \cong (C_2)^4$ (b) $G_6 = C_8 \rtimes^x_{id} C_2 \cong C_{16}$

Figura 3.1: Cada color representa el producto por un generador.

xyx y xy son conjugados; obteniendo así que los elementos del conjunto $\{y, xy, yx, xyx\}$ son conjugados entre sí. De la misma forma, y^2 y xy^2x son conjugados entre sí, al igual que y^2x y xy^2. Por otro lado, que $yxyx = xy^2$ nos lleva a que $xy^2x = yxy$ y usando esto podemos ver que $y(xy^2x)y^2 = y^2xy^3 = y^2x$; luego los elementos de $\{y^2, xy^2, y^2x, xy^2x\}$ son conjugados entre sí. Ahora es directo comprobar que los cuatro elementos de cada conjunto son diferentes entre sí y, como y es distinto de todos los elementos de $\{y^2, xy^2, y^2x, xy^2x\}$, ambos conjuntos son disjuntos. Así que ya tenemos todos los elementos de G que vienen dados en las clases de conjugación $\{e\}$, $Cl(x) = \{x, yxy^2, y^2xy\}$, $Cl(y) = \{y, xy, yx, xyx\}$ y $Cl(y^2) = \{y^2, xy^2, y^2x, xy^2x\}$. Además, si consideramos el homomorfismo $\phi : G \to A_4$ que lleva los generadores de G a generadores de A_4 mediante $\phi(x) = (12)(34)$ y $\phi(y) = (123)$, es inmediato ver que es biyectivo (ver tabla 3.1), con lo que $G \cong A_4$.

3.2. Grupos de orden 16

Como hemos visto en la Sección 1.2 del Capítulo 1, clasificar grupos de orden potencia de, a los más dos primos, es en general muy complicado[1] debido a la gran cantidad de

[1]G.A. Miller en 1916 en el artículo *Determination of all groups of order* 2^4, comenta que hay 1074 grupos de orden menor o igual que 100. Tan solo 37 de los 100 órdenes contienen un único grupo (podemos deducir cuáles son muchos de ellos pues hay 25 primos menores que 100). También comenta que los de orden potencia de dos, 2^n con $n = 5, 6$ son especialmente difíciles de clasificar por el número de casos distintos

posibles grupos. El uso de productos semidirectos mediante subgrupos normales es una técnica, como ya hemos visto en la Sección 3.1. Los Teoremas de Sylow pueden ayudar a localizar subgrupos normales, pero se necesitan al menos dos factores primos. Aquí nos encontramos con el Problema de la Extensión (ver Sección 1.2) que, si bien construye, no resuelve salvo isomorfismos. Consideremos S_3 y C_6 por ejemplo. Tenemos que $C_3 \trianglelefteq S_3$ y $C_3 \trianglelefteq C_6$ por ser subgrupos de índice 2 y que $S_3/C_3 \cong C_2 \cong C_6/C_3$ y sin embargo S_3 y C_6 son claramente no isomorfos ya que uno es abeliano y el otro no. Aunque en algunos casos especiales llegamos a la unicidad, por ejemplo, los grupos en los que todos sus elementos distintos de e de orden 2, son abelianos que, salvo isomorfismos, son productos directos del cíclico C_2. Así se establece en Lema 2.5 que proporciona C_2^4 como grupo de orden 16. Por suerte para nosotros, en el caso de que los cocientes considerados sean cíclicos, Hölder desarrolló unos argumentos de clasificación muy útiles, dando lugar a las extensiones cíclicas [2]. De forma similar a como explicamos los productos semidirectos en el Capítulo 2, empezaremos tratando las extensiones cíclicas de forma interna para después dar una definición general que nos permita obtener grupos nuevos a partir de otros más pequeños. Para ello supongamos N subgrupo normal de G tal que $G/N \cong C_n$, $n \geq 2$ y escojamos $a \in G$ un elemento de tal forma que aN tenga orden n como elemento del grupo cociente. En ese caso, si bien $a \notin N$, $v = a^n$ estará en N ya que $vN = a^nN = N$. Además, como n es el orden de aN, este es el menor natural (se entiende distinto de cero) que cumple que $a^n \in N$. Observamos que n divide a $|a|$ puesto que $(aN)^{|a|} = (a^{|a|})N = eN = N$ (aplicamos Teorema de Lagrange).

Nota: De ahora en adelante dado G grupo y $a \in G$, vamos a denotar t_a al *automorfismo interno* de G determinado por el elemento a, esto es, $t_a(x) = axa^{-1}$ para todo $x \in G$.

Sea $\tau = t_a|_N \in Aut(N)$ la restricción de t_a a N, posible ya que N debe ser normal en G. El automorfismo τ cumple tres propiedades que nos interesan:

$$\tau(v) = aa^na^{-1} = v \tag{3.1}$$

$$\tau^n(x) = a^nxa^{-n} = vxv^{-1} = t_v(x), \quad \text{para todo } x \in N, \tag{3.2}$$

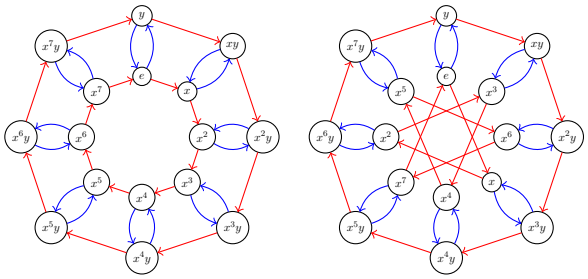
La segunda propiedad nos dice que $\tau^n = t_v$ es un automorfismo interno del subgrupo N. Así, si N es abeliano tenemos que:

$$\tau^n = id_N. \tag{3.3}$$

---

que aparecen (de 2^5 elementos hay 51 y un total de 267 de orden 2^6). En su tentativa de clasificación de los de orden 64, Miller comete errores (dice haber calculado 294). En 1964 Marshall Hall Jr. y James K. Senior publican la clasificación de los grupos de orden 2^n con $n \leq 6$, un total de 340. Senior dice en la introducción que inicia el trabajo de clasificación en 1935 con el profesor Philip Hall. La Segunda Guerra Mundial lo paraliza y, al término de la misma, Philip Hall desiste y se incorpora Marshall Hall Jr., con quien Senior termina la monografía.

[2] Hay otras técnicas de clasificación de grupos de orden 8 y 16 usando el centro del grupo. Las posibilidades de grupos se derivan de la estructura de su centro y de su grupo factor por el centro. Como ejmplo, se puede consultar [4], inspirado en el curso de David Clausen, Universidad de Puget Sound (USA), sobre la clasificación de grupos de orden 16 (Math 434, primavera 2012).



(a) $G_1 = C_8 \rtimes^{e}_{id} C_2 \cong C_8 \times C_2$ (b) $G_2 \cong C_8 \rtimes_{\varphi_2} C_2$

Figura 3.2: En rojo el producto por x y en azul el producto por y.

Los hechos comentados, motivan las siguientes definiciones.

Definición 3.1. Un grupo G se dice *extensión n-cíclica interna* del subgrupo N si N es un subgrupo normal de G distinto de G y el grupo cociente G/N es cíclico de orden n.

Toda extensión cíclica interna de G tiene asociada cuatro objetos distinguidos: un subgrupo normal, N, un número $n = [G : N] = |G/N| \geq 2$, un automorfismo $\tau \colon N \to N$ y un elemento $v \in N$ de modo que $\tau(v) = v$ y τ^n es el automorfismo interno de N dado por el elemento v. Por otro lado, como G/N es n-cíclico, $G = \langle a, N\rangle$ con $a \notin N$ y $a^n = v \in N$ y $a^i \notin N$ si $1 \leq i < n$. De este modo, para todo $g \in G$ existe algún $0 \leq i \leq n-1$ tal que $gN = a^i N$, es decir, $\left(a^i\right)^{-1} g = x \in N$. Esto nos indica que los elementos de G se puede escribir en la forma $g = xa^i$ con $x \in N$ y $0 \leq i \leq n-1$. Esta descomposición es, además, única ya que si $xa^i = ya^j$ con $j \geq i$, $y^{-1}x = a^{j-i} \in N$ y, como $0 \leq j - i < n$, la única posibilidad es que $j = i$ y entonces $x = y$. La unicidad de la descomposición nos permite recuperar el producto en G, gracias a la asociatividad subyacente, usando los cuatro objetos distinguidos determinados por su extensión cíclica. Dados $g, h \in G$, escribimos $g = xa^i, h = ya^j \in G$ con $x, y \in N$ y el producto gh los podemos expresar como sigue:

$$(xa^i)(ya^j) = x(a^i y a^{-i})a^i a^j = \underbrace{(x\tau^i(y))}_{u \in N} a^{i+j} = \begin{cases} (x\tau^i(y))a^{i+j} & \text{si } i+j < n. \\ (x\tau^i(y)v)a^{i+j-n} & \text{si } i+j \geq n. \end{cases} \tag{3.4}$$

Notar que es importante la forma en que la expresión $u = x\tau^i(y) \in N$ es definida en salida (3.4) y el ajuste de los superíndices de a: primero multiplicamos en N y luego ajustamos potencia (relación de intercambio). Además, como $G = \langle a, N\rangle = \langle a\rangle\, N$,

$$|G| = \frac{|\langle a\rangle\,||N|}{|\langle a\rangle \cap N|} = \frac{|a||N|}{|\langle a\rangle \cap N|} \quad \text{y} \quad \langle a\rangle \cap N = \langle a^n\rangle\,, \tag{3.5}$$

y, si $v = a^n$, entonces $|v| = \dfrac{|a|}{(n, |a|)} = \dfrac{|a|}{n}$. Así, las extensiones cíclicas internas tales que $|a| = n$ cumplen que $v = e$ y son productos semidirectos.

Ejemplo 3.1. *El grupo Q_8 no es producto semidirecto de subgrupos propios pues, si bien todos sus subgrupos son normales, los propios contienen a $Z(Q_8)$. Pero Q_8 es extensión 2-cíclica de cualquiera de sus subgrupos de orden 4. Podemos tomar $N = \langle i\rangle \cong C_4$ y $a = \pm j, \pm k$; elegimos $a = j$. El orden de a es 4 y $n = 2$ pues $a \notin N$ y $a^2 = -1 \in N$, luego $\langle a\rangle \cap N = \langle a^n\rangle = Z(Q_8)$. Así podemos describir Q_8 con los elementos $1, i, i^2 = -1 = v, i^3 = -i, j, ij, -j, -ij$ y la expresión (3.4) proporciona la relación de intercambio:*

$$ji = (ej)(ie) = et_j(i)j = \underbrace{(jij^{-1})}_{-i\in N} j = -ij = i^3 j.$$

Las consideraciones previas nos llevan al siguiente resultado, al que nos referiremos como Teorema de extensión cíclica[3] y a la noción de extensión cíclica externa, intrínsecamente relacionada con la cíclica interna. Esta construcción es la que nos va a permitir alcanzar la clasificación de los grupos de orden 16 de una forma unificada .

Teorema 3.2 (Teorema de extensión cíclica, Hölder, 1895)**.** *Sea N un grupo finito, n un natural ≥ 2, $v \in N$ y $\tau \in Aut(N)$ tales que $\tau(v) = v$ y $\tau^n(v) = t_v$. El producto cartesiano $N \times \langle a\rangle$ donde $\langle a\rangle = \{a^0 = e, a, \dots a^{n-1}\}$ y $a^n = e$, e denota también el neutro de N, es un grupo con la operación:*

$$(x, a^i) * (y, a^j) = \begin{cases} (x\tau^i(y), a^{i+j}) & si\ i + j < n \\ (x\tau^i(y)v, a^{i+j-n}) & si\ i + j \geq n. \end{cases} \tag{3.6}$$

Definición 3.2. Sea N un grupo que tenga un elemento v y un automorfismo τ, tales que $\tau(v) = v$ y $\tau^n = t_v$ para algún $n \geq 2$. El producto cartesiano $N \times \langle a\rangle$ con el producto definido en (3.6) se dice grupo extensión n-cíclica externa de N y lo denotaremos por $N \rtimes_\tau^v C_n$. Además, llamaremos *tipo de extensión* a la 4-tupla (N, n, τ, v).

Ejemplo 3.2. *Las 4-tuplas (N, n, φ, e) producen productos semidirectos $N \rtimes_\varphi C_n$ y, si $\varphi = id$, los directos $N \times C_n$. En efecto, si $G = N \rtimes_\varphi^e C_n$, usando el Lema 3.1, $N \cong N' = \{(x, e)|x \in N\} \trianglelefteq G$. La conjugación $t_{(y,a^i)}$, actúa en N' con la fórmula $(y, a^i) * (x, e) * (\varphi^{-1}(y^{-1}), a^{n-i}) = (y\varphi^i(x)y^{-1}, e)$. Además, $H' = \{(e, a^i)|\, i = 0, 1, \dots, n-1\} \cong C_n$ y $N' \cap H' = \{(e, e)\}$. Dado un elemento $(x, e) \in N'$, $t_{(e,a)}$ nos da $(e, a) * (x, e) * (e, a^{n-1}) = (\varphi(x), e)$. De este modo, tenemos $\phi\colon H' \to Aut(N')$ está determinada por $\phi_{(e,a)} = t_{(e,a)} = (\varphi, e)$ y $\phi_{(e,a)}^n = (\varphi^n, e) = t_{(e,e)} = (id, e)$. Con lo que $G \cong N \rtimes_\varphi C_n$.*

Nota: El Teorema 3.2 nos asegura las 4-tuplas (N, n, τ, v) introducidas en la Definición 3.2 producen grupos. Además, si G es extensión n-cíclica interna del subgrupo N, usando (3.4) y (3.6) G es isomorfo al grupo extensión cíclica externa $N \rtimes_{t_a|_N}^{a^n} C_n$. La aplicación $G \to N \rtimes_{t_a|_N}^{a^n} C_n$ dada por $xa^i \mapsto (x, a^i)$ es isomorfismo de grupos.

---

[3]Establecer la asociatividad del producto no es trivial, y menos para un principiante. Lo hizo Otto Hölder en 1895 en su artículo "Bildung zusammengesetzter Gruppen", que presenta en sociedad este Teorema marcando el inicio de la Teoría de Extensiones en grupos (finitos).

Ejemplo 3.3. *De acuerdo con el Lema 2.13 y su demostración, si x genera C_4, sus automorfismos $Aut(C_4)$ son Id y $\tau(x) = x^3$, que fijan e, x^2. El grupo $G = C_4 \rtimes_\tau^{x^2} C_2$ es isomorfo a Q_8. En efecto, si x es un generador de C_4, y $X^i = (x^i, e), Y = (e, a)$, tenemos $G = \langle X, Y \,|\, X^4 = Y^4 = (e,e),\ X^2 = Y^2 = (x,e)^2, Y * X * (x^2, a) = X^3 = X^{-1} \rangle \cong Q_8$.* [4]

En el siguiente lema, daremos visibilidad al neutro y los inversos de las extensiones cíclicas y probaremos la asociatividad en el caso de que N sea abeliano y $n = 2$, que es lo que necesitamos para nuestra clasificación. De este modo, el trabajo realizado será autocontenido. El lema incide además en el hecho de que las extensiones cíclicas externas descomponen también internamente.

Lema 3.1. *Para $n \geq 2$, la operación binaria en $N \rtimes_\tau^v C_n$ definida por la expresión* (3.6) *cumple que:*

a) Tiene elemento neutro: $\mathbf{e} = (e, a^0)$.

b) Cada elemento tiene inverso: $(x, a^i)^{-1} = \big(\tau^{-i}(x^{-1}v^{-1}), a^{n-i}\big)$.

c) $*$ es asociativa (prueba para el caso N abeliano y $n = 2$).

Además, el conjunto $N' = \{(x, e) | x \in N\}$ es un subgrupo normal de $N \rtimes_\tau^v C_n$ y el grupo cociente $N \rtimes_\tau^v C_n / N'$ es isomorfo a C_n.

Demostración. Vamos a comprobar primero que que (e, a^0) es el neutro de $*$. En efecto, dado $(x, a^i) \in G$, $(x, a^i) * (e, a^0) = (x\tau^i(e), a^i) = (x, a^i) = (e\tau^0(x), a^{0+i}) = (e, a^0) * (x, a^i)$. Usamos la definición nuevamente para probar que $(y, a^i)^{-1} = \big(\tau^{-i}(y^{-1}v^{-1}), a^{n-i}\big)$. En efecto, por un lado tenemos que

$$\begin{aligned}(y, a^i) * \big(\tau^{-i}(y^{-1}v^{-1}), a^{n-i}\big) &= \big(y\tau^i \circ \tau^{-i}(y^{-1}v^{-1})v, e\big) \\ &= (yy^{-1}v^{-1}v, e) = (e, e)\end{aligned}$$

y por otro

$$\begin{aligned}(\tau^{-i}(y^{-1}v^{-1}), a^{n-i}) * (y, a^i) &= \big(\tau^{-i}(y^{-1})\tau^{-i}(v^{-1})\tau^{n-i}(y)v, e\big) \\ &= \big(\tau^{-i}(y^{-1})v^{-1}\tau^n \circ \tau^{-i}(y)v, e\big) = \big(\tau^{-i}(y^{-1})v^{-1}v\tau^{-i}(y)v^{-1}v, e\big) \\ &= \big(\tau^{-i}(y^{-1}y), e\big) = (e, e).\end{aligned}$$

Esto prueba las afirmaciones a) y b). Comprobamos ahora las propiedades de N'. Es claro que es un subgrupo de $N \rtimes_\tau^v \langle a \rangle$ y es normal puesto que, si conjugamos (x, e) por (y, a^i) no nos salimos de N'.

$$\begin{aligned}(y, a^i) * (x, e) * \big(\tau^{-i}(y^{-1}v^{-1}), a^{n-i}\big) &= (y\tau^i(x), a^i) * \big(\tau^{-i}(y^{-1}v^{-1}), a^{n-i}\big) \\ &= (y\tau^i(x)y^{-1}v^{-1}v, e) = (y\tau^i(x)y^{-1}, e),\end{aligned}$$

[4] Además de Q_8, el resto de grupos de orden 8 que tienen un elemento de orden 4 también se pueden ver como extensiones cíclicas de C_4, en efecto, K_8 es extensión cíclica de los tipos $(C_4, 2, id, e)$ y $(C_4, 2, id, x^2)$; D_8 del tipo $(C_4, 2, \tau, e)$ y C_8 de los tipos $(C_4, 2, id, x)$ y $(C_4, 2, id, x^3)$. Notemos que los grupos que son extensiones cíclicas con $v = e$ se pueden ver como productos semidirectos de C_4 por C_2 y los que tienen $\tau = id$, son abelianos.

con independencia de la forma en que asociemos. Evidentemente $(y\tau^i(x)y^{-1}, e) \in N'$ pues $y\tau^i(x)y^{-1} \in N$, con lo que N' es normal. Ahora queremos ver qué forma tiene el cociente $(N \times_{\tau,v,n} \langle a \rangle)/N'$. Para ello, notemos que $(x, a^i) \sim (y, a^j)$ si y solo si $(y, a^j)^{-1} * (x, a^i) \in N'$. Si desarrollamos ese producto (suponiendo s.p.d.g. $n > j \geq i \geq 0$, luego $n - j + i \leq n$) obtenemos que $(y, a^j)^{-1} * (x, a^i) = \left(p = \tau^{-j}(y^{-1}x)v^{-1}, q = a^{n-j+i}\right)$ donde $n - j + i < n$ o bien $n - j + i - n = i - j$ si $n - j + i \geq n$, en cuyo caso $i = j$. Ahora (p, q) está en N' si y solamente si $q = e$, que es claro si $i = j$ y, si $n - j + i < n$, como $o(a) = n$, solo es posible si $j = n + i \geq n$, que no se da. Por tanto, $N \rtimes_\tau^v C_n \langle a \rangle \langle (e, a)N' \rangle \cong C_n$, para ello notemos que $((e, a)N')^n = (e, a)^n N' = (v, e)N' = (e, e)N'$. Notemos así que $N \times_{\tau,v,n} \langle a \rangle$ es una extensión n-cíclica interna de N'. En este caso, el automorfismo distinguido será $\tau' \colon N' \to N'; (x, e) \mapsto (\tau(x), e)$ y el elemento distinguido v' será (v, e). Que τ' es un automorfismo de N' se desprende inmediatamente de que τ lo es de N y además se cumple que $\tau'(v') = (\tau(v), e) = (v, e) = v'$ y que, dado $x' = (x, e) \in N'$, $\tau'^n(x') = (\tau^n(x), e) = (vxv^{-1}, e) = (v, e) * (x, e) * (v^{-1}, e) = v'x'v'^{-1} = \tau'_v(x')$.

Finalmente, probamos la asociatividad en el caso de que N sea abeliano y $n = 2$. Sean (x, a^i), (y, a^j), $(z, a^k) \in G$. Ahora aquí vamos a tener que considerar varios casos dependiendo de los valores de i, j y k. Si suponemos $j = 0$ y definimos $\alpha := \lfloor \frac{i+k}{2} \rfloor$ y $\beta := i + k$ (mód 2) tenemos que:

$$\begin{aligned}\left((x, a^i) * (y, a^0)\right) * (z, a^k) &= \left(x\tau^i(y), a^i\right) * (z, a^k) \\ &= (x\tau^i(y)\tau^i(z)v^\alpha, a^\beta) = (x\tau^i(yz)v^\alpha, a^\beta).\end{aligned}$$

Y, de la misma forma,

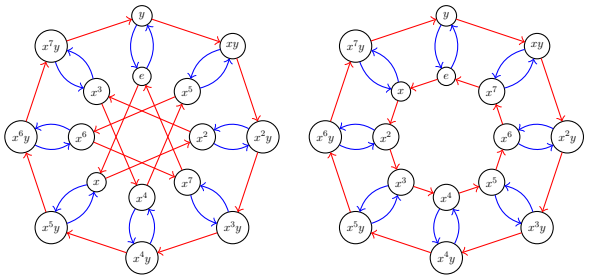
$$\begin{aligned}(x, a^i) * \Big((y, a^0) * (z, a^k)\Big) &= (x, a^i) * (yz, a^k) \\ &= (x\tau^i(yz)v^\alpha, a^\beta).\end{aligned}$$

Luego en este caso la asociatividad se cumple. Supongamos de ahora en adelante que $j = 1$. Ahora, si $i = 1$

$$\begin{aligned}((x, a) * (y, a)) * (z, a^k) &= (x\tau(y)v, a^0) * (z, a^k) \\ &= (x\tau(y)vz, a^k) = (x\tau(y)zv, a^k)\end{aligned}$$

Este último paso podemos hacerlo porque estamos suponiendo que N es conmutativo. Por otro lado, si $k = 1$,

$$\begin{aligned}(x, a) * ((y, a) * (z, a)) &= (x, a) * (y\tau(z)v, a^0) \\ &= \left(x\tau\left(y\tau(z)v\right), a\right) \underset{\tau \in Aut(N)}{=} (x\tau(y)\tau^2(z)\tau(v), a) \\ &\underset{\tau(v)=v}{=} (x\tau(y)\tau^2(z)v, a) \underset{\text{Propiedad (3.3)}}{=} (x\tau(y)zv, a).\end{aligned}$$



(a) $G_3 = C_8 \rtimes^e_{\varphi_3} C_2$ (b) $G_4 = C_8 \rtimes^e_{\varphi_4} C_2 \cong D_8$

Figura 3.3: En rojo el producto por x y en azul el producto por y.

Y si $k = 0$,

$$\begin{aligned}(x,a) * \big((y,a) * (z,a^0)\big) &= (x,a) * (y\tau(z),a)\\ &= (x\tau\left(y\tau(z)\right)v, a^0) \underset{\tau\in Aut(N)}{=} (x\tau(y)\tau^2(z)v, a^0)\\ &\underset{\text{Propiedad (3.3)}}{=} (x\tau(y)zv, a^0).\end{aligned}$$

Luego en este caso, el producto también es asociativo. De ahora en adelante supondremos que $i = 0$ y $j = 1$. Si $k = 0$

$$\begin{aligned}((x,a^0) * (y,a)) * (z,a^0) &= (xy,a) * (z,a^0)\\ &= (xy\tau(z),a) = (x,a^0) * (y\tau(z),a) = (x,a^0) * \big((y,a) * (z,a^0)\big).\end{aligned}$$

Por otro lado, si $k = 1$

$$\big(x,a^0) * (y,a)\big) * (z,a) = (xy,a) * (z,a) = (xy\tau(z)v, a^0).$$

Que a su vez es igual a,

$$(x,a^0) * ((y,a) * (z,a)) = (x,a^0) * (y\tau(z)v, a^0) = (xy\tau(z)v, a^0).$$

Luego para todas las combinaciones posibles de valores de i, j y k la asociatividad se mantiene, luego el producto $*$ es asociativo. □

En lo que sigue, trataremos con extensiones cíclicas, sin especificar si son externas o internas. La distinción la dará el contexto.

Definición 3.3. Diremos que dos tipos de extensión (N, n, τ, v) y (H, n, σ, w) son equivalentes si existe un isomorfismo $\varphi : N \to H$ de tal forma que $\sigma = \varphi \circ \tau \circ \varphi^{-1}$ y $\varphi(v) = w$.

Ahora bien, ¿qué relación hay entre la equivalencia de tipos de extensión que hemos definido y los isomorfismos de grupos de extensiones cíclicas?

Lema 3.2. *Sean G y G' extensiones cíclicas de tipos (N, n, τ, v) y (H, n, σ, w) respectivamente. Entonces:*

(a) Si G y G' son grupos isomorfos, y $\varphi : G \to G'$ es un isomorfismo, G' es extensión cíclica de tipo $(\varphi(N), n, \varphi|_N \circ \tau \circ (\varphi|_N)^{-1}, \varphi(v))$.

(b) Si (N, n, τ, v) y (H, n, σ, w) son equivalentes, entonces G y G' son grupos isomorfos.

Demostración. Pongámonos en las hipótesis del apartado (a). Como $N \trianglelefteq G$, tenemos que $N' := \varphi(N) \trianglelefteq G'$, luego G'/N' es un grupo. Consideremos ahora la aplicación $\Phi\colon G/N \to G'/N'; xN \mapsto \varphi(x)N'$. Esta aplicación está bien definida, pues dados $x, y \in G$ distintos tales que $xN = yN$ tenemos que $\varphi(x)N' = \varphi(y)N'$ ya que $\varphi(y^{-1}x) \in N'$ porque $\varphi(N) = N'$ y $y^{-1}x \in N$. De igual forma, el hecho de que φ sea isomorfismo nos permite asegurar que Φ es tanto inyectiva como suprayectiva, luego Φ es un isomorfismo de grupos y por tanto $G/N \cong G'/N' \cong C_n$. Tomemos entonces el $a \in G$ tal que $a^n = v \in N$ y sea $b = \varphi(a)$. Como se ha visto antes, tenemos que $|aN| = n$ y como Φ es un isomorfismo tenemos que $|bN| = n$. Sean $w = \varphi(v) = b^n$ y $\sigma = \varphi|_N \circ \tau \circ (\varphi|_N)^{-1}$. Tenemos que $\sigma(w) = \varphi|_N \circ \tau \circ (\varphi|_N)^{-1}(w) = \varphi|_N \circ \tau(v) = \varphi|_N(v) = w$ y que, dado $y = \varphi(x) \in N'$, con $x \in N$, tenemos que $\sigma^n(y) = \varphi|_N \circ \tau^n \circ (\varphi|_N)^{-1}(y) = \varphi|_N \circ \tau^n(x) = \varphi|_N(vxv^{-1}) = wyw^{-1}$ que es el automorfismo interno de N' dado por w. Con lo que concluimos que G' es la extensión cíclica de N' de tipo (N', n, σ, w).

Supongamos ahora que (N, n, τ, v) y (H, n, σ, w) son tipos equivalentes. Por definición, existe un isomorfismo $\varphi : N \to H$ tal que $\sigma = \varphi \circ \tau \circ \varphi^{-1}$ y $\varphi(v) = w$ y existen $a \in G \setminus N$y $b \in G' \setminus H$ tales que $v = a^n$ y $w = b^n$ y $\tau = t_a|_N$ y $\sigma = t_b|_H$ respectivamente (t_x automorfismo interno $y \mapsto xyx^{-1}$). De acuerdo con comentarios previos a (3.4), la unicidad de las expresiones de los elementos de G (respectivamente de G') como xa^i (yb^j) con $x \in N$ e $i \in \{0, 1, 2, \ldots, n-1\}$ ($y \in N'$ y $j \in \{0, 1, 2, \ldots, n-1\}$, nos permite definir la aplicación biyectiva, por serlo φ, $\Phi\colon G \to G'$ en la forma $\Phi(xa^i) = \varphi(x)b^i$. Falta comprobar que es un homomorfismo. Supongamos que $i + j < n$. Entonces tenemos que:

$$\Phi\left((xa^i)(ya^j)\right) = \Phi\left(x\tau^i(y)a^{i+j}\right) = \varphi\left(x\tau^i(y)\right)b^{i+j} = \varphi(x)(\varphi \circ \tau^i)(y)b^{i+j}$$

Mientras que :

$$\begin{aligned}\Phi\left(xa^i\right)\Phi\left(ya^j\right) &= \left(\varphi(x)b^i\right)\left(\varphi(y)b^j\right)\\ &= \varphi(x)\left(b^i\varphi(y)b^{-i}\right)b^ib^j = \varphi(x)(\sigma^i \circ \varphi)(y)b^{i+j}\end{aligned}$$

Por otro lado, si suponemos que $i + j \geq n$ tenemos que:

$$\begin{aligned}\Phi\left((xa^i)(ya^j)\right) &= \Phi\left(x\tau^i(y)va^{i+j-n}\right)\\ &= \varphi\left(x\tau^i(y)v\right)b^{i+j-n} = \varphi(x)(\varphi \circ \tau^i)(y)wb^{i+j-n}\end{aligned}$$

Mientras que:

$$\begin{aligned}\Phi\left(xa^i\right)\Phi\left(ya^j\right) &= \left(\varphi(x)b^i\right)\left(\varphi(y)b^j\right)\\ &= \varphi(x)\left(b^i\varphi(y)b^{-i}\right)b^ib^j = \varphi(x)(\sigma^i \circ \varphi)(y)wb^{i+j-n}\end{aligned}$$

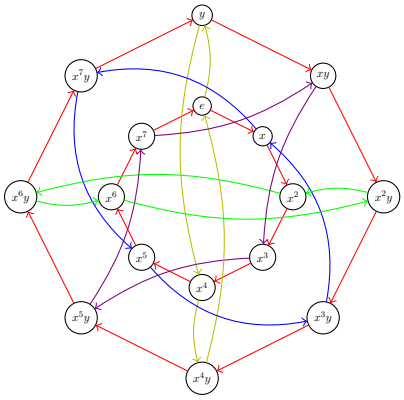


Figura 3.4: $G_5 = C_8 \rtimes_{\varphi_4}^{x^4} \cong Q_{16}$, en rojo el producto por x y el resto de colores dan las coclases de $\langle y \rangle$ en los distintos elementos.

Como $\sigma^i = \varphi \circ \tau^i \circ \varphi^{-1}$, en los dos casos ambas expresiones son iguales y por tanto Φ es un isomorfismo entre G y G'. □

Nota: Observemos que el Lema 3.2, no afirma que dados dos grupos isomorfos y que sean extensiones cíclicas de tipos $\mathcal{N}$ y $\mathcal{H}$, los tipos sean equivalentes. De hecho la afirmación es falsa.

Ejemplo 3.4. *Sea* $K_8 = \langle x, y | x^4 = y^2 = e \rangle \cong C_4 \times C_2$*, vamos a comprobar que es una extensión cíclica tanto de tipo* $(\langle x \rangle, 2, Id, e)$ *como de tipo* $(\langle x \rangle, 2, Id, x^2)$*, donde* Id *denota la aplicación identidad de* C_4*. Como* $[G : \langle x \rangle] = 2$*, tenemos que* $\langle x \rangle \trianglelefteq G$*, además* Id *cumple que* $Id(e) = e$*, que* $Id(x^2) = x^2$ *y que* $Id^2 = Id$*, luego tenemos que* K_8 *es extensión cíclica de ambos tipos. Sin embargo no existe ningún automorfismo* φ *de* K_8 *tal que* $\varphi(e) = x^2$*, luego son dos tipos de extensión no equivalentes.*

Así pues, extensiones no equivalentes pueden dar grupos isomorfos. Por tanto, la relación de equivalencia determinada por extensiones n-cíclicas equivalentes y la dada por clases de isomorfimos de grupos que sean extensiones n-cíclicas *no es tan buena como sería deseable*. Si usamos el apartado (b) del Lema 3.2 y denotamos por $[\mathcal{N}]$ la clase de equivalencia del tipo de extensión $\mathcal{N}$ y por $[G]$ la de grupos isomorfos a G:

$$\Delta([\mathcal{N}]) = [G_{\mathcal{N}}], \tag{3.7}$$

es una aplicación que no es inyectiva, de acuerdo con el ejemplo anterior. Otra limitación de esta técnica es que no todos los grupos finitos pueden construirse a partir de extensiones cíclicas. Por ejemplo, al necesitar tener un subgrupo normal propio N, los grupos simples no pueden ser extensiones cíclicas.

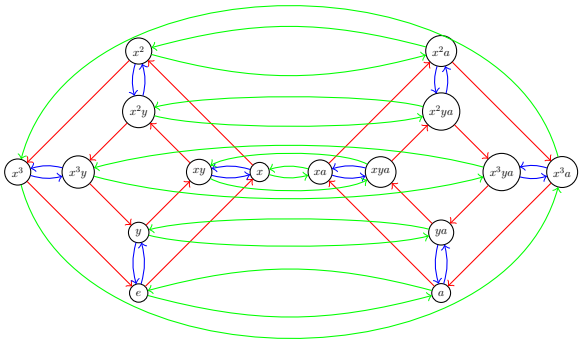


Figura 3.5: $G_7 \cong K_8 \times C_2$, en rojo el producto por x, en azul por y y en verde por a.

Lema 3.3. *Sea N grupo, $v, w \in N$, $Aut(N)$ su grupo de automorfismos, $n \in \mathbb{N}$ $(n \geq 2)$ y S un subconjunto de autormorfismos unión de clases de conjugación de $Aut(N)$. Si G_τ^u $(u = v, w)$ denota el grupo extensión cíclica de tipo $(N, n, \tau, v), \tau \in Aut(N)$, entonces:*

(a) Si existe $\varphi \in Aut(N)$ tal que $\varphi(v) = w$ y, las familias $\{G_\tau^v | \tau \in S\}$ y $\{G_\tau^w | \tau \in S\}$ contienen los mismos grupos salvo isomorfismos.

(b) Si $\varphi(v) = v$ para todo $\varphi \in Aut(N)$[5] y S una clase de conjugación, para cada $\sigma, \tau \in S$, G_σ^v y G_τ^v son isomorfos.

Demostración. Supongamos que estamos en las condiciones del apartado (a). Veamos que las familias $\mathcal{G} = \{G_\tau^v | \tau \in S\}$ y $\mathcal{F} = \{G_\tau^w | \tau \in S\}$ contienen exactamente los mismos grupos salvo isomorfismo. Sea $\varphi \in Aut(N)$ tal que $\varphi(v) = w$. Observamos que, como S es unión de clases de conjugación, $\varphi \circ \tau \circ \varphi^{-1} \in S$. Esto nos permite definir $\Phi : S \to S$; $\tau \mapsto \varphi \circ \tau \circ \varphi^{-1}$ Φ que es aplicación biyectiva. En efecto, como basta con probar que es inyectiva, si existen $\tau, \sigma \in S$ tales que $\phi \circ \tau \circ \phi^{-1} = \phi \circ \sigma \circ \phi^{-1}$, por las leyes cancelativas $\tau = \sigma$. Tomemos ahora un $\tau \in S$ y observemos que, aplicando el apartado (b) del Lema 3.2, los grupos G_τ^v y $G_{\Phi(\tau)}^w$ son isomorfos ya que sus tipos, (N, n, τ, v) y $(N, n, \varphi \circ \tau \circ \varphi^{-1}, \varphi(v) = w)$, son equivalentes (ver Definición 3.3). Por último, como Φ es una biyección de S, tenemos que $\tilde{\Phi} : \mathcal{G} \to \mathcal{F}$; $G_\tau^v \mapsto G_{\Phi(\tau)^w}$, es biyectiva y lleva los grupos de $\mathcal{G}$ a grupos isomorfos de $\mathcal{F}$.

Probemos ahora (b). Sea $\tau \in S$ fijo y $\varphi \in Aut(N)$. Conforme φ recorre todos los automorfismos de N, $\sigma = \varphi \circ \tau \circ \varphi^{-1}$ recorrerá todo S, pues es la clase de conjugación de τ. En virtud el apartado (a) del Lema 3.2, los grupos $G_\sigma^{\varphi(v)}$ ya que sus tipos $(N, n, \sigma = \varphi \circ \tau \circ \varphi^{-1}, \varphi(v))$ son equivalentes y, por hipótesis, $\varphi(v) = v$. □

Con los resultados obtenidos hasta el momento, podemos dar, de forma unificada, la clasificación salvo isomorfismos de los grupos de orden 16. Un total de 14 grupos no iso-

[5] El elemento v se dice, en tal caso, elemento característico de N.

morfos y todos ellos se pueden describir como extensiones 2-cíclicas de los grupos abelianos $(C_2)^3, C_8$ y K_8.

Teorema 3.3. *Cada grupo de orden 16 o bien es isomorfo a $(C_2)^4$ ó bien es extensión 2-cíclica externa de C_8 o de K_8. Los posibles grupos, salvo isomorfismos, son:*

(a) $C_8 \rtimes^e_{\varphi_i} C_2$ *con* $i = 1, 2, 3, 4$, $C_8 \rtimes^x_{\varphi_1} C_2$ *y* $C_8 \rtimes^{x^4}_{\varphi_4} C_2$.

(b) $K_8 \rtimes^e_{\psi_i} C_2$ *con* $i = 1, 2, 3, 5$, $K_8 \rtimes^y_{\psi_1} C_2$, $K_8 \rtimes^{x^2}_{\psi_5} C_2$ *y* $K_8 \rtimes^{x^2}_{\psi_3} C_2$.

Los automorfismos φ_i de C_8 y ψ_i de K_8 que los determinan son los descritos en la Tablas 2.1 y 2.3. Todos los grupos descritos son no isomorfos. Además $(C_2)^4$ es isomorfo al grupo extensión cíclica $(C_2)^4 \rtimes^e_{id} C_2$.

Demostración. Sea $G \neq C_2 \times C_2 \times C_2 \times C_2$. Por el Lema 2.12 G posee un subgrupo H isomorfo a C_8 ó K_8, luego de índice 2 y, por tanto, normal. Como $G/H \cong C_2$, el grupo G es extensión 2-cíclica interna de N por un elemento $v = a^2 \in H$ para algún $a \in G \setminus H$ tal que $|v| = \dfrac{|a|}{2}$. Además, $|v|$ debe ser divisor de 8 usando el Teorema de Lagrange. El caso $|v| = 8$ equivale a que $|a| = 16$, y a que $G = \langle a \rangle \cong C_{16}$. Es facil comprobar que C_{16} es isomorfo a la extensión cíclica $C_8 \rtimes^x_{id} C_2$. Por tanto, s. p. d. g., supondremos que G es extensión cíclica externa de tipo $(C_8, 2, \tau, v)$ o de tipo $(K_8, 2, \tau, v)$ y v un elemento de orden $4, 2$ ó $v = e$. Usando la Definición 3.2, si $N = C_8, K_8$, necesitamos que $\tau \in Aut(N)$ y que $v \in N$ satisfaga $\tau(v) = v$, condición (3.1) y, $\tau^2(x) = vxv^{-1} = t_v(x)$ (esto es, $\tau^2 = t_v$), condición (3.2)). La segunda condición se cumple tanto si τ es la identidad o τ es un automorfismo de orden 2 ya que N es abeliano. Así pues solo necesitamos verificar (3.1). Observamos que si $v = e$, ambas condiciones se cumplen trivialmente para cualquier $\tau \in Aut(C_8)$, $i = 1, 2$ y para los $\tau \in Aut(K_8)$ de orden ≤ 2. De hecho, e es un elemento característico y, aplicando el apartado (b) del Lema 3.3, podemos tomar un automorfismo por cada clase de conjugación. Este caso nos proporciona las extensiones cíclicas $C_8 \rtimes^e_{\varphi_i} C_2$ con $i = 1, 2, 3, 4$ y $K_8 \rtimes^e_{\psi_j} C_2$, con $j = 1, 2, 3, 5$ donde φ_i, ψ_j son los automorfismos definidos en las Tablas 2.1 y 2.3. Además, si una de las extensiones externas G' tiene un elemento (w, u) de orden 2 tal que $(w, u) \notin N'$, donde $N' = \{(w, e) : w \in N\} \cong C_8, K_8$ es el subgrupo descrito en Lema 3.1, entonces G' es una de las extensiones con $N = K_8, C_8$ y $v = e$.

1. Extensiones de tipo $(C_8, 2, \varphi_i, v)$ y $|v| = 2$. Aquí $v = x^4$ es la única posibilidad para todo $i = 1, 2, 3, 4$. Si llamamos G'_i al grupo extensión cíclica externa obtenido, observamos que, para φ_2, $(x, a) * (x, a) = (x\varphi_2(x)x^4, e) = (xx^4x^4, e) = (e, e)$, luego en G'_2, $|(x, a)| = 2$, por tanto este grupo es isomorfo a una externa con $v = e$. En los casos φ_1 y φ_3, tenemos que (x^2, a) es de orden 2 y G'_1, G'_3 son isomorfos a una externa con $v = e$. Así pues el único grupo extensión cíclica que nos queda es $C_8 \rtimes^{x^4}_{\varphi_4} C_2$.

2. Extensiones de tipo $(C_8, 2, \varphi_i, v)$ y $|v| = 4$. En este caso, $v = x^2$ o $v = x^6$, que son fijados por $S = \{\varphi_1, \varphi_3\}$ que es la unión de dos clases de conjugación de $Aut(C_8)$ de acuerdo con la Tabla 2.1. Además, $\varphi_2(x^2) = x^6$ y, por el apartado (a) del Lema 3.3, los elementos generan grupos isomorfos y, s.p.d.g. tomamos $v = x^2$. Aquí, para

G_1' tenemos que $(x^3,a)(x^3,a) = (x^3\varphi_1(x^3)x^2, a^2) = (x^3x^3x^2, e) = (e,e)$. En G_3', $(x,a)(x,a) = (x\varphi_3(x)x^2, a^2) = xx^5x^2, e) = (e,e)$. Luego los grupos son isomorfos a extensiones externas con $v = e$.

Esto proporciona las seis posibilidades del apartado (a). En los tipos $N = K_8$, que describiremos por generación como $\langle x, y | x^4 = y^2 = e,\ xy = yx\rangle$, vamos a suponer que $|x| < 8$ para todo $x \in G$ ya que de lo contrario podríamos encontrar un $C_8 \cong H \trianglelefteq G$ y G sería isomorfo a una de las extensiones previamente obtenidas. Por tanto solo hay que estudiar las extensiones de tipo $(K_8, 2, \psi_i, v)$ con $|v| = 2$. En vistas de aplicar el Lema 3.3 tenemos que las clases de conjugación de $Aut(K_8)$ válidas son $\{\psi_1\}$, $\{\psi_3\}$, $\{\psi_5, \psi_7\}$ y $\{\psi_2, \psi_4\}$, pues ψ_6 y ψ_8, al ser de orden 4, no cumplen la condición (3.3), tal y como se puede ver en la Tabla 2.3. Las posibilidades con $|v| = 2$ son $v = x^2, y, x^2y$.

3. Si $v = x^2$, como es característico, tenemos una extensión por cada representante de clase de conjugación aplicando (b) del Lema 3.3. Si $\tau = \psi_1$, $(x,a)(x,a) = (x\psi_1(x)x^2, e) = (x^4, e) = (e,e)$, y para $\tau = \psi_2$, $(x,a)(x,a) = (x\psi_2(x)x^2, e) = (xxx^2, e) = (e,e)$. Así que a la lista, salvo isomorfismos, solo añadimos los grupos $K_8 \rtimes^{x^2}_{\psi_3} C_2$ y $K_8 \rtimes^{x^2}_{\psi_5} C_2$.

4. Si $v = y$, los automorfismos que dejan fijo y son $S = \{\psi_1, \psi_3, \psi_5, \psi_7\}$. Para ψ_7, $(x,a)(x,a) = (x\psi_7(x)y, a^2) = (xx^3yy = (x^4y^2, e) = (e,e)$, ya tratado. Con ψ_5, en G_5' tenemos $(x,a)(x,a) = (x\psi_5(x)y, e) = (xxyy, e) = (x^2, e) = v$. Así, en el subgrupo N' de G_5' no está (x,a), lo que nos devuelve al caso previo. El caso $\tau = \psi_3$ es más delicado. Nos fijamos en que $(e,a) * (x^2,e) = (\psi_3(x^2), aa) = (x^6, a) = (x^2, a) = (x^2, e) * (e,a)$, luego conmutan. Además $(e,a) * (e,a) = (y,e)$, de donde $\langle (e,a)\rangle = \{(e,e), (e,a), (y,e), (y,a)\}$ y $\langle (x^2,e)\rangle = \{(e,e), (x^2,e)\}$ y, en G_3' localizamos el subgrupo normal $H' = \langle (e,a), (x^2,e)\rangle = \{e, a, y, ya, x^2, x^2a, x^2y, x^2ya\} \cong K_8$. Ahora, y es un elemento característico de H' y $(x,a)(x,a) = (x\psi_3(x), a^2) = (xx^3y, e) = (x^4y, e) = (y,e)$, si tomamos como $\tilde{a} = (x,a)$ nos volvemos a encontrar en el subcaso a). Por tanto, el único grupo en este caso es $K_8 \rtimes^{y}_{\psi_1} C_2$.

5. Si $v = x^2y$, los automorfismos válidos son los del conjunto S del caso 4, que es unión de clases de conjugación. Como $\psi_2(y) = x^2y = v$, por apartado (b) del Lema 3.3 los grupos que aparecen son los del caso $v = y$.

Esto nos da las 7 posibilidades del apartado (b). La afirmación sobre $(C_2)^4$ es clara dado que es producto directo de $(C_2)^3$ y C_2 pues $\varphi = id$ y $v = e$. Además, por el Lema 3.1 (Teorema de extensión cíclica, N abeliano y $n = 2$), todos los tipos de extensión producen grupos. Falta comprobar que los listados no son isomorfos 2 a 2 ni con $(C_2)^4$. Para ello vamos a argumentar basándonos en los órdenes de los elementos de los grupos que, a excepción de $(C_2)^4$, aparecen en la la Tabla 3.3 [6]. Los elementos distintos del neutro de $(C_2)^4$ son de orden 2, y, en el resto, hay al menos un elemento de orden 4, luego este grupo no es isomorfo a ninguno. Observando la tabla, podemos separar los grupos en dos grandes colecciones sin isomorfismos entre sí: la que tiene grupos con elementos de orden 8

[6] Esta tabla se ha realizado con SageMath y exportado a LaTeX tal y como se explica en el Apéndice.

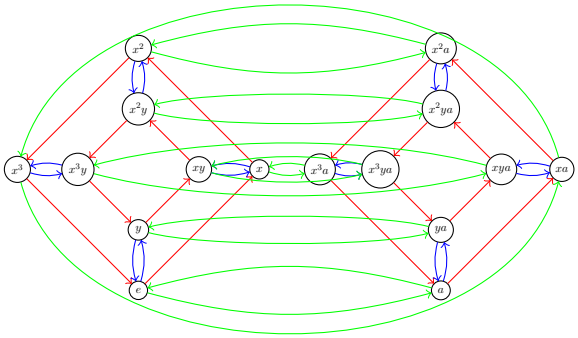


Figura 3.6: $G_9 \cong K_8 \rtimes_{\psi_3} C_2$, en rojo el producto por x, en azul por y y en verde por a.

$\{G_1, \ldots, G_6\}$ y la que no $\{G_9, \ldots, G_{13}\}$. En el primer conjunto, si contamos el número de elementos de cada orden vemos que los únicos que podrían ser isomorfos son G_1 y el G_3. Pero G_1 es abeliano y G_3 no. Por órdenes, G_9 no es isomorfo a ningún otro de su grupo. Comparamos ahora los grupos de los conjutos $\{G_7, G_8, G_{10}\}$. Tanto G_7 como G_{13} son abelianos, mientras que el resto de grupos de su conjunto no. Centrémonos en G_8 y G_{10}. En G_8 los subgrupos generados por elementos de orden 4 son $\langle x \rangle = \{e, x, x^2, x^3\}$, $\langle xy \rangle = \{e, xy, x^2, x^3y\}$, $\langle xa \rangle = \{e, xa, x^2, x^3ya\}$ y $\langle ya \rangle = \{e, ya, x^2, x^2ya\}$ tienen intersección no trivial. En G_{10} sin embargo el subgrupo $\langle x \rangle = \{e, x, x^2, x^3\}$ y $\langle xa \rangle = \{e, xa, x^2y, x^3ya\}$ tienen intersección trivial, luego no son isomorfos. Para distinguir G_{11} de G_{12} usaremos reducción al absurdo. Supongamos que existe un isomorfismo $\phi : G_{12} \to G_{11}$ y notemos que en G_{11} si elevas cualquier elemento de orden 4 al cuadrado te da x^2. Como en G_{12} x^2 es el cuadrado de x, $\phi(x^2)$ tendrá que ser el cuadrado de $\phi(x)$ y por tanto $\phi(x^2) = x^2$. De la misma forma, como en G_{12} $(xa)^2 = x^2y$, tendremos que $(\phi(xa))^2 = \phi\left((xa)^2\right) = \phi(x^2y)$ y como $\phi(xa) \in G_{11}$, $\phi(x^2y) = x^2$. Así que hemos demostrado que $\phi(x^2) = \phi(x^2y)$ cuando $x^2 \neq x^2y$, luego ϕ no es inyectiva, lo cual es una contradicción. Así que llegamos a que G_{11} y G_{12} no son isomorfos. Por tanto hay 14 grupos de orden 16 salvo isomorfismos. □

Nota: Los elementos del grupo del Teorema 3.2 los denotaremos en la forma $x \equiv (x, a^0)$, $a^i \equiv (e, a^i)$, $e \equiv (e, a^0)$ y $xa^i \equiv (x, a^i)$.

Una vez clasificados los grupo de orden 16 mediante extensiones cíclicas, vamos a dar presentaciones más habituales de los mismos. Ya hemos visto en el Ejemplo 3.2 que, si $v = e$, las extensiones cíclicas son producto semidirecto y si usamos además el homomorfismo identidad, son directos. También hemos visto en la demostración del Teorema 3.3, que $C_8 \rtimes^x_{id} C_2$ es C_{16}. El resto de casos hay que ir analizándolos con más cuidado uno por uno. Seguimos la enumeración de etiquetas de la Tabla 3.2

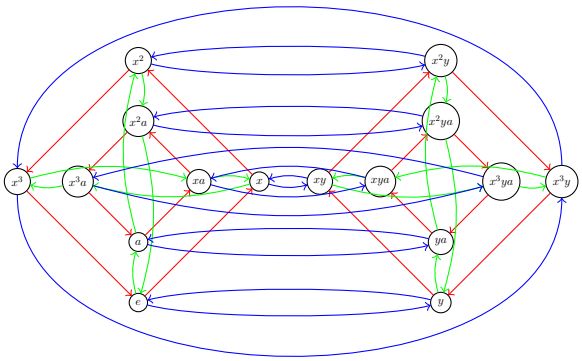


Figura 3.7: $G_{11} = K_8 \rtimes^{x^2}_{\psi_3} C_2$, en rojo el producto por x, en azul por y y en verde por a.

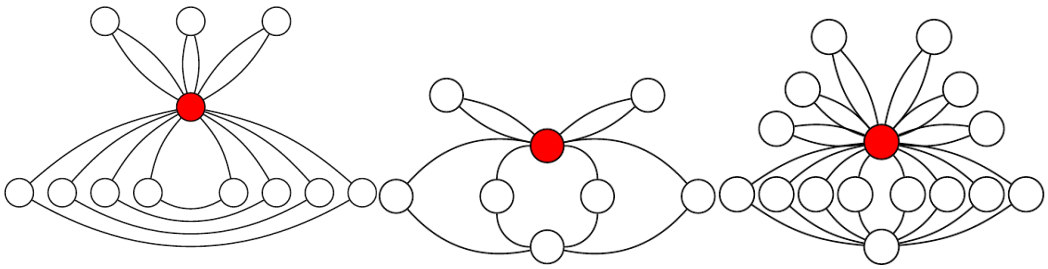
- $G_5 = C_8 \rtimes^{x^4}_{\varphi_4} C_2$. Este grupo es unión disjunta $\langle x\rangle \sqcup \langle x\rangle a$. Además, $ax = \varphi_4(x)a = x^{-1}a$, $a^2 = x^4$ y $(xa)(xa) = a^2 = x^4$, luego $G_5 = \langle x, a | x^8 = a^4 = e, x^4 = a^2 = (xa)^2\rangle$, que es la presentación habitual del grupo cuaternio generalizado Q_{16}.
- Sea $G_{11} = K_8 \rtimes^{x^2}_{\psi_3} C_2$. Descomponemos el grupo como $K_8 \sqcup K_8a$ y tenemos que $ax = x^3a$, $ay = ya$ y $a^2 = x^2$. El subgrupo $N = \langle x, a\rangle = \{e, x, x^2, x^3, a, xa, x^2a, x^3\}$ es normal por ser de índice dos e isomorfo a Q_8 y $N \cap \langle y\rangle = \{e\}$ y, como K_8 es conmutativo, y conmuta con x y a, Así llegamos al producto directo $Q_8 \times C_2$.
- $G_{12} = K_8 \rtimes^{x^2}_{\psi_5} C_2$. En este caso, $G_{12} = K_8 \sqcup K_8a$ y $ax = xya$, $ay = ya$ y $a^2 = x^2$. El subgrupo $\langle xa\rangle = \{e, xa, y, xya\}$ es cíclico y normal: $a(xa)a^{-1} = ax = xya \in \langle xa\rangle$, que $x(xa)x^3 = x^2ax^3 = x^5y^3a = xya$ y que $y(xa)y^{-1} = xa$. Además $\langle xa\rangle \cap \langle x\rangle = \{e\}$, lo que nos lleva al producto semidirecto $C_4 \rtimes_\tau C_4$ con $\tau(z) = z^3$.
- $G_{13} = K_8 \rtimes^{y}_{id} C_2$. Tenemos la descomposición $K_8 \sqcup K_8a$, $ax = xa$, que $ay = ya$ y $a^2 = y$. Como $\langle a\rangle$ y $\langle x\rangle$ cumplen las condiciones del producto directo, llegamos a $C_4 \times C_4$.

Tipo	Grupo	Tipo	Grupo
$(C_8, 2, id, e)$	$G_1 \cong C_8 \times C_2$	$(K_8, 2, id, e)$	$G_7 \cong K_8 \times C_2$
$(C_8, 2, \varphi_2, e)$	$G_2 \cong C_8 \rtimes_{\varphi_2} C_2$	$(K_8, 2, \psi_2, e)$	$G_8 \cong K_8 \rtimes_{\psi_2} C_2$
$(C_8, 2, \varphi_3, e)$	$G_3 \cong C_8 \rtimes_{\varphi_3} C_2$	$(K_8, 2, \psi_3, e)$	$G_9 \cong K_8 \rtimes_{\psi_3} C_2$
$(C_8, 2, \varphi_4, e)$	$G_4 \cong C_8 \rtimes_{\varphi_4} C_2 \cong D_8$	$(K_8, 2, \psi_5, e)$	$G_{10} \cong K_8 \rtimes_{\psi_5} C_2$
$(C_8, 2, \varphi_4, x^4)$	$G_5 \cong Q_{16}$	$(K_8, 2, \psi_3, x^2)$	$G_{11} \cong Q_8 \times C_2$
$(C_8, 2, id, x)$	$G_6 \cong C_{16}$	$(K_8, 2, \psi_5, x^2)$	$G_{12} \cong C_4 \rtimes_\tau C_4$
		$(K_8, 2, id, y)$	$G_{13} \cong C_4 \times C_4$

Cuadro 3.2: Tipos de extensión y extensión cíclica asociada

	e	x	x^2	x^3	x^4	x^5	x^6	x^7	a	xa	x^2a	x^3a	x^4a	x^5a	x^6a	x^7a
$G_1 = C_8 \rtimes^e_{id} C_2$	1	8	4	8	2	8	4	8	2	8	4	8	2	8	4	8
$G_2 = C_8 \rtimes^e_{\varphi_2} C_2$	1	8	4	8	2	8	4	8	2	4	2	4	2	4	2	4
$G_3 = C_8 \rtimes^e_{\varphi_3} C_2$	1	8	4	8	2	8	4	8	2	8	4	8	2	8	4	8
$G_4 = C_8 \rtimes^e_{\varphi_4} C_2$	1	8	4	8	2	8	4	8	2	2	2	2	2	2	2	2
$G_5 = C_8 \rtimes^{x^4}_{\varphi_4} C_2$	1	8	4	8	2	8	4	8	4	4	4	4	4	4	4	4
$G_6 = C_8 \rtimes^x_{id} C_2$	1	8	4	8	2	8	4	8	16	16	16	16	16	16	16	16
	e	x	x^2	x^3	y	xy	x^2y	x^3y	a	xa	x^2a	x^3a	ya	xya	x^2ya	x^3ya
$G_7 = K_8 \rtimes^e_{id} C_2$	1	4	2	4	2	4	2	4	2	4	2	4	2	4	2	4
$G_8 = K_8 \rtimes^e_{\psi_2} C_2$	1	4	2	4	2	4	2	4	2	4	2	4	4	2	4	2
$G_9 = K_8 \rtimes^e_{\psi_3} C_2$	1	4	2	4	2	4	2	4	2	2	2	2	2	2	2	2
$G_{10} = K_8 \rtimes^e_{\psi_5} C_2$	1	4	2	4	2	4	2	4	2	4	2	4	2	4	2	4
$G_{11} = K_8 \rtimes^{x^2}_{\psi_3} C_2$	1	4	2	4	2	4	2	4	4	4	4	4	4	4	4	4
$G_{12} = K_8 \rtimes^{x^2}_{\psi_5} C_2$	1	4	2	4	2	4	2	4	4	4	4	4	4	4	4	4
$G_{13} = K_8 \rtimes^y_{id} C_2$	1	4	2	4	2	4	2	4	4	4	4	4	4	4	4	4

Cuadro 3.3: Órdenes de los grupos G_1 al G_{13}



(a) Grupo $A_4 \cong K_4 \rtimes^e_\tau C_3$ (b) Grupo $K_8 \cong C_4 \rtimes^{x^2}_{id} C_2$ (c) Grupo $K_8 \times C_2 \cong K_8 \rtimes^e_{id} C_2$

Conclusiones

A lo largo de este trabajo hemos podido ver un breve resumen sobre el surgimiento y desarrollo de la teoría de grupos, una rama de las matemáticas que, aunque al principió me resultó muy complicada y extraña, conforme he ido trabajando más en ella, más me cautivaba, llegando a convertirse en una de mis favoritas, por su elegancia y el gran número de aplicaciones que tiene en diversas áreas de las matemáticas y la física. Como hemos contado en el Capítulo 1, una de las ramas surgidas en los años 20 es la que Teoría de Grupos Finitos. Hasta donde he leído en textos universitarios (niveles de estudiantes de segundo ciclo), a la hora de clasificar grupos, siempre se suele recurrir a resultados como el Teorema Fundamental de los Grupos Abelianos Finitamente Generados o los Teoremas de Sylow, debido a su potencia y versatilidad. En este trabajo, hemos planteado el uso de técnicas alternativas. En especial, al clasificar los grupos de orden menor o igual que 15, al no disponer de resultados generales tenía que considerar cada caso por separado y encontrar soluciones *ad hoc* a cada problema, lo cual me ha permitido entender en más profundidad cómo funciona la propia estructura de grupo. Por el contrario, para los grupos de orden 16, hemos necesitado de resultados más técnicos para poder clasificarlos con facilidad y me ha parecido especialmente elegante como Marcel M. Wolfgang Wild usa el Teorema de Extensión Cíclica para, de forma clara y elegante, dar una clasificación unificada de los mismos. Esta tarea, con las herramientas de que disponía inicialmente, se me hacía titánica.

Apéndice A

Grafos y SageMath

En esta última sección trataré los dos tipos de grafos que han salido a lo largo del trabajo y el proceso que he seguido para calcularlos y construirlos.

Definición A.1. Dado un grupo finito G construimos su *grafo cíclico* tomando un vértice por cada elemento $g \in G$ y unimos mediante aristas los ciclos que se obtienen al iterar g^n para cada $g \in G$ y para cada $n \in \mathbb{N}$. Habitualmente, para mejorar la claridad del grafo, la arista que se obtiene al multiplicar e por si mismo se suele omitir, al igual que las aristas redundantes de cada ciclo, como se puede ver en la figura A.1.

Definición A.2. Dado un grupo finito $G = \langle g_1, g_2, \ldots, g_r \rangle$ construimos su *grafo de Cayley* tomando un vértice por cada elemento $g \in G$ y un color $\{1, 2, \ldots, r\}$ por cada generador. A continuación, dados dos elementos $x, y \in G$ unimos x a y mediante una arista dirigida de color k si $y = g_k x$.

Mientras que los grafos cíclicos son útiles para ver los distintos ciclos que ocurren dentro del grupo G, los grafos de Cayley son más ricos pues muestran de manera inequívoca cómo funciona el producto de G, con la desventaja que son más costosos de calcular y, cuantos más elementos y más generadores tenga el grupo, más sucio será el grafo resultante perdiendo el propósito de que sea una buena representación visual de la estructura.

Los grafos cíclicos de este trabajo los hemos calculado a mano y representado mediante *tikz*. Sin embargo, para los grafos de Cayley nos hemos ayudado del sistema algebraico computacional SageMath, que implementa los grupos mediante GAP y te da la opción de

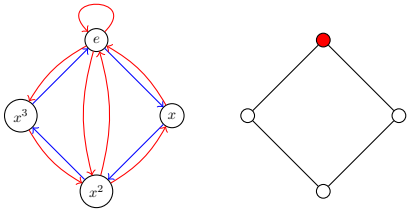


Figura A.1: Grafo cíclico completo (izq.) y reducido (der.) de C_4

construirlos de diversas formas. En un primer momento consideré construir los grupos de orden 16 mediante generadores y relaciones, sin embargo, SageMath lo hace como cocientes de grupos libres, lo cual provocó que a poco que se empezaran a complicar los cálculos, el servidor superara la memoria que tenía asignada e interrumpiera los cálculos, así que decidí implementarlos mediante grupos de permutaciones y los productos semidirectos establecidos en la sección anterior. De aquí en adelante usaremos como ejemplo el código usado para construir $G_{12} \cong C_4 \rtimes_\phi C_4$.

```
C4=CyclicPermutationGroup(4)
z=C4.gens()[0]
phi=PermutationGroupMorphism_im_gens(C4,C4, [z^3])
G12=C4.semidirect_product(C4, [C4.gens(), [phi]])
G12.cayley_graph().show()
```

La instrucción `CyclicPermutationGroup(n)` nos permite construir C_n como grupo de permutaciones. En la siguiente línea calculamos la lista de generadores de C_4 (`C_4.gens()`) y el único generador que hay se lo asignamos a la variable `z`. Esto nos permite construir el automorfismo ϕ mediante la instrucción `PermutationGroupMorphism_im_gens(G,H, l)` que construye un homomorfismo de G a H asignando a cada generador de G un elemento de la lista l. Una vez tenemos el automorfismo construido, podemos construir G_{12} teniendo en cuenta que la instrucción

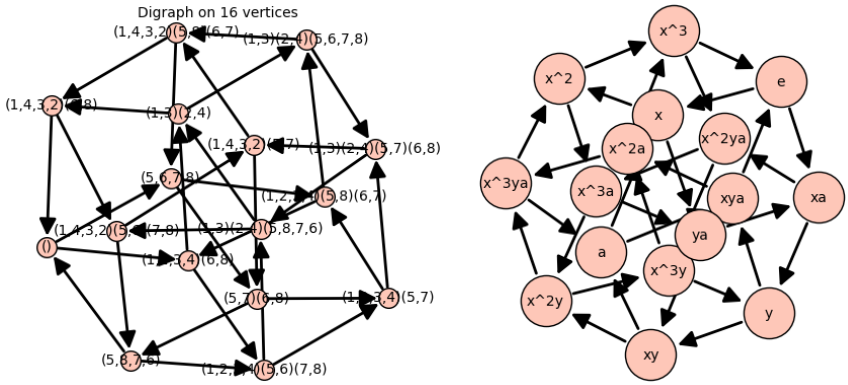
```
N.semidirect_product(H,[H_gens, aut_N])
```

te construye el producto semidirecto $N \rtimes_\phi H$ de forma que ϕ asigna a cada generador de la lista `H_gens` un automorfismo de N de la lista `aut_N`. Por último, construimos el grafo de Cayley con la función implementada en SageMath y lo mostramos. Como se puede ver en la Figura A.2 (a), al etiquetar los vértices mediante las permutaciones, estas etiquetas se solapan y no se distingue nada. Por suerte si construyes un diccionario `d` de forma que las claves sean las permutaciones y los valores el elemento expresado en la forma $x^i y^j a^k$ que lo representa, con las siguientes instrucciones se obtiene un grafo más claro y que la etiqueta de cada vértice quepa dentro del mismo, como se puede ver en la figura A.2 (b).

```
G12Cayley=G12.cayley_graph()
G12Cayley.relabel(d12)
G12Cayley.show(vertex_size=1300, edge_thickness=300)
```

A pesar de todo, SageMath te construye el grafo de Cayley sin tener en cuenta la estructura del grupo y sin colorear las aristas en función del generador por el que multiplicas, haciendo que el grafo no sea tan limpio como sería deseable. Por eso, una vez que tenía todos los grupos construidos, me he basado en los grafos que me proporcionaba SageMath para construir los míos propios en tikz, quedando como resultado los gráficos que se han ido viendo en el último Capítulo.

SageMath también me ha permitido sacar rápidamente los órdenes de cada grupo, mediante instrucciones similares a las siguientes, que a su vez me proporcionaban listas con las que he hecho que SageMath me construya la Tabla 3.3 automáticamente.



(a) Sin reetiquetar (b) Reetiquetando

Figura A.2: Grafos de Cayley de C_{12}.

```
x,xa=G12.gens()
y=xa^2
a=xa^3*x^3
aux=[]
for i in range(2):
    for j in range(2):
        for k in range(4):
            aux.append((x^k*y^j*a^i).order())
```

Nota: El proceso podría haber sido mucho más rápido si hubiera construído las listas mediante la instrucción [g.order() for g in G12.list()]. Sin embargo quería que las listas estuvieran ordenadas siguiendo un orden específico, motivo por el cual calculo los órdenes de los elementos en función de x, de y y de a.

Bibliografía

[1] Michael Aschbacher. «The status of the classification of the finite simple groups». En: *Notices of the American Mathematical Society* 51.7 (2004), págs. 736-740.

[2] Hans Ulrich Besche, Bettina Eick y Eamonn A O'brian. «A millennium project: constructing small groups». En: *International Journal of Algebra and Computation* 12.05 (2002), págs. 623-644.

[3] Israel Kleiner. «The evolution of group theory: A brief survey». En: *Mathematics Magazine* 59.4 (1986), págs. 195-215.

[4] Jérôme Lapuyade-Lahorgue. «Groups of order 8 and 16». En: *arXiv preprint arXiv:1807.10004* (2018).

[5] Stephen Lovett. *Abstract Algebra: Structures and Applications*. CRC Press, 2015.

[6] JJ O'Connor y EF Robertson. *A history of the Burnside Problem*. 2002. URL: https://mathshistory.st-andrews.ac.uk/HistTopics/Burnside_problem/.

[7] JJ O'Connor y EF Robertson. *The development of group theory*. 1996. URL: https://mathshistory.st-andrews.ac.uk/HistTopics/Development_group_theory/.

[8] Gerard Thompson y col. «Classifying groups of small order». En: *Advances in Pure Mathematics* 6.02 (2016), pág. 58.

[9] Bartel L Van der Waerden. *A history of algebra: From al-Khwārizmı to Emmy Noether*. Springer Science & Business Media, 2013.

[10] Marcel Wild. «The Groups of Order Sixteen Made Easy». En: *American Mathematical Monthly 2005-jan 01 vol. 112 iss. 1* 112 (1 ene. de 2005). DOI: 10.2307/30037381.