
Universidad Nacional Autónoma de México

Facultad de Ciencias


# SOBRE GRUPOS DE ORDEN MENOR A 32

## UNA CLASIFICACIÓN A TRAVÉS DE EXTENSIONES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

PRESENTA:


JOSÉ COLLINS CASTRO


DIRECTOR DE TESIS:

Dr. JUAN MORALES RODRÍGUEZ

MAYO, 2013

# Agradecimientos

Al Dr. Juan Morales Rodríguez por su enorme paciencia y guía a través de la elaboración del presente, y sobre todo por introducirme al maravilloso mundo del álgebra abstracta y la teoría de grupos, a través de la dedicación que imprime a sus clases. Sin mencionar otro montón de cosas que dejo fuera en esta ocación.

Al M. en C. Manuel Zorrilla, por su infinita dedicación y entusiasmo, este trabajo hubiera sido otra cosa sin tus invaluables correcciones.

A la Dra. Isabel Hubard, por su enorme apoyo a través de estos años, por presentarme los politopos abstractos y como conjugarlos con mi pasión por la teoría de grupos, por brindarme tantas oportunidades como mi tutora de posgrado.

Al Dr. Hugo Rincón, por la atención y aliento prestadas como sinodal. Además de sus excelentes clases, presentandome nuevas ramas del Álgebra que tanto disfruté estudiar.

A la M. en C. Ana Irene Ramírez, por enseñarme la mayoría de la geometría que conozco, convirtiéndola en una de mis grandes gustos matemáticos, además de su preocupación y consejo a través de mis años en la licenciatura.

Al Profr. Guillermo Zambrama, por su cobijo a lo largo de esta etapa, por enseñarme la importancia de la história y la filosofía en mi fomación como matemático, por las comidas y las charlas, por ofrecerme su amistad y camaradería.

A Adriana, por su infinita paciencia, por su apoyo incondicional en tantas cosas que ya no puedo ni contarlas, por casi una década de vivencias que atesoro, por ser parte fundamental de mi vida. Te amo.

A mis padres, por el amor y comprensión a lo largo de mi vida, por siempre creer en mí.

A mi tía, mis abuelos y mi hermana, mi familia, por quererme tanto y estar ahí para mí siempre.

A Víctor, Carmen, Ma. Luisa, María del Carmen, Alberto y Alfredo, mi otra familia, por acogerme tan cálidamente, hacerme parte de ustedes y ayudarme tanto como lo han hecho.

A Irene, Eniak, Carlos, Mariana, Olín, Lalo, Daniel, Iván, Julia, Ana y Omisis, "La Palomilla", por ser mis hermanos y cofrades durante los primeros años en esta ciudad, por todos estos años de amistad y, en palabras de Carlos, *risas alternativas*.

A Katleen, mi más antigua amiga, por todas las vivencias, las viejas y las nuevas, que aunque han sido intermitentes, su valía lo compensa con creces. Te quiero amiga.

A Cristina, Daniela, Manuel y Arturo, por todas esas largas noches de desvelo no académico, que espero no acaben.

A mis amigos de la facultad, Yanus, Lalo, Nahúm, Benito, Ricardo y Migueles por todas esas tardes de agradable discusión y debraye en el pulpo.

A Abú, Gasde, Jana, Luis Miguel y Violeta, mis compañeros y amigos de la maestría, por esas tardes de instituto que tanto he llegado a disfrutar. También por los congresos y noches de no-instituto que he disfrutado aún más.

# Índice general

# 1 Introducción

En 1854, el matemático inglés Arthur Cayley publicaba en su trabajo *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$ la primera definición de grupo finito. [1] A continuación, reproducimos el texto.

*A set of symbols* 1, $\alpha$, $\beta$, ..., *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***.[2]

La definición de Cayley continúa de la manera siguiente:

*These symbols are not in general convertible [commutative] but are associative . . . and it follows that if the entire group is multiplied by any one of the symbols, either as further or nearer factor [i.e., on the left or on the right], the effect is simply to reproduce the group.*[3]

La orientación de Cayley hacia una visión abstracta de los grupos respondía, al menos en parte, a su contacto con el trabajo de G. Boole. Esta precupación hacia la fundamentación abstracta de las matemáticas era característica de los círculos que rodeaban a Boole, Cayley y Sylvester ya en la década de los 40 del siglo XIX.

Sin embargo, la definición de Cayley no encontró mucho eco en la comunidad matemática de aquél tiempo; la cual, aparentemente, no se encontraba preparada para tal abstracción. Los grupos de permutaciones eran los únicos sometidos a una investigación seria, pues en aquél periodo la aproximación formal a las matemáticas estaba aún en

[1] En 1858 Richard Dedekind, en una de sus conferencias sobre teoría de Galois en Göttingen, proporcionó otra.

[2] Un conjunto de símbolos 1, $\alpha$, $\beta$, ..., todos ellos distintos, y de tal manera que el producto de cualesquiera dos de ellos (no importa en que orden), o el producto de cualquiera de ellos consigo mismo, pertenece al conjunto, se dice que es un **grupo.**

[3] Estos símbolos no son en general convertibles [conmutativos] pero son asociativos ... y se sigue que si el grupo completo es multiplicado por cualquiera de los símbolos, ya sea como factor lejano o cercano [i.e. por la derecha o por la izquierda], el efecto es simplemente reproducir el grupo.

su infancia. Al respecto, Morris Kline escribe en su obra *Mathematical Thought from Ancient to Modem Times:*

*Premature abstraction falls on deaf ears, wether they belong to mathematicians or students.*[4]

Tomó un cuarto de siglo adicional para que la definición abstracta de grupo empezara a considerarse. Fue Cayley de nuevo quien la introdujo en una serie de cuatro artículos cortos relacionados con teoría de grupos que escribió en 1878. Es aquí donde él planteaba el problema general de encontrar todos los grupos de un orden dado.

Estos artículos de Cayley, a diferencia de los de 1854, inspiraron el trabajo de múltiples matemáticos en el área -entre los que se encuentran H. M. Weber y W. F. A. von Dyck- provocando la rápida propagación del concepto de grupo abstracto durante las décadas de 1880 y 1890.

Esto motivó la redemostración y reintroducción de elementos pertenecientes a la teoría de grupos "concretos" en el contexto abstracto, así como a la aparición de estudios cuya génesis y preocupación estaba basado en el concepto abstracto.

Como ejemplo del primero de los acontecimientos descritos en el párrafo anterior tenemos el trabajo realizado en 1887 por Ferdinand Georg Frobenius, titulado *A new proof of Sylow's theorem*, donde redemuestra el famoso teorema en un contexto abstracto. Aunque Frobenius reconocía la validez del resultado para cualquier grupo finito, validez provista por el teorema de Cayley, publicado desde 1854; justifica así su deseo de encontrar una demostración abstracta del teorema:

*Since the symmetric group, which is introduced into all these proofs, is totally alien to the context of Sylow's theorem, I have tried to find a new derivation of it.*[5]

El matemático alemán Otto Hölder, quien contribuyo enormemente a la teoría de grupos abstracta a través de conceptos como grupo cociente [1889] y automorfismo, noción que introdujo en su artículo de 1893 *Die Gruppen der Ordnungen* $p^3$ *,* $pq^2$ *,* $pqr$*,* $p^4$, cuyos resultados y métodos dependían en gran medida del Teorema de Sylow.

Es también mérito de Hölder ser el primero en estudiar los grupos simples de manera abstracta, clasificando este tipo de grupos cuyo orden no es mayor a 200 y haciendo

[4] La abstracción prematura cae en oídos sordos, ya sea que estos pertenezcan a matemáticos o a estudiantes.

[5] Como el grupo simétrico, que se introduce en todas estas pruebas, es completamente ajeno al contexto del teorema de Sylow, he tratado de encontrar una nueva derivación del mismo.

incapié en la importancia de esta clasificación en su artículo de 1892 *Die einfachen Gruppen in ersten und zweiten Hundert der Ordnungszahlen*, donde escribe:

*Es ware von dem grossten Interesse, wenn eine Uebersicht der sammtlichen einfachen Gruppen von einer endlichen Zahl von Operationen gegeben werden konnte.*[6]

Es ahora un poco más claro que el problema de la clasificación de los grupos de un orden dado ha estado presente a lo largo de la historia de la teoría abstracta de grupos y tal vez ha motivado problemas tan importantes para ésta como la clasificación de los grupos simples, que en palabras de J. L. Alperin, constituye una de las *joyas de la corona de las matemáticas del siglo veinte.*

El presente trabajo prentende introducir, fuera del contexto histórico, un compendio de proposiciones y técnicas mediante las cuales es posible clasificar algunos grupos de orden pequeño, de manera que un estudiante de los últimos dos años de la licenciatura en Matemáticas sea capaz de estudiarlas sin gran dificultad.

El capítulo 2 presenta una recopilación de definiciones y resultados básicos de teoría de grupos y prentende establecer los requisitos básicos para leer el resto del texto, su lectura puede ser obviada por el lector con alguna experiencia.

El siguiente capítulo constituye el núcleo de este trabajo y contiene una clasificación de los grupos con órdenes de la forma $pq$ y $pq^2$e impares de la forma $p^3$ mediante el uso de una de las extensiones más conocidas, el producto semidirecto de un grupo $H$ por un grupo $G$. Hemos separado la clasificación de los grupos de órdenes 30, 8, 16 y 24, debido a que en estos casos la complejidad de la factorización en primos de éstos órdenes se refleja directamente en la estructura de los grupos en cuestión, excepto en el caso de orden 8, que fue separado con el propósito de ilustrar el uso de las extensiones cíclicas en la clasificación de grupos de un orden dado.

[6]Sería de gran interés, si fuera posible para dar una visión general del toda la colección de grupos simples finitos.

# 2 Nociones Básicas.

El propósito de este capítulo es presentar al lector un compendio de resultados y definiciones que constituirán los bloques primarios sobre los que se construirá el presente trabajo y en su mayoría constituyen resultados estándar de un primer curso de Teoría de Grupos, por lo que las pruebas de éstos serán prácticamente omitidas, referimos al lector interesado en éstas a los libros listados en la bibliografía.

Primeramente, recordamos que un ***grupo*** $G$ es un conjunto con una operación binaria (denotada simplemente como yuxtaposición y entendida como una multiplicación, siempre que no exista confusión posible) que cumple con las siguientes propiedades:

1. Dados $g, h, k \in G$, $g(hk) = (gh)k$.
2. *E*xiste $1 \in G$ tal que $1g = g1 = g$ para toda $g \in G$, este elemento es llamado la ***identidad*** o ***elemento idéntico*** de $G$.
3. Para cada $g \in G$, existe un elemento $g^{-1} \in G$ (denominado ***inverso de*** $g$) tal que $gg^{-1} = g^{-1}g = 1$.

No es difícil verificar la unicidad de los elementos 1, $g^{-1}$ descritos en (2), (3) respectivamente.

De (1) se sigue que dados $g_1, ...g_n \in G$, el producto $g_1...g_n$ queda unívocamente determinado. Sin embargo, es importante notar que en general, el orden en el que aparecen dichos elementos es de gran importancia; pues si $g, h \in G$, éstos no necesariamente ***conmutan*** (i.e. $gh = hg$). Cuando dicha condición es válida para todos los elementos de $G$, decimos que el grupo es ***abeliano*** o ***conmutativo*** y es usual denotar la operación en $G$ aditivamente; si no es este el caso, decimos que $G$ es ***no abeliano***. De manera más general, podemos definir el ***conmutador*** de $g, h$ como $[g, h] = ghg^{-1}h^{-1}$, es evidente que $g$ y $h$ conmutan si y solamente si $[g, h] = 1$.

Si $g \in G$, $n \in \mathbb{N}$, definimos $g^n$ inductivamente como $g^0 = 1$ y $g^{n+1} = g^n g$ y $g^{-n} = (g^{-1})^n$, en un grupo abeliano denotado aditivamente, escribimos $ng$ en lugar de $g^n$ con

$n \in \mathbb{Z}$. Es un ejercicio sencillo de inducción mostrar que son válidas las leyes usuales de los exponentes. Decimos que $g \in G$ es de ***orden finito*** si existe $m \in \mathbb{N}\backslash\{0\}$, tal que $g^m = 1$. En esta situación, definimos el ***orden*** de $g$ como el menor entero positivo $n$ tal que $g^n = 1$ y escribimos $|g| = n$, de no existir tal $n$, definimos $|g| = \infty$ y se dice que $g$ es de ***orden infinito***. Es una consecuencia inmediata del algoritmo de la división que $g$ es de orden $n$ si y sólo si $1, g, ..., g^{n-1}$ son elementos distintos de $G$ y $g^n = 1$.

Definimos también el ***orden*** de $G$ ($|G|$) como la cardinalidad del conjunto subyacente. Es claro que todos los elementos de un grupo finito son de orden finito; sin embargo, existen grupos infinitos que cumplen esta propiedad (denominados ***periódicos***). Si nos encontramos en el caso opuesto, es decir, si todos los elementos distintos de la identidad (llamados ***no triviales***) son de orden infinito, decimos que el grupo es ***libre de torsión***.

Llamamos a $H \subseteq G$ un ***subgrupo*** de $G$ ($H \leq G$), si $H$ es un grupo con la operación de $G$ restringida a $H$. Es elemental ver que esto es equivalente a pedir que $H$ cumpla:

1. $H \neq \emptyset$.
2. Si $g, h \in H$, $gh \in H$.
3. Para toda $g \in H$, $g^{-1} \in H$.

Claramente (2) y (3) son equivalentes a pedir que $gh^{-1} \in H$, siempre que $g, h \in H$; y si $G$ es finito, un subconjunto no vacío $H$ es un subgrupo de $G$ si y sólo si para cualesquiera $g, h \in H$, $gh \in H$. Es obvio que para cualquier grupo $G$, $\{1\}$ y $G$ son subgrupos de éste, llamados triviales; denominamos a $\{1\}$ el subgrupo ***idéntico*** de $G$ y lo denotamos como $\mathbf{1}$ por simplicidad, para $H, K \leq G$ denotamos $\mathrm{Lat}[H, K] := \{L \leq G : H \leq L \leq K\}$. Todos los subgrupos de un grupo finito son finitos; en contraste, en un grupo infinito, siempre existen grupos de orden finito e infinito, en particular $\mathbf{1}$ y $G$. De manera similar, todo subgrupo de un grupo abeliano es abeliano, mientras que en el caso no abeliano siempre se tienen de ambos tipos. Si $H$ está contenido propiamente en $G$ ($H \subsetneq G$), escribimos $H < G$. Evidentemente si $K \leq H$ y $H \leq G$, se tiene que$K \leq G$; y si $H, K \leq G$, entonces $H \cap K \leq G$, y en general, la intersección de cualquier familia de subgrupos también es un subgrupo.

El siguiente teorema, conocido como Teorema de Lagrange, es uno de los resultados más importante referente a subgrupos de grupos finitos y fue enunciado en una versión

particular por Joseph L. Lagrange, sin prueba, en su artículo *Réflexions sur la résolution algébrique des équations* (1772); sin embargo, se cree que la primera prueba del hecho general fue dada por Évariste Galois (hacia 1830).

**Teorema 2.1** (Teorema de Lagrange)**.** *En un grupo finito $G$, para todo $H \leq G$, $|H|$ divide a $|G|$.*

Si $X$ es un subconjunto de $G$, definimos $\langle X \rangle$, el ***subgrupo de*** $G$ ***generado por*** $X$, como la intersección de todos los subgrupos en los que $X$ está contenido. Esta intersección es no vacía, ya que al menos $G$ es un intersecando; además es en efecto un subgrupo, pues como se ha comentado arriba, la intersección de una familia de subgrupos de $G$ es un subgrupo de $G$; por supuesto si $X \leq G$, entonces $\langle X \rangle$ es simplemente $X$. Convenimos en escribir $\langle x_1, ..., x_n \rangle$ en lugar de $\langle \{x_1, ..., x_n\} \rangle$.

**Proposición 2.2.** *Sea $X$ un subconjunto no vacío de un grupo $G$. Entonces $\langle X \rangle$ consiste en todos los productos de la forma $x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n}$, donde $n \in \mathbb{N} \backslash \{0\}$, $x_i \in X$ y $\epsilon_i = \pm 1$ para cada $i \in \{1, ..., n\}$.*

Un grupo $G$ es llamado ***cíclico*** si existe $g \in G$ tal que $\langle g \rangle = G$. Si $G$ es cíclico y $\langle g \rangle = G$, $g$ se llama ***generador*** de $G$. De la proposición anterior, $\langle g \rangle = \{g^n | n \in \mathbb{Z}\}$ y por las leyes de los exponentes, cualquier grupo cíclico es abeliano. (No obstante, escribiremos generalmente los grupos cíclicos de manera multiplicativa.) Si $g$ es de orden finito $n$, $\langle g \rangle = \{1, ..., g^{n-1}\}$ y por lo tanto $|\langle g \rangle| = n$. Si $g$ es de orden infinito, $\langle g \rangle$ es un grupo abeliano infinito libre de torsión. Cualesquiera dos grupos cíclicos del mismo orden son *isomorfos*, en un sentido que se definirá un poco más adelante. El grupo cíclico infinito canónico es $\mathbb{Z}$, mientras que el cíclico canónico de orden $n$ es $\mathbb{Z}_n (= \mathbb{Z}/n\mathbb{Z})$, el grupo aditivo de clases residuales módulo $n$.

Por el teorema de Lagrange, el orden de cualquier elemento de un grupo divide al orden de éste; en particular, un grupo de orden primo debe ser cíclico generado por cualquiera de sus elementos no triviales.

En general, el siguiente teorema caracteriza a los grupos cíclicos finitos y describe la estructura de sus subgrupos.

**Teorema 2.3.** *Sea $G$ un grupo finito de orden $n$, $G$ es cíclico si y sólo si para cada divisor $d$ de $n$, existe exactamente un subgrupo de orden $d$.*

Se puede fortalecer ligeramente el teorema 2.3 de la manera siguiente.

**Teorema 2.4.** *Sea $G$ un grupo abeliano finito, entonces $G$ es cíclico si y sólo si para cada divisor $d$ del orden de $G$, existe a lo más un subgrupo de $G$ de ese orden.*

Si $X$ y $Y$ son subconjuntos de un grupo $G$, definimos el producto de $X$ y $Y$ como $XY = \{xy | x \in X, y \in Y\}$. Podemos extender esta definición de la manera obvia a un número finito de subconjuntos. De manera análoga al producto de elementos, la asociatividad de la operación en $G$ provee un significado único para la expresión $X_1 ... X_n$. Definimos también $X^{-1} = \{x^{-1} | x \in X\}$. Por supuesto, si $H$ es un subconjunto no vacío de $G$, éste será subgrupo de $G$ si y sólo si $HH = H$ y $H^{-1} = H$. Más aún, no es difícil probar el siguiente resultado.

**Proposición 2.5.** *Si $H, K \leq G$, $HK$ es subgrupo de $G$ si y solamente si $HK = KH$.*

Aunque en general el producto de subgrupos no es un subgrupo, la siguiente proposición establece el orden de $HK$.

**Proposición 2.6.** *Si $H$ y $K$ son subgrupos finitos de un grupo $G$, entonces $|HK| = |H||K|/|H \cap K|$.*

Si $H \leq G$ y $g \in G$, escribimos $gH := \{g\}H$ y llamamos a este subconjunto, ***clase lateral izquierda de $H$ en $G$***; de manera similar, $Hg := H\{g\}$ es llamada ***clase lateral derecha de $H$ en $G$***. Los conjuntos $G/H_I := \{gH\}_{g \in H}$ y $G/H_D := \{Hg\}_{g \in G}$ constituyen particiones de $G$ cuyos elementos tienen todos cardinalidad $|H|$; además existe una correspondencia biyectiva entre ambas particiones, digamos $gH \mapsto (gH)^{-1} = Hg^{-1}$, por lo que $|G/H_I| = |G/H_D|$. Denotamos $[G : H] := |G/H_I|$ y llamamos a éste, el ***índice de $H$ en $G$***.

En particular, en el caso finito, $H$ induce una partición de $G$ en $[G : H]$ clases laterales de cardinalidad $|H|$, i.e. $|G| = |H|[G : H]$ (este hecho constituye la prueba clásica del teorema de Lagrange). Generalmente, denotaremos el conjunto de clases laterales izquierdas simplemente como $G/H$ y llamamos a éste el ***espacio de clases laterales de $H$ en $G$***.

Podemos usar esta definición para dar una descripción general de los grupos cíclicos.

**Teorema 2.7.** *Sea $G = \langle g \rangle$ un grupo cíclico finito (infinito), entonces:*

1. *Para cada divisor $d$ del orden de $G$ (para todo $d \in \mathbb{N}$), existe exactamente un subgrupo de índice $d$, a saber $\langle g^d \rangle$. (Más aún, todo subgrupo de $G$ es de índice finito).*
2. *Sean $H$ y $K$ subgrupos de $G$ de índices $d$ y $e$ respectivamente, entonces $H \cap K$ es un subgrupo de índice $[d, e]$, donde $[d, e]$ denota el mínimo común múltiplo de $d$ y $e$.*
3. *Si $H$, $K$ son subgrupos de $G$ con $[G : H] = d$, $[G : K] = e$, entonces el producto de $H$ y $K$ es un subgrupo de $G$ de índice $(d, e)$, donde $(d, e)$ denota el máximo común divisor de $d$ y $e$.*

La siguiente generalización del teorema de Lagrange es llamado frecuentemente "factorización de índices".

**Teorema 2.8.** *Si $K \leq H \leq G$, entonces $[G : K] = [G : H][H : K]$.*

Llamamos a $N \leq G$ ***normal*** en $G$, si para todo $g \in G$, $gN = Ng$ (equivalentemente $gNg^{-1} \subseteq N$). Los subgrupos **1** y $G$ siempre son normales en $G$; y si $G$ es abeliano, todos sus subgrupos serán normales. Un grupo no trivial en el que ningún subgrupo propio no trivial es normal, es llamado ***simple***, por ejemplo los grupos de orden primo son simples. Si $N$ es normal en $G$, escribimos $N \trianglelefteq G$, reservando $N \triangleleft G$ para el caso en el que $N$ es subconjunto propio de $G$.

Observemos que si $N \trianglelefteq G$ y $H$ es un subgrupo de $G$, $NH = HN$ y así, $NH \leq G$. Más aún, se tiene la siguiente proposición.

**Proposición 2.9.** *Sean $H$ y $K$ subgrupos de un grupo $G$. Si $K \trianglelefteq G$, entonces $HK \leq G$ y $H \cap K \trianglelefteq H$; si además $H \trianglelefteq G$, entonces $H \cap K$ y $HK$ también serán subgrupos normales de $G$.*

Si ahora consideramos $H$ un subgrupo de índice 2 en $G$, para cualquier elemento de $G$ tal que $g \notin H$, $gH \dot{\cup} H = G = Hg \dot{\cup} H$, por lo que $gH = Hg$, por lo tanto hemos demostrado el siguiente enunciado.

**Proposición 2.10.** *Todo subgrupo de índice 2 es normal.*

Aunque un subgrupo arbitrario $H$ no sea normal en un grupo $G$, se tiene que el conjunto $N_G(H) = \{g \in G | gHg^{-1} = H\}$ es un subgrupo de $G$ en virtud de la observación

posterior a la definición de subgrupo y además $H \trianglelefteq N_G(H)$. Este subgrupo es llamado el ***normalizador de*** $H$ ***en*** $G$.

La condición de normalidad es justamente la condición necesaria para proveer al espacio de clases laterales de una estructura de grupo bajo la operación de producto de subconjuntos, el enunciado formal se puede formular como sigue:

**Teorema 2.11.** *Si $N \leq G$, se tiene que el espacio de clases laterales $G/N$ es un grupo bajo la operación $g_1Ng_2N = \{g_1n_1g_2n_2 | n_1, n_2 \in N\}$ si y sólo si $N \trianglelefteq G$. Llamamos a $G/N$ el* ***grupo cociente*** *de $G$ por $N$.*

La identidad en $G/N$ es $N$, mientras que $g^{-1}N$ es el inverso de $gN \in G/N$. Si $G$ es abeliano, $G/N$ es un grupo abeliano.

Si $g$ y $h$ son elementos de un grupo $G$, definimos el ***conjugado de*** $h$ ***por*** $g$ como $h^g := ghg^{-1}$, llamamos a $h^G := \{h^g | g \in G\}$ la ***clase de conjugación de*** $h$ ***en*** $G$ y diremos que $h$ y $k$ son ***conjugados*** si $h \in k^G$, las clases de conjugación conforman una partición de $G$. Es claro que un subgrupo $N \leq G$ es normal en $G$ si y solamente si $N$ es unión de clases conjugadas.

Un ***homomorfismo*** o simplemente ***morfismo*** entre los grupos $G$, $H$ es una función $\phi : G \to H$ tal que $\phi(xy) = \phi(x)\phi(y)$; es decir, una función que preserva la estructura de los grupos. Si $\phi$ es un homomorfismo, entonces $\phi(1) = 1$ y $\phi(x^n) = \phi(x)^n$, donde $x \in G$, $n \in \mathbb{Z}$; además si $x \in G$, entonces el orden de $\phi(x)$ divide al orden de $x$.

Denotamos al conjunto de homomorfismos de $G$ en $H$ como $Hom(G, H)$ y definimos $End(G) := Hom(G, G)$, los elementos de este conjunto son llamados ***endomorfismos*** de $G$. El ***homomorfismo trivial*** es la función que asigna a cada elemento de $G$ la identidad en $H$ y siempre es un elemento de $Hom(G, H)$, por lo que siempre $Hom(G, H) \neq \emptyset$. Un homomorfismo de grupos $\phi : G \to H$ es llamado ***monomorfismo*** si es inyectivo, ***epimorfismo*** si es suprayectivo e ***isomorfismo*** si es biyectivo, en esta última situación escribimos $\phi : G \xrightarrow{\sim} H$ (notemos que en este caso, $\phi^{-1}$ también es un isomorfismo). Se tiene la siguiente proposición referente a homomorfismos y conjuntos generadores.

**Teorema 2.12.** *Si $G$ y $H$ son grupos y $X = \{x_\alpha\}_{\alpha \in A} \subseteq G$ es un conjunto de generadores de $G$, para cualesquiera $\phi, \psi \in Hom(G, H)$, $\phi = \psi$ si y solamente si $\phi(x_\alpha) = \psi(x_\alpha)$ para cada $\alpha \in A$.*

Si $G$ y $H$ son grupos y $\phi : G \xrightarrow{\sim} H$, decimos que $G$ y $H$ son ***isomorfos*** y lo abreviamos como $G \cong_\phi H$ o $G \overset{\phi}{\cong} H$; y escribimos simplemente $G \cong H$, si $G \cong_\phi H$ para alguna $\phi$. La noción de isomorfismo induce una "relación" en la clase de los grupos tal que dados los grupos $G$, $H$, $K$, se tiene que $G \cong G$, $G \cong H$ implica $H \cong G$ y si $G \cong H$ y $H \cong K$, entonces $G \cong K$. Podemos entonces hablar de la ***clase de isomorfismo*** a la que un grupo pertenece y dos grupos que pertenezcan a la misma clase pueden ser considerados prácticamente idénticos en el sentido de que cualquier proposición hecha acerca de la estructura de un grupo será verdadera para cualquier elemento de la clase de isomorfismo de éste. Si decimos que un grupo con ciertas propiedades es ***único*** nos referimos a que es ***único salvo isomorfismo***.

Introducimos a continuación algunos ejemplos estándar.

- Si $G$ y $H$ son grupos arbitrarios, sus subgrupos triviales son isomorfos via la única función que existe entre estos conjuntos.
- Sean $G = \langle g \rangle$ y $H = \langle h \rangle$ dos grupos cíclicos finitos tales que el orden de $|H| = k|G|$, con $k \in \mathbb{Z}$, definimos $\phi : G \to H$ como $\phi(g^i) = h^{ki}$ para $i \in \mathbb{Z}$. Se tiene que $\phi$ es un monomorfismo, de lo que se sigue que cualesquiera dos grupos cíclicos finitos del mismo orden son isomorfos. En particular, cualquier grupo cíclico de orden $n$ es isomorfo a $\mathbb{Z}_n$, y para cada primo $p$ existe un único grupo con este orden. Usaremos $C_n$ para hablar de $\mathbb{Z}_n$ denotado multiplicativamente.
- Sean $G$ un grupo, $H \leq G$ y $g \in G$. El ***conjugado de*** $H$ ***por*** $g$ es el *subgrupo* $gHg^{-1} := \{h^g | h \in H\}$. Decimos que $K \leq G$ es un conjugado de $H$ en $G$ o que $K$ y $H$ son conjugados, si existe $g \in G$ tal que $gHg^{-1} = K$. Es claro que dos subgrupos conjugados son isomorfos, porque conjugar por un elemento de un grupo es un isomorfismo.
- Sea $G$ un grupo y $N \trianglelefteq G$. Existe una correspondencia natural entre $G$ y el grupo cociente $G/N$, a saber $\eta : G \to G/N$, definida como $\eta(g) = gN$. Es fácil verificar que $\eta$ es un epimorfismo, llamado ***epimorfismo natural*** de $G$ en $G/H$.

Si $\phi : G \to H$ es un homomorfismo, definimos el núcleo de $\phi$ como el conjunto $\ker\phi := \{g \in G | \phi(g) = 1\}$ , denotamos la imagen de la función $\phi$ como $\text{im}\phi$ o $\phi(G)$; y en general, si $K \leq G$, $L \leq H$, $\phi(K) := \{\phi(k) | k \in K\}$ y $\phi^{-1}(L) := \{g \in G | \phi(g) \in L\}$, en ambos casos los subconjuntos son subgupos de los grupos donde están contenidos. En el caso particular del epimorfismo natural $\eta : G \mapsto G/N$, $\ker\eta = N$ y si $K \leq G$,

$\eta(K) = KN/N$.

**Proposición 2.13.** *Si $\phi : G \to H$ es un homomorfismo de grupos, entonces $ker\phi \trianglelefteq G$ y $\phi(K) \leq H$, $\phi^{-1}(L) \leq G$ para cualesquiera $K \leq G$, $L \leq H$.*

La siguiente proposición es la piedra angular de la teoría de grupos.

**Teorema 2.14.** *[Teorema Fundamental de Homomorfismo]*

*Si $G$ y $H$ son grupos y $\phi : G \to H$ es un homomorfismo, existe un único isomorfismo $\psi : G/K \to \phi(G)$, tal que $\phi = \psi \circ \eta$, donde $K = ker\phi$ y $\eta : G \to G/K$ es el epimorfismo natural.*

Los siguientes resultados también son de gran importancia y su demostración se sigue del teorema fundamental.

**Teorema 2.15.** *[Primer Teorema de Isomorfismo] Si $G$ es un grupo, $N \trianglelefteq G$ y $H \leq G$, entonces $HN/N \cong H/H \cap N$.*

**Teorema 2.16.** *[Segundo Teorema de Isomorfismo] Si $G$ es un grupo y $H$ y $K$ son subgrupos normales de $G$ tales que $K \leq H$, entonces $G/H \cong (G/K)/(H/K)$.*

**Teorema 2.17.** *[Teorema de la Correspondencia] Si $\phi : G \to H$ es un epimorfismo con $K := ker\phi$, $\phi$ induce una correspondencia biyectiva $\pi : Lat[K, G] \to Lat[\mathbf{1}, H]$. Si $K \leq L \leq G$, esta correspondencia manda $L$ en $\phi(L)$ y si $L \leq H$, $\pi(\phi^{-1}(L)) = L$. Más aún, si $K_1, K_2 \in Lat[K, G]$:*

1. $K_1 \leq K_2$ si y sólo si $\phi(K_1) \leq \phi(K_2)$, y en este caso $[K_2 : K_1] = [\phi(K_2) : \phi(K_1)]$.
2. $K_1 \trianglelefteq K_2$ si y solamente si $\phi(K_1) \trianglelefteq \phi(K_2)$, y en esta situación, la función de $K_2/K_1$ en $\phi(K_2)/\phi(K_1)$ tal que $xK_1 \mapsto \phi(x)\phi(K_1)$ es un isomorfismo.

Como una consecuencia del teorema de la correspondencia, tenemos que si $G$ es un grupo y $N \trianglelefteq G$, entonces todos los subgrupos de $G/N$ son de la forma $H/N$, con $H \in \mathrm{Lat}[N, G]$.

### Automorfismos.

Un endomorfismo biyectivo de un grupo $G$ es llamado ***automorfismo*** de $G$, y el conjunto de éstos es denotado como $Aut(G)$. Si $\phi$ y $\psi$ son automorfismos de $G$, $\phi \circ \psi$ y $\phi^{-1}$también son automorfismos y $Aut(G)$ tiene una estructura de grupo bajo la composición, motivo por el cual a veces denotaremos $\phi\psi := \phi \circ \psi$, $Aut(G)$ es llamado el ***grupo de automorfismos de*** $G$**.**

Para cada $g \in G$, podemos definir el homomorfismo $\varphi_g : G \to G$ mediante $\varphi_g(x) := x^g = gxg^{-1}$, no es difícil ver que éste es de hecho biyectivo y por consiguiente $\varphi_g \in Aut(G)$. Estos automorfismos son llamados ***automorfismos interiores de*** $G$ y se tiene que $\varphi_g\varphi_h = \varphi_{gh}$ para cualesquiera $g, h \in G$; consecuentemente, tenemos un homomorfismo de $G$ en $Aut(G)$, cuya imagen $Inn(G)$ es conocida como el ***grupo de automorfismos interiores de*** $G$, mientras que su núcleo $Z(G)$ es llamado el ***centro de*** $G$. Obsérvese que $Z(G)$ consiste en todos los elementos de $G$ que conmutan con cualquier otro elemento de $G$ y claramente $G$ es abeliano si y sólo si $G = Z(G)$. De lo anterior, obtenemos el siguiente importante resultado acerca de la estructura de $Inn(G)$.

**Proposición 2.18.** *$Inn(G) \cong G/Z(G)$.*

El subgrupo $Z(G)$ también provee esta sencilla clasificación de los grupos abelianos.

**Proposición 2.19.** *Un grupo $G$ es abeliano si y sólo si $G/Z(G)$ es cíclico.*

Aunque un elemento $x \in G$ no sea ***central*** (i.e. $x \in Z(G)$), siempre existen elementos con los cuales conmuta, por ejemplo el idéntico de $G$; más aún, es sencillo verificar que el ***centralizador de*** $x$ ***en*** $G$, $C_G(x) := \{g \in G | gx = xg\}$ es un subgrupo de $G$. En general si $H \leq G$, definimos el centralizador que $H$ en $G$ como $C_G(H) := \bigcap_{h \in H} C_G(h)$ y es inmediato que $C_G(H) \trianglelefteq N_G(H)$.

Si $\sigma \in Aut(G)$ y $\varphi_g \in Inn(G)$, no es dificil hacer ver que $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)} \in Inn(G)$ y en consecuencia $Inn(G) \trianglelefteq Aut(G)$. $Out(G) := Aut(G)/Inn(G)$ es llamado el ***grupo de automorfismos exteriores de*** $G$; sin embargo, el término ***automorfismo exterior*** se usa para denominar a un elemento $\psi \in Aut(G) \backslash Inn(G)$. Si $G$ es abeliano, todos sus automorfismos no triviales serán exteriores, ya que $Inn(G) = \mathbf{1}$.

A lo largo del presente trabajo, frecuentemente nos encontraremos con el problema de determinar el grupo de automorfismos de un grupo dado, este es en general un problema difícil, sin embargo en el caso de un grupo cíclico, el más usual con el que trataremos, la situación es más bien fácil.

Sea $G = \langle g \rangle \cong C_\infty$ y sea $\phi \in Aut(G)$, $\phi(g)$ debe generar $G$; pero los únicos generadores de $G$ son $g$ y $g^{-1}$. Así, o bien $\phi$ fija todos los elementos de $G$, o envía cada uno a su inverso, y por lo tanto, $Aut(G) \cong C_2$.

Sean ahora $n \in \mathbb{N}\backslash\{0\}$ y $G = \langle g \rangle \cong C_n$. Si $\phi \in End(G)$, necesariamente $\phi(g) = g^m$, para alguna $0 \leq m < n$, se sigue de las observaciones posteriores a la definición de homomorfismo y el teorema 2.12 que $End(G) = \{\sigma_m | 0 \leq m < n\}$, donde $\sigma_m(x) := x^m$ para todo $x \in G$.

**Teorema 2.20.** *Sean $G = \langle g \rangle \cong C_n$ y $\sigma_m \in End(G)$ como fue definido arriba para $0 \leq m < n$. $Aut(G)$ consiste exactamente en aquellos $\sigma_m$ para los cuales $(m, n) = 1$. Más aun, $Aut(G)$ es abeliano e isomorfo a $\mathbb{Z}_n^\times$, el grupo de unidades del anillo de enteros módulo $n$.*

Definimos la función de Euler como $\bar{\phi} : \mathbb{N}\backslash\{0\} \to \mathbb{N}$ tal que

$$\bar{\phi}(n) = |\{m \in \mathbb{Z} | 1 \leq m \leq n \text{ y } (m, n) = 1\}|$$

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ con cada $p_i$ un primo, $p_i \neq p_j$ si $i \neq j$ y $\alpha_i > 0$, se tiene que

$$\bar{\phi}(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) ... (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = \prod_{l=1}^{k} (p_l^{\alpha_l} - p_l^{\alpha_l - 1})$$

De donde se sigue inmediatamente que el orden de los automorfismos de $C_n$ es precisamente $\bar{\phi}(n)$. En particular $|Aut(C_p)| = p - 1$ cuando $p$ es primo; de hecho este grupo es cíclico, resultado establecido en la proposición 2.22, cuya demostración depende del siguiente lema.

**Lema 2.21.** *Si $F$ es un campo y $G$ es un subgrupo finito del grupo multiplicativo $F^\times$, entonces $G$ es cíclico.*

*Demostración.* Para demostrar que $G$ es cíclico utilizaremos el Teorema 2.4 y algunos resultados elementales de álgebra de polinomios.

Sea $d$ un divisor de $|G|$ y supongamos que existe $H \leq G$ de orden $d$, entonces los elementos de $H$ son raíces del polinomio $x^d - 1 \in F[x]$, que sabemos sólo puede tener a lo más $d$ raíces en $F$. Concluimos que de existir $H$, éste es el único subgrupo de $G$ de orden $d$. Se sigue inmediatamente que $G$ es cíclico. □

**Proposición 2.22.** *Si $p$ es un primo, entonces $Aut(C_p) \cong C_{p-1}$.*

*Demostración.* Como $Aut(C_p) \cong \mathbb{Z}_p^\times$ [Teorema 2.20] y $\mathbb{Z}_p$ es un campo, por el lema anterior, $\mathbb{Z}_p^\times$es cíclico y $|\mathbb{Z}_p^\times| = p - 1$. □

**Corolario 2.23.** *Si $p$ es un primo, $Aut(C_{p^2})$ es un grupo cíclico de orden $p(p-1)$.*

*Demostración.* Como claramente $Aut(C_4) \cong C_2$, entonces podemos asumir que $p$ es un primo impar; además por la proposición anterior, $\mathbb{Z}_p^\times \cong Aut(C_p) \cong C_{p-1}$; por lo tanto existe un elemento $m \in \mathbb{Z}_p^\times$ tal que $\langle m \rangle = \mathbb{Z}_p^\times$. Probaremos que $\langle m \rangle = \mathbb{Z}_{p^2}^\times$ o $\langle m+p \rangle = \mathbb{Z}_{p^2}^\times$, notemos primeramente que al tenerse que $m^c \equiv 1 \,(\mathrm{mod}\, p^2)$ y $(m+p)^d \equiv 1 \,(\mathrm{mod}\, p^2)$ implican $m^c \equiv (m+p)^d \equiv 1 \,(\mathrm{mod}\, p)$, obtenemos que los órdenes de $m$ y $m+p$ en $\mathbb{Z}_{p^2}^\times$ son múltiplos de $p-1$, el orden de $m$ y $m+p$ módulo $p$. Supongamos que tanto $\langle m \rangle$ como $\langle m+p \rangle$ fueran subgrupos propios de $\mathbb{Z}_{p^2}^\times$, entonces $|\langle m \rangle| = |\langle m+p \rangle| = p-1$, debido a que $\mathbb{Z}_{p^2}^\times$ tiene orden $\bar{\phi}(p^2) = p(p-1)$. Se sigue de lo anterior que

$$1 \equiv (m+p)^{p-1} \equiv m^{p-1} + m^{p-2}p(p-1) + p^2 \sum_{i=2}^{p-1} \binom{p-1}{i} m^{p-i-1} p^{i-2} \equiv 1 + m^{p-2}p(p-1) \,(\mathrm{mod}\, p^2),$$

que tiene como consecuencia inmediata que $m^{p-2}p(p-1) \equiv 0 \,(\mathrm{mod}\, p^2)$, por lo cual $p | m^{p-2}(p-1)$, entonces, al ser $(p, p-1) = 1$, obtenemos $m^{p-2} \equiv 0 \,(\mathrm{mod}\, p)$, que es una contradicción (ninguna de las potencias de los elementos de $\mathbb{Z}_p^\times$ puede ser congruente con 0 módulo $p$).

Concluimos que $\mathbb{Z}_{p^2}^\times$ tiene que estar generado por $m$ o $m+p$, es decir $\mathbb{Z}_{p^2}^\times \cong Aut(C_{p^2})$ es un grupo cíclico de orden $p(p-1)$ . □

Sea $\phi$ un automorfismo de un grupo $G$ y $H \leq G$, es claro que $\phi(H)$ es un subgrupo de $G$ isomorfo a $H$; decimos que $H$ es ***invariante bajo*** $\phi$, si $\phi(H) = H$. En este caso, la restricción de $\phi$ a $H$ es un automorfismo de $H$. Si $L$ es un subgrupo de $Aut(G)$, decimos que $H$ ***es invariante bajo*** $L$, si $H$ es invariante bajo cualquier $\phi \in L$. Con esta nueva terminología, $H$ es normal en $G$ si y solamente si $H$ es invariante bajo $Inn(G)$. Se dice

que $H$ es un ***subgrupo característico de*** $G$ si $H$ es invariante bajo $Aut(G)$. Por ejemplo, $Z(G)$ siempre es un subgrupo característico. De manera análoga, decimos que $g \in G$ es un ***elemento característico*** si $\phi(g) = g$ para cualquier $\phi \in Aut(G)$; si ahora consideramos $L \leq Aut(G)$ y la relación $\simeq_L$, defiinida como $g \simeq h$, si existe un elemento $\phi \in L$ tal que $\phi(g) = h$, observamos que como en el caso de la conjugación, esta es una relación de equivalencia; de hecho notemos que $g$ y $h$ son conjugados si y sólo si $g \simeq_{Inn(G)} h$. Decimos que dos elementos son ***automorfos*** si $g \simeq_{Aut(G)} h$. En particular las relaciones $\simeq_{Inn(G)}$ y $\simeq_{Aut(G)}$ inducen una partición de $G$, por lo que se tienen las siguientes ecuaciones.

$$\begin{aligned} |G| &= |Z(G)| + \sum_{g \in \Gamma_G} |g^G| \\ |G| &= |\chi(G)| + \sum_{g \in \tilde{\Gamma}_G} |g^{Aut(G)}| \end{aligned}$$

Donde $g^{Aut(G)}$ es la clase de equivalencia de $g$ bajo la relación $\simeq_{Aut(G)}$ y $\Gamma_G$, $\tilde{\Gamma}_G$ son conjuntos de representantes de las clases de equivalencia no triviales en cada caso, finalmente $\chi(G)$ denota el subgrupo formado por los elementos que permanecen fijos bajo todo automorfismo de $G$, llamados ***característicos***. La primera ecuación se conoce como la ***ecuación de clase de*** $G$.

Es claro que los subgrupos de $G$ invariantes bajo la acción de $Aut(G)$, llamados también ***característicos***, son normales; sin embargo lo opuesto no necesariamente es cierto, de hecho existen grupos abelianos no simples y no triviales que no tienen subgrupos característicos propios no triviales (Por ejemplo, $Aut(C_8)$ o un $p$-grupo abeliano elemental[1], ¿Puede el lector decir por qué?).

Mientras que la normalidad no es transitiva, se tiene que la propiedad de ser un subgrupo característico sí lo es.

**Proposición 2.24.** *Sean $G$ un grupo y $H \trianglelefteq G$. Si $K$ es un subgrupo característico de $H$, entonces $K \trianglelefteq G$. Si además $H$ es característico en $G$, entonces $K$ también lo es.*

Recordemos que si $g$ y $h$ son elementos de un grupo $G$, su conmutador es el elemento $[g, h] = ghg^{-1}h^{-1}$. Observemos que$[g, h]^{-1} = hgh^{-1}g^{-1} = [h, g]$; sin embargo, en

[1]Esta definición será proporcionada más adelante en el texto.

general, el producto de conmutadores no es un conmutador. Definimos el ***subgrupo derivado de*** $G$ como $G' := \langle\{[g,h]|g,h \in G\}\rangle$. Observemos que a partir de la anotación anterior y la Proposición 2.2 obtenemos que un elemento arbitrario de $G'$ es un producto finito de conmutadores.

**Lema 2.25.** *El subgrupo derivado $G'$ es un subgrupo característico de$G$, para calquier grupo $G$.*

La siguiente es una de las propiedades más importantes de $G'$.

**Proposición 2.26.** *Si $G$ es un grupo y $N \leq G$. Se tiene que $N \trianglelefteq G$ y $G/N$ es abeliano si y sólo si $G' \leq N$.*

Un grupo $P$ es llamado ***$p$-grupo***, si existe un primo $p$ tal que todos los elementos de $P$ tienen como orden una potencia de $p$; y si $G$ es un grupo arbitrario, los $p$-grupos contenidos en éste son llamados los ***$p$-subgrupos de*** $G$, a los $p$-subgrupos de $G$ de orden máximo se les conoce como ***$p$-subgrupos de Sylow de*** $G$ y la colección de éstos se denota como $Syl_p(G)$.

Los $p$-subgrupos de Sylow juegan un papel fundamental en la clasificación de los grupos de orden pequeño. El siguiente teorema proporciona una descripción general de las relaciones que guardan en un grupo finito y será una herramienta de suma importancia a lo largo de nuestra clasificación.

**Teorema 2.27.** *[Teoremas de Sylow] Si $G$ es un grupo finito y $p$ es un primo que divide a su orden, entonces:*

1. *$G$ tiene al menos un $p$-subgrupo de Sylow.*
2. *Todos los $p$-subgrupos de Sylow de $G$ son conjugados.*
3. *Todo $p$-subgrupo de $G$ está contenido en algún $p$-subgrupo de Sylow.*
4. *El número $r_p$ de subgrupos de Sylow de $G$ es congruente con 1 módulo $p$. Más aún, $r_p = [G : N_G(P)]$ para cada $P \in Syl_p(G)$, en particular $r_p$ divide a $[G : P]$.*

Este resultado data de 1871 y es debido al matemático noruego Ludwig Sylow, quien para demostrarlo utilizó el siguiente teorema de Cauchy que ahora es presentado en algunos textos como una consecuencia de los teoremas de Sylow.

**Teorema 2.28.** *[Teorema de Cauchy] Un grupo finito $G$ tiene un elemento de orden $p$, para cualquier primo $p$ que divida a su orden.*

Es una consecuencia inmediata de este teorema y el teorema de Lagrange que un grupo finito es un $p$-grupo si y solamente si su orden es una potencia de $p$. La siguiente sección estudia brevemente estos grupos.

### $p$-Grupos Finitos

Los Teoremas de Sylow y su anunciada importancia en nuestra clasificación de los grupos de orden pequeño atraen a nuestra atención el estudio de los $p$-grupos finitos, es por eso que en esta sección desarrollaremos algunos resultados relativos a éstos.

En lo sucesivo, $p$ denotará un primo, a menos que se indique lo contrario.

**Teorema 2.29.** *Si $P$ es un $p$-grupo finito no trivial y $N$ es un subgrupo normal no trivial de $P$, entonces*

- *$Z(P)$ es también no trivial*
- *$Z(P) \cap N \neq \mathbf{1}$*

*Demostración.* Por la ecuación de clase:

$$|P| = |Z(P)| + \sum_{g \in \Gamma_P} |g^P|$$

Como los elementos de la suma de la derecha son tomados fuera del centro de $P$ y éste es un $p$-grupo, se tiene que $p$ divide a $|P|$ y $\sum_{g \in \Gamma_P} |g^P|$, se sigue que $p$ divide a $|Z(P)| > 0$ y por lo tanto $Z(P) \neq \mathbf{1}$.

Para probar la segunda parte observemos que por la definición de normalidad, $N$ es una unión de clases de conjugación, por lo que se tiene que

$$|N| = |N \cap P| = |N \cap Z(P)| + \sum_{g \in \Gamma_P} |N \cap g^P|$$

para cada sumando de la derecha, $N \cap g^P = \emptyset$ o $N \cap g^P = g^P$, de lo que se desprende que $p$ divide a $\sum_{g \in P} |N \cap g^P|$ y por lo tanto también divide a $|N \cap Z(P)|$, es decir $N \cap Z(P) \neq \mathbf{1}$. □

**Corolario 2.30.** *Si $P$ es un $p$-grupo finito de orden $p^n$, entonces $P$ tiene subgrupos de orden $p^i$ para cada $i \in \{1, ..., n\}$.*

*Demostración.* Se sigue por indución sobre $n$ del teorema anterior y el terema de la correspondencia. □

Tenemos además esta sencilla consecuencia del Teorema 2.29.

**Corolario 2.31.** *Si $P$ es un $p$-grupo finito no trivial de orden $p^n$ y $M$ es un subgrupo maximal de éste, entonces $[P : M] = p$ y $M \lhd P$.*

*Demostración.* La demostración se hará por inducción sobre $n$. El caso base $n = 1$ es inmediato. Notemos primero que si $M$ es un subgrupo maximal de $P$ y $Z$ es un subgrupo de $Z(P)$ de orden $p$, entonces se tiene que $Z \cap M = \mathbf{1}$ o $Z \leq M$. En el primer caso $ZM = P$, por ser $M$ un subgrupo maximal y $Z$ normal en $P$, se sigue inmediatamente de esto que $M \lhd P$ y, por el primer teorema de isomorfismo, $P/Z \cong M/Z \cap M \cong M$ y por lo tanto $[P : M] = p$. En el segundo caso $P/Z$ es un subgrupo de orden $p^{n-1}$ y $M/Z$ es un subgrupo maximal [Teorema 2.17], de la hipótesis de inducción se desprende que $M/Z$ es de índice $p$ y es normal; por el teorema de la correspondencia $M$ es un subgrupo normal de $P$ de índice $p$. □

**Proposición 2.32.** *Si $G$ es un grupo abeliano finito escrito multiplicativamente tal que para algún primo $p$, $x^p = 1$ para cada $x \in G$, entonces $G$ tiene estructura de espacio vectorial sobre el campo $\mathbb{Z}_p$; más aún, $Aut(G) \cong GL(n, p)$, donde $n = dim_{\mathbb{Z}_p}(G)$. En particular $G$ es isomorfo a $C_p^n$.*

*Demostración.* Si $x, y \in G$, definimos $x + y := xy$ y si $\alpha \in \mathbb{Z}_p$, $\alpha \cdot x := x^a$, donde $a \in \mathbb{Z}$ pertenece a la clase $\alpha \in \mathbb{Z}_p$, esta operación está bien definida, pues si $a, b \in \alpha$, $a = b + kp$ p.a. $k \in \mathbb{Z}$ y consecuentemente $x^a = x^{b+kp} = x^b(x^k)^p = x^b$, las propiedades aditivas de espacio vectorial se siguen de que $G$ es un grupo abeliano, las propiedades restantes son simplemente un replanteamiento de las leyes de los exponentes.

Es inmediato de lo anterior que cualquier endomorfismo de $G$ será una transformación lineal de $G$ en $G$, por lo tanto $Aut(G)$ coincide con el grupo de isomorfismos de espacio vectorial de $G$ en si mismo, i.e. $Aut(G) = GL(G) \cong GL(n, p)$, donde $n = dim_{\mathbb{Z}_p}(G)$.

Recordemos para finalizar que como cualesquiera dos espacios vectoriales de la misma dimensión sobre el mismo campo son isomorfos como espacios vectoriales, en particular son isomorfos como grupos, y así $G \cong C_p^n \cong \mathbb{Z}_p^n$. □

**Corolario 2.33.** *Si $p$ es un primo, todo grupo $G$ de orden $p^2$ es isomorfo a $C_{p^2}$ o a $C_p \times C_p$.*

*Demostración.* Basta demostrar que todo grupo de orden $p^2$ es abeliano; ya que si esto se tuviera, entonces todos los elementos no triviales de un grupo no cíclico de este orden tendrían orden $p$.

Observemos que al ser $G$ un $p$-grupo no trivial, entonces $Z(G) \neq \mathbf{1}$ [Proposición 2.29]. Tenemos entonces que $|G/Z(G)| \leq p$, lo que implica que este grupo es cíclico. Concluimos mediante la proposición 2.19 que $G$ es un grupo abeliano. □

Dada la importancia y recurrencia del caso en el que $p = 2$, definimos $V := C_2 \times C_2$;[2] $V$ viene del vocacablo Vierergruppe, que significa grupo de cuatro en alemán, nombrado así por Felix Klein en su artículo Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade (1884).

Por su utilidad a lo largo del trabajo, incluiremos aquí el siguiente resultado, que se vale de conocimientos básicos de Álgebra Lineal.

**Proposición 2.34.** *Sea $n \in \mathbb{N}\backslash\{0\}$, y sea $p$ un primo. Entonces*

$$|GL(n,p)| = \prod_{k=1}^{n}(p^n - p^{k-1}) = p^{\frac{n(n-1)}{2}} \prod_{k=1}^{n}(p^k - 1)$$

*Demostración.* Para obtener $|GL(n,p)|$, basta contar el número de matrices invertibles de $n \times n$ con coeficientes en $\mathbb{Z}_p$ y para determinar una matriz de éste tipo, basta escoger una base $\{v_1, ..., v_n\}$ de $\mathbb{Z}_p^n$ que constituirá las columnas de la matriz en cuestión; por tanto, para la primer columna es posible escoger cualquier vector no nulo, es decir, tenemos $p^n - 1$ opciones; para la siguiente debemos tomar algún vector que no sea linealmente dependiende con el primero, es decir, cualquiera de los $(p^n - p)$ que no esté en el espacio generado por $v_1$; podemos continuar de manera análoga para concluir

[2] Usualmente, $V$ es utilizado para denotar un subgrupo específico del grupo de permutaciones $S_4$; sin embargo en este texto esots grupos se han evitado deliberadamente, es por eso que hemos optado por esta definición alternativa.

que la $k$-ésima columna debe ser uno de los $p^n - p^{k-1}$ elementos que no están en el subespacio generado por $\{v_1, ..., v_{k-1}\}$.

Concluimos que $|GL(n,p)| = \prod_{k=1}^{n} (p^n - p^{k-1}) = p^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} (p^k - 1)$. □

# 3 Extensiones

## 3.1. Producto Directo

Dados dos grupos $H$ y $K$, llamamos a un grupo $G$ una ***extensión de*** $H$ ***por*** $K$, si $H$ es isomorfo a $H'$ un subgrupo normal de $G$ y $G/H' \cong K$. El primer ejemplo que veremos de una extensión de grupos es el llamado ***producto directo (exterior) de*** $H$ ***por*** $K$, que no es otra cosa que el producto cartesiano dotado de una multiplicación *componente a componente.* Formalmente, $H \times K := \{(h,k)|h \in H, k \in K\}$ con $(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2)$. Podemos generalizar esta idea y hablar del ***producto directo (exterior)*** de los grupos $G_1, ..., G_n$, definiendo en $G_1 \times ... \times G_n$ la operación $(g_1, ..., g_n)(g_1', ..., g_n') = (g_1g_1', ..., g_ng_n')$. Se tiene en esta situación que $(1, ..., 1)$ es el elemento idéntico del grupo y $(g_1^{-1}, ..., g_n^{-1})$ es el inverso de $(g_1, .., g_n) \in G_1 \times ... \times G_n$.

Observamos que $G := G_1 \times ... \times G_n$ tiene las siguientes propiedades:

- Para cada $i$, $G$ tiene un subgrupo normal $H_i$ que es isomorfo a $G_i$; específicamente, $H_i := \{(1, ..., g_i, ..., 1)| \mid g_i \in G_i\}$ (donde $g_i$ aparece en el $i-$ésimo lugar). Mas aún, $G/H_i$ es isomorfo al producto de los $G_j$ restantes[1].
- Todo $g \in G$ tiene una expresión única de la forma $h_1h_2...h_n$, donde $h_i \in H_i$; si $g = (g_1, ..., g_n)$, $h_i = (1, ..., g_i, ..., 1)$ para cada $i$ (de nuevo, aquí $g_i$ aparece en el $i-$ésimo lugar). Consecuentemente, si los grupos $G_1, ..., G_n$ son finitos, entonces $|G| = |G_1||G_2|...|G_n|$.

Supóngase ahora que $G$ es un grupo con subgrupos $H_1, ..., H_n$ tales que $H_i \trianglelefteq G$ para cada $i \in \{1, ..., n\}$. Se afirma que las siguientes son equivalentes:

[1]La observación se sigue de que

$$G_1 \times ... \times G_n \ni (g_1, ..., g_n) \mapsto (g_1, ..., g_{i-1}, g_{i+1}, ..., g_n) \in G_1 \times ... \times G_{i-1} \times G_{i+1} \times ... \times G_n$$

es un homomorfismo de grupos con nucleo $H_i$, cuya imagen es claramente $G_1 \times ... \times G_{i-1} \times G_{i+1} \times ... \times G_n$.

1. Todo $g \in G$ tiene una única expresión $g = h_1...h_n$, donde cada $h_i \in H_i$.
2. $G = H_1...H_n$ y para cada $i$, $H_i \cap H_1...H_{i-1}H_{i+1}...H_n = \mathbf{1}$.

(2) se sigue de (1), pues si $g \in G$ y $g = h_1...h_n$ es la expresión descrita en (1), $h_1...h_n \in H_1...H_n$. Por lo tanto $G = H_1...H_n$. Ahora, si $g_i = g_1...g_{i-1}g_{i+1}...g_n \in H_i \cap H_1...H_{i-1}H_{i+1}...H_n$, se tiene que $1..,1g_i1..,1 = g_1...g_{i-1}1g_{i+1}...g_n$ y (1) implica que $g_j = 1$ para cada $j$; así, $H_i \cap H_1...H_{i-1}H_{i+1}...H_n = \mathbf{1}$.

De manera inversa, si se tiene que $G = H_1...H_n$, es claro que cada elemento de $G$ es expresable como se requiere en (1), por lo basta hacer ver la unicidad de dicha expresión. Observemos que si $h_i \in H_i$, $h_j \in H_j$ y $j \neq i$, por ser $H_i$, $H_j$ subgrupos normales de $G$, $h_jh_ih_j^{-1} := h_i' \in H_i$ y $h_ih_j^{-1}h_i^{-1} := h_j' \in H_j$, por lo que

$h_jh_j' = h_jh_ih_j^{-1}h_i^{-1} = h_i'h_i^{-1}$, de donde $[h_i, h_j] \in H_i \cap H_j \subset H_i \cap H_1...H_{i-1}H_{i+1}...H_n = \mathbf{1}$. Por lo tanto, los elementos de $H_i$ conmutan con los de $H_j$.

Finalmente, si $h_i, h_i' \in H_i$, $i = 1, ..., n$ son tales que $h_1...h_n = h_1'...h_n'$, por la observación anterior, para cada $j \in \{1, ..., n\}$ $h_jh_j'^{-1} = h_1'h_1^{-1}...h_{j-1}'h_{j-1}^{-1}h_{j+1}'h_{j+1}^{-1}...h_n'h_n^{-1} \in H_j \cap H_1...H_{j-1}H_{j+1}...H_n = \mathbf{1}$ y por (2) $h_j = h_j'$ para cualquier $j$.

Se observó en la prueba anterior, que si se cumple alguna de las condiciones enunciadas en (1) ó (2), en presencia de la hipótesis inicial de normalidad de los subgrupos $H_i$, obtenemos:

- Los elementos de $H_i$ conmutan con los de $H_j$, si $i \neq j$.

Que evidentemente es equivalente a:

- Si $g = h_1...h_n$ y $g' = h_1'...h_n'$, donde $h_i, h_i' \in H_i$ para cada $i$, entonces $gg' = h_1h_1'...h_nh_n'$.

No es difícil ver que cualquiera de las anteriores en a~nadidura a (1) o (2) implica la normalidad de los subgrupos $H_1, ..., H_n$.

Decimos que $G$ es el ***producto directo (interior)*** de $H_1, ..., H_n$, si se cumple que $H_i \trianglelefteq G$ para cada $i$ y todo $g \in G$ tiene una única expresión $g = h_1...h_n$, donde cada $h_i \in H_i$.

Podemos resumir los resultados anteriores en el siguiente teorema.

**Teorema 3.1.** *Sea $G$ un grupo con subgrupos $H_1, ..., H_n$, las siguientes afirmaciones son equivalentes:*

*$G$ es el producto directo de $H_1, ..., H_n$.*

*$G = H_1H_2...H_n$, $H_i \trianglelefteq G$ para toda $i \in \{1, ..., n\}$ y $H_i \cap H_1H_2...H_{i-1}H_{i+1}...H_n = \mathbf{1}$.*

*$G = H_1...H_n$, $H_i \cap H_1H_2...H_{i-1}H_{i+1}...H_n = \mathbf{1}$ y para cada $h_i \in H_i$, $h_j \in H_j$ con $i \neq j$ $h_ih_j = h_jh_i$.*

Las observaciones anteriores hacen evidente que existe un isomorfismo de $G$ en el producto directo exterior $H_1 \times ... \times H_n$ tal que la imagen de $H_i$ bajo éste es $\mathbf{1} \times ... \times H_i \times ... \times \mathbf{1}$. Es por esto que $G$ es llamado producto directo de sus subgrupos $H_1, ..., H_n$ y frecuentemente escribiremos $G = H_1 \times ... \times H_n$, aunque en términos formales es un ligero abuso de notación.

**Lema 3.2.** *Sea $n \in \mathbb{N}\backslash\{0\}$ y tómese $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ la descomposición de $n$ en primos distintos, se tiene que $C_n \cong (C_{p_1^{\alpha_1}}) \times ... \times (C_{p_k^{\alpha_k}})$.*

El resultado anterior tiene la siguiente consecuencia inmediata.

**Corolario 3.3.** *Si $(a, b) = 1$ con $a, b \in \mathbb{N}\backslash\{0\}$, entonces $C_{ab} \cong C_a \times C_b$.*

Tenemos también esta otra sencilla consecuencia.

**Corolario 3.4.** *Si $G$ es un grupo abeliano tal que $|G| = p_1...p_t$, con $p_i$un primo y $p_i \neq p_j$, siempre que $i \neq j$, entonces $G \cong C_{p_1...p_t}$.*

## 3.2. Producto Semidirecto

Con la definición de producto directo de una pareja de grupos en mente, observemos que en el caso de que un grupo $G$ tenga subgrupos $H$ y $K$ con $H \cap K = \mathbf{1}$, $HK = G$ y $H \trianglelefteq G$, por el primer teorema de isomorfismo se tiene $HK/H = G/H \cong K$, por lo que $G$ es una extensión de $H$ por $K$. Aquí, como en el caso del producto directo o cualquier otra extensión, $G$ tiene una expresión única de la forma $hk$ con $h \in H$ y $k \in K$; y si $hk, h'k' \in G$, obtenemos $hkh'k' = hkh'k^{-1}kk' = h\varphi_k(h')kk'$. En esta situación, decimos que $G$ es el ***producto semidirecto (interior) de $H$ por $K$*** y escribimos $G = H \rtimes K$. Es claro que si también $K \trianglelefteq G$, entonces $G$ es el producto directo de $H$ por $K$ y nos referiremos a él como el ***producto semidirecto trivial de $H$ por $K$***.

Observemos que en el caso de un producto semidirecto interior $G = H \rtimes K$, la estructura multiplicativa del grupo queda determinada por los automorfismos interiores de $G$ asociados a los elementos de $K$ en el sentido descrito arriba, es por esto que la operación definida en $G$ puede ser recuperada de la restricción a $K$ del homomorfismo de $G$ en $Aut(G)$ que tiene como regla de correspondencia $k \mapsto \varphi_k$. Sin embargo, notemos que podemos prescindir de aún más información, ya que la operación de $G$ depende únicamente de la restricción de $\varphi_k$ a $H$; por supuesto, al ser $H$ normal en $G$, estas restricciones son automorfismos de $H$. Es con base en el análisis anterior que podemos afirmar que la estructura de $G$ puede ser codificada mediante el homomorfismo $\alpha : K \to Aut(H)$ tal que $\alpha(k) = \varphi_k|_H$, llamaremos a éste el ***homomorfismo de conjugación de*** $H \rtimes K$. Notemos finalmente que si dicho homomorfismo es no trivial, tendremos por fuerza que $G$ debe ser no abeliano, porque debe haber un elemento $k \in K$ tal que $\alpha(k) \neq 1 \in Aut(H)$ y por tanto existe $h \in H$ tal que $khk^{-1} = \alpha(k)(h) \neq h$, en cuyo caso $h$ y $k$ no conmutan.

El párrafo anterior sugiere que como en el caso del producto directo, la noción de producto semidirecto también tiene una contraparte *exterior*. Dados dos grupos arbitrarios $H$, $K$ y un homomorfismo $\alpha : K \to Aut(H)$, es posible investir al producto cartesiano de $H$ y $K$ con otra estructura multiplicativa diferente a la del producto directo de la manera siguiente. Si $(h,k),(h',k') \in H \times K$, definimos $(h,k)(h',k') = (h\alpha(k)(h'), kk')$. Esta definición da a $H \times K$ una estructura de grupo, cuyo elemento idéntico es $(1,1)$ y para cada $(h,k) \in H \times K$, el elemento inverso de éste es $(\alpha(k^{-1})(h^{-1}), k^{-1})$. Denominamos a este grupo el ***producto semidirecto (externo) de*** $H$ ***por*** $K$ ***correspondiente a*** $\alpha$ y diremos que es un ***producto semidirecto trivial*** $H$ ***por*** $K$, si $\alpha = 1$; denotamos a este grupo como $H \rtimes_\alpha K$, $H \overset{\alpha}{\rtimes} K$ o simplemente como $H \rtimes K$ si sólo existe salvo isomorfismo un producto semidirecto no trivial de $H$ por $K$.

Es evidente que la construcción recién realizada es el producto semidirecto interior de $\mathcal{H} := H \times \mathbf{1}$ por $\mathcal{K} := \mathbf{1} \times K$, ya que $\mathcal{HK} = H \rtimes_\alpha K$, $\mathcal{H} \cap \mathcal{K} = \mathbf{1}$ y si $(h,1) \in \mathcal{H}$, $(1,k) \in \mathcal{K}$, tenemos:

$$\varphi_{(1,k)}(h,1) = (1,k)(h,1)(1,k)^{-1} = (1,k)(h,1)(1,k^{-1}) = (\alpha(k)(h),1) \in \mathcal{H}$$

Por lo que $\mathcal{H} \trianglelefteq H \rtimes_\alpha K$.

Una consecuencia del hecho anterior es que el grupo $H \rtimes_\alpha K$ coincide con el producto directo de $H$ por $K$ si y solamente si $\alpha$ es el homomorfismo trivial, por lo que tambien en el caso externo la estructura de $H \rtimes_\alpha K$ en general difiere de la del producto directo.

A continuación enunciaremos algunos resultados que serán de vital importancia a lo largo del texto.

**Proposición 3.5.** *Si $H$,$K$ son grupos y $\alpha$,$\beta \in Hom(K, Aut(H))$, entonces $H \overset{\alpha}{\rtimes} K \cong H \overset{\beta}{\rtimes} K$ si existe $\gamma \in Aut(K)$ tal que $\beta \circ \gamma = \alpha$.*

*Demostración.* Sean $H$, $K$, $\alpha$, $\beta$, $\gamma$ como en la hipótesis y sea

$$\begin{array}{ccc} H \overset{\alpha}{\rtimes} K & \xrightarrow{\Phi} & H \overset{\beta}{\rtimes} K \\ (h,k)_\alpha & \mapsto & (h, \gamma(k))_\beta \end{array}$$

Es claro que $\Phi$ es biyectiva (pues $\gamma$ lo es); además es un homomorfismo, ya que si $(h_1,k_1)_\alpha, (h_2,k_2)_\alpha \in H \overset{\alpha}{\rtimes} K$, entonces:

$$\begin{aligned} \Phi((h_1,k_1)_\alpha(h_2,k_2)_\alpha) &= (h_1\alpha(k_1)(h_2), \gamma(k_1k_2))_\beta = (h_1\beta\circ\gamma(k_1)(h_2), \gamma(k_1)\gamma(k_2))_\beta \\ &= (h_1\beta(\gamma(k_1))(h_2), \gamma(k_1)\gamma(k_2))_\beta = (h_1, \gamma(k_1))_\beta(h_2, \gamma(k_2))_\beta \\ &= \Phi((h_1,k_1)_\alpha \Phi(h_2,k_2)_\alpha \end{aligned}$$

Por lo tanto $\Phi$ es un isomorfismo; y así $H \overset{\alpha}{\rtimes} K \overset{\Phi}{\cong} H \overset{\beta}{\rtimes} K$. □

**Corolario 3.6.** *Sean $H$ y $K$ grupos. Si $\alpha, \beta \in Hom(K, Aut(H))$ son monomorfismos cuyas imágenes coinciden y $K$ es cíclico, entonces $H \overset{\alpha}{\rtimes} K \cong H \overset{\beta}{\rtimes} K$.*

*Demostración.* Sea $x \in K$ tal que $\langle x \rangle = K$, por hipótesis:

$$\langle \alpha(x) \rangle = \mathrm{im}(\alpha) = \mathrm{im}(\beta) = \langle \beta(x) \rangle$$

Por lo tanto, existe $n \in \mathbb{N}$ tal que $\alpha(x) = \beta(x)^n$; y como $\alpha(x)$ es un generador de $\mathrm{im}\beta$, se tiene que la correspondencia $\beta(x) \mapsto \beta(x)^n$ define un automorfismo de $\mathrm{im}\beta$ (observemos que por el teorema fundamental del homomorfismo, $\mathrm{im}\beta \cong K/\ker\beta = K/\mathbf{1} \cong K$). Así, la función $\phi_n : K \to K$ tal que $x \mapsto x^n$ es un elemento de $Aut(K)$ para el que $\alpha(x) = \beta(x)^n = \beta(x^n) = \beta \circ \phi_n(x)$, lo que equivale a $\alpha = \beta \circ \phi_n$.

Se sigue de la proposición anterior que $H \overset{\alpha}{\rtimes} K \cong H \overset{\beta}{\rtimes} K$. □

**Proposición 3.7.** *Sean $H$, $K$ grupos y $\alpha : K \to Aut(H)$. Se tiene para cada $f \in Aut(H)$ que $H \overset{\alpha}{\rtimes} K \cong H \overset{\hat{f}\circ\alpha}{\rtimes} K$, donde $\hat{f}$ es el automorfismo interior asociado a $f$.*

*Demostración.* Sea $\Phi : H \overset{\alpha}{\rtimes} K \to H \overset{\hat{f}\circ\alpha}{\rtimes} K$ tal que $(h,k)_\alpha \overset{\Phi}{\mapsto} (f(h),k)_{\hat{f}\circ\alpha}$, se tiene que:

$$\begin{aligned}
\Phi((h_1,k_1)_\alpha(h_2,k_2)_\alpha) &= \Phi(h_1\alpha(k_1)(h_2),k_1k_2)_\alpha = (f(h_1\alpha(k_1)(h_2)),k_1k_2)_{\hat{f}\circ\alpha} \\
&= (f(h_1)f(\alpha(k_1)(h_2)),k_1k_2)_{\hat{f}\circ\alpha} \\
&= (f(h_1)f(\alpha(k_1)(f^{-1}(f(h_2)))),k_1k_2)_{\hat{f}\circ\alpha} \\
&= (f(h_1)f\circ\alpha(k_1)\circ f^{-1}(f(h_2)),k_1k_2)_{\hat{f}\circ\alpha} \\
&= (f(h_1)\hat{f}\circ\alpha(k_1)(f(h_2)),k_1k_2)_{\hat{f}\circ\alpha} \\
&= (f(h_1),k_1)_{\hat{f}\circ\alpha}(f(h_2),k_2)_{\hat{f}\circ\alpha} = \Phi(h_1,k_1)_\alpha\Phi(h_2,k_2)_\alpha
\end{aligned}$$

Por lo tanto $\Phi$ es un homomorfismo.

Concluimos que éste es un isomorfismo, pues la biyectividad de $\Phi$ se sigue de la de $f$.

En virtud de lo anterior, $H \overset{\alpha}{\rtimes} K \overset{\Phi}{\cong} H \overset{\hat{f}\circ\alpha}{\rtimes} K$. □

Una sencilla conjugación de la proposición anterior y el corolario 3.6 es el siguiente resultado, cuya prueba es omitida por su sencillez.

**Corolario 3.8.** *Si $H$,$K$ son grupos, $K$ cíclico y $\alpha, \beta \in Hom(K, Aut(H))$ son monomorfismos con imágenes conjugadas (i.e. existe $\phi \in Aut(H)$ tal que $Im(\alpha) = \phi Im(\beta)\phi^{-1}$), entonces $H \rtimes_\alpha K \cong H \rtimes_\beta K$.*

Como un primer ejemplo de producto semidirecto, consideremos $C_n \rtimes_\alpha C_2$, con $C_2 = \langle y \rangle$ y $\alpha : K \to Aut(C_n)$ el homomorfismo cuya imagen es el subgrupo generado por el automorfismo que envía a cada elemento de $C_n$ a su inverso, es decir $\alpha(y) = \sigma_{-1} = \sigma_{n-1}$. Denotamos al grupo $C_n \rtimes_\alpha C_2$ como $D_{2\cdot n}$. En el caso de $C_\infty$, podemos definir $\alpha$ análogamente y escribimos $C_n \rtimes_\alpha C_2 = D_\infty$. Los elementos de la familia así construida son llamados ***grupos diédricos*** y están caracterizados por estar generados por dos elementos de orden 2, a saber $y$ y $xy$; ya que siempre que un grupo sea generado por dos elementos de este tipo, será isomorfo al grupo diédrico del orden adecuado ([1,

proposición 1.13]). El nombre proviene del hecho de que $D_{2\cdot n}$ es isomorfo al grupo de simetrías de un polígono regular de $n$ lados. Es claro que el único caso en el que un grupo diédrico es abeliano es el de $D_{2\cdot 2}$, pues $C_2$ es el único grupo cíclico en el que todos los elementos coinciden con sus inverso.

Para simplificar la notación, siempre que se tengan $H = \langle x \rangle \cong C_n$, $K = \langle y \rangle \cong C_m$, y $\alpha \in Hom(K, H)$, denotaremos el producto directo $H \overset{\alpha}{\rtimes} K$ simplemente como $H \overset{k}{\rtimes} K$, donde $k \in \mathbb{Z}$ es tal que $\alpha(x) = \sigma_k$; es evidente que $k$ así definida caracteriza a $\alpha$ y por lo tanto a $H \overset{\alpha}{\rtimes} K$. En particular, $D_{2\cdot n} = C_n \overset{-1}{\rtimes} C_2$.

Siguiendo nuestra clasificación, los resultados anteriores permiten demostrar el siguiente resultado.

**Proposición 3.9.** *Si $p$ y $q$ son primos, con $q < p$, existen entonces a lo más 2 grupos de orden $pq$, siendo exactamente 2 si y solamente si $p \equiv 1 \,(mod\, q)$, a saber $C_{pq}$ y $C_p \rtimes C_q$.*

*Demostración.* Sea $G$ un grupo de orden $pq$. Si $G$ es abeliano, una sencilla aplicación de los teoremas de Sylow muestra que $G \cong C_p \times C_q$, el cual es isomorfo a $C_{pq}$ [Corolario 3.3]; y si cualquier grupo de orden $pq$ es isomorfo a $C_{pq}$, evidentemente todo grupo de ese orden es abeliano. Por lo tanto, existe más de una clase de isomorfismo de grupos de orden $pq$ si y solamente si existe algún grupo no abeliano de este orden. Probaremos que este grupo existe y es único si y solamente si $p \equiv 1 \,(\mathrm{mod}\, q)$, con lo que quedará demostrada la proposición.

Observemos primero que al tenerse un grupo $G$ de orden $pq$, con $q < p$, los teoremas de Sylow implican que $Syl_p(G)$ consta de un solo elemento $P$ y éste es un subgrupo normal de $G$; y si $Q$ es un $q$-subgrupo de Sylow de $G$, entonces $G = P \rtimes Q \cong C_p \rtimes_\alpha C_q$ . Por lo tanto, la existencia de grupos no abelianos de orden $pq$ se reduce a la existencia de productos semidirectos no triviales $C_p \rtimes_\alpha C_q$.

Supongamos que existe un producto semidirecto no trivial $C_p \overset{\alpha}{\rtimes} C_q$, con $\alpha : C_q \to Aut(C_p)$ un homomorfismo. La hipótesis de no trivialidad implica que necesariamente $\alpha$ es un monomorfismo, pues $\mathbf{1} \leq \ker(\alpha) \lneq C_q$ y $C_q$ no tiene subgrupos propios no triviales; por lo tanto $\mathrm{im}(\alpha) \cong C_q$. Además sabemos por la proposición 2.22 que $Aut(C_p) \cong C_{p-1}$, lo que implica que si existe este producto semidirecto no trivial, se tiene que $q | p - 1$ i.e. $p \equiv 1 \,(\mathrm{mod}\, q)$. Más aún, de existir, este grupo es único salvo

isomorfismo, pues el teorema 2.3 implica que $Aut(C_p)$ tiene un único subgrupo de orden $q$, y se ha dicho que cada homomorfismo no trivial de $C_q$ en $Aut(C_p)$ debe ser inyectivo; tenemos por el corolario 3.6 que para cualesquiera dos homomorfismos no triviales $\alpha : C_q \to Aut(C_p)$ y $\beta : C_q \to Aut(C_p)$, los grupos $C_p \overset{\alpha}{\rtimes} C_q$ y $C_p \overset{\beta}{\rtimes} C_q$ son isomorfos. Concluimos que si existe un grupo no abeliano de orden $pq$, este es único salvo isomorfismo y para su existencia es necesario que $p \equiv 1 \pmod q$.

Ahora, si suponemos que $p \equiv 1 \pmod q$, la existencia de un producto semidirecto no trivial sigue las mismas líneas que el párrafo anterior. Como $q|p-1$, entonces el grupo cíclico $Aut(C_p)$ posee exactamente un subgrupo de orden $q$, por lo cual es posible definir un monomorfismo $\alpha : C_q \to Aut(C_p)$, por ejemplo el que ha sido definido en el segundo ejemplo de la página 11[2]; se sigue de esto que el grupo $C_p \overset{\alpha}{\rtimes} C_q$ es no abeliano. Por lo tanto para la existencia de un (único) grupo no abeliano de orden $pq$, es suficiente que $p \equiv 1 \pmod q$. Esto concluye la prueba de la proposición. □

La observación de la unicidad de los grupos de orden primo, el corolario 2.33 y la proposición anterior, permiten elaborar una primera tabla con el avance de nuestra clasificación.

| Orden | Número de Grupos | Representantes |
|---|---|---|
| 2 | 1 | $C_2$ |
| 3 | 1 | $C_3$ |
| 4 | 2 | $C_4$, $V$ |
| 5 | 1 | $C_5$ |
| 6 | 2 | $C_6$, $D_{2\cdot 3}$ |
| 7 | 1 | $C_7$ |
| 9 | 2 | $C_9$, $C_3 \times C_3$ |
| 10 | 2 | $C_{10}$, $D_{2\cdot 5}$ |
| 11 | 1 | $C_{11}$ |
| 13 | 1 | $C_{13}$ |

[2]Es irrelevante cuál sea la correspondencia específica que se elija, ya que también en este caso el corolario 3.6 garantiza que todos los productos semidirectos no triviales $C_p \rtimes_\alpha C_q$ son isomorfos.

| Orden | Número de Grupos | Representantes |
|---|---|---|
| 14 | 2 | $C_{14}$, $D_{2\cdot 7}$ |
| 15 | 1 | $C_{15}$ |
| 17 | 1 | $C_{17}$ |
| 19 | 1 | $C_{19}$ |
| 21 | 2 | $C_{21}$, $C_7 \rtimes C_3$ |
| 22 | 2 | $C_{22}$, $D_{2\cdot 11}$ |
| 23 | 1 | $C_{23}$ |
| 25 | 2 | $C_{25}$, $C_5 \times C_5$ |
| 26 | 2 | $C_{26}$, $D_{2\cdot 13}$ |
| 29 | 1 | $C_{29}$ |
| 31 | 1 | $C_{31}$ |

## Grupos de Orden 30

Hasta ahora, tenemos en nuestra clasificación los grupos de órdenes de la forma $p$, $p^2$ y $pq$, el paso natural sería ahora proceder con los grupos con orden de la forma $pq^2$ o $p^3$; pero como veremos más adelante, aún son necesarios algunos resultados más para clasificar este tipo de grupos, sin embargo, la herramienta hasta ahora desarrollada sí nos permite clasificar los grupos de orden 30, aunque el orden de éstos sea de la forma $pqr$.

Supongamos que $G$ es un grupo de orden $30 = 2 \cdot 3 \cdot 5$, mostraremos que $G$ tiene un subgrupo de orden 15 (necesariamente normal), el cual debe isomorfo a $C_{15}$ por la proposición 3.9; concluimos en virtud de los teoremas de Sylow que $G$ es por fuerza de la forma $C_{15} \rtimes_\alpha C_2$, con $\alpha$ no trivial, o $C_{15} \times C_2 \cong C_{30}$ [Corolario 3.3]

Consideremos los conjuntos $Syl_3(G)$ y $Syl_5(G)$, sabemos que $r_3 \equiv 1 \pmod 3$ y $r_5 \equiv 1 \pmod 5$; además $r_3$ y $r_5$ son divisores de 30, de lo que se desprende que $r_3 \in \{1, 10\}$, $r_5 \in \{1, 6\}$. Si se tuviera que tanto $r_3$ como $r_5$ fueran mayores que 1, $G$ tendría $r_3(3-1) = 20$ elementos de orden 3 y $r_5(5-1) = 24$ elementos de orden 5, por lo que $G$ tendría al menos 44 elementos, lo cual es absurdo. Tenemos en consecuencia que alguno de los números es igual a 1.

Por la discusión anterior, si tomamos $H \in Syl_3(G)$ y $K \in Syl_5(G)$, al menos uno de los dos subgrupos es normal y en consecuencia, $HK$ es un subgrupo de $G$ de

orden $|HK| = |H||K|/|H \cap K| = 15$. Observemos que $[G : HK] = 2$ y por lo tanto $HK \lhd G$. Más aún, este subgrupo es único, ya que si tomamos el grupo cociente $G/HK$ y un elemento $g \in G$ de orden 15, entonces su imagen $\bar{g}$ bajo el epimorfismo natural será trivial, ya que por un lado $|\bar{g}| \mid 15$ y por otro lado $|\bar{g}| \mid |G/HK| = 2$, es decir $|\bar{g}| = 1$ y por lo tanto $g \in HK$. Notemos también que al ser $HK$ un subgrupo característico de $G$ y $H, K$ subgrupos característicos de $HK$, entonces también son subgrupos característicos de $G$ [Proposición 2.24], por lo que se tiene que $r_3 = r_5 = 1$.

Si ahora tomamos un subgrupo $L$ de $G$ de orden 2, se tiene que $HKL = G$ y $(HK) \cap L = \mathbf{1}$, entonces si $L$ es normal, $G = HK \times L \cong C_{15} \times C_2 \cong C_{30}$ [Teorema 3.1, corolario 3.3]; mientras que si $L$ no es normal, $G = HK \rtimes L$. En particular, existe una sola clase de isomorfismo de grupos abelianos de orden 30.

Para concluir la clasificación de los grupos de orden 30, resta únicamente determinar salvo isomorfismo los grupos de la forma $C_{15} \rtimes C_2$; es decir, clasificar los homomorfismos no triviales $\alpha : C_2 \to Aut(C_{15})$ que no producen grupos isomorfos $C_{15} \overset{\alpha}{\rtimes} C_2$. Por el resto de la discusión, los elementos $x \in C_{15}$, $y \in C_2$ serán tales que $\langle x \rangle = C_{15}$, $\langle y \rangle = C_2$.

Es consecuencia del teorema 2.20 que $Aut(C_{15})$ es isomorfo al grupo abeliano $\mathbb{Z}_{15}^{\times} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Observemos que en $\mathbb{Z}_{15}^{\times}$, $\langle 2 \rangle = \{1, 2, 4, 8\}$ y $\langle 11 \rangle = \{1, 11\}$ son dos grupos que se intersectan trivialmente y además $|\langle 2 \rangle \langle 11 \rangle| = 30$ [Proposición 2.6], como $\mathbb{Z}_{15}^{\times}$ es abeliano, se sigue que $\mathbb{Z}_{15}^{\times} = \langle 2 \rangle \times \langle 11 \rangle$ [Teorema 3.1] y por lo tanto $\mathbb{Z}_{15}^{\times} \cong C_4 \times C_2$. Concluimos que $Aut(C_{15}) \cong C_4 \times C_2$.

Por lo anterior $\sigma_2, \sigma_{11} \in Aut(C_{15})$ son tales que $|\sigma_2| = 4$, $|\sigma_{11}| = 2$ y $Aut(C_{15}) = \langle \sigma_2 \rangle \times \langle \sigma_{11} \rangle = \{1, \sigma_2, \sigma_2^2, \sigma_2^3, \sigma_{11}, \sigma_2\sigma_{11}, \sigma_2^2\sigma_{11}, \sigma_2^3\sigma_{11}\}$. Si consideramos $\alpha : C_2 \to Aut(C_{15})$ tal que $|\mathrm{im}(\alpha)| > 1$, es decir $|\mathrm{im}(\alpha)| = 2$, observamos que pueden darse únicamente 2 casos, que el subgrupo cíclico de orden máximo $M$ en el que $\mathrm{im}(\alpha)$ esté contenido tenga orden 2 o tenga orden 4. En el primer caso, tenemos por fuerza que $M = \langle \sigma_2 \rangle$ o $M = \langle \sigma_2\sigma_{11} \rangle$; y en cualquiera de estas situaciones obtenemos $\mathrm{im}(\alpha) = \{1, \sigma_2^2\}$, por lo tanto todos aquellos homomorfismos $\alpha$ con $\mathrm{im}(\alpha) = \langle \sigma_2^2 \rangle$ producirán grupos isomorfos por el corolario 3.6. En caso de que $|M| = 2$, tenemos únicamente dos posibilidades, $M = \langle \sigma_{11} \rangle$ o $M = \langle \sigma_2^2\sigma_{11} \rangle$, equivalentmente $\alpha(y) = \sigma_{11}$ o $\alpha(y) = \sigma_2^2\sigma_{11}$. Si $\alpha(y) = \sigma_2^2\sigma_{11}$, evidentemente tenemos $C_{15} \overset{\alpha}{\rtimes} C_2 \cong D_{2 \cdot 15}$; en cuyo caso, para cada $i \in \{0, ..., 14\}$, $(x^i y)^2 = x^i y x^i y = x^i x^{-i} = 1$. Por lo tanto todos los elementos de $C_{15} \overset{\alpha}{\rtimes} C_2 \backslash \langle x \rangle$ son de orden 2. Por otro lado, si $\alpha(y) = \sigma_{11}$, entonces $\alpha(y)(x) = x^{11}$, y en consecuencia $(xy)^2 = x^{12}$, de lo que se desprende que el orden de $|xy| > 2$. Además

tenemos que $xy \in C_{15} \overset{\alpha}{\rtimes} C_2 \backslash C_{15}$, esto demuesttra que existen en $C_{15} \overset{\alpha}{\rtimes} C_2$ menos de 15 elementos de orden 2. Concluimos que si $\alpha, \beta : C_2 \to Aut(C_{15})$ son homomorfismos tales que $\text{im}(\alpha) = \langle \sigma_{11} \rangle$, $\text{im}(\beta) = \langle \sigma_2^2 \sigma_{11} \rangle$ , los grupos $C_{15} \overset{\alpha}{\rtimes} C_2$y $C_{15} \overset{\beta}{\rtimes} C_2$ no son isomorfos. Análogamente podemos concluir que el grupo $C_{15} \overset{4}{\rtimes} C_2$ no es isomorfo a $D_{2\cdot 15}$. Para demostrar que los grupos $C_{15} \overset{4}{\rtimes} C_2$ y $C_{15} \overset{11}{\rtimes} C_2$ no son isomorfos, hagamos notar que si $\Phi : C_{15} \overset{4}{\rtimes} C_2 \to C_{15} \overset{11}{\rtimes} C_2$ es un isomorfismo con $\Phi(y) = x^i y$, $i \in \{0, ..., 14\}$, por un lado $\Phi(yxy) = \Phi(x^4) = \Phi(x)^4$ y por otro lado $\Phi(yxy) = x^i y \Phi(x) y x^{-i} = \Phi(x)^{11}$. Donde la última igualdad se sigue del hecho de que $\Phi(x) \in C_{15}$, ya que $|\Phi(x)| = 15$ y se hizo notar al principio de la discusión que todo grupo de orden 30 posee un único subgrupo de orden 15. Se sigue que $\Phi(x)^4 = \Phi(x)^{11}$, por lo tanto $\Phi(x)^7 = 1$, de donde obtenemos $\Phi(x) = 1$. Concluimos que los grupos $C_{15} \overset{4}{\rtimes} C_2$ y $C_{15} \overset{11}{\rtimes} C_2$ no son isomorfos.

Recapitulando, cualquier grupo de orden 30 es isomorfo a uno y sólo uno de los siguientes $C_{30}$, $C_{15} \overset{4}{\rtimes} C_2$, $C_{15} \overset{14}{\rtimes} C_2 \cong D_{2\cdot 15}$, $C_{15} \overset{11}{\rtimes} C_2$.

## Grupos de orden $p^3$, $p$ impar.

Es tiempo ahora de clasificar los grupos de la forma $p^3$, siendo $p$ un primo impar. Se requiere de nuevo en este punto que el lector tenga alguna familiaridad con los resultados estándar de Álgebra Lineal usualmente cubiertos en dos cursos semestrales. Siendo el caso abeliano el más sencillo, será ese el punto de partida en esta breve sección.

Sea $G$ es un grupo abeliano de orden $p^3$. Si $G$ es cíclico, no hay nada que hacer, pues es claro que $G \cong C_{p^3}$. En caso contrario, existen dos posibilidades, o bien $g^p = 1$ para cada $g \in G$, o existe en $G$ un elemento de orden $p^2$. Si se da la primera de estas, la proposición 2.32 implica que $G \cong C_p^3$. Si existe $g \in G$ de orden $p^2$, al escoger un elemento $x \in G \backslash \langle g \rangle$, tenemos dos casos; $x^p = 1$, o bien $|x| = p^2$. Si $x^p = 1$, entonces es claro que $G = \langle g \rangle \times \langle x \rangle$ [Teorema 3.1]. Mientras que si $|x| = p^2$, entonces al tenerse que $1 < |\langle x \rangle \cap \langle g \rangle| < p^2$ y ser $\langle g \rangle, \langle x \rangle$ grupos cíclicos, por el teorema 2.3, $\langle x^p \rangle = \langle g^p \rangle$. Por lo tanto, existe $k \in \mathbb{Z}$ tal que $x^p = g^{kp}$, equivalentemente $(xg^{-k})^p = x^p g^{-kp} = 1$, lo que implica que el elemento $xg^{-k}$ tiene orden $p$; como $xg^{-k} \notin \langle g \rangle$, concluimos que $G = \langle g \rangle \times \langle xg^{-k} \rangle$. En cualquier caso, se tiene que $G \cong C_{p^2} \times C_p$.

Por lo tanto, si $G$ es un grupo abeliano de orden $p^3$, entonces $G$ es isomorfo a uno y sólo uno de los grupos $C_{p^3}$, $C_{p^2} \times C_p$ y $C_p^3$.

Antes de continuar con los grupos no abelianos, es necesario demostrar el siguiente lema técnico.

**Lema 3.10.** *Sea $G$ un grupo con $x, y \in G$ tales que $[x, y] \in Z(G)$, entonces*

$$[x^n, y] = [x, y]^n \tag{3.1}$$

$$y$$

$$(xy)^n = x^n y^n [y, x]^{n(n-1)/2} \tag{3.2}$$

.

*Demostración.* Se hará por inducción matemática.

Supóngase que $[x^n, y] = [x, y]^n$, entonces $[x^{n+1}, y] = xx^n yx^{-n}y^{-1}yx^{-1}y^{-1} = x[x^n, y]yx^{-1}y^{-1} = x[x, y]^n yx^{-1}y^{-1}$; por lo tanto $[x^{n+1}, y] = [x, y]^{n+1}$.

Observemos que también $[y^n, x] = [y, x]^n$, pues $[x, y] \in Z(G)$ si y sólo si $[y, x] \in Z(G)$.

En la demostración utilizaremos (1) y las identidades $[x, y] = [y, x]^{-1}$, $xy = [x, y]yx$

$$\begin{aligned}
(xy)^{n+1} &= x^n y^n [y, x]^{n(n-1)/2} xy = x^n y^n (xy)[y, x]^{n(n-1)/2} \\
&= x^n y^n ([x, y]yx)[y, x]^{n(n-1)/2} \\
&= x^n y^n yx[x, y][y, x]^{n(n-1)/2} = x^n (y^{n+1}x)[x, y][y, x]^{n(n-1)/2} \\
&= x^n ([y, x]^{n+1} xy^{n+1})[x, y][y, x]^{n(n-1)/2} \\
&= x^{n+1} y^{n+1} [y, x]^{n+1} [y, x]^{-1} [y, x]^{n(n-1)/2} \\
&= x^{n+1} y^{n+1} [y, x]^{n(n+1)/2}.
\end{aligned}$$

□

**Lema 3.11.** *Sea $P$ un $p$-grupo no abeliano de orden $p^3$. Se tiene que $|Z(P)| = p$, $P'$ (el subgrupo conmutador de $P$) coincide con $Z(P)$ y $P/Z(P) \cong C_p \times C_p$.*

*Demostración.* Al ser $P$ un $p$-grupo no abeliano finito, entonces $\mathbf{1} \lneq Z(P) \lneq P$. Observemos además que $|Z(P)| \neq p^2$, ya que $P/Z(P)$ no puede ser un grupo cíclico [Proposición 2.18], se sigue entonces que $|Z(P)| = p$.

Al ser $P/Z(P)$ de orden $p^2$, $P/Z(P)$ es abeliano. Lo que implica que $P' \leq Z(P)$ [Proposición 2.26] y como $P' \neq \mathbf{1}$, se tiene que $P' = Z(G)$.

Finalmente, como $P/Z(P)$ no es cíclico, se tiene que $P/Z(P) \cong C_p \times C_p$ [Corolario 2.33]. □

El siguiente resultado es una consecuencia de los lemas anteriores.

**Proposición 3.12.** *Si $G$ es un grupo no abeliano de orden $p^3$, con $p$ un primo impar, entonces $G$ tiene un subgrupo normal $H$ tal que $H \cong C_p \times C_p$ y $Z(G) \subset H$.*

*Demostración.* Se tiene que $Z(G)$ es un subgrupo de $G$ de orden $p$ tal que $Z(G) = G'$, y como consecuencia del lema 3.10, para cualesquiera $x, y \in G$, se tiene que $(xy)^p = x^p y^p [y, x]^{p(p-1)/2}$, pero como $p$ es impar, entonces $2|(p-1)$. Por lo tanto $[y, x]^{p(p-1)/2} = ([y, x]^{(p-1)/2})^p = 1$, pues $[y, x] \in Z(G)$. En consecuencia, para cualesquiera $x, y \in G$, se tiene $(xy)^p = x^p y^p$ y por lo tanto la función $\phi : G \to G$ tal que $\phi(x) = x^p$ es un homomorfismo, cuyo núcleo $K := \ker(\varphi)$ es tal que $Z(G) \leq K$.

Observemos que no puede ser que $Z(G) = K$; ya que de ser así, entonces $\mathrm{im}(\varphi) \cong G/K = G/Z(G) \cong C_p \times C_p$ [Lema 3.11], por lo cual todos los elementos no triviales de la imágen de $\varphi$ tienen orden $p$. Se tiene entonces que$C_p \times C_p \cong \mathrm{im}(\phi) \subseteq \ker(\phi) = Z(G)$, lo que contradice el hecho de que $|Z(G)| = p$. Por lo anterior, es posible tomar un elemento $g \in \ker(\varphi) \backslash Z(G)$ de orden $p$; se sigue inmediatamente que $\langle g \rangle \cap Z(G) = \mathbf{1}$;[3] y así, $H := \langle g \rangle \times Z(G)$ es el subgrupo buscado [Teorema 3.1]. □

Tenemos ahora todas las herramientas para clasificar los grupos de la clase buscada.

**Teorema 3.13.** *Si $p$ es un primo impar, existe una sola clase de isomorfismo de grupos no abelianos de orden $p^3$ que tienen un elemento de orden $p^2$.*

*Demostración.* Sean $G$ un grupo de orden $p^3$, $x \in G$ tal que $|x| = p^2$ y $P := \langle x \rangle$. Si existe $y \in G \backslash P$ tal que $y^p = 1$, habremos mostrado que $G = P \rtimes \langle y \rangle$, ya que $P \lhd G$ por el corolario 2.31; y en este caso, $\langle x \rangle \cap \langle y \rangle = \mathbf{1}$ y $\langle x \rangle \langle y \rangle = G$. Probaremos que en efecto existe tal $y$.

[3] Sólo es necesario verificar esta condición, ya que claramente los elementos de $\langle g \rangle$ conmutan con los de $Z(G)$

Sabemos por el resultado anterior que existe un subgrupo $H$ de $G$ tal que $H \cong C_p \times C_p$, es claro entonces que $|\langle x\rangle \cap H| < p^2$ y por lo tanto existe $y \in H \backslash \langle x\rangle$, de lo cual se sigue que $y^p = 1$ y $\langle y\rangle \cap \langle x\rangle = \mathbf{1}$. Esto demuestra que $G = \langle x\rangle \rtimes \langle y\rangle$.

Como ya se ha visto, $G$ queda determinado por el monomorfismo $\alpha : \langle y\rangle \to Aut(P)$ (recordemos que $G$ es no abeliano y $|y| = p$) tal que $\alpha(y) = \varphi_y|_P$. Además, tenemos que $Aut(P) \cong Aut(\mathbb{Z}_{p^2})$ es un grupo cíclico de orden $p(p-1)$ [Corolario 2.23], por lo que existe una sola posibilidad para la imagen de $\alpha$, concluimos por el corolario 3.6 que sólo existe una clase de isomorfismo a la que puede pertenecer $G$, a saber, $C_{p^2} \rtimes C_p$. □

**Teorema 3.14.** *Si $p$ es un primo impar, existe exactamente una clase de isomorfismo de grupos no abelianos de orden $p^3$ que no tienen elementos de orden $p^2$.*

*Demostración.* Es inmediato de la proposición 3.12 que si $G$ es un grupo del tipo contemplado en la hipótesis del teorema, existen $P \lhd G$ y $y \in G\backslash P$ de orden $p$ tales que $P \cong C_p \times C_p$ y $G = P \rtimes \langle y\rangle$. Por lo tanto la demostración del teorema se reduce a probar que existe un solo producto semidirecto no trivial $(C_p \times C_p) \rtimes C_p$.

La proposición 2.32 provee $Aut(C_p \times C_p) \cong GL(2,p)$ y $|GL(2,p)| = p(p-1)^2(p+1)$ por la proposición 2.34, por consiguiente cualquier subgrupo de orden $p$ de $GL(2,p)$ es un $p$-subgrupo de Sylow; así, todos los subgrupos de orden $p$ de $Aut(C_p \times C_p)$ son conjugados. Por lo tanto, si $\psi$, $\tau$ son homomorfismos no triviales (monomorfismos) de $C_p$ en $Aut(C_p \times C_p)$, existe $f \in Aut(C_p \times C_p)$ tal que $\tau(C_p) = f\psi(C_p)f^{-1}$. Se sigue de esto que $(C_p \times C_p) \rtimes_\tau C_p \cong (C_p \times C_p) \rtimes_\psi C_p$ [Corolario 3.8]. □

En particular, existen (salvo isomorfismo) exactamente cinco grupos de orden 27, representados por $C_3^3$, $C_3 \times C_9$, $C_{27}$, $C_9 \rtimes C_3$ y $(C_3 \times C_3) \rtimes C_3$.

## Grupos de Orden $pq^2$

Es tiempo ahora de clasificar los grupos de orden $pq^2$, siendo $p$ y $q$ primos distintos. A lo largo de la subsección, $p$ y $q$ siempre denotarán primos distintos entre si. Se presupone también aquí que el lector tiene cierta familiaridad con el Álgebra Lineal; sin embargo, los resultados principales serán referidos apropiadamente.

El siguiente resultado es fundamental para nuestra clasificación.

**Teorema 3.15.** *Si $|G| = p^n q^m$, donde $G$ es un grupo tal que $|Syl_q(G)| = 1$, entonces $G = N \rtimes H$, donde $H$ es algún $p$-subgrupo de Sylow y $N$ un $q$-subgrupo de Sylow de $G$.*

*Mas aún, si definimos $\alpha : H \to Aut(N)$ como $\alpha(h)(n) := hnh^{-1}$, se tiene para $\beta : H \to Aut(N)$ que $N \overset{\alpha}{\rtimes} H \cong N \overset{\beta}{\rtimes} H$ si y solamente si existen $\gamma \in Aut(H)$, $\psi \in Aut(N)$ tal que $\beta = \hat{\psi} \circ \alpha \circ \gamma$, donde $\hat{\psi}$ es el automorfismo interior (de $Aut(N)$) tal que $\hat{\psi}(f) := \psi \circ f \circ \psi^{-1}$.*

*El enunciado del teorema se puede representar mediante el siguiente diagrama conmutativo:*

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & Aut(N) \\ {\scriptstyle\gamma}\uparrow & & \downarrow{\scriptstyle\hat{\psi}} \\ H & \xrightarrow{\beta} & Aut(N) \end{array}$$

*Demostración.* Se sigue de $|Syl_q(G)| = 1$ que si $N$ es un $q$-subgrupo de Sylow de $G$, éste es normal; además para toda $H \in Syl_p(G)$, $N \cap H = \mathbf{1}$ y por tanto $G = NH = N \rtimes H$.

Para probar la segunda parte del teorema, basta demostrar la necesidad de las condiciones establecidas, pues la suficiencia de éstas es simplemente una combinación de las proposiciones 3.5 y 3.7.

Observemos que si $N \overset{\beta}{\rtimes} H$ es isomorfo a $N \overset{\alpha}{\rtimes} H$, entonces necesariamente obtenemos $N \rtimes_\beta H \cong G = NH$. Sea $\Phi : N \rtimes_\beta H \to G$ un isomorfismo de grupos, al tenerse que $\Phi(\mathcal{N}) \cong N$ y $\Phi(\mathcal{H}) \cong H$ (donde $\mathcal{N} := N \times \mathbf{1}$, $\mathcal{H} := \mathbf{1} \times H$), se sigue de los teoremas de Sylow y las hipótesis del teorema que $\Phi(\mathcal{N}) = N$ y $\Phi(\mathcal{H})$ es un conjugado de $H$ en $G$, i.e. existe $n_0 h_0 \in G$ tal que $n_0 h_0 H h_0^{-1} n_0^{-1} = \Phi(\mathcal{H})$; pero claramente $hHh^{-1} = H$ para toda $h \in H$ y por tanto $\varphi_{n_0}(H) = n_0 H n_0^{-1} = \Phi(\mathcal{H})$; es decir, para cada $h \in H$, existe $h_1 \in H$ tal que $\Phi(1, h) = n_0 h_1 n_0^{-1}$. Por otro lado, $\Phi(\mathcal{N}) = N$ implica que $\rho(n) := \Phi(n, 1)$ es un automorfismo de $N$. De las observaciones:

$$\begin{array}{ccc} \Phi(\beta(h)(n), 1) & = \Phi(1,h)\Phi(n,1)\Phi(1,h^{-1}) = & n_0 h_1 n_0^{-1} \rho(n) n_0 h_1^{-1} n_0^{-1} \\ || & & || \\ \rho(\beta(h)(n)) & & \varphi_{n_0} \circ \alpha(h_1) \circ \varphi_{n_0}^{-1} \circ \rho(n) \end{array}$$

Sean $\psi := \rho^{-1} \circ \varphi_{n_0}|_N \in Aut(N)$ y $\gamma : H \to H$ tal que $\gamma(h) := \varphi_{n_0}^{-1} \circ \Phi(1, h)$, se

concluye de las ecuaciones anteriores que para cualesquiera $h \in H$, $n \in N$

$$\beta(h)(n) \;=\; \psi \circ (\alpha \circ \gamma)(h) \circ \psi^{-1}(n)$$

Por lo tanto existen $\gamma \in Aut(H)$, $\psi \in Aut(N)$ tales que $\beta = \hat{\psi} \circ \alpha \circ \gamma$. □

El siguiente resultado implica que para el caso particular en el que $|G| = pq^2$, todos los subgrupos de este orden son productos semidirectos.

**Proposición 3.16.** *Si $G$ es un grupo tal que $|G| = pq^2$, donde $p$ y $q$ son primos distintos, entontes $G$ tiene un subgrupo de Sylow normal.*

*Demostración.* La demostración se hará por casos.

*Caso* 1. $p < q$.
En esta situación $G$ tiene un $q-$subgrupo de Sylow normal; pues se sabe que si $r_q = |Syl_q(G)|$, entonces $r_q \mid p$ y $r_q \equiv 1 (\mathrm{mod}\, q)$, lo que implica $r_q = 1$.

*Caso* 2. $q < p$.
Es claro que aquí se tiene $q^2 < p$ o $p < q^2$. Si $q^2 < p$, por argumentos análogos a los del caso anterior, $G$ tiene un $p$-subgrupo de Sylow normal.
Si $p < q^2$, podemos suponer que $G$ no tiene un $p$-subgrupo de Sylow normal; pues si es así, hemos terminado.
Si $|Syl_p(G)| > 1$, las condiciones impuestas por los teoremas de Sylow implican que $|Syl_p(G)| = q^2$; por lo tanto, $A := \bigcup Syl_p(G)$ tiene $(p-1)q^2$ elementos distintos de la identidad, lo que implica que todos los $q$-subgrupos de Sylow de $G$ deben estar contenidos en $(G - A) \cup \mathbf{1}$, pero este conjunto tiene sólo $q^2$elementos, se concluye que $G$ tiene un único $q$-subgrupo de Sylow y por lo tanto, éste es normal.

Por lo tanto, si $G$ es un grupo de orden $pq^2$, $G$ tiene un subgrupo de Sylow normal. □

Incluiremos ahora una proposición que tomará parte en el final de la claisficación; utilizaremos resultados estándar de Álgebra Lineal, que también serán referidos.

**Proposición 3.17.** *Si $F$ es un campo y $E$ es una extensión finita de $F$ (i.e. $F$ es subcampo de $E$ y la dimensión como espacio vectorial de $E$ sobre $F$ es finita), entonces $GL(n, F)$ contiene una copia de $GL(1, E) \cong E^{\times}$, donde $n = dim_F E$.*

*Demostración.* Sean $E, F$ como en la hipótesis. Si consideramos $\alpha, x, y \in E$, con $\alpha \neq 0$ y $c, d \in F$, entonces las propiedades de campo de $E$ implican que $\alpha(cx + dy) = c(\alpha x) + d(\alpha y)$. Por lo tanto la asignación $\mu_\alpha : E \to E$ tal que $\mu_\alpha(x) = \alpha x$ es una transformación lineal. Más aún, esta correspondencia es un isomorfismo lineal, ya que si $\alpha x = \alpha y$, entonces $x = \alpha^{-1}\alpha x = \alpha^{-1}\alpha y = y$; por lo tanto $\mu_\alpha$ es inyectiva, y al ser una transformación de un espacio en sí mismo, se sigue que también es suprayectiva [2][4]. Podemos decir más, la correspondencia $\alpha \mapsto \mu_\alpha$ es además un monomorfismo de grupos, pues si $\alpha, \lambda \in E^\times$ y $\mu_\alpha = \mu_\lambda$, entonces $\alpha = \alpha 1 = \alpha(1) = \lambda(1) = \lambda 1 = \lambda$ y $\mu_\alpha \mu_\lambda(x) = \alpha(\lambda(x)) = (\alpha\lambda)x = \mu_{\alpha\lambda}(x)$. Por lo tanto existe un monomorfismo de $E^\times$ en $GL(E)$. Como $E$ es isomorfo a $F^n$como espacio vectorial, concluimos que $GL(n, F)$ contiene una copia de $E^\times \cong GL(1, E)$. □

Sea $G$ un grupo de orden $pq^2$. La aplicación conjunta de la proposición 3.16 y el teorema 3.15, implica que $G$ es un producto semidirecto de subgrupos de Sylow y además las clases de isomorfismo de los grupos de este orden están dadas por la relación de equivalencia provista por el teorema 3.15.

Supongamos que $P \subset G$ es un $p$-subgrupo de Sylow normal y $Q < G$ es de orden $q^2$, entonces si $\alpha, \beta \in Hom(Q, Aut(P))$ son tales que $|\ker(\alpha)| = |\ker(\beta)|$, necesariamente $|\mathrm{im}(\alpha)| = |\mathrm{im}(\beta)|$; y ya que $Aut(P)$ es un grupo cíclico de orden $p - 1$[Proposición 2.22], sus subgrupos están caracterizados por su orden [Teorema 2.6], por lo tanto $\mathrm{im}(\alpha) = \mathrm{im}(\beta)$. Además $Hom(Q, Aut(P)) \neq \mathbf{1}$ si y solamente si $q \mid p - 1$. Una vez hechas estas observaciones, estamos en posición de determinar las clases de isomorfismo que se presentan en este caso.

Dado $Q$ cíclico, digamos $Q = \langle x \rangle$; también por la proposición 2.22 y el teorema 2.6, $|\ker(\alpha)| = |\ker(\beta)|$ si y sólo si $\ker(\alpha) = \ker(\beta)$, entonces por los argumentos del párrafo anterior, $|\ker(\alpha)| = |\ker(\beta)|$ si y solamente si $\mathrm{im}(\alpha) = \mathrm{im}(\beta)$. Si además $\ker(\alpha) = \ker(\beta) \neq Q$, $\mathrm{im}(\alpha) = \mathrm{im}(\beta)$ es un $q$-grupo cíclico no trivial generado por $\alpha(x)$ y $\beta(x)$; en particular existe $k \in \mathbb{N}$ con $\alpha(x) = \beta(x)^k = \beta(x^k)$, lo que implica $(k, |\mathrm{im}(\alpha)|) = (k, q^i) = 1$, con $i \in \{1, 2\}$; de lo que a su vez concluimos $(k, q^2) = 1$. Por tanto, $\sigma_k \in Aut(Q)$ es tal que $\alpha = \beta \circ \sigma_k$. Se sigue inmediatamente de la proposición 3.5 que si $|\ker(\alpha)| = |\ker(\beta)|$, entonces $P \rtimes_\alpha Q \cong P \rtimes_\beta Q$, y obtenemos como resultado que si $i \in \mathbb{N}$ es tal que $q^i = (q^2, p - 1)$,[5] en esta situación hay a lo más $i + 1$ clases de

[4]Ver Capítulo 3, Teorema 9.

[5]Cada $q^j$, $0 \leq j \leq i$ provee un caso distinto para $\ker(\alpha)$, $\mathrm{im}(\alpha)$, a saber $|\ker(\alpha)| = q^j$, $|\mathrm{im}(\alpha)| = q^{2-j}$

isomorfismo, una de las cuales es el caso trivial $P \times Q$. Para ver que existen al menos $i+1$, observemos que el teorema 3.15 garantiza que si $P \rtimes_\alpha Q \cong P \rtimes_\beta Q$, entonces $|\ker(\alpha)| = |\ker(\beta)|$; por lo tanto existen exactamente $i+1$ clases de isomorfismo en este caso.

Si $Q$ no es cíclico, i.e. $Q \cong C_q \times C_q$, ningún homomorfismo de $Q$ en $Aut(P)$ puede ser inyectivo; ya que todos los subgrupos cíclicos de $Q$ son propios[6], por lo cual todo $\alpha \in Hom(Q, Aut(P))$ tiene núcleo no trivial; en particular, si $\alpha$ es definido como $\alpha(s)(t) = sts^{-1}$ con $s \in Q$, $t \in P$, existe $v \in Q \backslash \mathbf{1}$ tal que $vtv^{-1} = t$ para cada $t \in P$, es decir $v \in Z(G)$, además $Q_1 := \langle v \rangle \lhd G$ por ser un subgrupo central; y si $w \in Q \backslash \langle v \rangle$, entonces para $Q_2 := \langle w \rangle$ tenemos $Q_2 P < G$, pues $P$ es un subgrupo normal y $|Q_1 Q_2 P| = |Q_1||Q_2 P|/|Q_1 \cap Q_2 P| = |Q_1||Q_2||P|/|Q_1 \cap Q_2 P||Q_2 \cap P| = \frac{q \cdot pq}{1 \cdot 1} = pq^2$[Proposición 2.6], por lo tanto $Q_1 Q_2 P = G$. Además, si $a \in Q_2 P$, entonces $vav^{-1} = a$, de lo que se sigue $Q_2 P \lhd G$. Por lo tanto $G = Q_1 \times Q_2 P$ y $|Q_2 P| = pq$, lo que implica que $Q_2 P$ es isomorfo a $C_p \rtimes C_q$ o a $C_p \times C_q$. Concluimos que en este caso $G \cong C_q \times (C_p \rtimes C_q)$ o $G \cong C_q \times C_p \times C_q$. Es claro aquí que estos grupos no son isomorfos, pues $C_p \rtimes C_q \ncong C_p \times C_q$, por lo tanto en este caso existen exactamente dos clases de isomorfismo.

Hemos probado el siguiente teorema.

**Teorema 3.18.** *Sea $G$ un grupo de orden $pq^2$ con subgrupos $P$, $Q$ tales que $|P| = p$, $|Q| = q^2$ y $P \lhd G$*

- *Si $Q$ es un grupo cíclico con $q^i = (q^2, p-1)$, existen exactamente $i+1$ clases de isomorfismo a las que puede pertenecer $G$, una de las cuales es la del producto directo $C_p \times C_{q^2}$.*
- *Si $Q$ no es cíclico, entonces $G$ es isomorfo a uno y sólo uno de los siguientes $C_p \times C_q \times C_q$, $(C_p \rtimes C_q) \times C_q$, donde el caso no abeliano puede darse si y sólo si $p \equiv 1 \, mod \, q$.*

Por otro lado, si $Q$ es un $q$-subgrupo de Sylow normal y $P \in Syl_p(G)$, los productos semidirectos no triviales $Q \rtimes P$ quedan determinados por los monomorfismos de $Hom(P, Aut(Q))$ y como la cantidad de estos varía considerablmente según sea la estructura de $Q$, debemos distinguir nuevamente entre los casos $Q$ cíclico y $Q \cong C_q \times C_q$.

[6]Recordemos que si $\alpha : Q \to Aut(P)$ es un monomorfismo, se sigue del primer teorema de isomorfismo que $Q \cong Q/\ker(\alpha) \cong \mathrm{im}(\alpha) < Aut(P)$. Lo que implica $Q$ cíclico.

Sin embargo, podemos hacer una última observación que involucra ambos casos; notemos que estamos clasificando los grupos de la forma $Q \rtimes_\alpha P$, separados mediante la relación de equivalencia del teorema 3.15, pero como ya se ha dicho, todos los casos no triviales corresponderán a un monomorfismo $\alpha : P \to Aut(Q)$; por lo tanto, aplicando el teorema 3.15 y el corolario 3.8, determinar las clases de isomorfismo de los grupos no abelianos de la forma $Q \rtimes P$ se reduce a encontrar las clases de conjugación de los subgrupos de $Aut(Q)$ que tienen orden $p$.

Si $Q$ es un subgrupo cíclico de $G$, entonces por el corolario 2.23 $Aut(Q) \cong Aut(C_{q^2})$ es un grupo cíclico de orden $q(q-1)$, por lo cual existe a lo más un subgrupo de orden $p$ y la existencia de éste está garantizada si y solamente si $p|(q-1)$ [Teorema 2.7].

Es decir, $Aut(Q)$ tiene exactamente un subgrupo de orden $p$ si y sólo si $p|(q-1)$ y $|Hom(P, Aut(Q))| = 1$ en otro caso.

Por la observación anterior, existe exactamente un grupo de esta forma y por lo tanto, $G \cong C_{q^2} \rtimes C_p$.

El caso en el que $Q$ no es cíclico es el más complicado y lo desglosaremos en subcasos.

Si $Q$ es un grupo no cíclico de orden $q^2$, éste es isomorfo a $C_q \times C_q$ [Corolario 2.33]; y en virtud de la proposición 2.32 $Aut(Q) \cong GL(2, q)$, por lo que $|Aut(Q)| = q(q-1)^2(q+1)$ [Proposición 2.34]. Por los teoremas de Sylow, existirá en $Aut(Q)$ un subgrupo de orden $p$ si y solamente si $p|q(q-1)^2(q+1)$ , lo que es equivalente a $p|(q-1)(q+1)$. Supongamos que éste es el caso.

Puesto que por la observación inicial basta determinar las clases de conjugación de los subgrupos de $Aut(Q)$ de orden $p$, en este caso es suficiente determinar las clases de conjugación de los subgrupos de orden $p$ de $GL(2, q)$ , que a su vez se reduce a determinar las clases de conjugación de las matrices de $GL(2, q)$ que tienen orden $p$ y que no generen el mismo subgrupo.

Si $p|(q-1)$, al tenerse por el teorema 2.20 y la proposición 2.22 que $\mathbb{Z}_q^\times \cong Aut(C_q)$ es un grupo cíclico de orden $q-1$, el teorema de Cauchy y el teorema 2.3 proveen un elemento $a \in \mathbb{Z}_q^\times$ de orden $p$, tal que todo elemento $b \in \mathbb{Z}_q^\times$ de orden $p$ está contenido en $\langle a \rangle$. Por lo tanto, existen exactamente $p$ elementos $r \in \mathbb{Z}_q$ tales que $r^p - 1 = 0$. Por [2][7], todas las matrices $M \in GL(2, q)$ que satisfagan $M^p = 1$, serán tales que su polinomio

[7]Ver Capítulo 6, Teorema 4.

minimal $\mu_M(\lambda)$ es un divisor de $\lambda^p - 1$, y por lo anterior, $1, a^2, ..., a^{p-1}$ son sus únicas raices, es decir $\lambda^p - 1$ no tiene raíces repetidas, entonces $\mu_M(\lambda)$ tampoco las tiene. Es así que toda matriz $M$ con estas caractrísticas es diagonalizable ( [2], Capítulo 6, Teorema 6). Por lo cual existe $T \in GL(2,q)$ tal que $TMT^{-1} = \begin{pmatrix} a^i & 0 \\ 0 & a^j \end{pmatrix}$, con $i, j \in \{1, .., p\}$.

Observemos que dos matrices distintas de este tipo $M_1 = \begin{pmatrix} a^{i_1} & 0 \\ 0 & a^{j_1} \end{pmatrix}$, $M_2 = \begin{pmatrix} a^{i_2} & 0 \\ 0 & a^{j_2} \end{pmatrix}$ son conjugadas si y sólo si $i_2 = j_1$ y $j_2 = i_1$, ya que $\{a^{i_1}, a^{j_1}\}$ y $\{a^{i_2}, a^{j_2}\}$ son los conjuntos de valores propios de $M_1$ y $M_2$ respectivamente, y por [2][8] $M_1$ y $M_2$ son conjugadas si y solamente si $\{a^{i_1}, a^{j_1}\} = \{a^{i_2}, a^{j_2}\}$; al ser $M_1 \neq M_2$, esto es posible si y sólo si $i_2 = j_1$ y $j_2 = i_1$.

Resta únicamente determinar cuáles de estas matrices no generan el mismo grupo cíclico; para esto, observemos que para cada elemento de la forma $\begin{pmatrix} a^i & 0 \\ 0 & a^j \end{pmatrix}$, $\begin{pmatrix} a^i & 0 \\ 0 & a^j \end{pmatrix}^k = \begin{pmatrix} a^{ki} & 0 \\ 0 & a^{kj} \end{pmatrix}$, lo que implica que para cada $i, j$, $\langle \begin{pmatrix} a^i & 0 \\ 0 & a^j \end{pmatrix} \rangle \subseteq \left\{ \begin{pmatrix} a^r & 0 \\ 0 & a^s \end{pmatrix} | 0 \leq r, s \leq p \right\}$, además el número de elementos de esta forma es $p^2$, siendo una de las estas la matriz identidad y las restantes generadores de los grupos de orden $p$, y dado que existen $p-1$ generadores por grupo de orden $p$; entonces tenemos $(p+1)$ subgrupos de orden $p$ generados por estas matrices; de estos necesitamos descartar aquellos que sean generados por matrices conjugadas; observemos que dos matrices conjugadas, distintas de la identidad, $\begin{pmatrix} a^i & 0 \\ 0 & a^j \end{pmatrix}$, $\begin{pmatrix} a^j & 0 \\ 0 & a^i \end{pmatrix}$ generan el mismo grupo cíclico si y solamente si existe $k \in \mathbb{Z}$ tal que $\begin{pmatrix} a^{ki} & 0 \\ 0 & a^{kj} \end{pmatrix} = \begin{pmatrix} a^j & 0 \\ 0 & a^i \end{pmatrix}$, lo que implica $k^2 i \equiv i \pmod{p}$ (equivalentemente $k^2 \equiv 1 \pmod{p}$) , que evidentemente pasa si y sólo si $k \equiv \pm 1 \pmod{p}$.

Es evidente también que $k \equiv 1 \pmod{p}$ es un caso que pasa y sólo puede pasar cuando se trata de matrices escalares (e iguales) y todas las matrices diagonales del tipo que estamos considerando se encuentran en un mismo grupo cíclico.

Si $k \equiv -1 \pmod{p}$, se desprende que $i \equiv -j \pmod{p}$ y de nuevo todas las matrices de este estilo están en un mismo grupo cíclico.

[8]Ver nota al pie anterior.

Notemos además que $1 \equiv -1 \pmod{p}$ si y solamenente si $p = 2$. De donde si $p = 2$, los subgrupos que hemos referido anteriormente coinciden. Podemos concluir que si $p > 2$, entonces de los $p + 1$ subgrupos de orden $p$, $p - 1$ de éstos son generados por parejas de matrices conjugadas, y por lo tanto un conjunto de representantes de la relación de equivalencia inducida por el teorema 3.15 tiene $(p-1)/2 + 2 = (p+3)/2$ elementos; mientras que si $p = 2$, entonces se tienen 2 .

Concluimos que existen $(p+3)/2$ ó 2 clases de isomorfismo de grupos no abelianos de la forma $Q \rtimes P$, aparte el caso abeliano $Q \times P$.

Si sucede que $p \nmid (q-1)$, entonces debe tenerse que $p|q(q-1)^2(q+1)$ si y sólo si $p|(q+1)$ y por lo tanto $p^i|q(q-1)^2(q+1)$ si y sólo si $p^i|(q+1)$.

En virtud de la proposición 3.17, $GL(2,q)$ tiene un subgrupo isomorfo a $GL(1,q^2) \cong \mathbb{F}_{q^2}^{\times}$, el cual es cíclico de orden $q^2 - 1$ [Lema 2.21], en consecuencia $GL(2,q)$ tiene un subgrupo $H$ cíclico de orden $(q+1)$, y por la observación anterior, el único $p$-subgrupo de Sylow de éste (que es cíclico) es también un $p$-subgrupo de Sylow de $GL(2,q)$. Se sigue de los teoremas de Sylow que todos los $p$-subgrupos de Sylow de $GL(2,q)$ son conjugados; y por lo tanto todos los subgrupos de orden $p$ de $GL(2,q)$ también son conjugados, en consecuencia, existe una única clase de isomorfismo en este caso.

Podemos resumir la serie de resultados anteriores en el siguiente teorema.

**Teorema 3.19.** *Sea $G$ un grupo de orden $pq^2$ con subgrupos $P$, $Q$ tales que $|P| = p$, $|Q| = q^2$ y $Q \lhd G$.*

- Si $Q$ es un grupo cíclico, existen a lo más 2 clases de isomorfismo a las que puede pertenecer $G$, siendo exactamente dos si y sólo si $q \equiv 1 \pmod{p}$, cuyos representantes son $C_p \times C_{q^2} \cong C_{pq^2}$ y $C_{q^2} \rtimes C_p$.
- Si $Q$ no es cíclico, entonces el número de clases de isomorfismo a las que puede pertenecer $G$ es exactamente 3 si $p = 2$; y si $p > 2$, exactamente 1 si $p \nmid (q-1)(q+1)$, precisamente 2 si $p|(q-1)(q+1)$ y $p \nmid (q-1)$; y justamente $(p+5)/2$ si se tiene que $p|(q-1)$.

Es claro que en los casos no abelianos, los teoremas 3.18 y 3.19 separan las clases de isomorfismo en 4 clases, que forman una "partición" de las clases de isomorfismo de los grupos no abelianos de orden $pq^2$. Podemos entonces emplear estos teoremas para determinar las clases de isomorfismo a las que pertenecen los grupos de órdenes $12 = 3 \cdot 2^2$, $18 = 2 \cdot 3^2$, $20 = 5 \cdot 2^2$ y $28 = 7 \cdot 2^2$

**Teorema 3.20.** *Existen salvo isomorfismo cinco grupos de orden* 12, $C_{12}$, $C_2 \times C_6$, $D_{2\cdot 6} \cong C_3 \rtimes V$, $A_4 := V \rtimes C_3$ *y* $T := C_3 \rtimes C_4$.[9]

*Demostración.* Puesto que para el caso $3 \cdot 2^2$ se tiene que $2|3-1$, $2^1 = (2^2, 3-1)$, $3 \nmid (2-1)$ y $3|(2+1)$, entonces por los teoremas 3.18 y 3.19 existen exactamente $1+1=2$ clases de isomorfismo de grupos de orden 12 que tienen un subgrupo normal de orden 3 y un subgrupo cíclico de orden 4, a saber las de $C_3 \times C_4 \cong C_{12}$ y $C_3 \overset{-1}{\rtimes} C_4$, el último de los cuales hemos bautizado como $T$. De igual manera, existen exactamente 2 clases de isomorfismo de grupos que tengan un subgrupo normal de orden 3 y un subgrupo no cíclico de orden 4 (una de grupos abelianos y otra de grupos no abelianos); por lo tanto, éstas quedan determinadas por $C_2 \times C_6$ y $D_{2\cdot 6}$. Si a estas añadimos las clases de isomorfismo de grupos no abelianos que tienen un subgrupo normal de orden 4, la lista estará completa; sin embargo, existe una sola de estas clases, ya que por el teorema 3.19, no existen grupos no abelianos de orden 12 que tengan un subgrupo cíclico normal de orden 4 y existe una y sólo una clase de isomorfismo de grupos no abelianos de orden 12 que tengan subgrupos normales de orden 4 no cíclicos, a saber $A_4 := V \rtimes_\alpha C_3 := V \rtimes C_3$ (donde $\alpha(x,1) = (1,x)$ y $\alpha(1,x) = (x,x)$, si $C_2 = \langle x \rangle$). En conclusión, existen únicamente 5 clases de isomorfismo a las que un grupo de orden 12 puede pertenecer, las cuales están determinadas por los grupos enunciados en el teorema. □

**Teorema 3.21.** *Existen salvo isomorfismo cinco grupos de orden* 18.

*Demostración.* La demostración sigue las mismas lineas que la del teorema anterior, por lo cual se obviarán los argumentos simétricos. Puesto que $3 \nmid 2-1$, existe unicamente una clase de isomorfismo de grupos de orden 18 con un subgrupo normal de orden 2 y un elemento de orden 9, a saber $C_{18}$; por la misma razón, existe salvo isomorfismo sólo un grupo de orden 18 con subgrupos normales de orden 2 y sin elementos de orden 9, $C_3 \times C_6$.

Por otro lado, $2|(3-1)$ por lo que existe exactamente una clase de isomorfismo de grupos no conmutativos con subgrupos normales de orden 9 cíclicos, la de $D_{2\cdot 9}$.

[9] Aquí, como en el caso de $V$, hemos definido $A_4$ de manera diferente a la usual; ya que este grupo se define como el subgrupo de permutaciones pares de $S_4$. El lector interesado en las definiciones clásicas de $V$ y $A_4$ puede consultar [4].

En virtud del teorema 3.19, existen exactamene dos clases de grupos no abelianos con subgrupos normales de orden 9 no cíclicos. Para dar representatntes no isomorfos, recordemos que por la prueba del teorema 3.19, si $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\alpha C_2$ y $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\beta C_2$ son representantes de estas clases de isomorfismo y $C_2 = \langle x \rangle$, entonces $\alpha(x)$ y $\beta(x)$ deben ser conjugadas a $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ y $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, respectivamente. Por esto, podemos suponer sin pérdida de generalidad que $\alpha(x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ y $\beta(x) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

En el caso de $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\alpha C_2$, es elemental demostrar que $\langle (0,1,1), (0,0,x) \rangle \cong D_{2\cdot 3}$, $\langle (0,1,1), (0,0,x) \rangle \cap \langle (1,0,1) \rangle = 1$ y $[(0,1,1), (1,0,1)] = [(0,0,x), (1,0,1)] = (0,0,1)$. Por lo tanto, $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\alpha C_2 = \langle (0,1,1), (0,0,x) \rangle \times \langle (1,0,1) \rangle$ y así $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\alpha C_2 \cong D_{2\cdot 3} \times C_3$. Finalmente, a $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\beta C_2$, que es frecuentemente llamado grupo dihedrico generalizado de $\mathbb{Z}_3 \times \mathbb{Z}_3$ o $\mathrm{Dih}(\mathbb{Z}_3 \times \mathbb{Z}_3)$, lo denotaremos simplemente como $(\mathbb{Z}_3 \times \mathbb{Z}_3) \overset{-1}{\rtimes} C_2$.

En total tenemos cinco clases de isomorfismo a las que un grupo de orden 18 puede pertenecer; a saber, $C_{18}$, $C_3 \times C_6$, $D_{2\cdot 9}$, $D_{2\cdot 3} \times C_3$ y $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{-1} C_2$. □

**Teorema 3.22.** *Existen* 3 *clases de isomorfismo de grupos no abelianos de orden* 20 *y* 2 *clases de isomorfismo de grupos abelianos de orden* 20*.*

*Demostración.* Tenemos que $2^2 = (2^2, 5-1)$, por lo tanto existe salvo isomorfismo un grupo abeliano y dos grupos no abelianos de orden 20 con subgrupos normales de orden 5 y elementos de orden 4, $C_{20}$ y $C_5 \overset{2}{\rtimes} C_4$, $C_5 \overset{-1}{\rtimes} C_4$ respectivamente; además existe otra clase de isomorfismo de grupos no abelianos de orden 20 que no tiene subgrupos normales de orden 4 ni elementos de orden 4 y otra clase de grupos abelianos de orden 20 sin elementos de orden 4, digamos las de $D_{2\cdot 10}$ y $C_2 \times C_{10}$ respectivamente; y ya que $5 \nmid (2-1)(2+1)$, no hay más clases de isomorfismo que agregar.

Por lo tanto si $G$ es un grupo de orden 20, sólo puede ser isomorfo a uno y sólo uno de estos grupos $C_{20}$, $C_2 \times C_{10}$, $D_{2\cdot 10}$, $C_5 \overset{2}{\rtimes} C_4$ o $C_5 \overset{-1}{\rtimes} C_4$. Siendo los dos primeros grupos abelianos y los restantes grupos no conmutativos. □

**Teorema 3.23.** *Los grupos de orden* 28 *se dividen en cuatro clases de isomorfismo representadas por* $C_{28}$*,* $C_2 \times C_{14}$*,* $C_7 \overset{-1}{\rtimes} C_4$ *y* $D_{2\cdot 14}$*.*

*Demostración.* Dado que $2^1 = (2^2, 7-1)$, solamente existen dos clases de grupos abelianos de orden 20 con subgrupos normales de orden 7 y dos clases de grupos no abelianos con subgrupos normales de orden 7; $C_{28}$, $C_2 \times C_{14}$ y $C_7 \overset{-1}{\rtimes} C_4$, $D_{2\cdot 14}$ respectivamente; y puesto que $7 \nmid (2-1)(2+1)$, no existen grupos no abelianos de orden 28 sin subgrupos normales de orden 7. Hemos obtenido cinco clases de isomorfismo, representadas por $C_{28}$, $C_2 \times C_{14}$, $C_7 \overset{-1}{\rtimes} C_4$ y $D_{2\cdot 14}$. □

Los teoremas anteriores y los resultados de las dos secciones previas permiten ampliar nuestra tabla como sigue:

| Orden | Número de Grupos | Representantes |
|---|---|---|
| 2 | 1 | $C_2$ |
| 3 | 1 | $C_3$ |
| 4 | 2 | $C_4$, $V := C_2 \times C_2$ |
| 5 | 1 | $C_5$ |
| 6 | 2 | $C_6$, $C_3 \rtimes C_2 \cong D_{2\cdot 3}$ |
| 7 | 1 | $C_7$ |
| 9 | 2 | $C_9$, $C_3 \times C_3$ |
| 10 | 2 | $C_{10}$, $D_{2\cdot 5}$ |
| 11 | 1 | $C_{11}$ |
| 12 | 5 | $C_{12}$, $C_2 \times C_6$, $D_{2\cdot 6}$, $A_4$ , $T$ |
| 14 | 2 | $C_{14}$, $D_{2\cdot 7}$ |
| 15 | 1 | $C_{15}$ |
| 17 | 1 | $C_{17}$ |
| 18 | 5 | $C_{18}$, $C_3 \times C_6$, $D_{2\cdot 9}$, $D_{2\cdot 3} \times C_3$, $(C_3 \times C_3) \overset{-1}{\rtimes} C_2$ |
| 19 | 1 | $C_{19}$ |
| 20 | 5 | $C_{20}$, $C_2 \times C_{10}$, $D_{2\cdot 10}$, $C_5 \overset{2}{\rtimes} C_4$, $C_5 \overset{-1}{\rtimes} C_4$ |
| 21 | 2 | $C_{21}$, $C_7 \rtimes C_3$ |
| 22 | 2 | $C_{22}$, $D_{2\cdot 11}$ |
| 23 | 1 | $C_{23}$ |
| 25 | 2 | $C_{25}$, $C_5 \times C_5$ |
| 26 | 2 | $C_{26}$, $D_{2\cdot 13}$ |
| 27 | 5 | $C_3^3$, $C_3 \times C_9$, $C_{27}$, $C_9 \rtimes C_3$, $(C_3 \times C_3) \rtimes C_3$ |
| 28 | 4 | $C_{28}$, $C_2 \times C_{14}$, $D_{2\cdot 14}$, $C_7 \overset{-1}{\rtimes} C_4$ |
| 29 | 1 | $C_{29}$ |
| 30 | 4 | $C_{30}$, $D_{2\cdot 15}$, $C_{15} \overset{4}{\rtimes} C_2$, $C_{15} \overset{11}{\rtimes} C_2$ |
| 31 | 1 | $C_{31}$ |

El lector notará que los únicos órdenes que faltan en la tabla son 8, 16 y 24, los primeros serán abordados en la siguiente sección, mientras que el último se dejará para la sección posterior.

## 3.3. Extensiones Cíclicas

Sean $G$ un grupo, $H \trianglelefteq G$ tales que que $G/H \cong C_n$, a tal grupo $G$ se le llama extensión cíclica (interior) de $H$. Si tomamos $a \in G$ tal que $\langle \bar{a} \rangle = G/H$, entonces $a^n \in H$ y $n$ es mínimo con tal propiedad; y si $v := a^n$, $\tau := \varphi_a|_H$, $\varphi_a \in Inn(G)$, $\tau \in Aut(H)$, además $\tau^n = \varphi_v \in Inn(H)$.

Al ser $G/H = G/H_D$ una partición del grupo, cada elemento $g \in G$ tiene una representación única de la forma $g = ha^i$ con $0 \leq i < n$, $h \in H$ y la operación en $G$ puede ser recuperada de la manera siguiente:

$$h_1 a^i h_2 a^j = \begin{cases} h_1 a^i h_2 a^{-i} a^{i+j} = h_1 \tau^i(h_2) a^{i+j}, & \text{si } i+j < n \\ \\ h_1 a^i h_2 a^{-i} a^n a^{i+j-n} = h_1 \tau^i(h_2) v a^{i+j-n}, & \text{si } i+j \geq n \end{cases}$$

Así, el grupo queda determinado por $(H, n, \tau, v)$; decimos que $G$ ***da lugar a la clase de extensión*** $(H, n, \tau, v)$ y llamamos a $a \in G$ un ***elemento inductor de*** $(H, n, \tau, v)$ ***en*** $G$. En general, definimos la ***clase de extensión*** $(H, n, \tau, v)$ como un grupo $H$, $n \in \mathbb{N}\backslash\{0\}$, $\tau \in Aut(H)$ y $v \in H$ tales que $\tau(v) = v$ y $\tau^n = \varphi_v \in Inn(H)$.

Observemos que en el caso en el que $H$ es cíclico de orden $m$ y $v = 1$, $G$ es un producto semidirecto de la forma $C_m \rtimes_\alpha C_n$.

Como es usual, al introducir una nueva estructura matemática, es útil definir una noción de equivalencia; diremos que $(H, n, \tau, v)$ es ***equivalente*** a $(H', n, \sigma, w)$ si existe un isomorfismo $\Phi : H \to H'$tal que $\Phi \circ \tau \circ \Phi^{-1} = \sigma$ y $\Phi(v) = w$, en símbolos $(H, n, \tau, v) \sim (H', n, \sigma, w)$ o $(H, n, \tau, v) \overset{\Phi}{\sim} (H', n, \sigma, w)$ .

Si $(H, n, \tau, v)$ es una clase de extensión y $\Phi : H \to H'$es un isomorfismo, al tenerse que $(\Phi \circ \tau \circ \Phi)^n = \Phi \circ \tau^n \circ \Phi^{-1}$, obtenemos que $(H, n, \tau, v)$ es equivalente a $(H', n, \Phi \circ \tau \circ \Phi^{-1}, \Phi(v))$ por definición. En particular, si se tienen dos grupos isomorfos $G$, $G'$ y $G$ da lugar a una clase de extensión, entonces $G'$ da lugar a una clase de extensión equivalente. El recíproco de esto es más interesante y está enunciado en el siguiente lema

**Lema 3.24.** *Si $G$, $G'$ son grupos que dan lugar a clases de extensión equivalentes, entonces $G \cong G'$.*

*Demostración.* Sean $(H, n, \tau, v)$, $(H', n, \sigma, w)$ clases de extensión equivalentes y sean $G$, $G'$ tales que $H \trianglelefteq G$, $H' \trianglelefteq G'$, donde $\sigma = \phi \circ \tau \circ \phi^{-1}$ y $w = \phi(v)$ para algún isomorfismo $\phi : H \to H'$, por definición existen $a \in G$, $b \in G'$ tales que $\tau = \varphi_a$, $\sigma = \varphi_b$, $a^n = v$ y $b^n = w$. La función $\Phi : G \to G'$ tal que $\Phi(xa^i) := \phi(x)b^i$, con $0 \leq i \leq n-1$ y $x \in H$, está bien definida y es biyectiva. Para mostrar que $\Phi$ es un homomorfismo sean $i, j \in \mathbb{Z}$ con $i + j = qn + r$, $q, r \in \mathbb{Z}$, $|r| < n$ y $x, y \in H$, entonces

$$\begin{aligned}
\Phi((xa^i)(ya^j)) &= \Phi(x(a^i y a^{-i})a^{i+j}) = \Phi(x\tau^i(y)v^q a^{i+j-qn}) = \phi(x\tau^i(y)v^q)b^{i+j-qn} \\
&= \phi(x)[\phi \circ \tau^i \circ \phi^{-1}(\phi(y))]\phi(v)^q b^{i+j-qn} = \phi(x)\sigma^i(\phi(y))w^q b^{i+j-qn} \\
&= \phi(x)\sigma^i(\phi(y))b^{i+j} = \phi(x)b^i\phi(y)b^j = \Phi(xa^i)\Phi(ya^j)
\end{aligned}$$

Por lo tanto, $\Phi$ es un isomorfismo y consecuentemente $G \cong G'$. □

Como consecuencia inmediata del lema, obtenemos el siguiente resultado.

**Corolario 3.25.** *Si $G$ es un grupo que da lugar a la clase de extensión $(H, n, \tau, v)$, existe una correspondencia biyectiva entre $Aut(G)$ y el conjunto de sextetas ordenadas $(H', n, \rho, w, a, \Phi)$, donde $a$ es un elemento inductor de $(H', n, \rho, w)$ en $G$ y $(H, n, \tau, v) \overset{\Phi}{\sim} (H', n, \rho, w)$.*

*Demostración.* Sea $(H, n, \tau, v)$ una clase de extensión y $G$ un grupo que da lugar a ésta, digamos $G = \{ha_0^i | h \in H, 0 \leq i < n\}$, con $a_0 \in G$ un elemento inductor de $(H, n, \tau, v)$. Cada $\Phi \in Aut(G)$ está determinado por su restricción a $H$ y su valor en $a_0$, ya que $G = \{\Phi(h)\Phi(a_0)^i | h \in H, 0 \leq i < n\}$; abusando de la notación, identifiquemos $\Phi$ con su restricción a $H$, por definición tenemos que $(\Phi(H), n, \Phi \circ \tau \circ \Phi^{-1}, \Phi(v)) \sim (H, n, \tau, v)$ y si $\Phi, \Psi \in Aut(G)$, $\Phi = \Psi$ si y solamente si $\Phi(a_0) = \Psi(a_0)$ y $\Phi(h) = \Psi(h)$, para toda $h \in H$, por lo que la correspondencia $Aut(G) \ni \Phi \mapsto (\Phi(H), n, \Phi \circ \tau \circ \Phi^{-1}, \Phi(v), \Phi(a_0), \Phi)$ es inyectiva. La prueba del lema anterior provee una función inyectiva del conjunto de sextetas $(H', n, \rho, v, a, \Phi)$ en el grupo de automorfismos de $G$ . Por lo tanto ambos conjuntos son biyectables. □

La siguiente afirmación también es un corolario del lema 3.22, pero dada su importancia en la clasificación de los grupos de orden 16, será enunciada como teorema.

**Teorema 3.26.**

1. *Sean $v, w \in H$ elementos automorfos, y sea $S$ una unión fija de clases de conjugación de $Aut(H)$. Supóngase que para toda $\tau \in S$ existen grupos $G_\tau$, $F_\tau$ que dan lugar a las clases de extensión $(H, n, \tau, v)$, $(H, n, \tau, w)$ respectivamente. Entonces las familias $\{G_\tau | \tau \in S\}$ y $\{F_\tau | \tau \in S\}$ contienen las mismas clases de isomorfismo.*

2. *Sea $v \in H$ característico, y sea $S$ una clase de conjugación de $Aut(H)$. Para cualesquiera $\sigma, \tau \in S$, si $G$, $G'$ dan lugar a las clases de extensión $(H, n, \tau, v)$, $(H, n, \sigma, v)$ (respectivamente), entonces $G \cong G'$.*

*Demostración.*

1. Tómese $\rho \in Aut(H)$ con $\rho(v) = w$. Claramente la correspondencia dada por $\tau \mapsto \sigma = \rho \circ \tau \circ \rho^{-1}$ es una biyección de $S$ en $S$ y las clases de extensión $(H, n, \tau, v)$, $(H, n, \sigma, w)$ son equivalentes. Se sigue del lema que la misma correspondecia induce otra entre los conjuntos $\{G_\tau | \tau \in S\}$ y $\{F_\tau | \tau \in S\}$.

2. Sea $\tau \in S$ fijo, es claro que $S = \{\phi \circ \tau \circ \phi^{-1}\}_{\phi \in Aut(H)}$ y para todo $\phi \in Aut(H)$ las clases $(H, n, \tau, v)$ y $(H, n, \phi \circ \tau \circ \phi^{-1}, v)$ son equivalentes,; entonces, por el lema 3.24, si $G$ y $G'$ dan lugar a $(H, n, \sigma, v)$ y $(H, n, \rho, v)$ respectivamente, con $\sigma, \rho \in S$, se tiene que $G \cong G'$.

□

Hasta ahora hemos considerado las clases de extensión siempre constre~nidas a un grupo que les da lugar; sin embargo, la definición de una clase de extensión $(H, n, \tau, v)$ es independiente de cualquier grupo $G$ en el que $H$ esté inmerso, lo cual sugiere preguntarse si dada $(H, n, \tau, v)$ existe un grupo que da lugar a esta. El siguiente teorema, publicado por Otto Hölder en 1895[10], resuelve ese problema (en nuestro caso, exhibiendo un grupo apropiado que da lugar a la extensión).

**Teorema 3.27.** *Cada clase de extensión $(H, n, \tau, v)$ es llevada a cabo por un grupo apropiado.*

*Demostración.* Sean $A := \{a^0, a^1, a^2, \ldots, a^{n-1}\}$, $G := H \times A$ (considerado como producto cartesiano de conjuntos, aquí $A$ es meramente un agregado de símbolos; por

[10]O. Hölder, Bildung zusammengesetzter Gruppen, *Math Annalen* **46** (1895) 321-422.

ejemplo, tomemos $A$ como el conjunto subyacente de $\mathbb{Z}_n$, con $a^i = i$) y defínase $\star : G \times G \to G$ como sigue:

$$(x, a^i) \star (y, a^j) := (x\tau^i(y)v^q, a^r), \text{ con } i + j = qn + r,\ q \in \{0, 1\},\ 0 \leq r < n \quad (3.3)$$

Se afirma que la operación recién definida es asociativa pues si tomamos $(x, a^i), (y, a^j), (z, a^k) \in G$ con $0 \leq i, j, k < n$ y $i + j = q_1 n + r_1$; $j + k = q_2 n + r_2$; $i + j + k = q_3 n + r_3$; entonces $q_1, q_2 \in \{0, 1\}$, $0 \leq q_3 \leq 2$, por lo tanto

$$\begin{aligned}((x, a^i) \star (y, a^j)) \star (z, a^k) &= (x\tau^i(y)v^{q_1}, a^{r_1}) \star (z, a^k) = (x\tau^i(y)v^{q_1}\tau^{r_1}(z)v^{q_3-q_1}, a^{r_3}) \\ &= (x\tau^i(y)\tau^{q_1 n}\tau^{r_1}(z)v^{q_3}, a^{r_3}) = (x\tau^i(y)\tau^{i+j}(z)v^{q_3}, a^{r_3})\end{aligned}$$

y por otro lado

$$\begin{aligned}(x, a^i) \star ((y, a^j) \star (z, a^k)) &= (x, a^i) \star (y\tau^j(z)v^{q_2}, a^{r_2}) = (x\tau^i(y)\tau^{i+j}(z)v^{q_2}v^{q_3-q_2}, a^{r_3}) \\ &= (x\tau^i(y)\tau^{i+j}(z)v^{q_3}, a^{r_3})\end{aligned}$$

Por tanto, la operación es asociativa.

Se tiene de manera trivial que $(1, a^0) \star (x, a^i) = (x, a^i) \star (1, a^0) = (x, a^i)$, $(x, a^i) \star (\tau^{-i}(x^{-1})v^{-1}, a^{n-i}) = (x\tau^{i-i}(x^{-1})v^{-1}v, a^0) = (1, a^0)$ y $(\tau^{-i}(x^{-1})v^{-1}, a^{n-i}) \star (x, a^i) = (\tau^{-i}(x^{-1})v^{-1}\tau^{n-i}(x)v, a^0) = (1, a^0)$ para $1 \leq i < n$.

Se concluye de lo anterior que $G$ es un grupo, llamado ***extensión cíclica (exterior) de*** $H$.

Como $(x, a^0) \star (y, a^0) = (xy, a^0)$, la función $h \overset{\iota}{\mapsto} (h, a^0)$ es un isomorfismo de grupos, por lo que $(\bar{H}, n, \iota \circ \tau \circ \iota^{-1}, (v, a^0)) \sim (H, n, \tau, v)$, donde $\bar{H} := \iota(H)$ y ya que:

$$\begin{aligned}(1, a^1) \star (x, a^0) \star (v^{-1}, a^{n-1}) &= (1, a^1) \star (xv^{-1}, a^{n-1}) = (\tau(x)v^{-1}v, a^0) \\ &= (\tau(x), a^0) = \iota \circ \tau \circ \iota^{-1}(x, a^0)\end{aligned}$$

Entonces el subgrupo $\bar{H}$ es preservado por las conjugaciones de todos los elementos de $G$, dado que para cualesquiera $y \in H$ e $i \in \{0, ..., n-1\}$, $(y, a^i) = (y, a^0) \star (1, a^i)$, es decir $\bar{H} \trianglelefteq G$.

Ahora, $\varphi : G \to \mathbb{Z}_n$ es un epimorfismo con $\ker(\varphi) = \bar{H}$, por lo tanto $G/\bar{H} \cong \mathbb{Z}_n$.

Además $\varphi(1, a^1) = \bar{1}$ y $\bar{1}$ es un generador de $\mathbb{Z}_n$, se sigue de esto que $G/\bar{H} = \langle \bar{H}(1, a^1) \rangle$. Por último, notemos que $(1, a^1)^n = (v, a^0)$.

Todo lo anterior permite decir que $G$ da lugar a la clase de extensión $(\bar{H}, n, \iota \circ \tau \circ \iota^{-1}, (v, a^0))$, la cual es claramente equivalente a $(H, n, \tau, v)$. □

Tenemos en virtud del lema 3.24 y el teorema anterior que clases de extensión equivalentes *siempre* son llevadas a cabo por grupos isomorfos; sin embargo, a veces clases de extensión no equivalentes $(H, n, \tau, v)$, $(H', n, \rho, w)$ son llevadas a cabo por grupos isomorfos $G$, $G'$, esto claramente sucede si y sólo si para todo isomorfismo $\Phi : G \to G'$, $\Phi(v) \neq w \circ \Phi|_H \circ \tau \circ \Phi|_H^{-1} \neq \rho$ , a esta situación incómoda se le conoce como el ***problema de isomorfismo*** (*isomorphism problem*) y será ilustrada en la clasificación de grupos de orden 8.

## Grupos de orden 8 y 16

Ahora clasificaremos los grupos de orden 8 mediante las clases de extensión introducidos en esta sección, los cuales serán de vital importancia en la clasificación de los grupos de orden 16, desarrollada al final de esta subsección.

Antes de iniciar, es conveniente demostrar el siguiente lema.

**Lema 3.28.** *Si $G$ es un grupo tal que $x^2 = 1$ para cada $x \in G$, entonces $G$ es abeliano. Más aún, si $G$ es finito, $|G| = 2^n$ para alguna $n \in \mathbb{N}$ y $G \cong C_2^n$.*

*Demostración.* $G$ es abeliano si y solamente si $xy = yx$ para cualesquiera $x, y \in G$, pero observemos que $xy = yx \Leftrightarrow x(xy)y = x(yx)y \Leftrightarrow (xy)^2 = x^2y^2$ y se tiene por hipótesis $x^2 = y^2 = (xy)^2 = 1$, por lo tanto $G$ es un grupo abeliano.

La segunda parte de la afirmación se sigue directamente de la proposición 2.32. □

Sea $G$ un grupo de orden 8, debido a que la condición $x^2 = 1$ para toda $x \in G$ implica por el lema anterior (y es de hecho equivalente a) $G \cong C_2 \times C_2 \times C_2$, podemos pensar que $G \ncong C_2 \times C_2 \times C_2$. Bajo el supuesto anterior, existe un subgrupo $H$ de $G$ cíclico de orden 4 (y necesariamente normal por el corolario 2.31), digamos $\langle x \rangle = H$, se tiene que $H \lhd G$ y $G/H \cong C_2$, por lo tanto $G$ es una extensión cíclica de $H$ por $C_2$; y así, $G$ da lugar a un tipo de extensión $(H, 2, \tau, v)$, donde $\tau \in Aut(H)$ y

$v \in H$ son tales que $\tau(v) = v$ y $\tau^2 = \varphi_v|_H$. Puesto que $|Aut(H)| = 2$, existen a lo más $|Aut(H)||H| = 8$ tipos de extensión; de hecho existen exactamente 6, ya que la correspondencia $\sigma_3 \in Aut(H)$ es tal que $\sigma_3(x) \neq x$ y $\sigma_3(x^3) = x \neq x^3$. Se tiene entonces que los tipos de extensión posibles son $(H, 2, \sigma_1, 1)$, $(H, 2, \sigma_1, x)$, $(H, 2, \sigma_1, x^2)$, $(H, 2, \sigma_1, x^3)$, $(H, 2, \sigma_3, 1)$, $(H, 2, \sigma_3, x^2)$, como $Aut(H) \cong \mathbb{Z}_4^\times$ es abeliano y $\sigma_3(x) = x^3$, $(H, 2, \sigma_1, x) \sim (H, 2, \sigma_1, x^3)$ por definición, por lo que podemos descartar alguna, digamos $(H, 2, \sigma_1, x^3)$; ahora si suponemos que $G$ da lugar a $(H, 2, \sigma_1, x^2)$ y $a \in G$ es tal que $axa^{-1} = x$, $\langle \bar{a} \rangle = G/H$ y $a^2 = x^2$, tenemos que $(ax)x(ax)^{-1} = x$, $(ax)^2 = axax = a^2x^2 = 1$ y además $\langle \overline{ax} \rangle = G/H$ (ya que $ax \notin H$); por lo tanto $G$ también da lugar a $(H, 2, \sigma_1, 1)$.

La discusión anterior nos permite reducir las clases de isomorfismo a las que puede pertenecer $G$ a lo más 4, cada una de las cuales es no vacía, ya que el teorema 3.27 garantiza la existencia de grupos que dan lugar a los tipos de extensión correspondientes, para probar que existen en efecto exactamente 4 clases de isomorfismo, debemos estudiar un poco los grupos que dan lugar a estas extensiones. Sean $G_1 = \langle x, a_1 \rangle$, $G_2 = \langle x, a_2 \rangle$, $G_3 = \langle x, a_3 \rangle$, $G_4 = \langle x, a_4 \rangle$ grupos que dan lugar a $(H, 2, \sigma_1, 1)$, $(H, 2, \sigma_1, x)$, $(H, 2, \sigma_3, 1)$, $(H, 2, \sigma_3, x^2)$ respectivamente, con $a_1^2 = 1$, $a_2^2 = x$, $a_3^2 = 1$, $a_4^2 = x^2$, $a_1 x a_1^{-1} = x$, $a_2 x a_2^{-1} = x$, $a_3 x a_3^{-1} = x^{-1}$, $a_4 x a_4^{-1} = x^{-1}$.

Ninguno de los grupos de $\{G_1, G_2\}$ puede ser isomorfo a los de $\{G_3, G_4\}$ porque los primeros son abelianos, mientras que los segundos no lo son. Además, mientras que en $G_1$ $|x^i a^j| \leq 4$ para cada $i \in \{0, ..., 3\}$, $j \in \{0, 1\}$; en $G_2$, $a_2^2 = x$, que implica $\langle a_2 \rangle = \langle x, a_2 \rangle = G_2$, por lo tanto $G_1$ y $G_2$ no son isomorfos. En el caso de $G_3$, $|x^i a_3| = 2$ para $i \in \{0, .., 3\}$, mientras que en $G_4$ $(x^i a_4)^2 = x^i a_4 x^i a_4^{-1} a_4^2 = x^i x^{-i} a_4^2 = x^2$, por lo que existen en $G_4$ al menos 3 elementos de orden 4 , en contraste con $G_3$ donde existen exactamente dos; podemos concluir entonces que $G_3$ no es isomorfo a $G_4$.

Observemos algo más sobre los grupos en cuestión. Para $a_i \in G_i$, $i \in \{1, 3\}$, $|a_i| = 2$, entonces $G_i = H \rtimes \langle a_i \rangle$ o $G_i = H \times \langle a_i \rangle$; como $G_1$ es abeliano, obtenemos $G_1 = H \times \langle a_1 \rangle \cong C_4 \times C_2$. Para el caso de $G_3$, observemos que $a_3 x a_3 = x^{-1}$ y $|x| = 4$, lo que implica por definición que $G_3$ isomorfo a $D_{2\cdot 4}$. Hemos mencionado también que $G_2 = \langle a_2 \rangle$, es decir, $G_2$ es un grupo cíclico de orden 8. Por lo tanto $G_2 \cong C_8$.

Para hacer más fácil el tratamiento de $G_4$, introduciremos una presentación más clásica para éste debida a Hamilton. Consideremos el conjunto de símbolos $\mathbf{Q} =$

$\{1,-1,i,-i,j,-j,k,-k\}$[11] y la función $\xi : G_4 \to \mathbf{Q}$ tal que $\xi(1) = 1$, $\xi(x) = i$, $\xi(x^2) = -1$, $\xi(x^3) = -i$, $\xi(a_4) = j$, $\xi(xa_4) = k$, $\xi(x^2a_4) = -j$, $\xi(x^3a_4) = -k$, es evidente que $\xi$ es una biyección. Entonces podemos proveer a $\mathbf{Q}$ con una estructura de grupo si definimos para $q_1, q_2 \in \mathbf{Q}$, $q_1 \star q_2 = \xi(\xi^{-1}(q_1)\xi^{-1}(q_2))$; con esta estructura, $\xi$ es un homomorfismo y $G_4 \cong \mathbf{Q}$, en particular tenemos las relaciones $i^2 = j^2 = k^2 = ijk = -1$,[12] $\mathbf{Q}$ es denominado el grupo de los cuaternios.

Podemos recapitular los párrafos anteriores en el siguiente resultado.

**Teorema 3.29.** *Si $G$ es un grupo de orden 8, $G$ es isomorfo a uno y sólo uno de los siguientes grupos:*
$C_2 \times C_2 \times C_2$, $C_4 \times C_2$, $C_8$, $D_{2\cdot 4}$, $\mathbf{Q}$.

Antes de continuar con nuestra clasificación, será útil para la el desarrollo posterior discutir brevemente acerca de los grupos de automorfismos de los grupos de orden 8.

Para $C_2 \times C_2 \times C_2$, la proposición 2.32 provee $Aut(C_2 \times C_2 \times C_2) \cong GL(3,2)$, por lo tanto $Aut(C_2 \times C_2 \times C_2)$ es un grupo (no abeliano) de orden $2^{\frac{3(3-1)}{2}}(2^3-1)(2^2-1) = 2^3 \cdot 3 \cdot 7 = 168$ isomorfo al grupo de matrices invertibles de $3 \times 3$ con entradas en $\mathbb{Z}_2$ [Proposición 2.32].

Observemos que $D_{2\cdot 4} = \{1, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$ con $\beta\alpha\beta = \alpha^{-1}$, al tenerse que $(\alpha^i\beta)^2 = \alpha^i\beta\alpha^i\beta = \alpha^i\alpha^{-i} = 1$, obtenemos que la asignación $\alpha \mapsto \alpha^j$, $\beta \mapsto \alpha^i\beta$ con $1 \leq i, j \leq 4$ y $(j,4) = 1$ determina un elemento de $Aut(D_{2\cdot 4})$, y es claro que cualquier automorfismo de $D_{2\cdot 4}$está caracterizado por una pareja $(\alpha^j, \alpha^i\beta)$ de la forma anterior, por lo tanto $Aut(D_{2\cdot 4}) = \{\phi_{j,i} | \phi_{j,i}(\alpha) = \alpha^j, \phi_{j,i,}(\beta) = \alpha^i\beta, (j,4) = 1\}$, por lo tanto $|Aut(D_{2\cdot 4})| = 8$, además $\phi_{3,4}^2 = \phi_{3,1}^2 = 1$ y $\phi_{3,4}\phi_{1,1}\phi_{3,4} = \phi_{1,3}$, por lo tanto $Aut(D_{2\cdot 4})$ es un grupo no abeliano de orden 8 que tiene al menos dos elementos de orden 2, concluimos por el teorema anterior que $Aut(D_{2\cdot 4}) \cong D_{2\cdot 4}$.

[11] Digamos $1 := (1,0,0,0)$, $-1 := (-1,0,0,0)$, $i := (0,1,0,0)$, $-i := (0,-1,0,0)$, $j := (0,0,1,0)$, $-j = (0,0,-1,0)$, $k = (0,0,0,1)$, $-k = (0,0,0,-1)$, con $\pm 1 \in \mathbb{Z}_3^\times$.

[12] Una famosa anécdota cuenta que William R. Hamilton, al estar interesado en dotar a $\mathbb{R}^3$ con una estructura multiplicativa que reflejara movimientos del espacio, al tomar un paseo con su esposa por el *Royal Canal* en Dublín se le ocurrieron estas famosas relaciones y las grabó en una de las piedras de este puente; no existe a la fecha algún vestigio de las inscripciones de Hamilton, sin embargo, el gobieno irlandés irguió una placa en el puente Brougham para conmemorar el suceso; y desde 1989 el Departamento de Matemáticas de la Universidad de Irlanda en Maynooth organiza una peregrinación, donde científicos (entre los que se incluyen Murray Gell-Mann en 2002, Andrew Wiles en 2003, Steven Weinberg en 2005 y Frank Wilzek en 2007) caminan desde el Observatorio Dunsik hasta el puende del Royal Canal donde sucedió el famoso suceso.

Ya que el caso de $\mathbf{Q}$ es el más complejo, nos ayudaremos del corolario 3.25 para contar sus automorfismos. Consideremos $G_4$ como en la construcción pasada, al tenerse que $x^2 = a_4^2 = (xa_4)^2$, entonces los elementos $x$, $x^3$, $a_4$, $a_4^3$, $xa_4$ y $(xa_4)^3$ tienen orden 4; además $a_4xa_4^3 = a_4^3xa_4 = (xa_4)x(xa_4)^3 = (xa_4)^3x(xa_4) = x^3$, $xa_4x^3 = x^3a_4x = (xa_4)a_4(xa_4)^3 = (xa_4)^3a_4(xa_4) = a_4^3$ y $x(xa_4)x^3 = x^3(xa_4)x = a_4(xa_4)a_4^3 = a_4^3(xa_4)a_4^3 = (xa_4)^3$, por lo que $G_4$ da lugar a las clases de extensión

$$\begin{aligned}
(\langle x\rangle, 2, \varphi_{a_4}|_{\langle x\rangle}, x^2) = (\langle x\rangle, 2, \varphi_{xa_4}|_{\langle x\rangle}, x^2) &= (\langle x\rangle, 2, \varphi_{a_4^3}|_{\langle x\rangle}, x^2) = (\langle x\rangle, 2, \varphi_{(xa_4)^3}|_{\langle x\rangle}, x^2) \\
(\langle a_4\rangle, 2, \varphi_x|_{\langle a_4\rangle}, x^2) = (\langle a_4\rangle, 2, \varphi_{xa_4}|_{\langle a_4\rangle}, x^2) &= (\langle a_4\rangle, 2, \varphi_{x^3}|_{\langle a_4\rangle}, x^2) = (\langle a_4\rangle, 2, \varphi_{(xa_4)^3}|_{\langle a_4\rangle}, x^2) \\
&\text{y} \\
(\langle xa_4\rangle, 2, \varphi_x|_{\langle xa_4\rangle}, x^2) = (\langle xa_4\rangle, 2, \varphi_{a_4}|_{\langle xa_4\rangle}, x^2) &= (\langle xa_4\rangle, 2, \varphi_{x^3}|_{\langle xa_4\rangle}, x^2) = (\langle xa_4\rangle, 2, \varphi_{a_4^3}|_{\langle xa_4\rangle}, x^2)
\end{aligned}$$

que son por fuerza equivalentes, además para cualesquiera dos isomorfismos $\Phi : \langle x\rangle \to \langle a_4\rangle$, $\Psi : \langle x\rangle \to \langle xa_4\rangle$ $\Phi(x^2) = \Psi(x^2) = x^2$ y se tiene que $\Phi \circ \tau \circ \Phi^{-1} = \sigma_3 \in Aut(\langle a_4\rangle)$ si y sólo si $\tau = \sigma_3 \in Aut(\langle a_4\rangle)$ y $\Psi^{-1} \circ \tau \circ \Psi = \sigma_3 \in Aut(\langle xa_4\rangle)$ si y sólo si $\tau = \sigma_3 \in Aut(\langle x\rangle)$, entonces el corolario 3.25 dice que $Aut(G_4)$ es biyectable con el conjunto de sextetas ordenadas $(H, 2, \tau, x^2, \alpha, \Phi)$, donde $\alpha \in G_4$ induce $(H, 2, \tau, x^2)$ y $(H, 2, \tau, x^2) \overset{\Phi}{\sim} (\langle x\rangle, 2, \varphi_{a_4}|_{\langle x\rangle}, x^2)$, que tiene $4 \cdot |Aut(\langle x\rangle)| + 4 \cdot |Iso(\langle x\rangle, \langle a_4\rangle)| + 4 \cdot |Iso(\langle x\rangle, \langle xa_4\rangle)|$ elementos, donde $Iso(\langle x\rangle, \langle a_4\rangle)$, $Iso(\langle x\rangle, \langle a_4x\rangle)$ denotan el conjunto de isomorfismos de $\langle x\rangle$ a $\langle a_4\rangle$ y $\langle xa_4\rangle$ respectivamente, no es dificil ver que $|Aut(\langle x\rangle)| = |Iso(\langle x\rangle, \langle a_4\rangle)| = |Iso(\langle x\rangle, \langle xa_4\rangle)| = 2$, por lo que $|Aut(G_4)| = |Aut(Q)| = 3 \cdot 4 \cdot 2 = 24$.

Si $\langle x, t\rangle = C_4 \times C_2$ con $x^4 = t^2 = 1$, entonces cualquier automorfismo $\psi \in Aut(C_4 \times C_2)$ es tal que $|\psi(x)| = 4$ y $|\psi(t)| = 2$ por lo que $\psi(x) \in \{x, x^3, xt, x^3t\}$ y $\psi(t) \in \{t, x^2t, x^2\}$, además $\langle x\rangle \cap \langle t\rangle = \mathbf{1}$ implica $\psi(t) \notin \langle\psi(x)\rangle$, así los casos posibles son listados a continuación.

| $Aut(C_4 \times C_2)$ | Efecto sobre $x$ | Efecto sobre $t$ | Orden del automorfismo |
|---|---|---|---|
| 1 | $x$ | $t$ | 1 |
| $\alpha$ | $x^3t$ | $x^2t$ | 4 |
| $\alpha^2$ | $x^3$ | $t$ | 2 |
| $\alpha^3$ | $xt$ | $x^2t$ | 4 |
| $\beta$ | $xt$ | $t$ | 2 |
| $\alpha\beta$ | $x^3$ | $x^2t$ | 2 |
| $\alpha^2\beta$ | $x^3t$ | $t$ | 2 |
| $\alpha^3\beta$ | $x^3$ | $x^2t$ | 2 |

Por lo tanto $Aut(C_4 \times C_2)$ es un grupo de orden 8 sin elementos de orden 8, que posee dos elementos de orden 4, y cinco de orden 2 por lo tanto $Aut(C_4 \times C_2) \cong D_{2\cdot 4}$ [Teorema 3.29].

Finalmente, por el teorema 2.20 $Aut(C_8)$ es isomorfo a $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$, y como $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 (\text{mod } 8)$, obtenemos que $Aut(C_8)$ es un grupo de orden $4 = 2^2$ sin elementos de orden 4, por lo tanto $Aut(C_8) \cong V$ [Corolario 2.33].

La clasificación de los grupos de orden 16 se realizará de manera similar a la de los grupos de orden 8, pero con un obstáculo adicional; si $G$ es un grupo de orden 16 no isomorfo a $(C_2)^4$, no necesariamente tiene un subgrupo isomorfo a $C_8$; pero si no lo tiene, $C_4 \times C_2$ resulta ser un buen sustituto. Comenzaremos la clasificación mostrando de cada grupo de orden 16 tiene un grupo apropiado de orden 8 (i.e. isomorfo a $C_8$ o $C_4 \times C_2$) y posteriormente mostraremos que cada grupo de dicho orden da lugar a una extensión de los grupos considerados.

**Lema 3.30.** *Si* G *es un grupo de orden 16 no isomorfo a* $(C_2)^4$*, entonces existe* $N \lhd G$ *tal que* $N \cong C_8$ *o* $N \cong C_4 \times C_2$*.*

*Demostración.* Como los subgrupos de índice 2 en un grupo son normales, se supondrá que G no contiene un elemento de orden 8 y se probará que contiene una copia de $C_4 \times C_2$.

Al ser $G$ un 2-grupo, se sabe que $Z(G) \neq 1$, entonces existe $z \in Z(G)$ tal que $|z| = 2$, sea $C := \langle z \rangle$. A continuación se consideran dos casos:

- Caso 1: existe $g \in G$ con $|g| = 4$ y $g^2 \neq z$, entonces $\langle g \rangle \cap \langle z \rangle = 1$ y $gz = zg$. Si $N := \langle g \rangle \times C$, entonces $N \cong C_4 \times C_2$ .

- Caso 2: para toda $g \in G$ con $|g| = 4$, $g^2 = z$, entonces para toda $\overline{g} \in G/C$, $|\overline{g}| \leq 2$, y se sabe que un grupo tal es abeliano, de lo que es inmediato que para cualesquiera $g, h \in G$, $ghg^{-1} \in hC$, y así $|g^G| \leq 2$. Ahora si consideramos $g \in G$ de orden 4 y si $C_g$ es el centralizador de $g$ en $G$, $|C_g|[G : C_g] = |C_g||g^G| = 16$ y por la observación previa $|C_g| \geq 8$, por tanto existe $k \in C_g \backslash \langle g \rangle$. Si $|k| = 2$, entonces $N := \langle g \rangle \times \langle k \rangle \cong K_8$. Si $|k| = 4 \Rightarrow (gk)^2 = g^2k^2 = zz = 1$ y $k \neq g^{-1} \in \langle g \rangle$, por tanto $|gk| = 2$ y así $N := \langle g \rangle \times \langle gk \rangle \cong C_4 \times C_2$ provisto que $gk \notin \langle g \rangle$, pero $gk \in \langle g \rangle$ implica $k \in \langle g \rangle$ lo que contradice la elección de $k$.

□

La tabla de automorfismos de $C_4 \times C_2$, a quien llamaremos por comodidad $K_8$, permite acotar el número de clases de isomorfismo de los grupos de orden 16 mediante las clases de extensión a las que dan lugar. A lo largo de la siguiente demostración, tomaremos $K_8 = \langle x, t \rangle$, $x^4 = t^2 = 1$ y $C_8 = \langle y \rangle$

**Lema 3.31.** *Cada grupo de orden 16 no isomorfo a $(C_2)^4$ da lugar a una de las siguientes extensiones $(C_8, 2, \sigma_i, 1)$, $i \in \{1, 3, 5, 7\}$; $(C_8, 2, \sigma_7, y^4)$; $(C_8, 2, \sigma_1, y)$; $(K_8, 2, \alpha^i, 1)$, $i \in \{0, 2\}$;, $(K_8, 2, \alpha^j\beta, 1)$, $j \in \{0, 3\}$; $(K_8, 2, \alpha^2, x^2)$; $(K_8, 2, \beta, x^2)$;$(K_8, 2, 1, t)$.*

*Demostración.*

Sea $G$ un grupo de orden 16 no isomorfo a $(C_2)^4$, entonces, por el lema 3.30, $G$ es una extensión cíclica de $C_8$ o de $C_4 \times C_2$. La demostración se realizará por casos según el orden del elemento inductor $a \in G$. En lo subsiguiente $v = a^2$ y $\tau$ es la restricción de $\varphi_a$ a $C_8$ o $K_8$ según el caso lo amerite.

*Caso* 1. Caso 1: $|a| = 2$. Entonces $v = 1$. Como $Aut(C_8) \cong \mathbb{Z}_8^\times$, $i \in \{1, 3, 5, 7\}$ $\sigma_i^2 = 1$ y obtenemos las clases de extensión $(C_8, 2, \sigma_i, 1)$, $i \in \{1, 3, 5, 7\}$. Por lo tanto, podemos suponer que $|b| \geq 4$ para cada $b \in G \backslash C_8$, de lo contrario estamos de regreso en el caso 1.

*Caso* 2. Caso 2: $|a| = 4$. Aquí $v = y^4$. Si $\tau = \sigma_3$ entonces $(ya)(ya) = y\sigma_3(y)a^2 = yy^3a^2 = 1$; de donde $|ya| = 2$, pero se ha agregado la hipótesis $|b| \geq 4$ para cada $b \in G \backslash C_8$. De manera similar si $\tau$ es $\sigma_1$ o $\sigma_5$, entonces $|y^2a| = 2$. Se concluye que a lo más $(C_8, 2, \sigma_7, y^4)$ es una clase de extensión que no ha sido considerada.

*Caso* 3. Caso 3: $|a| = 8$. En tal situación $v = y^2$ o $v = y^6$. En cualquier caso $\tau(v) = v$ ocurre solamente para $\tau \in \{\sigma_1, \sigma_5\}$. Sea $v = y^2$, entonces $y^3ay^3a = y^3\sigma_1(y^3)a^2 = 1$ y $yaya = y\sigma_5(y)a^2 = 1$, se sigue (por la misma razón que en el caso anterior) que $G$ también da lugar a alguna de las clases ya consideradas. Como $y^2$ y $y^6$ son automorfos, se sigue del teorema 3.26 (1) que obtenemos los mismos grupos de las extensiones cíclicas $(C_8, 2, \sigma_i, y^6)$, $i \in \{1, 5\}$.

*Caso* 4. Caso 4: $|a| = (16)$. Se tiene que $G \cong C_{16}$, el cual da lugar a $(C_8, 2, \sigma_1, y^i)$, $0 \leq i < 8$, $i$ impar. Además $y$, $y^3$, $y^5$, $y^7$son automorfos por ser generadores de $C_8$, de donde se sigue que podemos considerar sólo $(C_8, 2, \sigma_1, y)$.

Derivamos ahora las siete clases de extensión $(K_8, 2, \tau, v)$, como antes $K_8 = \langle x, t\rangle$, $x^4 = t^2 = xtx^{-1}t^{-1} = 1$. Como lo muestra la tabla de automorfismos de $C_4 \times C_2$, $\tau \in Aut(K_8)$, $\tau^2 = 1$ solo ocurre para los elementos de las clases de conjugación $\{1\}$, $\{\alpha^2\}$, $\{\beta, \alpha^2\beta\}$ y $\{\alpha\beta, \alpha^3\beta\}$.

Ya que han sido considerados los casos en los que $G$ contiene una copia de $C_8$, podemos suponer que $G$ sólo tiene elementos de orden menor a 8.

*Caso* 1. Caso 5: $|a| = 2$. Entonces $v = 1$ es característico en $K_8$ y por el Teorema 3.26 (2) sólo es necesario considerar un representante de cada una de las clases de conjugación arriba mencionadas. Así obtenemos las clases de extensión $(K_8, 2, 1, 1)$, $(K_8, 2, \alpha^2, 1)$, $(K_8, 2, \beta, 1)$, $(K_8, 2, \alpha^3\beta, 1)$.

*Caso* 2. Caso 6: $|a| = 4$. Se sigue que $v \in \{x^2, x^2t, t\}$ y el caso anterior nos permite suponer $|b| \geq 4$ para todo elemento $b \in G\backslash K_8$. Se consideran tres subcasos.

*Caso* I. Subcaso $v = x^2$. Como $v$ es característico, de nuevo basta restringirse a 1, $\alpha^2$, $\beta$ y $\alpha^3\beta$. Si $\tau = 1$, $|xa| = 2$; y $\tau = a^3\beta$ implica $|xta| = 2$, por lo que las únicas clases de extensión realizadas por grupos de alguna clase de isomorfismo nueva son a lo mas $(K_8, 2, \alpha^2, x^2)$ y $(K_8, 2, \alpha\beta, x^2)$.

*Caso* II. Subcaso $v = t$. La condición $\tau(v) = v$ restringe este automorfismo a $\{1, \alpha^2, \beta, \alpha^2\beta\}$. Si $\tau = \alpha^2\beta$, entonces $|xa| = 2$. Si $\tau = \beta$, se tiene $xaxa = x\beta(x)a^2 = x(xt)t = x^2$ y si definimos $\hat{a} := xa$, estamos de regreso en el subcaso anterior. Si $\tau = \alpha^2$ tenemos $[x^2, a] = x^2ax^2a^{-1} = x^2\alpha^2(x^2) = 1$ y así $N := \langle x^2, a\rangle =$

$\{1, a, t, ta, x^2, x^2a, x^2t, x^2ta\} \cong K_8$, siendo $t$ el único elemento característico no trivial. Como $xaxa = x\alpha^2(x)a^2 = xx^3t = t$ si tomamos $\hat{a} := xa \notin N$ volveremos al primer subcaso. Por lo tanto solo queda $(K_8, 2, 1, t)$ sin descartar.

*Caso* III. Subcaso $v = x^2t$. Los únicos $\tau \in Aut(K_8)$ que satisfacen $\tau(v) = v$ son los elementos de $S := \{1, \alpha^2, \beta, \alpha^2\beta\}$. Ya que $v$ es automorfo a t ($\alpha\beta(x^2t) = x^2x^2t = t$) y $S$ es una unión de clases de conjugación, usando de nuevo el teorema 3.26 (1) concluimos que este caso nos trae de vuelta a (II).

□

Hasta ahora hemos logrado clasificar mediante extensiones las posibles clases de isomorfismo a las que pertenecen los grupos de orden 16, el teorema de la extensión cíclica de Hölder nos permite asegurar que en ningún caso la clase considerada es vacía i.e. existe un grupo de orden 16 que de lugar a dicha clase de extensión; sin embargo, nos resta hacer ver que los grupos considerados proveen una lista irredundante de representantes de dichas clases.

Una vez que contamos con grupos que den lugar a las extensiones listadas en el lema 3.31, observamos que, a la luz de la discusión anterior, éstos admiten descripciones más simples. Sean $G_1, ..., G_{13}$ grupos que dan lugar a las extensiones $(C_8, 2, \sigma_i, 1)$, $i \in \{1, 3, 5, 7\}$; $(C_8, 2, \sigma_7, y^4)$; $(C_8, 2, \sigma_1, y)$; $(K_8, 2, 1, 1)$; $(K_8, 2, \alpha^2, 1)$; $(K_8, 2, \beta, 1)$; $(K_8, 2, \alpha^3\beta, 1)$ $(K_8, 2, \alpha^2, x^2)$; $(K_8, 2, \beta, x^2)$; $(K_8, 2, 1, t)$ respectivamente. Para $G_1$, $G_2$, $G_3$ y $G_4$, $C_8 \cap \langle a \rangle = \mathbf{1}$, por lo tanto $G_1 \cong C_8 \times C_2$, $G_2 \cong C_8 \overset{3}{\rtimes} C_2$, $G_3 \cong C_8 \overset{5}{\rtimes} C_2$, $G_4 \cong C_8 \overset{7}{\rtimes} C_2 = D_{2\cdot 8}$, $G_6 \cong C_{16}$; en $G_7$ $at = ta$ y $a^2 = t^2 = 1$, por lo que $\langle a, t \rangle \cong C_2 \times C_2 =: K_4$; además $K_4 \cap C_4 = \mathbf{1}$ y los elementos de éstos conmutan, de lo que es inmediato que $G_7 \cong K_4 \times C_4$; en el caso de $G_8$ $\langle x, a \rangle \cong D_{2\cdot 4}$ y $at = \varphi_a(t)a = \alpha^2(t)a = ta$,$xt = tx$, entonces $G_8 \cong D_{2\cdot 4} \times C_2$; en $G_9$ $\langle a, t \rangle \cong K_4$, $xax^{-1} = a\varphi_a^{-1}(x)x^3 = a\beta(x)x^3 = axtx^3 = at$, $xt = tx$ y $C_4 \cap \langle a, t \rangle = \mathbf{1}$, así $G_9$ da lugar a una extensión cíclica de tipo $(K_4, 4, \tau, 1)$, lo cual implica $G_9 \cong K_4 \rtimes C_4$;[13] $G_{10}$ y $G_{11}$ tienen como subgrupos (normales) a

[13]El hecho que éste es en efecto el único producto semidirecto propio de $K_4$ y $C_4$ descansa en el hecho de que $Aut(K_4)$ es un grupo de orden $2 \cdot 3 = 6$; y si $(K_4, 4, \tau, 1)$ es una extensión cíclica, se tiene que $\tau^4 = 1$ y si $\tau \neq 1$, entonces $|\tau| = 2$; pero por los teoremas de Sylow, todos estos elementos son conjugados, esto en conjunto con el teorema 3.26 (2) implica que todas las extensiones cíclicas de esta forma dan lugar la mismo grupo. Se concluye de esto que existe un solo producto semidirecto

$\langle x, ta\rangle$ y $\langle x, a\rangle$ respectivamente, los cuales dan lugar a extensiones equivalentes a $(C_4, 2, \sigma_3, x^2)$, por lo tanto éstos son isomorfos a $\mathbf{Q}$; sucede además que en $G_{11}$ $xt = tx$ y $at = \varphi_a(t)a = \alpha^2(t)a = ta$, por tanto $G_{11} = \langle x, a\rangle \times \langle t\rangle \cong Q \times C_2$; de manera similar, en $G_{10}$ $\langle x, ta\rangle \cap \langle t\rangle = \mathbf{1}$, pero en este caso $|\varphi_t|_{\langle x,ta\rangle}| = 2$ y $G_{10}$ da lugar a una extensión cíclica de la forma $(\mathbf{Q}, 2, \tau, 1)$, por lo que $G_{10} \cong \mathbf{Q} \rtimes C_2$, que resulta ser el único producto semidirecto no trivial de éstos que no posee elementos de orden 8;[14] procediendo de manera análoga en $G_{12}$, $G_{13}$ observamos que $\langle xa\rangle \lhd G_{12}$, $\langle a\rangle \lhd G_{13}$ y ambos subgrupos son de orden 4, además en $G_{13}$ $xa = ax$ y $\langle x\rangle \cap \langle a\rangle = \mathbf{1}$ i.e. $G_{13} \cong C_4 \times C_4$ y en el otro caso $\langle xa\rangle \cap \langle a\rangle = \mathbf{1}$, $\varphi_a(xa) = \varphi_a(x)\varphi_a(a) = \beta(x)a = xta = (xa)^{-1}$, de lo que es inmediato que $G_{12}$ da lugar a $(C_4, 4, \sigma_3, 1)$ por lo que $G_{12} \cong C_4 \rtimes C_4$ (la unicidad de este producto es consecuencia directa de que $Aut(C_4) \cong C_2$).

Por el lema 3.24 y el teorema 3.27, extensiones equivalentes siempre son llevadas a cabo por grupos isomorfos, sin embargo como lo muestra el caso de $K_8$, clases de extensión no equivalentes $((C_4, 2, \sigma_1, x^2), (C_4, 2, \sigma_1, 1))$ pueden ser llevadas a cabo por grupos isomorfos $(K_8)$. Situación poco favorable que hemos llamado el problema de isomorfismo. Una manera clásica de probar que dos grupos no son isomorfos es mostrar que uno tiene más elementos de cierto orden que el otro. Así, para concluir la solución del problema que nos ata~ne, consideraremos los órdenes de los elementos en cada uno de los grupos que dan lugar a las extensiones del lema 3.31. La información referente a los órdenes de sus elementos queda codificada en la siguiente tabla:

no trivial de $K_4$ y $C_4$.

[14]Esta afirmación se probará una vez que se hayan clasificado los grupos de orden 24

| | $y$ | $y^2$ | $y^3$ | $y^4$ | $y^5$ | $y^6$ | $y^7$ | $a$ | $ya$ | $y^2a$ | $y^3a$ | $y^4a$ | $y^5a$ | $y^6a$ | $y^7a$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $G_1$ | 8 | 4 | 8 | 2 | 8 | 4 | 8 | 2 | 8 | 4 | 8 | 2 | 8 | 4 | 8 |
| $G_2$ | 8 | 4 | 8 | 2 | 8 | 4 | 8 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 |
| $G_3$ | 8 | 4 | 8 | 2 | 8 | 4 | 8 | 2 | 8 | 4 | 8 | 2 | 8 | 4 | 8 |
| $G_4$ | 8 | 4 | 8 | 2 | 8 | 4 | 8 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| $G_5$ | 8 | 4 | 8 | 2 | 8 | 4 | 8 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $G_6$ | 8 | 4 | 8 | 2 | 8 | 4 | 8 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
| | $x$ | $x^2$ | $x^3$ | $t$ | $xt$ | $x^2t$ | $x^3t$ | $a$ | $xa$ | $x^2a$ | $x^3a$ | $ta$ | $xta$ | $x^2ta$ | $x^3ta$ |
| $G_7$ | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 |
| $G_8$ | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| $G_9$ | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 |
| $G_{10}$ | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 2 | 2 | 2 | 4 | 4 | 4 | 4 |
| $G_{11}$ | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $G_{12}$ | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $G_{13}$ | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |

Todos los elementos distintos de la identidad de $G_0 := (C_2)^4$ tienen orden 2, y es el único de los grupos de orden 16 con tal característica [Lema 3.28], por lo que no es isomorfo a ninguno de los grupos de la tabla.

Contando los elementos de orden $2^i$, $1 \leq i \leq 4$, se concluye que de entre $G_1, .., G_6$, a lo más $G_1 \cong G_3$ podría ocurrir; pero esto es imposible, pues $G_1 \cong C_8 \times C_2$ es abeliano, mientras que $G_3 \cong C_4 \overset{5}{\rtimes} C_2$ no lo es.

Dado que los miembros de $\{G_i\}_{i=1}^{6}$ poseen elementos de orden 8, mientras que los de $\{G_j\}_{j=7}^{13}$ no, ningun grupo del primer conjunto es isomorfo a alguno del segundo.

Apelando de nuevo al número de elementos de orden 2 y 4, resta solo descartar que en $\{G_7, G_9G_{10}\}$, $\{G_{11}, G_{12}, G_{13}\}$ haya dos representantes de la misma clase de isomorfismo. La descripción de la parte superior nos permite separar $G_7$ y $G_{13}$ pues a diferencia del resto, éstos son abelianos. El mostrar que $G_9 \ncong G_{10}$ y $G_{12} \ncong G_{11}$ requiere de observaciones más sutiles.

Nortemos primero que aunque tanto $G_9$ como $G_{10}$ tienen exactamente 4 copias de $C_4$, dado que ambos poseen 8 elementos de orden 4, en $G_{10}$ cualesquiera dos copias de $C_4$ se intersectan en una copia de $C_2$; mientras que en $G_9$ existen dos copias de $C_4$ que se intersectan trivialmente, a saber $\langle x \rangle$ y $\langle xa \rangle$.

Tomando $\mathbf{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$, $C_2 = \langle t \rangle$, $C_4 = \langle x \rangle$ tenemos que $Z(\mathbf{Q} \times C_2) = \{(1,1), (1,t), (-1,1), (-1,t)\}$, $Z(C_4 \rtimes C_4) = \{(1,1), (x^2,1), (1,x^2), (x^2,x^2)$, en el primer caso sólo $(-1,1) = (i,1)^2$ es un cuadrado no trivial, y por otro lado $(1,x^2) = (1,x)^2 = (x,x)^2$ y $(x^2,1) = (x,1)^2$ concluimos que $G_{11} \cong \mathbf{Q} \times C_2 \ncong C_4 \rtimes C_4 \cong G_{12}$.

Como en el caso de los grupos de orden 8 podemos sumar las discusiones en el siguiente teorema.

**Teorema 3.32.** *Existen salvo isomorfismo exactamente catorce grupos de orden 16, los cuales pueden ser listados como sigue (junto con las extensiones cíclicas a las que dan lugar)*

| | |
|---|---|
| $G_0 \cong (C_2)^4$ | $((C_2)^3, 2, Id, 1)$ |
| $G_1 \cong C_8 \times C_2$ | $(C_8,\ 2, \sigma_1, 1)$ |
| $G_2 \cong C_8 \overset{3}{\rtimes} C_2$ | $(C_8, 2, \sigma_3, 1)$ |
| $G_3 \cong C_8 \overset{5}{\rtimes} C_2$ | $(C_8, 2, \sigma_5, 1)$ |
| $G_4 \cong C_8 \overset{7}{\rtimes} C_2 = D_{2\cdot 8}$ | $(C_8, 2, \sigma_7, 1)$ |
| $G_5 =: Q_{16}$ | $(C_8, 2, \sigma_7, y^4)$ |
| $G_6 \cong C_{16}$ | $(C_8, 2, \sigma_1, y)$ |
| $G_7 \cong V \times C_4$ | $(K_8, 2, 1, 1)$ |
| $G_8 \cong D_{2\cdot 4} \times C_2$ | $(K_8, 2, \alpha^2, 1)$ |
| $G_9 \cong V \rtimes C_4$ | $(K_8, 2, \beta, 1)$ |
| $G_{10} \cong \mathbf{Q} \overset{\tau}{\rtimes} C_2$ | $(K_8, 2, \alpha^3\beta, 1)$ |
| $G_{11} \cong \mathbf{Q} \times C_2$ | $(K_8, 2, \alpha^2, x^2)$ |
| $G_{12} \cong C_4 \rtimes C_4$ | $(K_8, 2, \beta, x^2)$ |
| $G_{13} \cong C_4 \times C_4$ | $(K_8, 2, 1, t)$ |

La siguiente sección concluye nuestra clasificación.

## Clasificación de los grupos de orden 24

Es necesario el siguiente par de resultados antes de la discusión subsiguiente, que a pesar de ser relevante únicamente al final, es vital para el desarrollo para la misma

**Lema 3.33.** $Z(A_4) = \mathbf{1}$

*Demostración.* Sea $A_4 = \langle x, y, z\rangle$, con $\langle x, y\rangle \cong V$, $z^3 = 1$ y $zxz^2 = y$, $zyz^2 = xy$.

Es claro que cualquier elemento $a \in A_4$ es central si y solamente si $[a, x] = [a, y] = [a, z] = 1$, por lo que para demostrar el lema, basta mostrar que para cada elemento no trivial de $A_4$ no se cumple alguna de estas relaciones.

Si tenemos $x^i y^j z$, con $i, j \in \mathbb{Z}$, entonces $x^i y^j z x z^{-1} y^{-j} x^{-i} = x^i y^j y y^{-j} x^{-i} = y \neq x$, por lo tanto $[x^i y^i z, x] \neq 1$.

De manera semejante $x^i y^j z^2 x z^{-2} y^{-j} x^{-i} = x^i y^j x y y^{-j} x^{-i} = xy \neq x$ y por tanto $[x^i y^i z^{-1}, x] \neq 1$.

Los casos de $x$, $y$ y $xy$ son también sencillos, ya que no es dificil hacer ver que $xzx^{-1} = xyz \neq z$, $yzy^{-1} = xz \neq z$ y $(xy)z(xy)^{-1} = yz \neq z$, de donde $Z(A_4) \cap \langle x, y\rangle = \mathbf{1}$.

Concluimos que $Z(A_4) = \mathbf{1}$. □

**Lema 3.34.** $|Aut(A_4)| = 24$*; más aún,* $Aut(A_4)$ *es de la forma* $A_4 \rtimes_\varphi C_2$.

*Demostración.* Sea $A_4 = \langle x, y, z\rangle$ como arriba (y permítase el ligero abuso de notación $V = \langle x, y\rangle$), al tenerse que $A_4$ da lugar a la clase de extensión $(V, 3, \varphi_z, 1)$ y $z$ es un elemento inductor de ésta[15], como en el caso de $Aut(\mathbf{Q})$, es suficiente determinar las diferentes sextetas $(W, 3, \varphi_a, 1, a, \Phi)$ de la forma descrita por el corolario 3.25. Démonos pues a esta tarea.

Como $V$ es un 2-subgrupo de Sylow normal de $A_4$, éste es único; por lo tanto todas las clases de extensión $(V, 3, \varphi_z, 1) \overset{\Phi}{\sim} (W, 3, \varphi_a, 1)$, son tales que $W = V$, $\Phi, \varphi_a \in Aut(V)$ y $|\varphi_z| = |\varphi_a| = 3$; Además $Aut(V)$ es isomorfo al grupo (no abeliano) $GL(2, 2)$ de orden 6, por lo tanto $Aut(V) = \langle \alpha, \beta\rangle = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$, con $\beta\alpha\beta = \alpha^2$, y más aún, puede elegirse $\alpha$ de manera que coincida con la restricción de $\varphi_z$ a $V$. Por otro lado, $A_4$ también da lugar a la clase de extensión $(V, 3, \varphi_{z^2}, 1)$; no es dificil ver que $(V, 3, \alpha, 1)$ y $(V, 3, \alpha^2, 1)$ son las únicas extensiones a las que $A_4$ da lugar y que $z$, $xz$, $yz$ y $xyz$ inducen la primera, mientas que $\{z^2, xz^2, yz^2, xyz^2\}$ es un conjunto de elementos inductores de la segunda.

Finalmente tenemos que $(V, 3, \alpha, 1) \overset{\Phi_i}{\sim} (V, 3, \alpha, 1)$ y $(V, 3, \alpha, 1) \overset{\Psi_j}{\sim} (V, 3, \alpha^2, 1)$, con $\Phi_i \in \{1, \alpha, \alpha^2\}$ y $\Psi_i \in \{\beta, \alpha\beta, \alpha^2\beta\}$. Este hecho en conjunto con las observaciones anteriores, implica que $|Aut(A_4| = 4 \cdot 3 + 4 \cdot 3 = 24$.

[15]Con el fin de no hacer más engorrosa la notación, a lo largo de esta demostración, no se hará distinción entre el elemento $\varphi_a \in Inn(A_4)$, $a \in A_4$, y sus restricciones $\varphi_a|_N$, con $N \leq A_4$.

Para demostrar la última parte del resultado, observemos que por el lema anterior y la proposición 2.18, existe un homomorfismo inyectivo de $A_4 \cong Inn(A_4)$ en $Aut(A_4)$ cuya imagen es normal, a saber, la correspondencia $a \mapsto \varphi_a$.

La prueba del lema 3.24 y el teorema 2.12, hacen ver que la correspondencia $\tau :: A_4 \to A_4$, definida tal que $\tau(x) = \beta(x)$, $\tau(y) = \beta(y)$ y $\tau(z) = z^2$ induce un ***automorfismo exterior*** de $A_4$; ya que no es dificil verificar que, para cada $a \in A_4$, $aza^{-1} = x^i y^j z$, con $i, j \in \mathbb{Z}$. Además $\tau^2 = 1$, ya que $\tau^2|_V = \beta^2 = 1$ y $\tau^2(z) = z^4 = z$.

Por lo tanto $\tau$ es un elemento de orden 2 tal que $Inn(A_4) \cap \langle\tau\rangle = \mathbf{1}$, con $|Inn(A_4)| = 12$ y $|\langle\tau\rangle| = 2$, entonces $Aut(A_4) = Inn(A_4) \rtimes \langle\tau\rangle$.

Se sigue que $Aut(A_4)$ es de la forma $A_4 \rtimes_\varphi C_2$. □

A lo largo de

**Lema 3.35.** *Existen en $Aut(A_4)$ exactamente dos clases de conjugación de elementos de orden 2, una de las cuales está conformada por los elementos no triviales de un subgrupo de orden 4.*

*Demostración.* Como primera observación, notemos que $\langle\varphi_x, \varphi_y\rangle \lhd Aut(A_4) = \langle\varphi_x, \varphi_y, \varphi_z\rangle \rtimes \langle\tau\rangle$, ya que $\tau\varphi_x\tau^{-1} = \varphi_{\beta(x)}$, $\tau\varphi_y\tau^{-1} = \varphi_{\beta(y)}$. Además todos los elementos de $\langle\varphi_x, \varphi_y\rangle\backslash\mathbf{1}$ son conjugados entre si, lo que implica que $\langle\varphi_x, \varphi_y\rangle\backslash\mathbf{1}$ es una clase completa de conjugación de elementos de orden 2.

Observemos también que al ser $Aut(A_4)$ un grupo de orden $24 = 2^3 \cdot 3$, por el teorema 2.27, éste tiene un subgrupo de orden 8 y todos los subgrupos de este orden son conjugados, además por este mismo teorema, $\langle\varphi_x, \varphi_y\rangle$ está contenido en algún subgrupo de este orden, concluimos por la observación inicial que $\langle\varphi_x, \varphi_y\rangle$ está contenido en cada 2-subgrupo de Sylow de $Aut(A_4)$; más aún, como $\tau$ es un automorfismo exterior de orden 2i , entonces $D := \langle\varphi_x, \varphi_y\rangle\langle\tau\rangle$ es un subgrupo de $Aut(A_4)$ y $|\langle\varphi_x, \varphi_y\rangle\langle\tau\rangle| = |\langle\varphi_x, \varphi_y\rangle||\langle\tau\rangle|/|\langle\varphi_x, \varphi_y\rangle \cap \langle\tau\rangle| = 8$, como además $\tau\varphi_x\tau^{-1} = \varphi_{\beta(x)} \neq \varphi_x$ o $\tau\varphi_y\tau^{-1} = \varphi_{\beta(y)} \neq \varphi_y$, podemos concluir que $D$ es un subgrupo no abeliano de orden 8 que tiene una copia de $V$ como subgrupo, de esto concluimos que $D \cong D_{2\cdot 4}$. Por lo anterior, $D$ tiene exactamente 5 elementos de orden 2, tres de los cuales son los elementos no triviales de $\langle\varphi_x, \varphi_y\rangle$, tomando en cuenta las clases de conjugación de $D_{2\cdot 4}$, los dos elementos restantes deben componer una clase de conjugación completa

en $D$, digamos $\{d_1, d_2\}$. Es por esto que para cada $\phi \in Aut(A_4)$, $\phi\{d_1, d_2\}\phi^{-1}$ es una clase de conjugación de $\phi D\phi^{-1}$. Concluimos que $\bigcup_{\phi \in Aut(A_4)} \phi\{d_1, d_2\}\phi^{-1}$ es una clase de conjugación completa de $Aut(A_4)$.

Ya que los elementos de $\langle \varphi_x, \varphi_y \rangle \backslash \mathbf{1}$ constituyen una clase de conjugación completa, concluimos que $Aut(A_4)$ tiene exactamente dos clases de conjugación de elementos de orden 2, una de las cuales consiste en los elementos no triviales de un subgrupo de orden 4. □

**Corolario 3.36.** *$Aut(A_4)$ no tiene subgrupos de Sylow normales.*

*Demostración.* Basta hacer ver que $r_3 > 1$ y $r_2 > 1$.

Se ha demostrado en el lema 3.34 que $Aut(A_4)$ es de la forma $A_4 \rtimes_\varphi C_2$, y al tener una copia de $A_4$ como subgrupo, se sigue inmediatamente que $Aut(A_4)$ contiene al menos 4 copias de $C_3$ (de hecho, contiene exactamente 4).

Por otro lado, la demostración del lema 3.34 implica que $Aut(A_4) = \langle \varphi_x, \varphi_y, \varphi_z \rangle \rtimes \langle \tau \rangle$ y se ha demostrado además en el lema 3.35 que $D = \langle \varphi_x, \varphi_y, \tau \rangle$ es un 2-subgrupo de Sylow de $Aut(A_4)$; si este fuera el único, entonces contendría a todos los elementos de orden 2 de $Aut(A_4)$, sin embargo $|\varphi_z \tau \varphi_z^{-1}| = 2$ y $\varphi_z \tau \varphi_z^{-1} = \varphi_z \tau \varphi_{z^2} = \varphi_z \varphi_{\tau(z^2)} \tau = \varphi_z^2 \tau$ no es un elemento de $\langle \varphi_x, \varphi_y, \tau \rangle$, debido a que todos los elementos de $Aut(A_4)$ tienen una representación única de la forma $\varphi_x^r \varphi_y^s \varphi_z^t \tau^u$, con $r, s, u \in \{0, 1\}$, $t \in \{0, 1, 2\}$ y $D$ consta exactamente de los elementos en cuya representación $t = 0$. Se sigue de esto que $Aut(A_4)$ tiene más de un 2-subgrupo de Sylow.

Concluimos que $Aut(A_4)$ no tiene subgrupos de Sylow normales. □

**Corolario 3.37.** *Existen, salvo isomorfismo, dos productos semidirectos no triviales de $A_4$ por $C_2$, de los cuales uno tiene un subgrupo isomorfo a $C_2^3$, y el otro contiene una copia de $D_{2\cdot 4}$.*

*Demostración.* Es claro por el lema anterior y el corolario 3.8 que existen a lo más dos clases de isomorfismo a las que pueden pertenecer los productos semidirectos no triviales de $A_4$ por $C_2$, por lo que resta únicamente verificar la segunda parte de la afirmación; ya que en un grupo dado, todos los subgrupos de Sylow de éste son isomorfos, de donde obtenemos que de existir los productos semidirectos buscados, éstos no pueden ser isomorfos.

Observemos que de las clases de conjugación de $Aut(A_4)$ obtenidas, la que está conformada por elementos del subgrupo de orden 4 es tal que fija cada uno de los elementos de $V$. Por lo tanto, si $C_2 = \langle c \rangle$ y $\gamma : C_2 \to Aut(A_4)$ es un homomorfismo no trivial cuya imagen deja fijos a los elementos de $V$, entonces el producto $A_4 \rtimes_\gamma C_2$ es tal que $\langle x, y, c \rangle$ es un grupo abeliano de orden 8 isomorfo a $C_2^3$.

Por otro lado, se ha demostrado que $Aut(A_4)$ es un producto no trivial $A_4 \rtimes_\varphi C_2$ y contiene una copia de $D_{2\cdot 4}$, lo que concluye la prueba. □

Una vez desarrollados los resultados anteriores, estamos preparados para discutir la estructura de los grupos de orden 24.

Sea $G$ un grupo de orden $24 = 2^3 \cdot 3$ y $H, K < G$ con $|H| = 8$, $|K| = 3$. Consideraremos casos dependientes de la normalidad de estos subgrupos.

Caso $H \lhd G$, $K \lhd G$. Sabemos que aquí, $G$ es isomorfo al producto directo de $H$ y $K$, necesariamente $K \cong C_3$ pero para $H$ tenemos 5 subcasos que llevan a grupos no isomorfos, a saber:

- Si $H \cong C_8 \Rightarrow G \cong C_8 \times C_3 \cong C_{24}$.
- Si $H \cong C_2 \times C_4 \Rightarrow G \cong (C_2 \times C_4) \times C_3 \cong C_2 \times (C_4 \times C_3) \cong C_2 \times C_{12}$.
- Si $H \cong C_2 \times C_2 \times C_2 \Rightarrow G \cong (C_2 \times C_2) \times (C_2 \times C_3) \cong V \times C_6$.
- Si $H \cong D_{2(4)} \Rightarrow G \cong D_{2(4)} \times C_3$.
- Si $H \cong Q \Rightarrow G \cong Q \times C_3$.

Caso $H \lhd G$, $K \not\lhd G$. Aquí $G = H \rtimes K$. Recordemos que para definir un producto semidirecto, basta tener un homomorfismo (no trivial) $\varphi : K \to Aut(H)$, lo cual implica $3 || Aut(H)|$; y por la discusión posterior a la clasificación de los grupos de orden 8, sabemos que esto sólo puede suceder si $H \cong C_2 \times C_2 \times C_2$ o $H \cong Q$.

- Si $H \cong Q$, Como $|Aut(Q)| = 24 = 2^3 \cdot 3$; entonces todos los subgrupos de orden 3 son de Sylow, lo que implica que estos son conjugados, y por el corolario 3.8, sólo existe en este caso un producto semidirecto salvo isomorfismo.
- Si $H \cong C_2 \times C_2 \times C_2$ por la misma discusión arriba mencionada, $Aut(C_2 \times C_2 \times C_2) \cong GL(3, 2)$ y $|GL(3, 2)| = 2^3 \cdot 3 \cdot 7$; por lo que de nuevo en este caso tenemos que los subgrupos de orden 3 serán conjugados (por ser de Sylow) y en virtud del

corolario 3.8 aquí también surge una sola clase de producto semidirecto módulo isomorfismo.

Caso $H \not\lhd G$, $K \lhd G$. Por la proposición 2.22, $|Aut(C_3)| = 2$; por lo que todo $\varphi : H \to Aut(C_3)$ con imagen no trivial debe ser un epimorfismo con $|\ker(\varphi)| = 4$, lo último implicando que $\ker(\varphi) \cong C_4$ o $\ker(\varphi) \cong V$.

- Si $H = \langle x \rangle \cong C_8$, entonces $\bar{K} := \ker(\varphi) = \langle x^2 \rangle$ (recordemos que los grupos cíclicos están caracterizados por poseer un único subgrupo de cada orden), y por el primer teorema de isomorfismo $H/K \cong_f Aut(K)$, donde $f(x\bar{K}) = \varphi(x)$ y $f(x\bar{K}) \neq \sigma_1$, lo que implica $\varphi(x) = \sigma_2$, de lo que se concluye que en este caso, sólo un producto semidirecto es posible.
- Ahora, si $H = \langle x, y, z \rangle \cong C_2 \times C_2 \times C_2$, es obvio que $\ker(\varphi) = \langle x_1, x_2 \rangle \cong V$, y por motivos de orden, existe $x_3 \in H \setminus \ker(\varphi)$. Además es claro que $\psi(x) = x_1$, $\psi(y) = x_2$, $\psi(z) = x_3$ define un elemento de $Aut(H)$ tal que $\phi = \varphi \circ \psi$, donde $\phi$ es el único homomorfismo de $H$ en $Aut(K)$ que manda $x$, $y$, $z$ en $\sigma_1$, $\sigma_1$, $\sigma_2$ respectivamente. La proposición 3.5 permite concluir que cualquier producto semidirecto $K \rtimes H$ es isomorfo a $K \rtimes_\phi H$
- Para finalizar los casos en que $H$ es abeliano, si tenemos $H = \langle x, y \rangle \cong C_4 \times C_2$ ($|x| = 4$, $|y| = 2$)), como se ha mencionado arriba, podemos discernir en este punto entre dos posibilidades: $\ker(\varphi) \cong C_4$ y $\ker(\varphi) \cong V$.
  Consideremos primero $\bar{\varphi} : H \to Aut(K)$ el homomorfismo tal que $\bar{\varphi}(x) = \sigma_1$ y $\bar{\varphi}(y) = \sigma_2$, es claro que $\ker(\bar{\varphi}) \cong C_4$. Sea $\ker(\varphi) = \langle z_1 \rangle \cong C_4$, como $H$ tiene tres elementos de orden 2 y solo uno pertenece a $\ker(\varphi)$, existe $z_2 \in H \setminus \ker(\varphi)$ tal que $z_2^2 = 1$, con lo que $H = \langle z_1 \rangle \times \langle z_2 \rangle$ y $\bar{\psi}(x) = z_1$, $\bar{\psi}(y) = z_2$ define un automorfismo de $H$ tal que $\bar{\varphi} = \varphi \circ \bar{\psi}$, que a la luz de la proposición 3.5 implica que todos los productos semidirectos en este caso son isomorfos a $K \rtimes_{\bar{\varphi}} H$.
  Por otra parte, si tomamos ahora $\hat{\varphi} \in Hom(H, Aut(K))$ tal que $\hat{\varphi}(x) = \sigma_2$ y $\hat{\varphi}(y) = \sigma_1$, tenemos que $\hat{\varphi}(x)^2 = \sigma_1$ y $x^2 \in \ker(\hat{\varphi}) \cap Z(H)$, por lo tanto $V \cong \langle x^2, y \rangle \subseteq \ker(\hat{\varphi})$, y así $\ker(\hat{\varphi}) \cong V$. Si $\varphi$ es cualquier otro homomorfismo con $\ker(\varphi) \cong V$, necesariamente, todos los elementos de $H$ de orden 4 pertenecen a $H \setminus \ker(\varphi)$, en particular, $1 \neq \varphi(x) = \sigma_2$, además $\ker(\varphi) \setminus \langle x \rangle \neq \emptyset$ y por tanto existe $z \in \ker(\varphi)$ tal que $\langle x, z \rangle = H$, de esto obtenemos que existe un automorfismo $\hat{\psi}$ de $H$ tal que $\hat{\psi}(x) = x$ y $\hat{\psi}(y) = z$ lo que implica $\hat{\varphi} = \varphi \circ \hat{\psi}$, por lo tanto aquí también existe una sola clase de isomorfismo.

- De manera similar al caso anterior, si $H = \langle x, y\rangle \cong D_{2(4)}$ con $x^4 = y^2 = yxy^{-1}x = 1$, podemos definir los homomorfismos auxiliares $\bar{\varphi} : H \to Aut(K)$, $\hat{\varphi} : H \to Aut(K)$ tales que $\bar{\varphi}(x) = \sigma_1$, $\bar{\varphi}(y) = \sigma_2$ y $\hat{\varphi}(x) = \sigma_2$, $\hat{\varphi}(y) = \sigma_1$, y por los mismos argumentos que en el inciso pasado, $\ker(\bar{\varphi}) \cong C_4$ y $\ker(\hat{\varphi}) \cong V$.
  Si $\ker(\varphi) \cong C_4$, al tener $H$ un único subgrupo cíclico de orden 4, esta situación fuerza a que $\ker(\varphi) = \langle x\rangle$, por lo que $\varphi(x) = \sigma_1$, además al ser $\varphi$ un homomorfismo no trivial y $x$ e $y$ generadores de $H$, sus imágenes bajo $\varphi$ no pueden anularse simultaneamente, por lo tanto en esta situación $\varphi(y) = \sigma_2$, de lo que se concluye que $\varphi = \bar{\varphi}$.
  Si por el contrario, $\ker(\varphi) \cong V$, aquí $x \in H \backslash \ker(\varphi)$, lo que implica $\varphi(x) = \sigma_2$; además, porque $|\ker(\varphi)| = 4$, existe $z \in \ker(\varphi)\backslash\langle x^2\rangle$ que necesariamente cumple: $zxz^{-1} = zxz = x^3$. Lo anterior implica que $\psi(x) = x$ y $\psi(y) = z$ define un automorfismo de $H$ tal que $\hat{\varphi} = \varphi \circ \psi$. Como es usual, esto implica que existe bajo esta suposición, una sola clase de isomorfismo $K \rtimes H$.

- Finalmente, si $H = \langle x, y\rangle \cong \mathbf{Q}$, con $x^4 = y^4 = x^2y^{-2} = yxy^{-1}x = 1$, la única posibilidad es $\ker(\varphi) \cong C_4$, al ser $x$, $y$ generadores, debe tenerse $\varphi(x) = \sigma_2$ o $\varphi(y) = \sigma_2$ (que en este contexto es equivalente a $\varphi(x) \neq \sigma_1$ o $\varphi(y) \neq \sigma_1$). Distinguimos 3 casos que se probará son equivalentes, si $\varphi_1(x) = \sigma_1$ y $\varphi_1(y) = \sigma_2$, si $\varphi_2(x) = \sigma_2$ y $\varphi_2(y) = \sigma_1$ y si $\varphi_3(x) = \sigma_2$ y $\varphi_3(y) = \sigma_2$, $\varphi_1, \varphi_2, \varphi_3 \in Hom(H, Aut(K))$. Observemos que de la discusión donde se determinó el orden de $Aut(\mathbf{Q})$ y la prueba del corolario 3.24 obtenemos que las correspondencias $\phi : H \to H$, $\psi : H \to H$ tales que $\phi(x) = y$, $\phi(y) = x$, $\psi(x) = xy$, $\psi(y) = y$ definen automorfismos de $H$ tales que $\varphi_1 = \varphi_2 \circ \phi = \varphi_3 \circ \psi$, por lo tanto $K \rtimes_{\varphi_1} H \cong K \rtimes_{\varphi_2} H \cong K \rtimes_{\varphi_3} H$ por la proposición 3.5.

Caso $H \not\lhd G$, $K \not\lhd G$. Por el corolario 3.36, sabemos que $Aut(A_4)$ carece de subgrupos de Sylow normales. Probaremos aquí que si $G$ también tiene esta caacterística, entonces $G \cong Aut(A_4)$.

Tomemos $H' \in Syl_2(G)\backslash\{H\}$ (existe, pues $H \not\lhd G$), recordemos que $|HH'| = {}^{|H||H'|}/_{|H\cap H'|}$, entonces $|H \cap H'| = {}^{|H||H'|}/_{|HH'|}$ y al tenerse que $HH' \subseteq G$, obtenemos $|H \cap H'| \geq |H||H'|/|G|$, lo que implica $|H \cap H'| \geq \frac{64}{24} > 2$, que a su vez implica $|H \cap H'| = 4$ ($H \neq H'$). Como $[H : H\cap H'] = [H' : H\cap H'] = 2$, sabemos que $H\cap H' \lhd H, H'$, por lo tanto $|N_G(H\cap H')| \geq 8+4 = 12$, esto en conjunto con el hecho de que $|N_G(H\cap H')|||G|$, implica que $3||N_G(H \cap H')|$ y por lo tanto existe un elemento de un 3-subgrupo de

Sylow de $G$ contenido en $N_G(H \cap H')$ y con esto, $|N_G(H \cap H')| \geq 12 + 2 > 12$, que nos permite concluir que $N_G(H \cap H') = G$, es decir, $H \cap H' \lhd G$. De aquí, $G$ tiene como subgrupo normal a $A := (H \cap H')K$ de orden 12, que tiene un único subgrupo de orden 4 y además tiene como subgrupos a todos los 3-subgrupos de Sylow de $G$ (esto se deduce de la normalidad de $A$), la discusión sobre grupos de orden 12 implica que $A \cong A_4$, esto último debido a que $|Syl_3(A)| = |Syl_3(G)|$.

En particular, $H \cap H' \cong V$, que conlleva que $H$ y $H'$ son no abelianos, pues de ser así, un cálculo análogo al de $N_G(H \cap H')$ muestra que existe $K' \in Syl_3(G)$ contenido en $C_G(H \cap H')$, por lo tanto $HK' = G \subseteq C_G(H \cap H')$, lo que evidentemente es una contradicción. Concluimos que los 2-subgrupos de Sylow de $G$ son no abelianos y que además contienen una copia de $V$, lo cual sólo es posible si son isomorfos a $D_{2\cdot 4}$. De lo anterior, existe un elemento $x$ de $H$ de orden 2 que no está contenido en $H \cap H'$; por lo tanto[16] $G$ es de la forma $A_4 \rtimes_\varphi C_2$ y contiene una copia de $D_{2\cdot 4}$, concluimos en virtud del corolario 3.37 que $G \cong Aut(A_4)$ con lo que hemos finalizado la clasificación de los grupos de orden 24.

Resumiendo, hemos obtenido 15 grupos, separados en 4 clases:

1. $C_{24}$, $C_2 \times C_{12}$, $V \times C_6$, $D_{2(4)} \times C_3$, $Q \times C_3$, si $H \lhd G$, $K \lhd G$.
2. $Q \rtimes C_3$, $(C_2 \times C_2 \times C_2) \rtimes C_3 \cong A_4 \times C_2$, si $H \lhd G$, $K \not\lhd G$.
3. $C_3 \rtimes C_8$, $C_3 \rtimes (C_2 \times C_2 \times C_2)$, $C_3 \rtimes_{\bar{\varphi}} (C_4 \times C_2)$, $C_3 \rtimes_{\hat{\varphi}} (C_4 \times C_2)$, $C_3 \rtimes_{\bar{\varphi}} (D_{2(4)})$, $C_3 \rtimes_{\hat{\varphi}} (D_{2(4)})$, $C_3 \rtimes Q$, si $H \not\lhd G$, $K \lhd G$.[17]
4. $Aut(A_4)$, si $H \not\lhd G$, $K \not\lhd G$.

Es claro que los grupos listados en una clase no pueden ser isomorfos a los de otra clase por las condiciones de normalidad de sus subgrupos de Sylow; y más aún, los grupos listados en los incisos 1 y 2 representan clases irredundantes de isomorfismo, ya que entre grupos isomorfos sus subgrupos de Sylow también lo son.

[16] Observemos que además $x$ no pude conmutar con todos los elementos de $A$; pues de ser así, en particular $x$ conmutaría con los elementos de $H \cap H'$, haciendo de $H$ un grupo abeliano.

Por otro lado; si $x \in A$, al ser de orden 2, entonces debe estar contenido en algún 2-subgrupo de Sylow de $A$, pero el único elemento de $Syl_2(A)$ que éste tiene es $H \cap H'$. Por lo tanto $x$ no puede ser un elemento de $A$.

[17] Hemos un poco abusado de la notación para denotar por $\bar{\varphi}$ y $\hat{\varphi}$ homomorfismos análogos a los usados en el caso $H \not\lhd G$, $K \lhd G$ cuando $H \cong C_4 \times C_2$ y $H \cong D_{2(4)}$, en aras de la simplicidad en la notación.

También por la razón anterior, basta ver que $C_3 \rtimes_{\bar{\varphi}} (C_4 \times C_2) \ncong C_3 \rtimes_{\hat{\varphi}} (C_4 \times C_2)$ , $C_3 \rtimes_{\bar{\varphi}} (D_{2(4)}) \ncong C_3 \rtimes_{\hat{\varphi}} (D_{2(4)})$ para concluir que existen exactamente 15 clases de isomorfismo de grupos de orden 24, pero esto se concluye del teorema 3.15.

Por lo tanto existen exactamente 15 clases de isomorfismo de grupos de orden 24, cuyos representantes están listados en las 4 clases mencionadas.

Como una aplicación de las proposiciones desarrolladas en esta sección, y como final del texto, demostraremos las siguientes proposiciones, una de las cuales fue enunciada durante la clasificación de los grupos de orden 16.

**Proposición 3.38.** *$Aut(\mathbf{Q}) \cong Aut(A_4)$.*

*Demostración.* Basta hacer ver que $Aut(\mathbf{Q})$ es un producto semidirecto no trivial de $A_4$ por $C_2$ que contiene una copia de $D_{2\cdot 4}$, lo que a su vez se reduce a demostrar que $Aut(\mathbf{Q})$ no tiene subgrupos de Sylow normales.

Recordemos que $\mathbf{Q}$ es un grupo que da lugar a una extensión equivalente a $(C_4, 2, \sigma_3, x^2)$, a saber $(\langle i\rangle, 2, \varphi_j|_{\langle i\rangle}, -1)$ y la prueba del corolario 3.25 permite biyectar los elementos de $Aut(\mathbf{Q})$ con las extensiones equivalentes a $(C_4, 2, \sigma_3, x^2)$ a las que $\mathbf{Q}$ da lugar. Observemos que por la proposición 2.18 $Inn(\mathbf{Q}) \cong \mathbf{Q}/Z(\mathbf{Q}) \cong V$ y que los elementos de este subgrupo de $Aut(\mathbf{Q})$ se identifican con las correspondencias $(\langle i\rangle, 2, \varphi_j|_{\langle i\rangle}, -1, j, \sigma_1) \mapsto 1$, $(\langle i\rangle, 2, \varphi_j|_{\langle i\rangle}, -1, j, \sigma_3) \mapsto \varphi_j$, $(\langle i\rangle, 2, \varphi_j|_{\langle i\rangle}, -1, -j, \sigma_1) \mapsto \varphi_i$, $(\langle i\rangle, 2, \varphi_j|_{\langle i\rangle}, -1, -j, \sigma_3) \mapsto \varphi_k$; recordemos del capítulo anterior que $Inn(\mathbf{Q}) \lhd Aut(\mathbf{Q})$; además $(\langle j\rangle, 2, \varphi_k|_{\langle j\rangle}, -1, k, \phi)$, con $\phi(i) = j$, induce un elemento $\gamma' \in Aut(\mathbf{Q})$ tal que $\gamma'(i) = j$, $\gamma'(j) = k$ y $\gamma'^3 = 1$, lo que implica que $|\gamma'| = 3$; también $\gamma'^{-1} \circ \varphi_i \circ \gamma'(i) = -i$ y $\gamma'^{-1} \circ \varphi_i \circ \gamma'(j) = -j$ i.e. $\gamma'^{-1} \circ \varphi_i \circ \gamma' = \varphi_k$, podemos afirmar entonces que $Inn(\mathbf{Q})\langle\gamma'\rangle$ es un subgrupo de $Aut(\mathbf{Q})$ isomorfo a $A_4$, ya que es isomorfo a un producto semidirecto no trivial de $V$ por $C_3$, esto último se sigue de que $Inn(\mathbf{Q}) \lhd Aut(\mathbf{Q})$ y $\gamma'^{-1} \circ \varphi_i \circ \gamma' \neq \varphi_i$. Obtenemos de esto que $Aut(\mathbf{Q})$ no tiene 3-subgrupos de Sylow normales.

Por otro lado, como $(\langle j\rangle, 2, \varphi_i|_{\langle j\rangle}, -1, i, \phi)$ induce un elemento $\beta' \in Aut(\mathbf{Q})\backslash Inn(\mathbf{Q})$ tal que $\beta'(i) = j$, $\beta'(j) = i$, entonces $|\beta'| = 2$. Observemos además que $\beta' \circ \varphi_i \circ \beta'(i) = -i$ y $\beta' \circ \varphi_i \circ \beta'(j) = j$, es decir, $\beta' \circ \varphi_i \circ \beta' = \varphi_j$; concluimos que $Inn(\mathbf{Q})\langle\beta'\rangle$ es un subgrupo de $Aut(\mathbf{Q})$ tal que es isomorfo a un grupo diédrico, para determinar el orden de éste, basta ver el orden de $\beta' \circ \varphi_i$, para esto observemos que $\beta' \circ \varphi_i \circ \beta' \circ \varphi_i = \varphi_j \circ \varphi_i = \varphi_k$, que tiene

como conecuencia $|\beta' \circ \varphi_i| = 4$. Se sigue inmediatamente de esto que $Inn(\mathbf{Q})\langle\beta'\rangle \cong D_{2\cdot 4}$. Resta únicamente ver que este subgrupo no es normal; para esto, notemos que para todo $\alpha \in Inn(\mathbf{Q})\langle\beta'\rangle$, $\alpha(i), \alpha(j) \in \{\pm i, \pm j\}$, esto último ya que en particular esto pasa para $\varphi_i, \beta'$; de esto podemos concluir que $Inn(\mathbf{Q})\langle\beta'\rangle \not\trianglelefteq Aut(\mathbf{Q})$, pues $\gamma' \circ \beta' \circ \gamma'^{-1}(j) = k$.

Por lo tanto $Aut(\mathbf{Q})$ es un grupo de orden 24 sin subgrupos de Sylow normales. Se sigue entonces que $Aut(\mathbf{Q}) \cong S_4 \cong Aut(A_4)$. □

**Corolario 3.39.** *Existen salvo isomorfismo exactamente dos productos semidirectos no triviales de* $\mathbf{Q}$ *por* $C_2$*, sólo uno de los cuales no posee elementos de orden 8.*

*Demostración.* Como se ha mostrado en la proposición anterior que $Aut(\mathbf{Q}) \cong Aut(A_4)$ y el lema 3.35 limita las clases de conjugación de $Aut(A_4)$ a precisamente 2; por el corolario 3.8 la demostración de este corolario requiere solamente exhibir un elemento $\alpha \in Hom(C_2, Aut(\mathbf{Q}))$ tal que $\mathbf{Q} \rtimes_\alpha C_2$ no tenga elementos de orden 8 y otro $\mathbf{Q} \rtimes_{\alpha'} C_2$ que sí los tenga. Sea $\langle x\rangle = C_2$, si consideramos $\beta'$ como en la prueba de la proposición, y hacemos $\alpha(x) = \beta'$, entonces $(ix)^2 = ixix = i\beta'(i) = ij = k$, esto implica que $|ix| = 8$. Por otro lado, ninguno de los elementos no triviales de $Inn(\mathbf{Q})$ está en la misma clase de conjugación de $\beta'$, ya que $Inn(\mathbf{Q}) \trianglelefteq Aut(\mathbf{Q})$; se sigue entonces que $Inn(\mathbf{Q})\backslash\mathbf{1}$ es la otra clase de conjugación de elementos de orden 2. No es difícil ver que si ahora $\alpha'(x) = \varphi_i$, entonces $|\pm ix| = |\pm i| = |\pm j| = |\pm k| = 4$, $|\pm jx| = |\pm kx| = |-1| = 2$, por lo tanto la clase de isomorfismo a la que pertenece este producto semidirecto no tiene elementos de orden 8. □

# Bibliografía


[1] Rowen B. Bell Jonathan L. Alperin, *Groups and representations*, Springer, 1995.

[2] Ray Kunze Kenneth M. Hoffman, *Álgebra lineal*, Prentice Hall, 1973.

[3] Israel Kleiner, *A history of abstract algebra*, Birkhäuser, 2007.

[4] Joseph Rotman, *An introduction to the theory of groups*, Springer, 1999.

[5] Marcel Wild, *The groups of order sixteen made easy*, The American Mathematical Monthly **112** (2005), no. 1, 20–31.