CLASIFICACIÓN DE DETERMINADAS FAMILIAS DE GRUPOS FINITOS

TRABAJO FIN DE GRADO

Curso 2020/2021

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

DOBLE GRADO EN MATEMÁTICAS Y FÍSICA

DEPARTAMENTO DE ALGEBRA, GEOMETRÍA Y TOPOLOGÍA

Estudiante: Alberto Angurel Andrés

Tutor: José Javier Etayo Gordejuela

Madrid, a 29 de Junio de 2021

Resumen:

En este trabajo se realiza una clasificación de los grupos abelianos finitos y de los no abelianos de órdenes menores que 32. Para ello se desarrolla la teoría de Lagrange, el producto semidirecto y los teoremas de Sylow. Posteriormente, se prueba el teorema de clasificación de los grupos abelianos finitos. Por último, se caracterizan los grupos de órdenes p, p^2, p^3, pq y $4p$, que sirven como base para realizar una clasificación completa de los grupos de órdenes bajos, menores que 32.

Abstract:

In this work we establish a classification of finite abelian groups and non-abelian ones whose orders are less than 32. To do that, we develop Lagrange theory, semidirect product and Sylow theorems. Then, finite abelian groups classification theorem is proven. Lastly, groups whose orders can be written as p, p^2, p^3, pq, and $4p$ are classified. This characterisation is the base for a whole classification of groups of low order, under 32.

Índice

Introducción

El objetivo final de este trabajo es realizar una clasificación salvo isomorfismo de los grupos de órdenes bajos. Para ello, en las secciones 1 y 2 se recogen definiciones y resultados básicos de la teoría de grupos y homomorfismos. Posteriormente, en la sección 3 se ve el teorema de Lagrange, según el cual el orden de todo subgrupo divide al orden del grupo y en la sección 4 se define el producto semidirecto de grupos, el cual juega un papel fundamental en la construcción de grupos de órdenes mayores a partir de grupos de orden más bajo. En la sección 5, se estudian los teoremas de Sylow, los cuales tienen una enorme importancia en la teoría de grupos finitos, pues establecen la existencia y una serie de propiedades de los subgrupos de Sylow de un grupo finito G, que no son otra cosa que subgrupos de orden p^n, donde p es un divisor primo del orden de G y n es el mayor número natural tal que p^n es divisor del orden del grupo y, por tanto, puede existir un subgrupo de tal orden sin violar la teoría de Lagrange. Toda esta discusión puede verse con más detalle en [2].

Por último, en las secciones 6, 7 y 8 se establecen las clasificaciones de distintas familias de grupos. En primer lugar, en la sección 6 se caracterizan todos los grupos abelianos finitos a partir de sus coeficientes de torsión, mientras que en las siguientes secciones se clasifican grupos no abelianos. En la sección 7 se caracterizan los grupos cuyos órdenes tienen descomposiciones en producto de números primos sencillas, tales que el orden del grupo se escribe bien como p, p^2, p^3, donde p es un número primo, bien como un producto pq, donde q es otro número primo, o bien cuando el orden del grupo es $4p$, donde p es un número primo mayor o igual que 5. En la sección 8 se caracterizan los grupos de órdenes hasta 31 que no están incluidos en las familias anteriores, es decir, los grupos de órdenes 12, 16, 18, 24 y 30. El motivo de finalizar aquí la clasificación es que existen 51 grupos de orden 32, según viene demostrado en [6], y su clasificación se escapa a los objetivos de este trabajo.

La caracterización de los grupos abelianos finitos es completa a partir de los coeficientes de torsión. Por otro lado, la clasificación de los grupos no abelianos se ha llevado a cabo, principalmente, por dos procedimientos distintos. El primero de ellos sirve para los grupos G cuyo orden es una potencia de un número primo. Por los teoremas de Sylow, dicho grupo contiene subgrupos cuyos órdenes recorren todas las potencias menores de dicho número primo y, además, el centro del grupo es no trivial. De este modo, el subgrupo $\mathcal{Z}(G)$ y el grupo cociente $G/\mathcal{Z}(G)$ son grupos cuyos órdenes son una potencia menor de p, los cuales ya habían sido clasificados previamente. A partir de los distintos tipos de isomorfía del centro y del grupo cociente se construyen los distintos grupos de orden mayor.

El segundo método de caracterización utilizado sirve para clasificar grupos cuyos órdenes tienen una descomposición formada por más de un número primo. A excepción del grupo de permutaciónes $\mathcal{S}_4$ de orden 24, en todos los grupos clasificados los teoremas de Sylow garantizaban la existencia de dos subgrupos, al menos uno de ellos normal, que intersecaban en el elemento neutro y cuyo producto era el grupo original G. De este modo, los grupos de orden mayor podían construirse como productos semidirectos de grupos de menor orden.

1. Nociones básicas de teoría de grupos

Definición 1.1. Un *grupo* es un par $(G, \cdot)$, donde G es un conjunto y $\cdot : G \times G \to G : \ (a, b) \mapsto a \cdot b$ es una operación que verifica las siguientes propiedades:

1. Propiedad asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \ \forall a, b, c \in G$.
2. Existencia del elemento neutro: $\exists 1_G \in G$ tal que $a \cdot 1_G = 1_G \cdot a = a \ \forall a \in G$.
3. Existencia del elemento inverso $\forall a \in G, \ \exists a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1_G$.[1]

En adelante, si no hay riesgo de confusión, se denotará el grupo por G en lugar de $(G, \cdot)$ y se escribirá ab en lugar de $a \cdot b$.

Definición 1.2. Un grupo G se dice *abeliano* si

$$ab = ba \ \forall a, b \in G$$

Definición 1.3. El *orden* de un grupo G es el número de elementos de este, suponiéndose que sea finito.

Definición 1.4. Dado un grupo $(G, \cdot)$, un subconjunto $H \subset G$ se dice que es un *subgrupo* de G si es un grupo con la operación heredada de G, esto es, con la restricción de la aplicación $\cdot$ a $H \times H$.

Observación 1.5. Un subconjunto $H \subset G$ es subgrupo si y sólo si $1_G \in H$ y $ab^{-1} \in H \ \forall a, b \in H$. De aquí se deduce que la intersección arbitraria de subgrupos de un grupo G también es un subgrupo de este.

Definición 1.6. Dado un grupo G y un elemento $x \in G$, los elementos de G que pueden escribirse como $g^{-1}xg$ para algún $g \in G$ se denominan *elementos conjugados* de x. El conjunto de elementos conjugados de x se denomina *clase de conjugación* de x en G.

Definición 1.7. El *centro* de un grupo G, denotado por $\mathcal{Z}(G)$, se define como el subgrupo de G dado por

$$\mathcal{Z}(G) = \{z \in G : zg = gz \ \forall g \in G\}$$

Definición 1.8. Un subgrupo $N \subset G$ se dice *normal* si verifica que $g^{-1}Ng := \{g^{-1}ng : n \in N\}$[2] es igual a N para cada $g \in G$. La normalidad de N se denota por $N \triangleleft G$.

Observación 1.9. Equivalentemente, un subgrupo N de G es normal si y sólo si

$$Ng = \{ng : n \in N\} = \{gn : n \in N\} = gN \ \forall g \in G$$

Definición 1.10. Dado un subgrupo $H \subset G$, el *normalizador* de H en G, denotado por $N_G(H)$, es el subgrupo

$$N_G(H) := \{g \in G : g^{-1}Hg = H\}$$

que verifica ser el mayor subgrupo de G que contiene a H como subgrupo normal.

[1] Puede demostrarse que el elemento neutro y el inverso de cada elemento son únicos.

[2] Dichos conjuntos $g^{-1}Ng$ son subgrupos de G si N también lo es. Se denominan *subgrupos conjugados* de N.

Definición 1.11. Dado un subgrupo normal $H \triangleleft G$,[3] se define el grupo cociente G/H como el conjunto de clases de equivalencia en G dadas por $g_1 \sim g_2 \Leftrightarrow g_1 g_2^{-1} \in H$, con la operación

$$G/H \times G/H \to G/H,\ (Ha, Hb) \mapsto Hab\ ^4$$

Definición 1.12. Dado un grupo G y un subconjunto $S \subset G$, el subgrupo generado por S, y denotado por $\langle S \rangle$, es la intersección de todos los subgrupos que contienen a S. [5] Puede comprobarse que $\langle S \rangle$ es el conjunto de elementos de G que pueden expresarse como producto de una cantidad finita de elementos de S, posiblemente repetidos, o de sus inversos.

2. Homomorfismos y teoremas de isomorfía

Definición 2.1. Un *homomorfismo* de grupos es una aplicación $f : G_1 \to G_2$, donde G_1 y G_2 son grupos, que verifica que $f(ab) = f(a)f(b)\ \forall a, b \in G_1$. [6]

Definición 2.2. El *núcleo* de un homomorfismo de grupos $f : G_1 \to G_2$ es el subgrupo normal dado por:

$$\ker f := f^{-1}(\{1_{G_2}\}) = \{x \in G_1 : f(x) = 1_{G_2}\}$$

Observación 2.3. Si un homomorfismo $f : G_1 \to G_2$ es biyectivo, su aplicación inversa también es un homomorfismo. En tal caso, se dice que f es un *isomorfismo* y que los grupos G_1 y G_2 son *isomorfos*, lo que se denota por $G_1 \cong G_2$.

Observación 2.4. Dado un homomorfismo de grupos $f : G_1 \to G_2$, el conjunto

$$\operatorname{Im} f = \{f(x) : x \in G_1\} \subset G_2$$

es un subgrupo de G_2. El homomorfismo f es sobreyectivo si y sólo si $\operatorname{Im} f = G_2$. En este caso, se dice que f es un *epimorfismo*.

A continuación, se presentan algunos teoremas que afirman que determinados grupos son isomorfos.

Teorema 2.5. Dado un homomorfismo de grupos $f : G_1 \to G_2$, existe un isomorfismo dado por:

$$\overline{f} = G_1/\ker f \to \operatorname{Im} f :\ (\ker f)\ a \mapsto f(a)$$

Demostración. La aplicación $\overline{f}$ está bien definida y es inyectiva puesto que

$$(\ker f)\, a = (\ker f)\, b \Leftrightarrow ab^{-1} \in \ker f \Leftrightarrow f(a)f(b)^{-1} = f(ab^{-1}) = 1_{G_2} \Leftrightarrow f(a) = f(b)$$

Además, $\overline{f}$ es sobreyectiva por la propia definición de $\operatorname{Im} f$ y es un homomorfismo por serlo f. □

Teorema 2.6. Dados dos subgrupos normales, H y K, de un grupo G tales que $H \subset K \subset G$, se verifica que los grupos G/K y $(G/H)/(K/H)$ son isomorfos.

[3] La normalidad de H es condición necesaria para que la operación de G/H esté bien definida.
[4] Puede demostrarse que esta definición verifica los axiomas de grupo.
[5] Equivalentemente, $\langle S \rangle$ es el menor subgrupo que contiene a S.
[6] Esta definición implica que que $f(1_{G_1}) = 1_{G_2}$ y que $f(a^{-1}) = f(a)^{-1}\ \forall a \in G_1$.

Demostración. Se sigue de aplicar el teorema 2.5 al homomorfismo

$$\psi : G/H \to G/K : \ Ha \mapsto Ka$$

□

Por otro lado, existe una correspondencia entre los subgrupos de G que contienen a H y los subgrupos de G/H, la cual es expuesta en el siguiente teorema 2.8.

Definición 2.7. Dado un subgrupo $H \subset G$, el homomorfismo suprayectivo dado por

$$\pi : G \to G/H : \ g \mapsto Hg$$

se denomina *homomorfismo cociente*.

Teorema 2.8. Dado un subgrupo normal H de un grupo G, sean $\Sigma_H(G)$ y $\Sigma(G/H)$ la familia de subgrupos de G que contienen a H y la familia de subgrupos de G/H, respectivamente. Entonces, la aplicación

$$\psi : \Sigma_H(G) \to \Sigma(G/H), \ K \mapsto \pi(K) = K/H$$

es biyectiva.

Demostración. ψ está bien definida porque $\psi(K) = \pi(K)$, donde π es el homomorfismo cociente, y la imagen de un subgrupo por un homomorfismo es también un subgrupo. Además, ψ es suprayectiva puesto que, dado P, subgrupo de G/H, entonces $\pi\left(\pi^{-1}(P)\right) = P$, por ser π suprayectiva, y $\pi^{-1}(P)$ es un subgrupo de G que contiene a H

Por último, ψ es inyectiva puesto que si $\pi(K_1) = \pi(K_2)$ y $K_1 \neq K_2$, podemos suponer sin pérdida de generalidad que $\exists x \in K_1 \setminus K_2$. Entonces $\pi(x) \in \pi(K_1) = \pi(K_2)$, de modo que existe $k_2 \in K_2$ tal que $\pi(x) = \pi(k_2)$, luego $x^{-1}k_2 \in \ker \pi = H \subset K_2$. De este modo, $x = k_2\left(x^{-1}k_2\right)^{-1} \in K_2$. Esta contradicción prueba que si $\pi(K_1) = \pi(K_2)$, con $K_1, K_2 \in \Sigma_H(G)$, entonces $K_1 = K_2$. Por tanto, ψ también es inyectiva. □

Proposición 2.9. Dados dos subgrupos $K \subset H \subset G$ tales que $K \triangleleft G$, se verifica que:

$$N_G(H)/K = N_{G/K}(H/K)$$

Demostración. Dado $g \in N_G(H)$, se tiene que $g^{-1}Hg = H$, de modo que $(Kg)^{-1}(H/K)(Kg) = (g^{-1}Hg)/K = H/K$, por lo que $Kg \in N_{G/K}(H/K)$. Por tanto, $N_G(H)/K \subset N_{G/K}(H/K)$.

Recíprocamente, si $Kg \in N_{G/K}(H/K)$, se tiene que $(g^{-1}Hg)/K = (Kg)^{-1}(H/K)(Kg) = H/K$. Como $K \triangleleft G$ y $K \subset H$, también se cumple que $K = g^{-1}Kg \subset g^{-1}Hg$, luego por el teorema 2.8, $g^{-1}Hg = H$. Por tanto, $g \in N_G(H)$, luego $Kg \in N_G(H)/K$. □

3. Teoría de Lagrange

3.1. Orden del Producto

Definición 3.1. Dados dos subgrupos H y K de un grupo G, se define su *producto* como el conjunto

$$HK = \{hk : h \in H, k \in K\}$$

A continuación, se presenta una caracterización acerca de cuándo el producto de dos subgrupos es también un subgrupo.

Proposición 3.2. Dados dos subgrupos H y K de un grupo G, el producto HK es un subgrupo de G si y sólo si $HK = KH$. En particular, si G es abeliano, HK es un subgrupo.

Demostración. ($\Rightarrow$): Si HK es un subgrupo, se tiene que

$$kh \in KH \Rightarrow (kh)^{-1} = h^{-1}k^{-1} \in HK \Rightarrow kh = \left((kh)^{-1}\right)^{-1} \in HK$$

donde la última implicación se debe a que el inverso de un elemento de un subgrupo está en el subgrupo. De este modo $KH \subset HK$. Recíprocamente,

$$hk \in HK \Rightarrow (hk)^{-1} \in HK \Rightarrow \exists h_1 \in H, k_1 \in K : (hk)^{-1} = h_1k_1 \Rightarrow hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

Por tanto, $HK \subset KH$, luego $HK = KH$.

($\Leftarrow$): Como $1_G \in H \cap K$ y $1_G = 1_G \cdot 1_G$, se tiene que $1_G \in HK$.

Por otro lado, dados $h_1k_1, h_2k_2 \in HK$, donde $h_1, h_2 \in H$ y $k_1, k_2 \in K$, se verifica que $(h_1k_1)(h_2k_2)^{-1} = h_1\left(k_1k_2^{-1}\right)h_2^{-1}$. Como $HK = KH$, existen $h_3 \in H$ y $k_3 \in K$ tales que $h_3k_3 = \left(k_1k_2^{-1}\right)h_2^{-1}$. Entonces, $(h_1k_1)(h_2k_2)^{-1} = (h_1h_3)k_3 \in HK$. Así, por la observación 1.5, HK es un subgrupo. □

Corolario 3.3. Dados dos subgrupos H y K de un grupo G tales que $K \triangleleft G$, el producto HK es un subgrupo.

Demostración. Como K es un subgrupo normal, por la observación 1.9,

$$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$$

Entonces, por la proposición 3.2, HK es un subgrupo de G. □

El cardinal de un producto viene dada por la denominada *fórmula de Lagrange*, expuesta en la siguiente proposición.

Proposición 3.4. Dados dos subgrupos finitos H y K de un grupo G, se verifica la relación

$$ord(H)ord(K) = |HK|ord(H \cap K)$$

En particular, $|HK| \leq ord(H)ord(K)$.

Demostración. Considérese en el producto cartesiano $H \times K$, la relación de equivalencia $\mathcal{R}$ dada por

$$(h_1, k_1) \sim (h_2, k_2) \Leftrightarrow h_1k_1 = h_2k_2$$

Entonces, el cardinal de $H \times K$ es $ord(H)ord(K)$ y el de cada clase de equivalencia es $ord(H \cap K)$. Esta última afirmación se debe a que, dada la clase de equivalencia $[(h, k)]$, la aplicación

$$\phi : [(h, k)] \to H \cap K,\ (h_1, k_1) \mapsto h_1^{-1}h$$

es biyectiva. En efecto, está bien definida puesto que $hk = h_1k_1 \Rightarrow h_1^{-1}h = k_1k^{-1} \in H \cap K$ y su biyectividad se ve porque, dado $x \in H \cap K$, el elemento (hx^{-1}, xk) es el único de la clase de equivalencia cuya imagen es x.

Ahora, considérese la aplicación

$$\psi : (H \times K)/\mathcal{R} \to HK,\ [(h, k)] \mapsto hk$$

que está bien definida y es biyectiva. Entonces, el cardinal de ambos conjuntos coincide, lo que implica la igualdad buscada.

La segunda parte es consecuencia inmediata de que $ord(H \cap K) \geq 1$. □

3.2. Transitividad del índice

Definición 3.5. Dado un subgrupo $H \subset G$, el conjunto de *clases laterales por la derecha* es el formado por las clases de equivalencia dadas por la relación

$$\mathcal{R}_H : a \sim b \Leftrightarrow ab^{-1} \in H$$

Puede verse que dichas clases son:

$$Hg := \{hg : h \in H\} \ \ \forall g \in G$$

Definición 3.6. El número de clases de equivalencia se denomina *índice* de H en G, lo que se denota por $[G : H]$.

El índice verifica una propiedad transitiva, enunciada en el siguiente teorema.

Teorema 3.7. Dados dos subgrupos H y K de un grupo finito G tales que $K \subset H$, se verifica que:

$$[G : K] = [G : H] \cdot [H : K]$$

Demostración. Sean $a_1, \ldots, a_n$, representantes de las clases laterales de H en G, donde $n = [G : H]$, de modo que

$$G = \bigsqcup_{i=1}^{n} Ha_i$$

donde $\sqcup$ denota la unión disjunta.

Análogamente, sean $b_1, \ldots, b_m$ representantes de las clases laterales de K en H, de manera que

$$H = \bigsqcup_{j=1}^{m} Kb_j$$

Combinando los dos resultados, se llega a que

$$G = \bigsqcup_{i=1}^{n} Ha_i = \bigsqcup_{i=1}^{n} \left(\bigsqcup_{j=1}^{m} Kb_j \right) a_i = \bigsqcup_{i=1}^{n} \bigsqcup_{j=1}^{m} K(b_j a_i)$$

Como la unión es disjunta, cada $K(b_j a_i)$ representa a una clase lateral distinta de K en G, por lo que

$$[G : K] = n \cdot m = [G : H] \cdot [H : K]$$

□

La transitividad del índice tiene algunas consecuencias interesantes.

Corolario 3.8. Dado un subgrupo H de un grupo finito G, se verifica la fórmula de Lagrange

$$ord(G) = ord(H) \cdot [G : H]$$

En particular, el orden de cada subgrupo H divide al orden de G.

Demostración. Tomando $K = \{1_G\}$, el teorema 3.7 implica que

$$ord(G) = [G : K] = [G : H] \cdot [H : K] = [G : H] \cdot ord(H)$$

□

Corolario 3.9. Dados dos subgrupos H y K de un grupo finito G cuyos órdenes son primos entre sí, su intersección verifica que $H \cap K = \{1_G\}$.

Demostración. Como $H \cap K$ es un subgrupo tanto de H como de K, su orden ha de dividir tanto al orden de H como al de K. Como estos son primos entre sí, se tiene que $ord(H \cap K) = 1$, luego $H \cap K = \{1_G\}$. □

Otro aspecto de gran importancia en la clasificación de grupos es la restricción en el orden de sus elementos.

Definición 3.10. Dado un grupo G y un elemento $a \in G$, se define el *orden* de a en G, denotado por $o(a)$, como el menor $n \in \mathbb{N}$ tal que $a^n = 1_G$. Puede verse que el conjunto de números enteros $m \in \mathbb{Z}$ tales que $a^m = 1_G$ son los múltiplos de $o(a)$.

El teorema 3.7 también restringe los órdenes de cada uno de los elementos de un grupo finito a los divisores del orden del grupo.

Corolario 3.11. Dado un grupo finito G, el orden de todo elemento $a \in G$ divide al orden del grupo.

Demostración. Dado $a \in G$, el conjunto $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ es un subgrupo cuyo orden coincide con el orden de a. El resultado se sigue, entonces, del corolario 3.8. □

En este punto, resulta intuitivo definir la siguiente clase de grupos.

Definición 3.12. Un grupo G se dice *cíclico* si existe un elemento $a \in G$ tal que $G = \langle a \rangle$. De este modo, un grupo finito es cíclico si y sólo si contiene un elemento cuyo orden coincide con el orden del grupo.

4. Producto semidirecto de grupos

Antes de definir qué es el producto semidirecto de dos grupos, vamos a definir el grupo de automorfismos de un grupo.

Definición 4.1. Dado un grupo G, se define su *grupo de automorfismos*, denotado por $Aut(G)$, como el grupo formado por el conjunto de isomorfismos de G en G, denominados *automorfismos*, con la operación

$$(\phi_1 \cdot \phi_2)(g) := (\phi_2 \circ \phi_1)(g) \ \forall g \in G$$

Definición 4.2. Dados dos grupos G_1 y G_2, se define su *producto directo* $G_1 \times G_2$ como el producto cartesiano de G_1 y G_2 con la operación

$$(x_1, x_2) \cdot (y_1, y_2) := (x_1 y_1, x_2 y_2) \ \forall x_1, y_1 \in G_1, \ \forall x_2, y_2 \in G_2$$

Definición 4.3. Dados dos grupos G_1 y G_2 y un homomorfismo $\phi : G_1 \to Aut(G_2)$, se define el producto semidirecto de G_1 y G_2 via ϕ, denotado por $G_1 \ltimes_\phi G_2$, al producto cartesiano de G_1 y G_2, con la operación

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, \phi(y_1)(x_2)\, y_2) \ \ \forall x_1, y_1 \in G_1, \ \forall x_2, y_2 \in G_2$$

La consistencia de esta definición se ve en la siguiente proposición, que muestra que, efectivamente, el producto semidirecto de grupos es un grupo.

Proposición 4.4. El producto semidirecto de grupos, tal como se ha definido anteriormente, verifica los axiomas de la definición de grupo 1.1.

Demostración. En primer lugar, demostraremos la propiedad asociativa

$$((x_1,x_2)\cdot(y_1,y_2))\cdot(z_1,z_2) = (x_1y_1,\phi(y_1)(x_2)y_2)\cdot(z_1,z_2) = (x_1y_1z_1,\phi(z_1)\left(\phi(y_1)(x_2)y_2\right)z_2) =$$
$$(x_1y_1z_1,(\phi(z_1)\circ\phi(y_1))\left(x_2\right)\phi(z_1)(y_2)\,z_2) = (x_1y_1z_1,\phi(y_1z_1)(x_2)\,\phi(z_1)(y_2)\,z_2) =$$
$$(x_1,x_2)\cdot(y_1z_1,\phi(z_1)(y_2)z_2) = (x_1,x_2)\cdot((y_1,y_2)\cdot(z_1,z_2))$$

Por otro lado, veamos que $(1_{G_1},1_{G_2})$ es el elemento neutro del producto semidirecto. Para ello, cabe destacar que, por las propiedades de los homomorfismos de grupos, $\phi(1_{G_1})$ es el automorfismo identidad de G_2. Entonces,

$$(x_1,x_2)\cdot(1_{G_1},1_{G_2}) = (x_1 1_{G_1},\phi(1_{G_1})(x_2)1_{G_2}) = (x_1,x_2)$$
$$(1_{G_1},1_{G_2})\cdot(x_1,x_2) = (1_{G_1}x_1,\phi(x_1)(1_{G_2})x_2) = (x_1,x_2)$$

Por último, veamos la existencia del elemento inverso a partir de la igualdad $(x_1,x_2)^{-1} = \left(x_1^{-1},\phi(x_1^{-1})(x_2^{-1})\right)$. Esto es cierto, dado que

$$(x_1,x_2)\cdot\left(x_1^{-1},\phi(x_1^{-1})(x_2^{-1})\right) = \left(x_1x_1^{-1},\phi\left(x_1^{-1}\right)(x_2)\phi(x_1^{-1})(x_2^{-1})\right) = \left(1_{G_1},\phi\left(x_1^{-1}\right)(x_2x_2^{-1})\right) = (1_{G_1},1_{G_2})$$
$$\left(x_1^{-1},\phi(x_1^{-1})(x_2^{-1})\right)\cdot(x_1,x_2) = \left(x_1^{-1}x_1,\left(\phi(x_1)\circ\phi(x_1^{-1})\right)(x_2^{-1})x_2\right) = (1_{G_1},\phi(1_{G_1})(x_2^{-1})x_2) = (1_{G_1},1_{G_2})$$

□

Observación 4.5. Si $\phi : H \to Aut(K)$ es el homomorfismo nulo, es decir, el homomorfismo que verifica que $\phi(h) = Id_K\ \forall h \in H$, entonces el producto semidirecto $H \ltimes_\phi K$ coincide con el producto directo.

El producto semidirecto es muy útil a la hora de clasificar los distintos grupos de un orden dado, debido a la siguiente proposición.

Proposición 4.6. Dado un grupo G y dos subgrupos de este, H y K, tales que $K \triangleleft G$, $HK = G$ y $H \cap K = \{1_G\}$, entonces G es isomorfo a un producto semidirecto de H y K.

Demostración. Como K es un subgrupo normal de G, es invariante bajo la conjugación por elementos de H, es decir, que para cada $h \in H$, la aplicación

$$\widetilde{h} : K \to K,\ x \mapsto h^{-1}xh$$

es un automorfismo de K. Entonces, puede considerarse la aplicación

$$\phi : H \to Aut(K),\ h \mapsto \widetilde{h}$$

que es un homomorfismo de grupos puesto que:

$$(\phi(h_1)\cdot\phi(h_2))\,(x) = (\phi(h_2)\circ\phi(h_1))\,(x) = \left(\widetilde{h_2}\circ\widetilde{h_1}\right)(x) = h_2^{-1}h_1^{-1}xh_1h_2 =$$
$$(h_1h_2)^{-1}x(h_1h_2) = \widetilde{h_1h_2}(x) = \phi(h_1h_2)(x) \Rightarrow \phi(h_1)\cdot\phi(h_2) = \phi(h_1h_2)$$

De este modo, ϕ define una estructura de producto semidirecto $H \ltimes_\phi K$, que queremos ver que es isomorfo a G. Para ello, se considera la aplicación

$$\psi : H \ltimes_\phi K \to G,\ (h,k) \mapsto hk$$

que es sobreyectiva por la condición $G = HK$. Además, es homomorfismo porque

$$\psi\left((h_1,k_1)\cdot(h_2,k_2)\right) = \psi\left(h_1h_2, \widetilde{h}_2(k_1)k_2\right) = \psi\left(h_1h_2, h_2^{-1}k_1h_2k_2\right) =$$
$$h_1h_2h_2^{-1}k_1h_2k_2 = h_1k_1h_2k_1 = \psi(h_1,k_1)\psi(h_2,k_2)$$

Por último, ψ es inyectiva puesto que

$$(h,k) \in \ker\psi \Rightarrow hk = 1_G \Rightarrow h = k^{-1} \in H \cap K = \{1_G\} \Rightarrow (h,k) = (1_H, 1_K) = 1_{H\ltimes_\phi K}$$

Por tanto, ψ es un isomorfismo, luego $G \cong H \ltimes_\phi K$. □

Corolario 4.7. En las condiciones de la proposición 4.6, si además $H \triangleleft G$, entonces $G \cong H \times K$ es el producto directo de H y K.

Demostración. Como H y K son subgrupos normales, se verifica que $k^{-1}h^{-1}kh \in H \cap K = \{1_G\}$, de modo que $\widetilde{h}(k) = k\ \forall h \in H,\ \forall k \in K$.

De este modo, en la demostración de la proposición 4.6, los automorfismos $\widetilde{h}$ son el automorfismo identidad, luego $\phi(h) = Id_K\ \forall h \in H$. En este caso, por la observación 4.5, el producto semidirecto coincide con el producto directo. □

Ahora se van a exponer dos proposiciones que determinan ciertas condiciones bajo las cuales dos productos semidirectos son isomorfos.

Proposición 4.8. Sean H y K dos grupos y sean $\phi_1, \phi_2 : H \to Aut(K)$ dos homomorfismos. Si existe $\theta \in Aut(H)$ tal que $\phi_1 = \phi_2 \circ \theta$, entonces los productos semidirectos $H \ltimes_{\phi_1} K$ y $H \ltimes_{\phi_2} K$ son isomorfos.

Demostración. Considérese entonces la aplicación

$$\overline{\theta} : H \ltimes_{\phi_1} K \to H \ltimes_{\phi_2} K :\ (h,k)_{\phi_1} \mapsto (\theta(h),k)_{\phi_2}$$

donde los subíndices denotan el producto semidirecto en el que se considera cada par.

Veamos que $\overline{\theta}$ es un homomorfismo. En efecto,

$$\overline{\theta}\left((h_1,k_1)_{\phi_1}\cdot(h_2,k_2)_{\phi_1}\right) = \overline{\theta}\left((h_1h_2, \phi_1(h_2)(k_1)k_2)_{\phi_1}\right) = (\theta(h_1h_2), \phi_1(h_2)(k_1)k_2)_{\phi_2}$$
$$(\theta(h_1)\theta(h_2), \phi_2(\theta(h_2))(k_1)k_2)_{\phi_2} = (\theta(h_1),k_1)_{\phi_2}\cdot(\theta(h_2),k_2)_{\phi_2} = \overline{\theta}\left((h_1,k_1)_{\phi_1}\right)\cdot\overline{\theta}\left((h_2,k_2)_{\phi_1}\right)$$

Además, $\overline{\theta}$ es una biyección por serlo θ, luego los dos productos semidirectos son isomorfos. □

Proposición 4.9. Sean H y K dos grupos y sean $\phi_1, \phi_2 : H \to Aut(K)$ dos homomorfismos. Si existe $\theta \in Aut(K)$ tal que $\theta \circ \phi_1(h) = \phi_2(h) \circ \theta\ \forall h \in H$, entonces los productos semidirectos $H \ltimes_{\phi_1} K$ y $H \ltimes_{\phi_2} K$ son isomorfos.

Demostración. Considérese la aplicación

$$\overline{\theta} : H \ltimes_{\phi_1} K \to H \ltimes_{\phi_2} K :\ (h,k)_{\phi_1} \mapsto (h,\theta(k))_{\phi_2}$$

donde el subíndice denota el producto semidirecto al que pertenece el par (h,k). $\overline{\theta}$ es una aplicación biyectiva por serlo θ y, además, es un homomorfismo porque

$$\overline{\theta}\left((h_1,k_1)_{\phi_1}\cdot(h_2,k_2)_{\phi_1}\right) = \overline{\theta}\left((h_1h_2, \phi_1(h_1)(k_1)k_2)_{\phi_1}\right) = (h_1h_2, (\theta\circ\phi_1(h_1))(k_1)\theta(k_2))_{\phi_2} =$$
$$= (h_1h_2, \phi_2(h_1)(\theta(k_1))\theta(k_2))_{\phi_2} = (h_1,\theta(k_1))_{\phi_2}\cdot(h_2,\theta(k_2))_{\phi_2} = \overline{\theta}\left((h_1,k_1)_{\phi_1}\right)\cdot\overline{\theta}\left((h_2,k_2)_{\phi_1}\right)$$

□

Veamos ahora un resultado que determina el centro de un producto semidirecto:

Proposición 4.10. Dados dos grupos H y K y un homomorfismo $\phi : H \to Aut(K)$, el par (h, k), donde $h \in H$ y $k \in K$, pertenece al centro de $H \ltimes_\phi K$ si y sólo si $h \in \mathcal{Z}(H)$, $k \in Fix(\phi) := \{k \in K : \phi(h)(k) = k \ \forall h \in H\}$ y $\phi(h)(x) = kxk^{-1} \ \forall x \in K$.

Demostración. Si $(h, k) \in \mathcal{Z}(H \ltimes_\phi K)$, para cada $(h_1, k_1) \in H \ltimes_\phi K$ se tiene que

$$(hh_1, \phi(h_1)(k)k_1) = (h, k) \cdot (h_1, k_1) = (h_1, k_1) \cdot (h, k) = (h_1h, \phi(h)(k_1)k)$$

En particular $hh_1 = h_1h \ \forall h_1 \in H$, luego $h \in \mathcal{Z}(h)$. Por otro lado,

$$\phi(h)(k_1)k = \phi(h_1)(k)k_1 \ \forall h_1 \in H \ \forall k_1 \in K$$

Entonces, $\phi(h_1)(k)$ toma el mismo valor para todo $h_1 \in H$. Luego $\phi(h_1)(k) = \phi(1_H)(k) = k$, es decir, $k \in Fix(\phi)$. En este caso,

$$\phi(h)(k_1)k = kk_1 \ \forall k_1 \in K \Rightarrow \phi(h)(k_1) = kk_1k^{-1} \ \forall k_1 \in K$$

Recíprocamente, si se cumplen estas condiciones, (h, k) claramente conmuta con todos los elementos de $H \ltimes_\phi K$, luego pertenece al centro de dicho grupo. □

Corolario 4.11. Si H y K son grupos abelianos y $\phi : H \to Aut(K)$ un homomorfismo, entonces

$$\mathcal{Z}(H \ltimes_\phi K) = \ker \phi \times Fix(\phi)$$

Demostración. Las condiciones de la proposición 4.10 son equivalentes, cuando H y K son abelianos, a que $h \in \ker \phi$ y a que $k \in Fix(\phi)$. Además, la restricción de ϕ a $\ker \phi$ da el homomorfismo nulo, luego la restricción del producto semidirecto es un producto directo. □

5. Teoremas de Sylow

5.1. Acciones de grupos

Para definir qué es la acción de un grupo sobre un conjunto, conviene resaltar que, dado un conjunto X, el conjunto de biyecciones de X en X, denotado por $Biy(X)$ es un grupo con la operación dada por

$$\phi_1 \cdot \phi_2 = \phi_2 \circ \phi_1$$

Si $X = \{1, \ldots, n\}$ para algún $n \in \mathbb{N}$, se dice que $Biy(X)$ es el *n-ésimo grupo simétrico*, denotado por $\mathcal{S}_n$.

Definición 5.1. Se denomina *acción* de un grupo G sobre un conjunto no vacío X a cualquier homomorfismo de grupos $G \to Biy(X)$. Se denota por $\widetilde{g}$ a la imagen de cualquier elemento $g \in G$ bajo dicho homomorfismo.

Definición 5.2. Dada una acción de un grupo G sobre un conjunto X, se dicen *órbitas* a cada una de las clases de equivalencia dadas por la relación $x \sim y$ si existe $g \in G$ tal que $y = \widetilde{g}(x)$. Nótese que esta relación es de equivalencia por ser

- Simétrica: $x = \widetilde{1}_G(x) \Rightarrow x \sim x$.

- Reflexiva: $x \sim y \Rightarrow \exists g \in G : y = \widetilde{g}(x) \Rightarrow x = \widetilde{g^{-1}}(y) \Rightarrow y \sim x$.
- Transitiva: $x \sim y,\ y \sim z \Rightarrow \exists g, h \in G : y = \widetilde{g}(x),\ z = \widetilde{h}(y) \Rightarrow z = \widetilde{gh}(x) \Rightarrow x \sim z$

Definición 5.3. Dado un grupo G actuando sobre un conjunto X, se denomina *subgrupo estabilizador* del punto $x \in X$ al subgrupo

$$Stab_G(x) := \{g \in G : \widetilde{g}(x) = x\}$$

Puede comprobarse que, efectivamente, es un subgrupo haciendo uso de la observación 1.5.

A continuación, se va a ver que existe una relación entre el cardinal de una órbita y el índice del estabilizador de cada uno de sus puntos.

Proposición 5.4. Dado un grupo G que actúa sobre un conjunto X, para cualquier $x \in X$, se verifica que

$$|\mathcal{O}_x| = [G : Stab_G(x)]$$

donde $\mathcal{O}_x$ es la órbita a la que pertenece x.

Demostración. Sea $\Omega = \{(Stab_G(x))\, g : g \in G\}$ el conjunto de clases laterales de $Stab_G(x)$, cuyo cardinal coincide con el índice del estabilizador. Considérese ahora la aplicación

$$\psi : \Omega \to \mathcal{O}_x,\ Stab_G(x)g \mapsto \widetilde{g}(x)$$

En primer lugar, ψ está bien definida y, además, es inyectiva, puesto que

$$Stab_G(x)g_1 = Stab_G(x)g_2 \Leftrightarrow g_1 g_2^{-1} \in Stab_G(x) \Leftrightarrow \widetilde{g_1 g_2^{-1}}(x) = x \Leftrightarrow \left(\widetilde{g_2}^{-1} \circ \widetilde{g_1}\right)(x) = x \Leftrightarrow \widetilde{g_1}(x) = \widetilde{g_2}(x)$$

Por otro lado, ψ es claramente suprayectiva a partir de la definición de órbita. Por tanto, ψ es una biyección, luego se verifica que

$$|\mathcal{O}_x| = |\Omega| = [G : Stab_G(x)]$$

□

Como las órbitas son una partición del conjunto X sobre el que actúa un grupo G, se obtiene el siguiente corolario.

Corolario 5.5. Dado un grupo G que actúa sobre un conjunto X, si tomamos un conjunto R que contenga exactamente un elemento de cada órbita (denominado conjunto de representantes) se verifica que

$$|X| = \sum_{x \in R} |\mathcal{O}_x| = \sum_{x \in R} [G : Stab_G(x)]$$

La teoría de acciones es especialmente interesante para el estudio de grupos cuyo orden es una potencia de un número primo p. Un ejemplo de ello es el siguiente lema que se utilizará posteriormente en la demostración de los teoremas de Sylow.

Lema 5.6. Sean un número primo p, un grupo finito G y un subgrupo de este, H, cuyo orden es potencia de p. Entonces, $[G : H] \equiv [N_G(H) : H] \mod p$.

Demostración. Considérese el conjunto $\Omega = \{Hx : x \in G\}$ cuyo cardinal coincide con el índice de H en G y considérese la acción de H sobre dicho conjunto dada por

$$\widetilde{h}(Hg) = Hgh$$

Puede comprobarse que esta definición verifica que $H \mapsto Biy(\Omega) : \ h \mapsto \widetilde{h}$ es un homomorfismo bien definido, luego es una acción. Tomando un conjunto de representantes de cada órbita, por el corolario 5.5 se cumple que:

$$[G : H] = |\Omega| = \sum_{Hx \in R} [H : Stab_H(Hx)]$$

Como se está estudiando la congruencia módulo p, interesa conocer qué estabilizadores coinciden con H, pues en caso contrario su índice será múltiplo de p.

$$Stab_H(Hx) = H \Leftrightarrow \widetilde{h}(Hx) = Hx \ \forall h \in H \Leftrightarrow Hxh = Hx \ \forall h \in H \Leftrightarrow xhx^{-1} \in H \ \forall h \in H \Leftrightarrow$$
$$xHx^{-1} \subset H \Leftrightarrow xHx^{-1} = H \Leftrightarrow x \in N_G(H) \Leftrightarrow Hx \in N_G(H)/H$$

donde la implicación $\Leftarrow$ de la última equivalencia se debe a que

$$Hg \in N_G(H)/H \Rightarrow \exists g_1 \in N_G(H) : Hg = Hg_1 \Rightarrow gg_1^{-1} \in H \subset N_G(H) \Rightarrow g \in N_G(H)$$

De este modo, la fórmula de las órbitas del corolario 5.5 se escribe

$$[G : H] = [N_G(H) : H] + \sum_{Hx \in R,\, x \notin N_G(H)} [H : Stab_H(Hx)]$$

Entonces, como el orden de H es una potencia de p, los elementos del sumatorio son múltiplos de p, de modo que $[G : H] - [N_G(H) : H]$ también lo es. □

5.2. Teorema de Cauchy

Teorema 5.7. Sea p un número primo y G un grupo cuyo orden es múltiplo de p. Entonces, el número de subgrupos de orden p es congruente con 1, módulo p. En particular, G tiene algún elemento de orden p.

Demostración. Considérese el conjunto

$$X = \{(g_1, \ldots, g_p) \in G^p : g_1 \cdots g_p = 1_G\}$$

Como, por la existencia y unicidad del elemento inverso, para cada conjunto de $p-1$ elementos $\{g_1, \ldots, g_{p-1}\}$, existe un único g_p tal que $g_1 \cdots g_p = 1_G$, el cardinal del conjunto X es $|X| = ord(G)^{p-1}$.

Considérese el subgrupo del grupo de permutaciones $H := \langle (1, \ldots, p) \rangle \subset \mathcal{S}_p$, que actúa sobre X de la siguiente forma:

$$\widetilde{\sigma}\,(g_1, \ldots, g_p) = \left(g_{\sigma(1)}, \ldots, g_{\sigma(p)}\right)$$

Esta definición es una acción puesto que claramente se verifica que $\widetilde{\sigma\tau} = \widetilde{\sigma}\widetilde{\tau}$. Además, $\widetilde{\sigma}$ está bien definida por ser σ una potencia del ciclo $(1, \ldots, n)$, de modo que $\widetilde{\sigma}(g_1, \ldots, g_p) = (g_{i+1}, \ldots g_p, g_1, \ldots, g_i)$ para algún $i \in \{1, \ldots, p\}$. Entonces, por el hecho de que todo elemento de G conmuta con su inverso, $g_{i+1} \cdots g_p \cdot g_1 \cdots g_i = 1_G$, luego $\widetilde{\sigma}(X) \subset X$.

Por el corolario 5.5, dado un conjunto de representantes R se verifica que

$$ord(G)^{p-1} = |X| = \sum_{u \in R} [H : Stab_H(u)]$$

Como $ord(H) = p$ y, por el corolario 3.8, es un múltiplo de $[H : Stab_H(u)]$, este último puede valer 1 ó p. De este modo, el número de elementos (que denotaremos por m) $u \in R$ tal que $[H : Stab_H(u)] = 1$ o, equivalentemente, $Stab_H(u) = H$ es múltiplo de p. Además, puede verse que, si $u = (g_1, \ldots, g_p)$, esta condición es equivalente a que para cada $\sigma \in H$ se cumpla que

$$\widetilde{\sigma}\,(g_1, \ldots, g_p) = \left(g_{\sigma(1)}, \ldots, g_{\sigma(p)}\right) = (g_1, \ldots, g_p) \Leftrightarrow g_1 = g_2 = \cdots = g_p \Rightarrow g_1^p = 1_G$$

De este modo, G tiene m elementos cuyo orden divide a p, siendo m un múltiplo de p. De ellos, todos menos el elemento neutro tienen orden p, es decir, el número l de elementos de orden p en G es congruente con $p - 1$, módulo p.

Así, como cada elemento de orden p genera un subgrupo de orden p que contiene al elemento neutro y a $p - 1$ elementos de orden p y, además, dos grupos distintos de orden p intersecan en el elemento neutro, el número de subgrupos de orden p es congruente con 1, módulo p. □

5.3. Primer Teorema de Sylow

Definición 5.8. Dado un grupo G cuyo orden se escribe como $ord(G) = p^n m$, donde p es un número primo y m y n son enteros positivos tales que p no divide a m, se denominan *p-subgrupos de Sylow* de G a los subgrupos de G cuyo orden es p^n.

El conjunto de p-subgrupos de Sylow de un grupo G se denota $Syl_p(G)$, que, como consecuencia del siguiente teorema, es un conjunto no vacío.

Teorema 5.9. Sea un grupo finito G cuyo orden se escribe como $ord(G) = p^n m$, donde p es un número primo y m y n son enteros positivos tales que p no divide a m. Entonces, para cada $i \in \{0, \ldots, n-1\}$ y cada subgrupo $H_i \subset G$ de orden p^i, existe un subgrupo H_{i+1} de orden p^{i+1} tal que $H_i \triangleleft H_{i+1}$.

En particular, todo subgrupo de G cuyo orden es potencia de p está contenido en algún p-subgrupo de Sylow de G.

Demostración. Se va a proceder por inducción sobre i. Para $i = 0$, el único subgrupo de orden 1 es $H_0 = \{1_G\}$. Por el teorema de Cauchy 5.7, existe un subgrupo H_1 de G de orden p que, obviamente, contiene a H_0 como subgrupo normal.

Considérese ahora el caso en el que $0 < i < n$. Entonces, por el lema 5.6,

$$[G : H_i] = p^{n-i} m \in p\mathbb{Z} \Rightarrow [N_G(H_i) : H_i] \in p\mathbb{Z}$$

Entonces, por el teorema de Cauchy 5.7, el grupo cociente $N_G(H_i)/H_i$ contiene a un subgrupo de orden p. De este modo, por el teorema 2.8, existe un subgrupo H_{i+1} contenido en $N_G(H_i)$ que contiene a H_i (como subgrupo normal, debido a que $H_{i+1} \subset N_G(H_i)$) tal que $ord(H_{i+1}/H_i) = p$.

Así, se verifica tanto que $H_i \triangleleft H_{i+1}$ como que $ord(H_{i+1}) = p^{i+1}$.

La segunda parte se obtiene aplicando el teorema $n - i$ veces hasta obtener un subgrupo de orden p^n (de Sylow) que contenga al subgrupo original. □

Corolario 5.10. Sea un grupo finito G cuyo orden se escribe como $ord(G) = p^n m$, donde p es un número primo y m y n son enteros positivos tales que p no divide a m. Entonces, la familia de p-subgrupos de Sylow de G, $Syl_p(G)$, es no vacía.

5.4. Segundo Teorema de Sylow

Una vez hemos probado que todo grupo G cuyo orden es múltiplo de p contiene algún p-subgrupo de Sylow, veamos que la familia $Syl_p(G)$ es el conjunto de grupos conjugados de cualquier $H \in Syl_p(G)$.

Teorema 5.11. Dado un grupo finito G cuyo orden se escribe como $ord(G) = p^n m$, donde p es un número primo y m y n son enteros positivos tales que p no divide a m, si $H, K \in Syl_p(G)$, entonces H y K son subgrupos conjugados.

De este modo, $Syl_p(G)$ es el conjunto de subgrupos conjugados de cualquier $H \in Syl_p(G)$.

Demostración. Considérese la acción de H sobre el conjunto de clases laterales $\Omega = \{Kx : x \in G\}$ dada por

$$\widetilde{h}(Kx) = Kxh$$

Por el corolario 5.5, se tiene que

$$m = [G : K] = |\Omega| = \sum_{Kx \in R} [H : Stab_H(Kx)]$$

donde R es un conjunto de representantes. Como el orden de H es p^n, si $Stab_H(Kx) \neq H$, entonces $[H : Stab_H(Kx)]$ es múltiplo de p por el corolario 3.8. Como $p \nmid m$, tiene que existir $x \in G$ tal que $Stab_H(Kx) = H$, es decir,

$$\widetilde{h}(Kx) = Kx \ \forall h \in H \Rightarrow Kxh = Kx \ \forall h \in H \Rightarrow xhx^{-1} \in K \ \forall h \in H \Rightarrow xHx^1 \subset K \Rightarrow xHx^{-1} = K$$

donde la última implicación se debe a que $ord(K) = ord(H) = ord(xHx^{-1})$.

La segunda parte se sigue de que, dado $H \in Syl_p(G)$, todo subgrupo conjugado de H tiene orden p^n, luego pertenece a $Syl_p(G)$. □

5.5. Tercer Teorema de Sylow

Una vez se ha visto que la familia $Syl_p(G)$ es no vacía, siendo G un grupo finito cuyo orden es múltiplo de p, y que los subgrupos de esta familia son subgrupos conjugados, se busca obtener condiciones sobre el cardinal de esta familia, que se denotará por $n_p(G) = |Syl_p(G)|$ (o simplemente n_p cuando no haya riesgo de confusión sobre el grupo G).

Empezamos exponiendo un lema sobre el índice del normalizador de un subgrupo.

Lema 5.12. Dado un grupo finito G, un subgrupo H y el conjunto $\Sigma := \{a^{-1}Ha : a \in G\}$, entonces $|\Sigma| = [G : N_G(H)]$.

Demostración. Se denota $N := N_G(H)$ y $\Omega = \{Nx : x \in G\}$, cuyo cardinal es $[G : N]$. Entonces, se define la aplicación

$$\psi : \Omega \to \Sigma, \ Na \mapsto a^{-1}Ha$$

En primer lugar, veamos que ψ está bien definida y es inyectiva, puesto que:

$$Na = Nb \Leftrightarrow ab^{-1} \in N \Leftrightarrow (ab^{-1})^{-1}H(ab^{-1}) = H \Leftrightarrow ba^{-1}Hab^{-1} = H \Leftrightarrow a^{-1}Ha = b^{-1}Hb \Leftrightarrow \psi(Na) = \psi(Nb)$$

Además, ψ es claramente suprayectiva por la definición de Σ, luego es una biyección. De este modo,

$$|\Sigma| = |\Omega| = [G : N_G(H)]$$

□

A continuación, presentamos el tercer teorema de Sylow

Teorema 5.13. Sea un grupo finito G cuyo orden se escribe como $ord(G) = p^n m$, donde p es un número primo y m y n son enteros positivos tales que p no divide a m. Entonces, el número n_p de p-subgrupos de Sylow de G verifica:

1. $n_p = [G : N_G(H)]$ para cada $H \in Syl_p(G)$.
2. n_p divide a m, y p divide a $n_p - 1$.

Demostración. Dado $H \in Syl_p(G)$, el teorema 5.11 afirma que los elementos de $Syl_p(G)$ son los subgrupos conjugados de H. Entonces, por el lema 5.12,

$$n_p(G) = |Syl_p(G)| = [G : N_G(H)]$$

En cuanto a la segunda parte, por el teorema 3.7, se verifica que

$$m = [G : H] = [G : N_G(H)] \cdot [N_G(H) : H] = n_p(G) \cdot [N_G(H) : H]$$

de modo que $n_p | m$ y, además, por el lema 5.6,

$$m = [G : H] \equiv [N_G(H) : H] \mod p \Rightarrow n_p(G) \equiv 1 \mod p$$

□

6. Teorema de Clasificación de Grupos Abelianos Finitos

El objetivo de esta sección es proporcionar una clasificación de los grupos abelianos finitos de un orden dado. Para ello, probaremos que todo grupo abeliano finito puede expresarse como el producto directo de varios grupos cíclicos.

Definición 6.1. El *exponente* de un grupo G, denotado por $e(G)$, es el mínimo común múltiplo de los órdenes de los elementos de G.

A continuación, presentamos dos lemas técnicos que se utilizarán para demostrar algunas propiedades del exponente de un grupo abeliano finito.

Lema 6.2. Dado un grupo G y un elemento $a \in G$ de orden n, para todo $k \in \mathbb{Z}$ se verifica que

$$o\left(a^k\right) = \frac{n}{mcd(n,k)}$$

Demostración. Sean $d := mcd(n,k)$ y $l := k/d \in \mathbb{Z}$. Entonces,

$$\left(a^k\right)^{n/d} = a^{kn/d} = (a^n)^l = 1_G^l = 1_G \Rightarrow o\left(a^k\right) \left| \frac{n}{d} \right.$$

Por otro lado, por la definición de orden, se verifica que

$$a^{ko\left(a^k\right)} = \left(a^k\right)^{o\left(a^k\right)} = 1_G \Rightarrow n = o(a) \left| ko\left(a^k\right) \Rightarrow \frac{n}{o\left(a^k\right)} \right| k$$

Cabe destacar que para la última implicación se ha tenido en cuenta que $\dfrac{n}{o\left(a^k\right)}$ es un entero, lo cual se deduce de la primera parte de esta demostración. Por otro lado, es claro que $\dfrac{n}{o\left(a^k\right)}$ divide a n, luego por la definición de máximo común divisor,

$$\frac{n}{o\left(a^k\right)}\Big| d \Rightarrow \frac{n}{d}\Big| o\left(a^k\right)$$

Por tanto, ha de verificarse la igualdad buscada. □

Lema 6.3. Dado un grupo G y dados $a, b \in G$ de órdenes n y m, respectivamente, tales que $mcd(n, m) = 1$, si $ab = ba$, entonces $o(ab) = nm$.

Demostración. Como a y b conmutan,

$$(ab)^{nm} = a^{nm}b^{nm} = 1_G \Rightarrow o(ab)|nm$$

Por otro lado, si $r := o(ab)$, como a y b conmutan se tiene que $a^r b^r = (ab)^r = 1_G$. De este modo, $a^r = b^{-r} \in \langle a\rangle \cap \langle b\rangle = \{1_G\}$, puesto que los grupos generados por a y b tienen órdenes primos entre sí (corolario 3.9). Entonces $a^r = b^r = 1_G$, luego r es múltiplo de n y m. Por tanto, como n y m son primos entre sí, r también es múltiplo de $nm = mcm(n, m)$. □

A continuación, se exponen algunas propiedades del exponente de un grupo abeliano.

Proposición 6.4. El exponente de un grupo abeliano finito G es el máximo de los órdenes de los elementos de G.

Demostración. Como G es finito, existe $x \in G$ tal que $m = o(x) \geq o(g)\ \forall g \in G$. Queremos ver que $e(G) = o(x)$. Para ello, supongamos por reducción al absurdo que existe $y \in G$ tal que $n = o(y)$ no divide a $o(x)$. Entonces, por el teorema fundamental de la aritmética, existe un número primo p tal que

$$r := \text{máx}\{k \in \mathbb{Z} : k \geq 0, p^k|m\} < \text{máx}\{k \in \mathbb{Z} : k \geq 0, p^k|n\} =: s$$

Por el lema 6.2,

$$o\left(x^{p^r}\right) = \tfrac{m}{mcd(m,p^r)} = \tfrac{m}{p^r} \notin p\mathbb{Z}; \quad o\left(y^{n/p^s}\right) = \tfrac{n}{mcd(n,n/p^s)} = p^s$$

Como estos elementos conmutan (por ser G abeliano) y tienen órdenes primos entre sí, el lema 6.3 implica que

$$o\left(x^{p^r}y^{n/p^s}\right) = o\left(x^{p^r}\right)\left(y^{n/p^s}\right) = mp^{s-r} > m$$

lo que contradice el hecho de que m es el máximo de los órdenes de los elementos de G. □

Proposición 6.5. Sea G un grupo abeliano finito de exponente e y sea $x \in G$ un elemento de orden e. Si $H := \langle x\rangle$ e $y \in G$, existe $z \in Hy \in G/H$ tal que $o(z) = o(Hy)$.

Demostración. Sean $l := o\,(y)$ y $m := o\,(Hy)$. Entonces, $H = (Hy)^m = Hy^m$, luego $y^m \in H$, siendo esto equivalente a que exista $r \in \mathbb{Z}$ tal que $y^m = x^r$.

Como Hy es la imagen de y por el homomorfismo cociente, l es un múltiplo de m, de modo que, por el lema 6.2,

$$\frac{l}{m} = \frac{l}{mcd(l,m)} = o\,(y^m) = o\,(x^r) = \frac{e}{mcd(e,r)} \Rightarrow mcd(e,r) = m\frac{e}{l} \in m\mathbb{Z}$$

puesto que, por la definición de exponente, e es un múltiplo de l. De este modo, r es un múltiplo de m, existiendo $s \in \mathbb{Z}$ tal que $r = sm$.

Definimos $z := x^{-s}y \in Hy$. Como G es un grupo abeliano:

$$z^m = x^{-sm}y^m = x^{-r}y^m = 1_G \Rightarrow o(z)|m$$

Recíprocamente, por ser imagen del homomorfismo cociente, se verifica que $m = o(Hy) = o(Hz)$ divide a $o(z)$, luego se tiene la igualdad buscada. □

Ahora se presenta una clasificación de los grupos abelianos como producto directo de grupos cíclicos $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, cuyos órdenes están perfectamente determinados bajo ciertas condiciones.

Teorema 6.6. Dado un grupo abeliano finito G, existen enteros positivos $m_1, \ldots, m_r$, tales que $m_i|m_{i-1}$ $\forall i \in \{2, \ldots, r\}$ y $G \cong \mathbb{Z}_{m_1} \times \cdots \mathbb{Z}_{m_r}$. Además, bajo estas condiciones, los números $m_1, m_2, \ldots, m_r$ son únicos y se denominan *coeficientes de torsión* de G.

Demostración. Se va a demostrar la existencia por inducción sobre $n = ord(G)$. Para $n = 1$, tomamos $r = 1$ y $m_1 = 1$.

En el caso en el que $n > 1$, escogemos $z_1 \in G$ tal que $o(z_1) = e(G) = m_1$, que existe por la proposición 6.4.

Denotando $H := \langle z_1 \rangle$, el cociente G/H es un grupo abeliano y finito cuyo orden es $n/m_1 < n$, luego la hipótesis de inducción implica que existen números enteros $m_2, \ldots, m_r$ que verifican las condiciones del teorema. Sea $\phi : \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \to G/H$ un isomorfimo y $u_i \in \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ es el elemento con todas las coordenadas nulas a excepción de la asociada al grupo $\mathbb{Z}_{m_i}$, que es $1 + m_i\mathbb{Z}$.

Según la proposición 6.5, $\exists z_i \in G$ tal que $\phi(u_i) = Hz_i$ y $o(z_i) = m_i$. Denotando $H_i := \langle z_i \rangle$, como G es abeliano, el producto $N := H_2 \cdots H_r$ es un subgrupo cuyo orden, por la proposición 3.4 aplicada repetidas veces, verifica que

$$ord(N) \leq ord(H_2) \cdots ord(H_r) = m_2 \cdots m_r = n/m_1 = ord(G/H)$$

Recíprocamente, el homomorfismo formado por la composición de la inclusión y el homomorfismo cociente $\pi \circ j : N \hookrightarrow G \to G/H$ es suprayectivo. En efecto, dado $Hg \in G/H$, existen números naturales $a_2, \ldots a_r$ tales que

$$Hg = \phi(a_2 + m_2\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z}) = \phi(a_2u_2 + \cdots + a_ru_r) = \phi(u_2)^{a_2} \cdots \phi(u_r)^{a_r} = Hz_2^{a_2} \cdots z_r^{a_r}$$

De este modo, como $z_2^{a_2} \cdots z_r^{a_r} \in N$, se tiene que Hg está en la imagen de $\pi \circ j$ para todo $g \in G$, luego dicho homomorfismo es suprayectivo. Por tanto, $ord(N) \geq ord(G/H)$ y, en virtud de lo probado anteriormente, se verifica la igualdad.

Esta igualdad en el número de elementos, junto a la sobreyectividad, prueba que $\pi \circ j$ es un isomorfismo. En particular, la sobreyectividad implica que $G = HN$ y la inyectividad, que $N \cap H = \{1_G\}$. De este modo, como H y N son subgrupos normales por ser G abeliano, el corolario 4.7 afirma que

$$G \cong H \times N = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$$

Además, por un lado la hipótesis de inducción implica que $m_i|m_{i-1}$ $\forall i \in \{3, \ldots, r\}$ y, por otro lado, la definición de exponente implica que $m_2 = o(z_2)|e(G) = o(z_1) = m_1$.

Para ver la unicidad, si los grupos

$$G_1 = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}; \quad G_2 = \mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_s}$$

son isomorfos (donde cada m_i divide a m_{i-1} y cada n_i a n_{i-1}), entonces $m_1 = e(G_1) = e(G_2) = n_1$.

Por reducción al absurdo, supóngase que existe un índice mínimo k tal que $m_k \neq n_k$. Sin pérdida de generalidad, puede suponerse que $m_k < n_k$ y, entonces, considérese el homomorfismo $\phi : G_1 \to G_1 :\ a \mapsto a^{m_k}$, cuya imagen es

$$\text{Im }\ \phi = m_k\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times m_k\mathbb{Z}/m_{k-1}\mathbb{Z} \times \{0\}$$

Por el segundo teorema de isomorfía 2.6, si $m|n$, como $n\mathbb{Z} \subset m\mathbb{Z}$, se verifica que

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z} \Rightarrow ord\,(m\mathbb{Z}/n\mathbb{Z}) = \frac{n}{m}$$

De este modo, $ord(\text{Im}(\phi)) = \dfrac{m_1 \cdots m_{k-1}}{(m_k)^{k-1}}$

Consideremos ahora el mismo homomorfismo, pero esta vez aplicado al grupo G_2; $\psi : G_2 \to G_2 :\ a \mapsto a^{m_k}$, cuya imagen verifica que

$$\text{Im }\ \psi \supset m_k\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times m_k\mathbb{Z}/n_{k-1}\mathbb{Z} \times \{0 + n_k\mathbb{Z}, m_k + n_k\mathbb{Z}\} \times \{0\}$$

Como $m_k < n_k$, entonces $0 + n_k\mathbb{Z} \neq m_k + n_k\mathbb{Z}$, luego

$$ord(\text{Im }\ \psi) \geq \frac{2n_1 \cdots n_{k-1}}{(m_k)^{k-1}} = 2ord(\text{Im }\ \phi)$$

Sin embargo, si G_1 y G_2 son isomorfos, ha de cumplirse que $ord(\text{Im }\ \phi) = ord(\text{Im }\ \psi)$, obteniéndose así una contradicción que prueba que $m_i = n_i\ \forall i \in \{1, \ldots, \text{mín}\{r, s\}\}$. Además,

$$m_1 \cdots m_r = ord(G_1) = ord(G_2) = n_1 \cdots n_s$$

de modo que $r = s$.

□

7. Clasificación de determinadas familias de grupos finitos

7.1. Grupos de orden primo

Observación 7.1. Dado un grupo G y un elemento $a \in G$, el conjunto $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$ es un subgrupo cíclico de G.

Proposición 7.2. Dado un número primo p, todo grupo finito G de orden p es cíclico.

Demostración. Tomando $a \in G \setminus \{1_G\}$, por el corolario 3.8, el orden del subgrupo $\langle a \rangle$ divide a p. Sin embargo, como $\{1_G, a\} \subset \langle a \rangle$, el orden de $\langle a \rangle$ no puede ser 1, luego ha de ser p. Por tanto, $G = \langle a \rangle$, de modo que G es cíclico. □

Corolario 7.3. Dado un número primo p, dos grupos cualesquiera, G_1 y G_2, de orden p son isomorfos. En particular, todo grupo de orden p es isomorfo a $\mathbb{Z}_p$.

7.2. Grupos de orden p^2

Lema 7.4. Dado un número primo p, sea G un grupo finito cuyo orden es p^n para algún $n \in \mathbb{N}$. Dado $H \neq \{1_G\}$, subgrupo normal de G, entonces la intersección $H \cap \mathcal{Z}(G) \neq \{1_G\}$. En particular, $\mathcal{Z}(G) \neq \{1_G\}$.

Demostración. Como H es normal, puede considerarse la acción de G dada por $\psi : G \to Biy(X)$, $g \mapsto \widetilde{g}$, donde $X := H \setminus \{1_G\}$ y $\widetilde{g} : X \to X,\ x \mapsto g^{-1}xg$.

Además, como $H \neq \{1_G\}$ es un subgrupo de G, por el corolario 3.8, existe $m \in \{1, \dots, n\}$ tal que $ord(H) = p^m$. Entonces, el corolario 5.5 implica que

$$p^m - 1 = |X| = \sum_{h \in R} [G : Stab_G(h)]$$

donde R es un conjunto de representantes. Además, por el corolario 3.8, $[G : Stab_G(h)]$ es 1 o un múltiplo de p. Entonces, ha de existir $h \in X$ tal que $Stab_G(h) = G$, es decir, $\widetilde{g}(h) = g^{-1}hg = h\ \forall g \in G \Rightarrow hg = gh\ \forall g \in G \Rightarrow h \in (H \cap \mathcal{Z}(G)) \setminus \{1_G\}$

La segunda parte se deduce tomando $H = G$. □

Lema 7.5. Todo grupo G tal que $G/\mathcal{Z}(G)$ es cíclico es abeliano.

Demostración. Sea a perteneciente a una clase generadora de $G/\mathcal{Z}(G)$. Entonces, todo $x, y \in G$ pueden escribirse como $x = z_1 a^{n_1}$ e $y = z_2 a^{n_2}$ para algunos $z_1, z_2 \in \mathcal{Z}(G)$ y $n_1, n_2 \in \mathbb{N}$. Así,

$$xy = z_1 a^{n_1} z_2 a^{n_2} = z_1 z_2 a^{n_1+n_2} = z_2 z_1 a^{n_2} a^{n_1} = z_2 a^{n_2} z_1 a^{n_1} = yx$$

□

Corolario 7.6. Dado un número primo p, todo grupo G de orden p^2 es abeliano.

Demostración. Supongamos que G no es abeliano. Entonces, $\mathcal{Z}(G) \neq G$. Además, por el lema 7.4, $\mathcal{Z}(G) \neq \{1_G\}$. Entonces, la única posibilidad que deja el corolario 3.8 es que $ord\,(\mathcal{Z}(G)) = p$. Entonces, $G/\mathcal{Z}(G)$ tiene orden p, luego, por la proposición 7.2, es un grupo cíclico. Entonces, el lema 7.5 implicaría que G es abeliano. Esta contradicción implica que todo grupo de orden p^2 es abeliano. □

En este contexto, los grupos de orden p^2 pueden clasificarse mediante el teorema de clasificación de grupos abelianos finitos 6.6.

Corolario 7.7. Dado un número primo p, todo grupo G de orden p^2 es isomorfo a $\mathbb{Z}_{p^2}$ o a $\mathbb{Z}_p \times \mathbb{Z}_p$.

7.3. Grupos de orden p^3

Observación 7.8. Según el teorema de clasificación de los grupos abelianos finitos 6.6, para cada número primo p existen tres grupos abelianos no isomorfos de orden p^3. Estos vienen dados por:

$$G_1^{(p^3)} = \mathbb{Z}_{p^3}, \quad G_2^{(p^3)} = \mathbb{Z}_{p^2} \times \mathbb{Z}_p, \quad G_3^{(p^3)} = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$$

Ahora, vamos a estudiar los grupos no abelianos de orden p^3. Para ello, consideramos por separado los casos en que $p = 2$ y que p es un número primo impar. Comenzamos considerando los siguientes lemas.

Lema 7.9. Un grupo G tal que todo elemento distinto del neutro tiene orden 2 es abeliano.

Demostración. Dados $a, b \in G$, se tiene que

$$abab = (ab)^2 = 1_G = a^2b^2 = aabb \Rightarrow ba = a^{-1}(abab)b^{-a} = a^{-1}(aabb)b^{-1} = ab$$

Por tanto, todo par de elementos de G conmutan, es decir, G es abeliano. □

Lema 7.10. Dado un subgrupo $H \subset G$ tal que $[G : H] = 2$, entonces $H \triangleleft G$.

Demostración. Si $x \in H$, se verifica que $Hx = H = xH$, mientras que si $x \notin H$, se cumple que $Hx = G \setminus H = xH$. Entonces, por la observación 1.9, $H \triangleleft G$. □

Proposición 7.11. Existen únicamente dos grupos no abelianos no isomorfos de orden 8, los cuales se denotan por $\mathcal{D}_4$ y $\mathcal{Q}_8$.

Demostración. Sea G un grupo no abeliano de orden 8. Entonces, G no puede tener ningún elemento de orden 8 porque entonces sería cíclico y, por tanto, abeliano. Además, si todos los elementos de G tuvieran orden 2, G sería abeliano por el lema 7.9.

Por tanto, todo grupo no abeliano de orden 8 tiene algún elemento de orden 4, denotado por a. Así, $H := \langle a \rangle$ tiene índice 2, luego $H \triangleleft G$ por el lema 7.10. Sea $b \in G \setminus H$. Entonces, $b^{-1}ab \in H$ por ser H un subgrupo normal y, además, tiene orden 4 por ser un elemento conjugado de a. Por tanto, $b^{-1}ab \in \{a, a^3\}$.

Si $b^{-1}ab = a$, entonces a y b conmutarían y G sería abeliano. Por tanto, $b^{-1}ab = a^3$ o, equivalentemente, $aba = b$.

Por otro lado, Hb tiene orden 2 en G/H, luego $b^2 \in H$. Si $b^2 \in \{a, a^3\}$, b tendría orden 8 por el lema 6.2, lo que implicaría que G sería abeliano. Por tanto, quedan dos opciones.

Si $b^2 = 1_G$, tenemos el denominado grupo diedral, dado por

$$G_4^{(8)} \cong \mathcal{D}_4 \cong \langle a, b | a^4 = 1_G, b^2 = 1_G, aba = b \rangle$$

De este modo, $\mathcal{D}_4$ es isomorfo al único producto semidirecto no abeliano $\langle b \rangle \ltimes_\phi \langle a \rangle \cong \mathbb{Z}_2 \ltimes_\phi \mathbb{Z}_4$, denominándose n-ésimo grupo diedral para $n = 4$. En la notación habitual, se escribe $\rho = a$ y $\tau = b$.

Si, por el contrario, $b^2 = a^2$, entonces tenemos el denominado grupo cuaternión dado por

$$G_5^{(8)} \cong \mathcal{Q}_8 = \langle a, b | a^4 = 1_G, a^2 = b^2, aba = b \rangle$$

En la notación habitual, se escribe $-1 = a^2$, $i = a$, $j = b$, $k = ab$ y $-i$, $-j$ y $-k$ a sus inversos.

Es fácil ver que $\mathcal{D}_4$ tiene dos elementos de orden 4 y cinco de orden 2, mientras que $\mathcal{Q}_8$ tiene un único elemento de orden 2 y seis de orden 4. Por tanto, $\mathcal{D}_4$ y $\mathcal{Q}_8$ no son isomorfos. □

Ahora vamos a considerar el caso en el que p es un número primo impar. Esta clasificación se basa en una discusión más detallada que puede verse en [3]. Para ello, enunciamos primero un teorema sobre congruencias módulo p, debido a Fermat.

Teorema 7.12. Dado un número primo p, para cada $a \in p$ se verifica que

$$a^p \equiv a \mod p$$

Demostración. Dados $n, m \in \mathbb{Z} \setminus p\mathbb{Z}$, se verifica que

$$na \equiv ma \mod p \Leftrightarrow p | na - ma = (n - m)a$$

Si se cumple esta condición y $a \notin p\mathbb{Z}$, entonces $n \equiv m \mod p$.

Por tanto, $1a, 2a, \ldots, (p-1)a$ recorren todas las clases de equivalencia desde 1 hasta $p - 1$. Entonces,

$$1 \cdots (p-1) \equiv (1a) \cdots (p-1)a \equiv 1 \cdots (p-1) \cdot a^{p-1} \mod p \Rightarrow a^{p-1} \equiv 1 \mod p$$

puesto que $1 \cdots (p-1)$ no es múltiplo de p. Entonces $a^p \equiv a$ para cada $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Por otro lado, si $a \in p\mathbb{Z}$, también se cumple que $a^p \equiv 0 \equiv a \mod p$. □

Proposición 7.13. Dado un número primo impar p, existen únicamente dos grupos no abelianos no isomorfos de orden p^3.

Demostración. En primer lugar, G no tiene ningún elemento de orden p^3, pues en tal caso sería cíclico y, por tanto, abeliano.

Supongamos que existe $a \in G$ de orden p^2. Del primer teorema de Sylow 5.9 se deduce que $H := \langle a \rangle$ es un subgrupo normal. Tomamos también $b \in G \backslash H$. Como $ord(G/H) = p$, la proposición 7.2 implica que es cíclico y que, además, está generado por cualquiera de sus elementos distinto del neutro, por lo que Hb genera G/H. Como H es un subgrupo normal, $b^{-1}ab \in H$, luego $\exists r \in \mathbb{Z}_{p^2}$ tal que $b^{-1}ab = a^r$. Podemos suponer que $r \not\equiv 1 \mod p^2$, pues en caso contrario G sería abeliano porque a y b generan G.

Como $b^p \in H$, conmuta con a, luego $a = b^{-p}ab^p = a^{r^p}$. Por tanto, $r^p \equiv 1 \mod p^2$. Por el teorema 7.12, $r \equiv 1 \mod p$, por lo que escribimos $r = 1 + sp$, donde, como $r \not\equiv 1 \mod p^2$, $s \notin p\mathbb{Z}$. Por tanto, existe $j \in \mathbb{Z}$ tal que $js \equiv 1 \mod p$. Definiendo $c := b^j$,

$$c^{-1}ac = b^{-j}ab^j = a^{(1+sp)^j} = a^{1+jsp} = a^{1+p}$$

Como $j \notin p\mathbb{Z}$, Hc también genera el grupo G/H, luego a y c generan G. Como $c^p \in H$, existe $t \in \mathbb{Z}$ tal que $c^p = a^t$. Además, t ha de ser un múltiplo de p, pues en caso contrario, por el lema 6.2, el orden de c sería p^3 y, consecuentemente, G sería cíclico y, por tanto, abeliano. Entonces, podemos escribir $c^p = a^{up}$. Entonces, utilizando las reglas de conmutación de a y c,

$$\left(ca^{-u}\right)^p = c^p a^{-u(1+(1+p)+(1+p)^2+\cdots(1+p)^{p-1})} = c^p a^{-u(1+(1+p)+(1+2p)+\ldots(1+(p-1)p))} =$$
$$c^p a^{-up-up(1+\cdots+(p-1))} = c^p a^{-up} a^{-up^2(p-1)/2} = c^p a^{-up} = 1_G$$

donde se ha utilizado que $\frac{p^2(p-1)}{2}$ es múltiplo de p^2 por ser p un número impar.

Si definimos $d := ca^{-u}$, a y d siguen generando el grupo y se tiene $d^p = 1_G$ y que

$$d^{-1}ad = a^u c^{-1} aca^{-u} = a^u a^{1+p} a^{-u} = a^{1+p}$$

Entonces, $G_4^{(p^3)}$ viene dado por la presentación:

$$G_4^{(p^3)} \cong \langle a, d | a^{p^2} = 1_G, d^p = 1_G, d^{-1}ad = a^{1+p} \rangle$$

Según la demostración de la proposición 4.6, $G_4^{(p^3)} \cong \mathbb{Z}_p \ltimes_\phi \mathbb{Z}_{p^2}$, donde $\phi : \mathbb{Z}_p \to Aut(\mathbb{Z}_{p^2})$ es el único automorfismo que verifica que $\phi\left(1 + p\mathbb{Z}\right)\left(1 + p^2\mathbb{Z}\right) = 1 + p + p^2\mathbb{Z}$.

Por último, si G no tiene elementos de orden p^2, entonces todos los elementos del grupo tienen orden p. Por el lema 7.4, $\mathcal{Z}(G) \neq 1_G$ y, por el lema 7.5, $ord(\mathcal{Z}(G)) = p$ por ser G no abeliano. Entonces, $G/\mathcal{Z}(G)$ tiene orden p^2 y, por el mismo lema 7.5, $G/\mathcal{Z}(G)$ no es cíclico, luego $G/\mathcal{Z}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Sean entonces $a, b \in G$ tales que $\mathcal{Z}(G)a$ y $\mathcal{Z}(G)b$ generan $G/\mathcal{Z}(G)$. Como $G/\mathcal{Z}(G)$ es abeliano, $c := a^{-1}b^{-1}ab \in \mathcal{Z}(G)$. Además, $c \neq 1_G$, pues en caso contrario, a y b conmutarían y, como a, b y $\mathcal{Z}(G)$ generan G, este sería abeliano. Entonces, $\mathcal{Z}(G) = \langle c \rangle$ y G viene dado por la presentación

$$G_5^{(p^3)} \cong \langle a, b, c | a^p = b^p = c^p = 1_G, ab = bac, ac = ca, bc = cb \rangle$$

Efectivamente, $G_5^{(p^3)}$ contiene únicamente elementos de orden p, puesto que todo elemento puede escribirse como $c^i a^j b^k$ para ciertos números enteros i, j y k, de modo que:

$$\left(c^i a^j b^k\right)^p = c^{ip} a^{pj} b^{pk} c^{jk(1+2+\cdots+(p-1))} = c^{jkp(p-1)/2} = 1_G$$

puesto que p es un número impar. Entonces, como $G_4^{(p^3)}$ sí tiene un elemento de orden p^2, se verifica que $G_4^{(p^3)} \ncong G_5^{(p^3)}$.

También es posible expresar este último grupo en forma de producto semidirecto de la siguiente forma: $G_5^{(p^3)} \cong \mathbb{Z}_p \ltimes_\phi (\mathbb{Z}_p \times \mathbb{Z}_p)$, donde el homomorfismo $\phi : \mathbb{Z}_p \to Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$ es el único que verifica que $\phi(l + p\mathbb{Z})(m + p\mathbb{Z}, n + p\mathbb{Z}) = (m + p\mathbb{Z}, lm + n + p\mathbb{Z}) \, \forall l, m, n \in \mathbb{Z}_p$. □

7.4. Grupos de orden pq

Proposición 7.14. Dados dos números primos $p < q$, todo grupo G de orden pq tiene un único subgrupo normal de orden q.

Demostración. Por el tercer teorema de Sylow 5.13, $n_q | p$ y $n_q \equiv 1 \mod q$. Así, como $p < q$, la única opción es que $n_q = 1$, por lo que existe un único subgrupo de Sylow de orden q que, por el teorema 5.11, es un subgrupo normal. □

Sean H y K subgrupos de Sylow de órdenes p y q, de manera que, por la proposición 7.14, $K \triangleleft G$. Por el corolario 3.9, $H \cap K = \{1_G\}$, de modo que por la proposición 3.4, $|HK| = ord(H)ord(K) = pq = ord(G)$, luego $HK = G$. Entonces, nos encontramos en las hipótesis de la proposición 4.6, de modo que $G \cong H \ltimes_\phi K$ para algún homomorfismo $\phi : H \to Aut(K)$.

Como $ord(K) = q$, la proposición 7.2 implica que $K \cong \mathbb{Z}_q$, luego existe $a \in K$ tal que $K = \langle a \rangle$. Entonces, todo $\phi \in Aut(K)$ queda determinado por $\phi(a)$. Además existe $m \in \mathbb{Z}_q$ tal que $\phi_m(a) = a^m$. Por otro lado, ϕ_m es biyectiva si y sólo si m no es múltiplo de q. Estos automorfismos verifican la relación $\phi_{m_1} \cdot \phi_{m_2} = \phi_{m_1 m_2}$. De este modo, $Aut(K)$ es isomorfo a $\mathbb{Z}_q^*$, grupo formado por las distintas clases de congruencia módulo q con la operación multiplicativa. Queremos ver ahora que $\mathbb{Z}_q^*$ es cíclico y, para ello, necesitamos desarrollar una teoría sobre las raices de polinomios en $\mathbb{Z}_p[x]$, la cual está basada en [4].

Definición 7.15. Dados dos polinomios $f(x)$ y $g(x)$, se dice que $f(x)$ es divisible por $g(x)$ módulo q si existe otro polinomio $h(x)$ tal que

$$f(x) \equiv g(x)h(x) \mod q$$

donde esta equivalencia se entiende como una equivalencia en cada uno de los coeficientes.

Lema 7.16. Una clase $a \in \mathbb{Z}_q$ es una raíz de $f(x)$, es decir, $f(a) \equiv 0 \mod q$, si y sólo si

$$(x - a) | f(x) \mod q$$

Demostración. Si $(x-a)|f(x) \mod q$, entonces existe un polinomio $h(x)$ tal que $f(x) \equiv (x-a)h(x)$ mód q, de modo que

$$f(a) \equiv (a - a)h(a) \equiv 0 \mod q$$

Recíprocamente, si $f(a) \equiv 0 \mod q$, entonces $f(x) \equiv f(x) - f(a) \mod q$. Pero si

$$f(x) = \sum_{r=0}^{deg(f)} c_r x^r \equiv f(x) - f(a) = \sum_{r=0}^{deg(f)} c_r (x^r - a^r) = (x - a) \sum_{r=0}^{deg(f)} c_r \left(\sum_{i=0}^{r-1} x^i a^{r-1-i} \right) \mod q$$

de modo que $(x - a)|f(x) \mod q$. □

Lema 7.17. Dado un número primo p y un polinomio $f(x)$, el número de raíces distintas de f, módulo p, es menor o igual que el grado de f.

Demostración. Sean $a_1, \ldots, a_d$ las raíces distintas de f. El lema 7.16 implica que $(x - a_1)|f(x)$, luego existe un polinomio $h_1(x)$ tal que $f(x) = (x - a_1)h_1(x)$.

Como $a_2 \neq a_1$ es raíz de f, se tiene que $h_1(a_2) \equiv 0$, de modo que, nuevamente por el lema 7.16, $(x - a_2)|h_1(x)$, lo que implica que $(x - a_1)(x - a_2)|f(x)$. Repitiendo este argumento con todas las raices, se llega a que

$$(x - a_1) \cdots (x - a_d)|f(x)$$

de modo que el número de raíces, y grado del polinomio $(x - a_1) \cdots (x - a_d)$, es menor o igual que el grado de f. □

Lema 7.18. Dado un número primo p y un divisor d de $p - 1$, existen exactamente d elementos en $\mathbb{Z}_p^*$ cuyo orden divide a d.

Demostración. Se verifica que

$$x^{p-1} - 1 = (x^d - 1)\left(x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1\right) = (x^d - 1)g(x)$$

Como el orden de todo elemento de $\mathbb{Z}_p^*$ divide a $p - 1$, $x^{p-1} - 1$ tiene $p - 1$ raíces, que son raíces bien de $x^d - 1$ o bien de $g(x)$. Como el número de raíces de un polinomio no puede ser superior a su grado por el lema 7.17, exactamente d corresponden a $x^d - 1$ y $p - 1 - d$ a $g(x)$.

Por tanto, las d raíces de $x^d - 1$ son los d elementos cuyo orden divide a d.

□

Proposición 7.19. El grupo $\mathbb{Z}_p^*$ es cíclico.

Demostración. Sea $p - 1 = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$ la descomposición en factores primos de $p - 1$. Para cada $i \in \{1, \ldots, s\}$, por el lema 7.18, hay $q_i^{\alpha_i}$ elementos cuyo orden divide a $q_i^{\alpha_i}$, pero tan solo hay $q_i^{\alpha_i - 1}$ elementos cuyo orden divide a $q_i^{\alpha_i - 1}$, de modo que existe un elemento $x_i \in \mathbb{Z}_p^*$ tal que $o(x_i) = q_i^{\alpha_i}$.

Vamos a probar por inducción que $o(x_1 \cdots x_r) = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$ para todo $r \leq s$. Para $r = 1$, es claro por la definición de x_i. Supongamos que se cumple para $r - 1$. Como $\mathbb{Z}_p^*$ es abeliano y, por la hipótesis de inducción, los órdenes de $x_1 \cdots x_{r-1}$ y x_r son primos entre sí, de modo que el lema 6.3 implica que

$$o\left(x_1 \cdots x_r\right) = o\left(x_1 \cdots x_{r-1}\right) o\left(x_r\right) = q_1^{\alpha_1} \cdots q_{r-1}^{\alpha_{r-1}} q_r^{\alpha_r}$$

Particularizando para $r = s$, existe $y := x_1 \cdots x_s$ tal que

$$o(y) = q_1^{\alpha_1} \cdots q_s^{\alpha_s} = p - 1 = ord\left(\mathbb{Z}_p^*\right)$$

□

En este punto, estamos en disposición de clasificar los grupos de orden pq.

Proposición 7.20. Dados dos números primos $p < q$ tales que $p \not| q - 1$, todo grupo G de orden pq es cíclico.

Demostración. Por la proposición 7.14, se verifica que $n_q(G) = 1$. Por otro lado, por el tercer teorema de Sylow 5.13, $n_p(G) \in \{1, q\}$ y además $n_p(G) \equiv 1 \mod p$. Pero como $p \not| q - 1$, entonces $n_p(G) = 1$.

Así, existen subgrupos normales H y K de órdenes p y q respectivamente. Entonces, el corolario 3.9 implica que $ord(H \cap K) = \{1_G\}$, luego, por la proposición 3.4, $|HK| = pq = ord(G)$. Entonces $G = HK$, luego el corolario 4.7 implica que $G \cong H \times K$. Así, si $a \in H$ y $b \in K$ son generadores de sus respectivos grupos, el elemento de G identificado con $(a, b) \in H \times K$ tiene orden pq, de modo que G es cíclico. □

Proposición 7.21. Dados dos números primos $p < q$ tales que $p|(q-1)$, existen dos grupos no isomorfos de orden pq. Uno de ellos es cíclico y el otro, no abeliano.

Demostración. Dado un grupo G de orden pq, sean H y K subgrupos de Sylow de órdenes p y q. Hemos visto que estamos en las condiciones de la proposición 4.6, de modo que $G \cong H \ltimes_\phi K$ para algún $\phi : H \to Aut(K)$. Como H y K son cíclicos por la proposición 7.2, el homomorfismo ϕ queda determinado por $\phi(h)(k)$, para ciertos generadores h y k de H y K, respectivamente. Denotamos entonces por ϕ_m el homomorfismo que verifica que $\phi_m(h)(k) = k^m$. Según la proposición 7.19, el grupo $Aut(K) \cong \mathbb{Z}_q^*$ es cíclico, luego está generado por algún ϕ_u.

Como el orden de $\phi(h)$ es divisor de p (por ser la imagen de h por ϕ) y ϕ_u tiene orden $q-1$, entonces $\phi(h) = (\phi_u(h))^{nl}$, donde $l := \frac{q-1}{p} \in \mathbb{Z}$ y $n \in \{0, \dots, p-1\}$.

Si $n = 0$, ϕ es el homomorfismo nulo y el producto semidirecto es, en realidad, el producto directo. De este modo,

$$G_1^{(pq)} \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$$

Por otro lado, dados ϕ_{lu} y ϕ_{nlu}, para algún $n \in \{1, \dots, p-1\}$, entonces se considera el automorfismo de H dado por

$$\theta_n : H \to H,\ x \mapsto x^n$$

que verifica que $\phi_{lu} \circ \theta_n = \phi_{nlu}$. Entonces, por la proposición 4.8, $H \ltimes_{\phi_{lu}} K \cong H \ltimes_{\phi_{nlu}} K$ para todo $n \in \{1, \dots, p-1\}$. Entonces, todos los productos semidirectos no abelianos son isomorfos a

$$G_2^{(pq)} \cong \mathbb{Z}_p \ltimes_\phi \mathbb{Z}_q$$

donde $\phi(h)(k) = k^u$, para algún generador h de $\mathbb{Z}_p$, algún generador u de $\mathbb{Z}_q^*$ y para cada $k \in \mathbb{Z}_q$. □

Observación 7.22. En el caso en el que $ord(G) = 2p$, siendo p un número primo impar, la proposición 7.21 establece que existen dos grupos no isomorfos de tal orden: uno de ellos sería el grupo cíclico $\mathbb{Z}_{2p}$ y el otro, no abeliano, sería el p-ésimo grupo diedral $\mathcal{D}_p$.

7.5. Grupos de orden $4p$

El objetivo de esta sección es realizar una clasificación de los grupos de orden $4p$, donde p es un número primo tal que $p \geq 5$. Distinguiremos dos casos: bien $p \equiv 1 \mod 4$, o bien $p \equiv 3 \mod 4$.

El tercer teorema de Sylow 5.13 implica que $n_p|4 \Rightarrow n_p \in \{1, 2, 4\}$ y que $n_p \equiv 1 \mod p$. Como $p \geq 5$, la única posibilidad es que $n_p = 1$. Por tanto, todo grupo G de orden $4p$, con $p \geq 5$, contiene un subgrupo de Sylow K normal de orden p.

Por otro lado, el primer teorema de Sylow 5.9 implica que existe un 2-grupo de Sylow H, cuyo orden es 4. Por el corolario 3.9, $H \cap K = \{1_G\}$ y por la proposición 3.4, $|HK| = 4p = ord(G)$. De este modo, la proposición 4.6 implica que $G \cong H \ltimes_\phi K$ para algún homomorfismo $\phi : H \to Aut(K)$.

Buscamos ahora los grupos G de orden $4p$, donde $p \geq 5$ y $p \equiv 1 \mod 4$. Hemos visto que $G \cong H \ltimes_\phi K$, donde H es un subgrupo de Sylow de orden 4, K es el único subgrupo de orden p y ϕ es un homomorfismo $\phi : H \to Aut(K)$.

- Si $H \cong \mathbb{Z}_4$, sea h un generador de este. Entonces $\phi(h)$, que determina por completo a ϕ, ha de tener orden divisor de 4. Como, por la proposición 7.19, $\mathbb{Z}_p^*$ es cíclico, sea $\phi_u \in Aut(K) \cong \mathbb{Z}_p^*$ un generador del grupo. De este modo, como $4|(p-1) = ord\left(\mathbb{Z}_p^*\right)$, los elementos de $Aut(K)$ cuyo orden divide a 4 son los pertenecientes al subgrupo generado por $\alpha := \phi_u^{(p-1)/4}$, es decir, α, $\alpha^2 = \phi_{-1}$, α^3 y $\alpha^4 = Id_K$.

  Si $\phi(h) = Id_K$, ϕ es el homomorfismo nulo y $H \ltimes_\phi K = H \times K$. De este modo, el primer grupo de orden $4p$ obtenido es

  $$G_1^{(4p)} \cong \mathbb{Z}_4 \times \mathbb{Z}_p \cong \mathbb{Z}_{4p}$$

Por otro lado, si $\phi_2(h) = \alpha^2 = \phi_{-1}$, según la identificación de $Aut(K)$ con $Aut(\mathbb{Z}_p)$, tenemos un segundo grupo

$$G_2^{(4p)} \cong \mathbb{Z}_4 \ltimes_{\phi_2} \mathbb{Z}_p$$

donde $\phi_2(h)(x) = x^{-1}$, para cualquier generador h de $\mathbb{Z}_4$ y para cualquier $x \in \mathbb{Z}_p$. Este grupo es conocido como grupo dicíclico, y se denota por Dic_p.

Por último, si ϕ_1 y ϕ_3 son los homomorfismos que verifican que $\phi_1(h) = \alpha$ y $\phi_3(h) = \alpha^3$ y consideramos $\theta \in Aut(H)$ dado por $\theta(x) = x^3\ \forall x \in H$, se verifica que

$$\phi_3(h) = \alpha^3 = (\phi_1(h))^3 = \phi_1(h^3) = (\phi_1 \circ \theta)(h) \Rightarrow \phi_3 = \phi_1 \circ \theta$$

por ser h un generador de H. Entonces, la propsición 4.8 implica que

$$H \ltimes_{\phi_1} K \cong H \ltimes_{\phi_3} K$$

Por tanto, únicamente hay que considerar un grupo más:

$$G_3^{(4p)} = \mathbb{Z}_4 \ltimes_{\phi} \mathbb{Z}_p$$

donde, en este caso, ϕ es el homomorfismo que manda un generador de H a un automorfismo de orden 4 en $Aut(\mathbb{Z}_p)$, que ya hemos visto que existe.

Además, el corolario 4.11 implica que $\mathcal{Z}\left(G_1^{(4p)}\right) = G_1^{(4p)}$, $\mathcal{Z}\left(G_2^{(4p)}\right) \cong \mathbb{Z}_2 \times \{0\}$ y $\mathcal{Z}\left(G_3^{(4p)}\right) = \{1_G\}$, de manera que dos cualesquiera de ellos no son isomorfos.

- Si, por el contrario, $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces $\phi : H \to Aut(K)$ no puede ser inyectivo puesto que, en tal caso, H sería isomorfo a un subgrupo de $Aut(K)$, lo cual es imposible por ser $Aut(K)$ cíclico y H no. Entonces, $ord(\ker\phi)$ vale 2 ó 4.

  En el segundo caso, ϕ es el homomorfismo nulo, luego el producto semidirecto es, en realidad, un producto directo. De este modo,

  $$G_4^{(4p)} \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_p = \mathbb{Z}_{2p} \times \mathbb{Z}_2$$

  Por otro lado, sean $\phi_1, \phi_2 : H \to Aut(K)$ tales que $ord(\ker\phi_1) = ord(\ker\phi_2) = 2$. Escribimos $\ker\phi_1 = \{1, a_1\}$ y $\ker\phi_2 = \{1, a_2\}$ y sean $b_1 \in H \setminus \ker\phi_1$ y $b_2 \in H \setminus \ker\phi_2$. Por otro lado, todo elemento en $\operatorname{Im}\phi_i$ ha de tener orden 1 ó 2, luego $\operatorname{Im}\phi_i \subset \{Id_K, \psi\}$, donde ψ es el único elemento de orden 2 en $Aut(K)$.

  Entonces, si consideramos el automorfismo $\theta \in Aut(H)$ tal que $\theta(a_1) = a_2$ y $\theta(b_1) = b_2$, se verifica que $\phi_1 = \phi_2 \circ \theta$, luego la proposición 4.8 implica que

  $$H \ltimes_{\phi_1} K \cong H \ltimes_{\phi_2} K$$

  De este modo, únicamente hay un grupo más de orden $4p$, que es

  $$G_5^{(4p)} = (\mathbb{Z}_2 \times \mathbb{Z}_2) \ltimes_{\phi} \mathbb{Z}_p$$

  donde $\phi(l + 2\mathbb{Z}, m + 2\mathbb{Z})(n + p\mathbb{Z}) = (-1)^m n + p\mathbb{Z}\ \forall l, m \in \mathbb{Z}_2,\ \forall n \in \mathbb{Z}_p$. Este grupo es, precisamente, el grupo diedral $\mathcal{D}_{2p}$.

  En esta situación, $G_4^{(4p)}$ es abeliano, mientras que $G_5^{(4p)}$ no lo es, luego no son isomorfos.

Por otro lado si $p \equiv 3 \mod 4$, el orden $ord\left(\mathbb{Z}_p^*\right) = p - 1$ no es múltiplo de 4. De este modo, el corolario 3.11 implica que no hay ningún elemento de orden 4 en $Aut(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$. Como por la proposición 7.19, $\mathbb{Z}_p^*$ es cíclico, únicamente hay dos elementos cuyo orden divide a 2: ϕ_1 y ϕ_{-1}. El razonamiento realizado cuando $p \equiv 1 \mod 4$ se puede realizar en este caso, siendo los únicos grupos que aparecen, en este caso, $G_1^{(4p)}$, $G_2^{(4p)}$, $G_4^{(4p)}$ y $G_5^{(4p)}$.

8. Grupos de órdenes menores que 32

El objetivo de esta sección es realizar una clasificación, salvo isomorfía, de todos los grupos de orden menor o igual que 31. Según se ha visto anteriormente, todo grupo de orden 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 y 31 es cíclico por ser números primos (proposición 7.2).

Para órdenes 4, 9 y 25, se ha visto en el corolario 7.7 que existen dos grupos abelianos no isomorfos, mientras que para órdenes 8 y 27, las proposiciones 7.11 y 7.13 implican la existencia de tres grupos abelianos y dos no abelianos.

Por otro lado, para órdenes 6, 10, 14, 21, 22 y 26, la 7.21 implica que, salvo isomorfía, existen dos grupos: el grupo cíclico y otro grupo no abeliano, mientras que la proposición 7.20 implica que todo grupo de orden 15 es cíclico.

Por último, los órdenes 20 y 28 son de la forma $4p$, donde $p \geq 5$. Como $p_1 = 5 \equiv 1 \mod 4$, existen cinco grupos de orden 20, salvo isomorfía, mientras que $p_2 = 7 \equiv 3 \mod 4$, luego tan solo hay 4 de orden 28.

De este modo, únicamente queda clasificar los grupos de órdenes 12, 16, 18, 24 y 30, lo cual se expone a continuación.

La razón por la cual se escoge el número 31 como el límite de esta clasificación es la complejidad de clasificar los grupos de orden 32, puesto que puede verse en [6] que existen 51 grupos de dicho orden salvo isomorfía.

8.1. Grupos de orden 12

En primer lugar, veamos una proposición que garantiza la existencia de, al menos, un subgrupo de Sylow normal.

Proposición 8.1. Dados dos números primos p y q y un grupo G de orden p^2q, G tiene un subgrupo normal de Sylow de orden p^2 o de orden q.

Demostración. Supongamos, por reducción al absurdo, que $n_p(G) > 1$ y que $n_q(G) > 1$. Entonces, por el tercer teorema de Sylow 5.13, $n_p = q \equiv 1 \mod p$. Entonces, se verifica que $q > p$. Por otro lado, el mismo teorema 5.13 implica que $n_q \equiv 1 \mod q$, de modo que, como hay más de un único q-subgrupo de Sylow, $n_q > q > 1$. Como $n_q | p^2$, la única opción es que $n_q = p^2$. Así, el número de elementos de orden q es $p^2(q-1) = ord(G) - p^2$.

Como los elementos de orden q no pertenecen a ningún subgrupo de orden p^2, por el corolario 3.11, la unión de todos los p-subgrupos de Sylow tiene, a lo sumo, p^2 elementos. Por tanto, únicamente existe un único subgrupo de orden p^2, es decir, $n_p(G) = 1$.

Esta contradicción implica que $n_p(G) = 1$ ó $n_q(G) = 1$. Luego G tiene un subgrupo normal de orden p^2 o un subgrupo normal de orden q. □

Dado un grupo G de orden p^2q, el primer teorema de Sylow 5.9 implica que existen subgrupos H y K de órdenes p^2 y q, respectivamente. Por el corolario 3.9, $H \cap K = \{1_G\}$ y, por la proposición 3.4, $|HK| = p^2q = ord(G)$. De este modo, $G = HK$. Además, la proposición 8.1 implica que bien H o bien K es un subgrupo normal.

Si K es un subgrupo normal, por la proposición 4.6, $G \cong H \ltimes_\phi K$, para algún homomorfismo $\phi : H \to Aut(K)$. Por otro lado, si H es normal, $G \cong K \ltimes_\phi H$ para algún otro homomorfismo $\phi : K \to Aut(H)$.

Por último, la proposición 7.2 implica que K es cíclico e isomorfo a $\mathbb{Z}_q$ y el corolario 7.7 implica que H es isomorfo a $\mathbb{Z}_{p^2}$ o a $\mathbb{Z}_p \times \mathbb{Z}_p$.

En el caso particular en el que $ord(G) = 12$, es decir, $p = 2$ y $q = 3$, supongamos primero que $n_3 = 1$, siendo K el único subgrupo de orden 3. Entonces, los 2-subgrupos de Sylow pueden ser isomorfos a $\mathbb{Z}_4$ o a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

- Primeramente, sea $H \cong \mathbb{Z}_4$ un subgrupo de Sylow, de modo que G es isomorfo a $H \ltimes_\phi K$, para algún $\phi : H \to Aut(K)$. Dados h y k generadores de H y K, respectivamente, tenemos dos homomorfismos distintos que verifican que $\phi_1(h)(k) = k$ y que $\phi_2(h)(k) = k^2$.

  En el primer caso, $G_1^{(12)}$ es un producto directo, es decir,

  $$G_1^{(12)} \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$$

  En el segundo caso, el grupo $G_2^{(12)}$ resulta ser:

  $$G_2^{(12)} \cong \mathbb{Z}_4 \ltimes_\phi \mathbb{Z}_3$$

  donde $\phi(h)(k) = k^2$ para cualesquiera generadores h y k de $\mathbb{Z}_4$ y $\mathbb{Z}_3$. Este grupo se conoce como el *grupo dicíclico* de orden 12, y se denota por Dic_3.

  Según se ha visto en la demostración de la proposición 4.6, $\phi(h) = h^{-1}kh = k^2 \neq k$, de modo que $G_2^{(12)}$ no es abeliano, luego no es isomorfo a $G_1^{(12)}$.

- En segundo lugar, supongamos que $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Dado un homomorfismo $\phi : H \to Aut(K)$, el primer teorema de isomorfía 2.5 implica que $H/\ker\phi \cong \operatorname{Im}\phi \subset Aut(K) \cong \mathbb{Z}_2$.

  Entonces, bien $\ker\phi = H$, de modo que $H \ltimes_\phi K = H \times K$ y tendríamos un tercer grupo de orden 12 dado por

  $$G_3^{(12)} = (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \times \mathbb{Z}_2$$

  que, por el teorema 6.6, es, salvo isomorfía, el único grupo abeliano de orden 12 junto a $G_1^{(12)}$.

  Por otro lado, también es posible que $[H : \ker\phi] = 2$, de modo que por el corolario 3.8, $ord(\ker\phi) = 2$, es decir, $\ker\phi = \{1_H, a\}$ para algún $a \in H$.

  Dados dos homomorfismos no nulos $\phi_1, \phi_2 : H \to Aut(K)$, sus núcleos se pueden escribir como $\ker\phi_1 = \{1_H, a_1\}$ y $\ker\phi_2 = \{1_H, a_2\}$. Sean también $b_1 \in H \setminus \ker\phi_1$ y $b_2 \in H \setminus \ker\phi_2$. Si se considera el homomorfismo $\theta : H \to H$ que verifica que $\theta(a_1) = a_2$ y que $\theta(b_1) = b_2$, verifica que $\phi_1 = \phi_2 \circ \theta$, luego la proposición 4.8 implica que $H \ltimes_{\phi_1} K \cong H \ltimes_{\phi_2} K$. Así, únicamente tenemos un nuevo grupo

  $$G_4^{(12)} = (\mathbb{Z}_2 \times \mathbb{Z}_2) \ltimes_\phi \mathbb{Z}_3$$

  donde $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to Aut(\mathbb{Z}_3) :\ (m + 2\mathbb{Z}, n + 2\mathbb{Z}) \mapsto \psi^m$, donde ψ es el único automorfismo de $\mathbb{Z}_3$ distinto de la identidad. Este grupo es, precisamente, el grupo diedral $\mathcal{D}_6$.

Ahora, consideremos el caso en el que $n_2(G) = 1$, de manera que existe un único 2-subgrupo de Sylow normal.

- Supongamos que G tiene un subgrupo normal cíclico de orden 4, denotado por H. Entonces, por la proposición 4.6, $G \cong K \ltimes_\phi H$, donde K es un subgrupo de Sylow de orden 3 y $\phi : K \to Aut(H)$ es un homomorfismo. Así, $Aut(H)$ tiene dos elementos (dados por $\theta_1(x) = x$ y $\theta_2(x) = x^{-1}\ \forall x \in H$), de órdenes 1 y 2, respectivamente. Como, dado un generador k de K, el orden de $\phi(k)$ ha de dividir a tres por ser la imagen de k por ϕ, se tiene que $\phi(k) = \theta_1 = Id_K$. Por tanto, ϕ es el homomorfismo nulo y el producto semidirecto coincide con el producto directo, es decir, $G \cong G_1^{(12)}$.

- Por último, sea $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ un subgrupo de Sylow normal, de modo que $G \cong K \ltimes_\phi H$ para algún $\phi : K \to Aut(H)$. Sean $a, b \in H$ tales que $H = \langle a, b \rangle$ y sea k un generador de K. Denotamos $\alpha := \phi(k)$, cuyo orden ha de dividir a 3. Si $\alpha = Id_H$, entonces $G \cong K \times H \cong G_3^{(12)}$. Por tanto, supondremos que el orden de α es 3.

  Si $\alpha(a) = a$, entonces $\alpha(b) = ab$, pues en caso contrario α sería la identidad. Entonces $\alpha(ab) = b$, de modo que $\alpha^2 = Id_H$, lo que contradice el hecho de que α tenga orden 3. De esta manera, α no tiene puntos fijos.

  Sean, por tanto, $\phi_1, \phi_2 : K \to Aut(H)$ dos homomorfismos no nulos distintos. Denotando por $\alpha_1 = \phi(k)$ y por $\alpha_2 = \phi_2(k)$, podemos suponer que $\alpha_1(a) = b$ y $\alpha_2(a) = ab$. Entonces, como los automorfismos α_i no tienen puntos fijos,

  $$\alpha_1(b) = ab, \quad \alpha_1(ab) = a, \quad \alpha_2(b) = a, \quad \alpha_2(ab) = b.$$

  es decir, se verifica que $\alpha_1 = \alpha_2^2$.

  Considérese $\theta \in Aut(K)$ tal que $\theta(k) = k^2$. Se cumple que

  $$\phi_1(k) = \alpha_1 = \alpha_2^2 = (\phi_2(k))^2 = \phi_2(k^2) = (\phi_2 \circ \theta)(k) \Rightarrow \phi_1 = \phi_2 \circ \theta$$

  Entonces, la proposición 4.8 implica que $K \ltimes_{\phi_1} H \cong K \ltimes_{\phi_2} H$.

  Por tanto, existe un quinto y último grupo de orden 12 dado por

  $$G_5^{(12)} = \mathbb{Z}_3 \ltimes_\phi (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

  donde $\phi : \mathbb{Z}_3 \to Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ es el homomorfirmo que verifica que $\phi(1+3\mathbb{Z})(a+2\mathbb{Z}, b+2\mathbb{Z}) = (b+2\mathbb{Z}, a+b+2\mathbb{Z})\ \forall a, b \in \mathbb{Z}_2$.

  Este grupo, comúnmente conocido como el *grupo alternado* $\mathcal{A}_4$, no es isomorfo a ninguno de los anteriores puesto que no contiene ningún subgrupo normal de orden 3.

8.2. Grupos de orden 16

La clasificación de los grupos de orden 16 la vamos a realizar, de manera análoga a la clasificación que aparece en [1], mediante el orden de $\mathcal{Z}(G)$. Como $\mathcal{Z}(G)$ es un subgrupo de G, el corolario 3.8 implica que su orden ha de ser un divisor de 16. Por el lema 7.4, $ord(\mathcal{Z}(G)) > 1$. Además, si $ord(\mathcal{Z}(G)) = 8$, entonces $G/\mathcal{Z}(G)$ sería cíclico por la proposición 7.2, deduciéndose del lema 7.5 que G sería abeliano y, por tanto, $\mathcal{Z}(G) = G$. De este modo, las únicas opciones que quedan son que $ord(\mathcal{Z}(G))$ valga 16, 4 ó 2.

8.2.1. $\boxed{ord(\mathcal{Z}(G)) = 16}$

Según el teorema 6.6, existen cinco grupos abelianos de orden 16:

- $G_1^{(16)} \cong \mathbb{Z}_{16}$
- $G_2^{(16)} \cong \mathbb{Z}_8 \times \mathbb{Z}_2$
- $G_3^{(16)} \cong \mathbb{Z}_4 \times \mathbb{Z}_4$
- $G_4^{(16)} \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $G_5^{(16)} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

8.2.2. $\boxed{ord\,(\mathcal{Z}(G)) = 4}$

Si $ord\,(\mathcal{Z}(G)) = 4$, entonces $G/\mathcal{Z}(G)$ también tiene orden 4, de modo que sólo puede ser isomorfo a $\mathbb{Z}_4$ o a $\mathbb{Z}_2 \times \mathbb{Z}_2$. El primer caso no es posible puesto que, en tal caso, $G/\mathcal{Z}(G)$ sería cíclico y, por el lema 7.5, G sería abeliano.

Por tanto, $G/\mathcal{Z}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, que tiene tres subgrupos de orden 2. Por tanto, el teorema 2.8 implica que existen tres subgrupos, que denotaremos por H_1, H_2 y H_3, de orden 8 y que contienen a $\mathcal{Z}(G)$. Además, es claro que $\mathcal{Z}(G) \subset \mathcal{Z}(H_i)$, luego $\mathcal{Z}(H_i)$ tiene orden mayor o igual que 4. Si se diese la igualdad, $H_i/\mathcal{Z}(H_i)$ sería cíclico, por lo que el lema 7.5 implica que los grupos H_i son abelianos.

Por otro lado, cada subgrupo H_i está formado por dos clases laterales de $\mathcal{Z}(G)$. Entonces, cada subgrupo H_i cubre una clase de $G/\mathcal{Z}(G)$ distinta de la identidad. De este modo, $H_1 \cup H_2 \cup H_3 = G$.

Por otro lado, $\mathcal{Z}(G)$ es un subgrupo de orden 4, por lo que es isomorfo a $\mathbb{Z}_4$ o a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

- Si $\mathcal{Z}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, como $\mathbb{Z}_8$ no contiene subgrupos isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$, entonces los tres subgrupos H_1, H_2 y H_3 han de ser isomorfos a $\mathbb{Z}_4 \times \mathbb{Z}_2$ ó a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

  Como estamos buscando grupos no abelianos, si $H_1 \cong H_2 \cong H_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, todo elemento de G tendría orden 2, luego G sería abeliano en virtud del lema 7.9.

  Si se puede escribir $H_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ y $H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (reordenando índices si fuese necesario), entonces existe $h_2 \in H_2 \setminus H_1$ de orden 2. Denotando $K := \langle h_2 \rangle$, se tiene que $K \cap H_1 = \{1_G\}$ y de la proposición 3.4 se deduce que $KH_1 = G$. Como $H_1 \triangleleft G$ por el lema 7.10, la proposición 4.6 implica que $G \cong K \ltimes_\phi H_1$ para algún homomorfismo $\phi : K \to Aut(H_1)$.

  Sabemos que $\mathcal{Z}(G)$ es el subgrupo de H_1 isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Por el corolario 4.11, el subgrupo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ han de ser los puntos fijos de ϕ. Sean $a, b \in H_1$ elementos de órdenes 4 y 2 que generan H_1. Como b es un punto fijo, $\phi(h_2)(b) = b$. Entonces, ϕ queda determinada por $\phi(h_2)(a)$, que pertenece a $\{a, a^3, ab, a^3b\}$ por tener orden 4. Si $\phi(h_2)(a)$, ϕ es el homomorfismo nulo, dando lugar a un grupo abeliano.

  Si $\phi(a) = a^3$, entonces tenemos que considerar el grupo

  $$G_6^{(16)} = \mathbb{Z}_2 \ltimes_\phi (\mathbb{Z}_4 \times \mathbb{Z}_2)$$

  donde $\phi(1 + 2\mathbb{Z})(x) = x^{-1}\ \forall x \in \mathbb{Z}_4 \times \mathbb{Z}_2$.

  Por otro lado, consideremos los homomorfismos $\phi_1, \phi_2 : K \to Aut(H_1)$ que verifican que $\phi_1(h_2)(a) = ab$ y $\phi_2(a) = a^3b$. Entonces, sea $\theta \in Aut(H_1)$ tal que $\theta(a) = a$ y $\theta(b) = ba^2$. Entonces, puede verse que $\theta \circ \phi_1(h_2) = \phi_2(h_2) \circ \theta$, luego por la proposición 4.9, $K \ltimes_{\phi_1} H_1 \cong K \ltimes_{\phi_2} H_1$. Por tanto, únicamente hay que considerar un grupo.

  $$G_7^{(16)} = \mathbb{Z}_2 \ltimes_\phi (\mathbb{Z}_4 \times \mathbb{Z}_2)$$

  donde $\phi(1 + 2\mathbb{Z})(m + 4\mathbb{Z}, n + 2\mathbb{Z}) = (m + 4\mathbb{Z}, m + n + 2\mathbb{Z})\ \forall m \in \mathbb{Z}_4,\ \forall n \in \mathbb{Z}_2$.

  Puede observarse que $G_6^{(16)}$ tiene 11 elementos de orden 2 y 4 de orden 4, mientras que $G_7^{(16)}$ tiene 7 elementos de orden 2 y 8 de orden 4. Por tanto, $G_6^{(16)}$ y $G_7^{(16)}$ no son isomorfos.

  Si $H_1 \cong H_2 \cong H_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, tomamos $h_1 \in H_1 \setminus \mathcal{Z}(G)$ y $h_2 \in H_2 \setminus \mathcal{Z}(G)$ que, por tanto, tienen orden 4. Sea $h_3 := h_1h_2 \in G \setminus (H_1 \cup H_2) = H_3 \setminus \mathcal{Z}(G)$, por lo que también tiene orden 4. Como $G/\mathcal{Z}(G)$ es abeliano, $z := h_2^{-1}h_1^{-1}h_2h_1 \in \mathcal{Z}(G)$ y es distinto de 1_G puesto que, en caso contrario, al generar h_1, h_2 y $\mathcal{Z}(G)$ el grupo, G sería abeliano. Por otro lado, como todo elemento de $G/\mathcal{Z}(G)$ tiene orden 2, entonces $z_1 := h_1^2 \in \mathcal{Z}(G)$, $z_2 := h_2^2 \in \mathcal{Z}(G)$

y $z_3 := h_3^2 \in \mathcal{Z}(G)$ y, además, no son el elemento neutro porque h_1, h_2 y h_3 tienen orden 4. Además,

$$z_3 = h_3^2 = (h_1h_2)^2 = h_1h_2h_1h_2 = zh_1^2h_2^2 = zz_1z_2 \Rightarrow z = z_1z_2z_3$$

Entonces, por la estructura de $\mathcal{Z}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, como ninguno de los elementos z, z_1, z_2 y z_3 es el neutro, al menos dos de los elementos z_1, z_2 y z_3 son iguales.

En el caso en el que $z_1 = z_2 = z_3$, entonces $z = z_1^3 = z_1$, luego el conjunto

$$M = \{1_G, h_1, h_2, h_3, z, h_1^3, h_2^3, h_3^3\}$$

es un subgrupo isomorfo a $\mathcal{Q}_8$. Tomando $x \in \mathcal{Z}(G) \setminus \{1_G, z\}$ y denotando $K := \langle x \rangle$, se tiene que $M \cap K = \{1_G\}$. Entonces, por la proposición 3.4, $MK = G$. Además, $M \triangleleft G$ por el lema 7.10 y $K \triangleleft G$ porque $K \subset \mathcal{Z}(G)$. Entonces, del corolario 4.7 se deduce que $G \cong M \times K$, es decir,

$$G_8^{(16)} = \mathcal{Q}_8 \times \mathbb{Z}_2$$

Si $z_1 \neq z_2 = z_3$, entonces $z = z_1z_2z_3 = z_1$. Entonces, los subgrupos de orden 4, $M_1 = \langle h_1 \rangle = \{1_G, h_1, z_1, h_1z_1\}$ y $M_2 = \langle h_2 \rangle = \{1_G, h_2, z_2, h_2z_2\}$, verifican que $M_1 \cap M_2 = \{1_G\}$, luego, por la proposición 3.4, $M_1M_2 = G$. Además,

$$h_2^{-1}h_1h_2 = zh_1 = h_1^3 \in M_1 \Rightarrow h_2 \in N_G(M_1) \Rightarrow M_1\langle h_2 \rangle \subset N_G(M_1) \Rightarrow N_G(M_1) = G$$

Por tanto, $M_1 \triangleleft G$, luego se deduce de la proposición 4.6 que $G \cong M_2 \ltimes_\phi M_1$. En los casos en los que $z_1 = z_2 \neq z_3$ y $z_1 = z_3 \neq z_2$, se obtiene de manera análoga que $G \cong \mathbb{Z}_4 \ltimes_\phi \mathbb{Z}_4$. Como G no es abeliano, el producto semidirecto no puede ser el producto directo, luego la única opción es

$$G_9^{(16)} = \mathbb{Z}_4 \ltimes_\phi \mathbb{Z}_4$$

donde $\phi(1 + 4\mathbb{Z})(x) = x^{-1}$ $\forall x \in \mathbb{Z}_4$.

Tanto $G_8^{(16)}$ como $G_9^{(16)}$ tienen 3 elementos de orden 2 y 12 de orden 4, por lo que no son isomorfos ni a $G_6^{(16)}$ ni a $G_7^{(16)}$. No obstante, esto es algo que ya sabíamos puesto que, si esto ocurriese, los subgrupos de orden 8 conteniendo al centro de $\mathcal{Z}(G)$ serían isomorfos.

Además, $G_8^{(16)}$ y $G_9^{(16)}$ no son isomorfos porque $\{x^2 : x \in G_8^{(16)}\}$ consta de dos elementos y $\{x^2 : x \in G_9^{(16)}\}$ lo hace de 3.

- Si $\mathcal{Z}(G) \cong \mathbb{Z}_4$ entonces los subgrupos H_i no pueden ser isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, pues dicho grupo no tiene elementos de orden 4. Por tanto, los subgrupos H_i son isomorfos a $\mathbb{Z}_8$ ó a $\mathbb{Z}_4 \times \mathbb{Z}_2$.

  En el caso en el que los tres subgrupos H_1, H_2 y H_3 sean isomorfos a $\mathbb{Z}_8$, entonces tomamos $h_2 \in H_2 \setminus \mathcal{Z}(G)$ y $h_3 \in H_3 \setminus \mathcal{Z}(G)$, ambos de orden 8, tales que $z := h_2^2 = h_3^2 \in \mathcal{Z}(G)$. Entonces, $h_1 := h_2h_3 \in G \setminus (H_2 \cup H_3) = H_1 \setminus \mathcal{Z}(G)$, luego tiene orden 8.

  Como $G/\mathcal{Z}(G)$ es abeliano, entonces $z' = h_2^{-1}h_3^{-1}h_2h_3 \in \mathcal{Z}(G)$ y, además, como $h_3^2 \in \mathcal{Z}(G)$, se tiene que

$$h_2h_3^2 = z'h_3h_2h_3 = z'^2(h_3^2h_2) = z'^2(h_2h_3^2) \Rightarrow z'^2 = 1_G$$

  Si $z' = 1_G$, entonces h_2 y h_3 conmutarían y, como también generan el grupo, G sería abeliano.

  Por tanto, z' es el elemento de $\mathcal{Z}(G)$ de orden 2. De este modo,

$$h_1^2 = (h_2h_3)^2 = z'h_2^2h_3^2 = z'z^2$$

tiene orden 1 ó 2, lo que junto al lema 6.2 contradice el hecho de que $o(h_1) = 8$.

De este modo, alguno de los tres subgrupos, sin pérdida de generalidad, H_1, es isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$. Entonces, existe $h_1 \in H_1 \setminus \mathcal{Z}(G)$ de orden 2. Se denota $K := \langle h_1 \rangle$.

Suponemos primero que uno de los subgrupos H_i es isomorfo a $\mathbb{Z}_8$; sin pérdida de generalidad, H_3. Entonces, como $K \cap H_3 = \{1_G\}$, por la proposición 3.4, $|KH_3| = 16$, es decir, $KH_3 = G$. Como $H_3 \lhd G$ por el lema 7.10, la proposición 4.6 implica que $G \cong K \ltimes_\phi H_3$ para algún homomorfismo $\phi : K \to Aut(H_3)$.

El homomorfismo ϕ queda determinado por $\phi(h_1)$, el cual queda determinado por $\phi(h_1)(h_3)$, siendo h_3 un elemento de orden 8 de H_3. Además, como $\phi(h_1)(h_3)$ tiene que tener orden 8, se verifica que $\phi(h_1)(h_3) \in \{h_3, h_3^3, h_3^5, h_3^7\}$. Si $\phi(h_1)(h_3) = h_3$, ϕ es el homomorfismo nulo, luego $G \cong \mathbb{Z}_2 \times \mathbb{Z}_8$ sería abeliano.

Puede comprobarse que los otros tres $\phi(h_1)$ mencionados tienen orden 2, de modo que ϕ es un homomorfismo bien definido, luego determina un producto semidirecto. Sin embargo, si $\phi(h_1)(h_3) = h_3^3$ o $\phi(h_1)(h_3) = h_3^7$, entonces $Fix(\phi) = \{1_K, h_3^4\}$. Entonces, del corolario 4.11 se deduce que $ord(\mathcal{Z}(G)) = 2$, en contra de lo que se está suponiendo.

En cambio, si $\phi(h_1)(h_3) = h_3^5$, se tiene que $Fix(\phi) = \{1_K, h_3^2, h_3^4, h_3^6\}$, luego el corolario 4.11 implica que $\mathcal{Z}(G) \cong \mathbb{Z}_4$. Por tanto, tenemos un nuevo grupo en esta sección:

$$G_{10}^{(16)} = \mathbb{Z}_2 \ltimes_\phi \mathbb{Z}_8$$

donde $\phi(1 + 2\mathbb{Z})(x) = x^5 \ \forall x \in \mathbb{Z}_8$.

En cambio, si los tres subgrupos H_i son isomorfos a $\mathbb{Z}_4 \times \mathbb{Z}_2$, análogamente se cumple también que $G \cong K \ltimes_\phi H_3$, para algún homomorfismo $\phi : K \to Aut(H_3)$. Como sabemos que $\mathcal{Z}(G) \subset H_3$ y que $\mathcal{Z}(G) \cong \mathbb{Z}_4$, $Fix(\phi)$ es uno de los dos subgrupos de orden 4 de H_3. Entonces, sea $h_3 \in H_3 \setminus Fix(\phi)$ de orden 4. Como $\phi(h_1)(h_3) \neq h_3$ tiene orden 4 y no pertenece a $Fix(\phi)$, la única opción restante es que $\phi(h_1)(h_3) = h_3^{-1}$.

De este modo, $\phi(h_1)$, y por tanto ϕ, queda determinada por qué subgrupo es el subgrupo de puntos fijos. Sean M_1 y M_2 los dos subgrupos de orden 4 de H_3 y sean a_1 y a_2 respectivos generadores. Sean también $b_1 \in H_3 \setminus M_1$ y $b_2 \in H_3 \setminus M_2$, ambos de orden 4. Sean, por último, $\phi_1, \phi_2 : K \to Aut(H_3)$ los homomorfismos que tienen por subgrupos de puntos fijos a M_1 y a M_2, respectivamente. Considérese entonces el automorfismo $\theta : H_3 \to H_3$ que verifica que $\theta(a_1) = a_2$ y que $\theta(b_1) = b_2$. Entonces,

$$\theta \circ \phi_1(h_1)(a_1) = a_2 = \phi_2(h_1) \circ \theta(a_1), \quad \theta \circ \phi_1(b_1) = b_2^{-1} = \phi_2(h_1) \circ \theta(b_1)$$

De este modo, $\theta \circ \phi_1(h_1) = \phi_2(h_1) \circ \theta$. Por tanto, de la proposición 4.9 se deduce que $K \ltimes_{\phi_1} H_3 \cong K \ltimes_{\phi_2} H_3$. Por tanto, únicamente queda por considerar un nuevo grupo en esta sección:

$$G_{11}^{(16)} = \mathbb{Z}_2 \ltimes_\phi (\mathbb{Z}_4 \times \mathbb{Z}_2)$$

donde $\phi(1+2\mathbb{Z})(n+4\mathbb{Z}, m+2\mathbb{Z}) = (n+2m+4\mathbb{Z}, m+2\mathbb{Z}) \ \forall n \in \mathbb{Z}_4, \ \forall m \in \mathbb{Z}_2$. Puede comprobarse que $G_{11}^{(16)}$ no tiene elementos de orden 8, es decir, que no contiene ningún subgrupo isomorfo a $\mathbb{Z}_8$, de modo que no puede ser isomorfo a $G_{10}^{(16)}$.

8.2.3. $\boxed{ord\,(\mathcal{Z}(G)) = 2}$

En este caso, $G/\mathcal{Z}(G)$ tiene orden 8, de modo que es isomorfo a $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathcal{D}_4$ o $\mathcal{Q}_8$.

- Si $G/\mathcal{Z}(G) \cong \mathbb{Z}_8$, entonces, por el lema 7.5, G es abeliano. Por tanto, no hay que considerar nuevos grupos en este caso.

- Si $G/\mathcal{Z}(G) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, tiene dos subgrupos de orden 4 isomorfos a $\mathbb{Z}_4$, que contienen un único subgrupo de orden 2, y otro subgrupo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, que contiene tres subgrupos de orden 2. Por el teorema 2.8, existen dos subgrupos H_1 y H_2, de orden 8, que únicamente tienen un subgrupo de orden 4 conteniendo a $\mathcal{Z}(G)$ y otro subgrupo H_3, también de orden 8, que tiene tres subgrupos de orden 4 conteniendo a $\mathcal{Z}(G)$.

  Si $H_1 \cong \mathcal{D}_4$ ó $H_1 \cong \mathcal{Q}_8$, entonces, como $\mathcal{Z}(G) \subset \mathcal{Z}(H_1)$, se tiene la igualdad debido a que $\mathcal{Z}(G)$ y $\mathcal{Z}(H_1)$ tienen el mismo orden. Sin embargo, tanto $\mathcal{D}_4$ como $\mathcal{Q}_8$ tienen tres subgrupos de orden 4 que contienen al centro, lo que contradice lo mencionado anteriormente. Algo similar ocurre con H_2.

  En particular, H_1 y H_2 son abelianos. Entonces, como $H_1H_2 \subset G$, se tiene que $|HK| \leq 16$. Entonces, por la proposición 3.4, $ord(H_1 \cap H_2) \geq 4$, y se tienen las igualdades porque $H_1 \neq H_2$ y ambos tienen orden 8. Entonces, $G = H_1H_2$ y todo $x \in H_1 \cap H_2$ conmuta con todo elemento de H_1H_2 por ser estos abelianos, luego $H_1 \cap H_2 \subset \mathcal{Z}(G)$. En particular, $ord(\mathcal{Z}(G)) \geq 4$, en contradicción con lo que se está suponiendo.

- Si $G/\mathcal{Z}(G) \cong \mathcal{Q}_8$, ocurre algo similar. Como $\mathcal{Q}_8$ tiene tres subgrupos de orden 4, todos ellos isomorfos a $\mathbb{Z}_4$, que contienen al único subgrupo de orden 2, por el teorema 2.8 existen tres subgrupos H_1, H_2 y H_3 de G de orden 8, los cuales contienen a un único subgrupo de orden 4 conteniendo a $\mathcal{Z}(G)$. Por lo comentado en el caso anterior, H_1, H_2 y H_3 son abelianos y, por tanto, $ord(\mathcal{Z}(G)) \geq 4$, lo que supone una contradicción.

- Si $G/\mathcal{Z}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces todo elemento $x \in G$ verifica que $x^2 \in \mathcal{Z}(G)$. Como G no es abeliano, el lema 7.9 implica que existe un elemento $g \in G \setminus \{1_G\}$ cuyo orden no es 2. Entonces, $z := g^2$ es el elemento de $\mathcal{Z}(G)$ distinto del neutro.

  Por el teorema 2.8, como cada subgrupo de orden 2 de $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ está contenido en tres subgrupos de orden 4, existen tres subgrupos de orden 8, denotados por H_1, H_2 y H_3, que contienen a $\langle g \rangle$.

  Por la proposición 3.4, el producto de dos subgrupos H_i y H_j es G, de modo que si dos de ellos fuesen abelianos, $\langle g \rangle = H_i \cap H_j \subset \mathcal{Z}(G)$, lo que contradice que $ord(\mathcal{Z}(G)) = 2$.

  Supongamos entonces, sin pérdida de generalidad, que H_2 y H_3 son no abelianos. Tomemos $h_2 \in H_2 \setminus \langle g \rangle$ y $h_3 \in H_3 \setminus \langle g \rangle$. Si h_2 y g conmutaran, entonces H_2 sería abeliano y, como $G/\mathcal{Z}(G)$ es abeliano, $h_2^{-1}g^{-1}h_2g \in \mathcal{Z}(G)$, luego ha de ser z, de modo que $h_2g = zgh_2$. Análogamente, $h_3g = zgh_3$.

  De este modo, $h_2h_3 \in G \setminus (H_2 \cup H_3) = H_1 \setminus \langle g \rangle$ y verifica que:

  $$(h_2h_3)g = h_2zgh_3 = z^2g(h_2h_3) = g(h_2h_3)$$

  de modo que H_1 es abeliano.

  Tomamos $h_1 \in H_1 \setminus \langle g \rangle$. Si h_1 y h_2 no conmutan, entonces $h_1h_2 = zh_2h_1$ (por ser $G/\mathcal{Z}(G)$ abeliano) y, en tal caso, $(gh_1)h_2 = h_2(gh_1)$. Tanto si h_1 y h_2 conmutan, como si lo hacen h_1g y h_2, existe un elemento distinto de z y del neutro que conmuta con todos los elementos de H_1 y también de H_2 (puesto que es generado por g y por h_2). Entonces, como $G = H_1H_2$, dicho elemento pertenece a $\mathcal{Z}(G)$, lo que contradice que $ord(\mathcal{Z}(G)) = 2$.

- Si $G/\mathcal{Z}(G) \cong \mathcal{D}_4$, entonces tiene un subgrupo de orden 4 isomorfo a $\mathbb{Z}_4$ y dos más isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Entonces, existen tres subgrupos de G, denotados por H_1, H_2 y H_3, todos ellos de

orden 8, de manera que H_1 contiene un único subgrupo de orden 4 conteniendo a $\mathcal{Z}(G)$ y H_2 y H_3 contienen tres cada uno.

Según hemos visto en casos anteriores, H_1 tiene que ser abeliano. Además, $H_1 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ porque, en tal caso, cada subgrupo de orden 2 está contenido en tres subgrupos de orden 4.

Por último, si $H_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, el subgrupo de orden 4 que contiene a $\mathcal{Z}(G)$ es el isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, puesto que los dos subgrupos isomorfos a $\mathbb{Z}_4$ contienen al mismo subgrupo de orden 2. Por la proposición 3.4, $H_1 \cap H_2$ es el subgrupo de orden 4 de H_1 que contiene a $\mathcal{Z}(G)$, luego es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Si H_2 fuese abeliano, ya hemos visto que $H_1 \cap H_2 \subset \mathcal{Z}(G)$, contradiciéndose que $ord(\mathcal{Z}(G)) = 2$. Por otro lado, H_2 contiene un subgrupo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, de modo que $H_2 \ncong \mathcal{Q}_8$. Por tanto, $H_2 \cong \mathcal{D}_4$, de modo que tiene cinco elementos de orden 2, así que existe $h_2 \in H_2 \setminus H_1$ de orden 2. Se denota $K := \langle h_2 \rangle$.

El lema 7.10 implica que $H_1 \triangleleft G$. Además, como $H_1 \cap K = \{1_G\}$, la proposición 3.4 implica que $H_1 K = G$. Entonces, la proposición 4.6 implica que $G \cong K \ltimes_\phi H_1$ para algún homomorfismo $\phi : K \to Aut(H_1)$. Del corolario 4.11 se tiene que $Fix(\phi)$ ha de ser un subgrupo de orden 2 para que el centro de G tenga orden 2.

Sean a y b generadores de H_1 de órdenes 4 y 2, respectivamente. Entonces, $\phi(h_2)(a) \in \{a, a^3, ba, ba^3\}$ por tener que ser un elemento de orden 4. Entonces, $\phi(h_2)(a^2) = (\phi(h_2)(a))^2 = a^2$, de modo que $a^2 \in Fix(\phi)$. Entonces, $\phi(h_2)(b) = ba^2$, por no ser b un punto fijo.

En el caso en el que $\phi(h_2)(a) = a$, $a \in Fix(\phi)$ y si $\phi(a) = a^3$, entonces $\phi(ba) = ba$, luego $ba \in Fix(\phi)$. En ambos casos, $Fix(\phi)$ no sería un subgrupo de orden 2. Por otro lado, si $\phi(h_2)(a) \in \{ba, ba^3\}$, se verificaría que $\phi^2(h_2)(a) = a^3 \neq a$, luego ϕ no estaría bien definido como homomorfismo desde K.

Por tanto, si $H_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, entonces $ord(\mathcal{Z}(G)) > 2$, luego la única opción posible es que $H_1 \cong \mathbb{Z}_8$.

Ya se ha visto que si alguno de los subgrupos H_2 ó H_3 fuese abeliano, entonces $ord(\mathcal{Z}(G)) \geq 4$. Por tanto, suponemos que son isomorfos a $\mathcal{D}_4$ o a $\mathcal{Q}_8$. Si alguno de ellos, sin pérdida de generalidad H_2, es isomorfo a $\mathcal{D}_4$, entonces existe $h_2 \in H_2 \setminus H_1$ de orden 2. Denotando $K := \langle h_2 \rangle$, se tiene que $K \cap H_1 = \{1_G\}$, luego la proposición 3.4 implica que $KH_1 = G$. Como $H_1 \triangleleft G$ por el lema 7.10, la proposición 4.6 implica que $G \cong K \ltimes_\phi H_1$ para algún homomorfismo $\phi : K \to Aut(H_1)$.

Si h_1 es un generador de H_1, entonces hemos visto que ϕ queda determinada por $\phi(h_2)(h_1)$, que pertenece a $\{h_1, h_1^3, h_1^5, h_1^7\}$[7]. Si $\phi(h_2)(h_1) = h_1$, el producto semidirecto resulta ser un producto directo, luego G sería abeliano. En cambio, el caso $\phi(h_2)(h_1) = h_1^5$ ya se ha considerado cuando $ord(\mathcal{Z}(G)) = 4$. Entonces, quedan por considerar los dos siguientes grupos. Por un lado,

$$G_{12}^{(16)} = \mathbb{Z}_2 \ltimes_\phi \mathbb{Z}_8$$

donde $\phi(1 + 2\mathbb{Z})(x) = x^3 \ \forall x \in \mathbb{Z}_8$. Por otro lado,

$$G_{13}^{(16)} = \mathbb{Z}_2 \ltimes_\phi \mathbb{Z}_8$$

donde $\phi(1 + 2\mathbb{Z})(x) = x^{-1} \ \forall x \in \mathbb{Z}_8$.

[7]Sabemos que $\phi(h_2)(h_1)$ tiene orden 8, luego ha de pertenecer a dicho conjunto. Recíprocamente, los cuatro automorfismos $\phi(h_2)$ que se generan con estos valores de $\phi(h_2)(h_1)$ tienen orden 1 ó 2, luego están bien definidos como homomorfismos desde K.

Puede comprobarse que $G_{12}^{(16)}$ tiene 5 elementos de orden 2, 6 de orden 4 y 4 de orden 8, mientras que $G_{13}^{(16)}$ tiene 9 elementos de orden 2, 2 de orden 4 y 4 de orden 8. Por tanto, $G_{12}^{(16)}$ y $G_{13}^{(16)}$ no son isomorfos.

Por último, si $H_2 \cong H_3 \cong \mathcal{Q}_8$, sean h_1 generador de H_1, y $h_2 \in H_2 \setminus H_1$. De este modo, h_1 y h_2 generan G y tienen órdenes 8 y 4, respectivamente. Como $H_1 \triangleleft G$ y $H_2 \triangleleft G$ por el lema 7.10, $h := h_2 h_1 h_2^{-1} h_1^{-1} \in H_1 \cap H_2$ y, por tanto, conmuta con h_1. Así, $h_3 := h_1 h_2 \in G \setminus (H_1 \cup H_2) \subset H_3 \setminus \mathcal{Z}(G)$, luego tiene orden 4, puesto que $H_3 \cong \mathcal{Q}_8$. Además, por la estructura de $\mathcal{Q}_8$, $z := h_2^2 = h_3^2 \in \mathcal{Z}(G) \setminus \{1_G\}$. De este modo,

$$z = h_3^2 = (h_1 h_2)^2 = h_1 h_2 h_1 h_2 = h_1 h h_1 h_2^2 = h h_1^2 z \Rightarrow h h_1^2 = 1_G \Rightarrow h = h_1^{-2} = h_1^6$$

Por otro lado, $h_2^2 \in H_1 \cup H_2$ porque $H_2/(H_1 \cap H_2)$ tiene orden 2. Además, $o(h_2^2) = 2$ por el lema 6.2, luego $h_2^2 = h_1^4$. Por tanto, G admite la presentación

$$G_{14}^{(16)} = \langle h_1, h_2 | h_1^8 = 1_G, h_2^2 = h_1^4, h_1 h_2 h_1 = h_2 \rangle$$

8.3. Grupos de orden 18

Dado un grupo G de orden 18, el tercer teorema de Sylow 5.13 implica que $n_3(G) = 1$, de modo que existe un subgrupo normal K de orden 9. Además, por el primer teorema de Sylow 5.9, también existe un subgrupo H de orden 2. De este modo, el corolario 3.9 implica que $H \cap K = \{1_G\}$ y, por tanto, la proposición 3.4 implica que $|HK| = ord(H)ord(K) = 18 = ord(G)$, luego $HK = G$.

Por tanto, de la proposición 4.6 se deduce que $G \cong H \ltimes_\phi K$ para algún homomorfismo $\phi : H \to Aut(K)$. Sabemos por el corolario 7.3 que $H \cong \mathbb{Z}_2$ y por el corolario 7.7 que K es isomorfo a $\mathbb{Z}_9$ ó a $\mathbb{Z}_3 \times \mathbb{Z}_3$.

- Si $K \cong \mathbb{Z}_9$, entonces, dados dos generadores h y k de H y K, respectivamente, todo homomorfismo ϕ queda determinado por el único entero $n \in \mathbb{Z}_9$ tal que $\phi(h)(k) = k^n$. Como $\phi^2(h) = \phi(h^2) = \phi(1_H) = Id_K$, se tiene que:

  $$k = \phi^2(h)(k) = \phi(h)(k^n) = k^{n^2} \Rightarrow n^2 \equiv 1 \mod 9 \Rightarrow n \equiv \pm 1 \mod 9$$

  Entonces, si $n = 1+9\mathbb{Z}$, $\phi(h) = Id_K$, luego ϕ es el automorfismo nulo y el producto semidirecto resulta ser el producto directo. De este modo,

  $$G_1^{(18)} \cong \mathbb{Z}_2 \times \mathbb{Z}_9 \cong \mathbb{Z}_{18}$$

  Por otro lado, si $n = -1 + 9\mathbb{Z}$, el producto semidirecto a considerar es:

  $$G_2^{(18)} \cong \mathcal{D}_9 \cong \mathbb{Z}_2 \ltimes_\phi \mathbb{Z}_9$$

  donde $\phi(1 + 2\mathbb{Z})(x) = x^{-1}\ \forall x \in \mathbb{Z}_9$.

- Si $K \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, dado un homomorfismo $\phi : H \to Aut(K)$, el conjunto $Fix(\phi) = \{k \in K : \phi(h)(k) = k\ \forall h \in H\}$ es un subgrupo de K, luego por el corolario 3.8 puede tener orden 1, 3 ó 9. En adelante, denotaremos $\alpha := \phi(h)$, donde h es el elemento no neutro de H.

  Supongamos en primer lugar que $Fix(\phi) = K$, de modo que ϕ es el homomorfismo nulo y, por tanto, el producto semidirecto resulta ser el producto directo. De este modo,

  $$G_3^{(18)} \cong \mathbb{Z}_2 \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \cong \mathbb{Z}_6 \times \mathbb{Z}_3$$

Si $Fix(\phi) = 1_K$, entonces, dados $a, b \in K$ tal que $\alpha(a) = b$. Como $\alpha^2 = Id_K$, se verifica que $\alpha(b) = a$. Entonces $\alpha(ab) = ab$, luego $ab \in Fix(\phi) = \{1_K\}$. Entonces, $b = \alpha(a) = a^{-1}\ \forall a \in K$. De este modo,

$$G_4^{(18)} = \mathbb{Z}_2 \ltimes_\phi (\mathbb{Z}_3 \times \mathbb{Z}_3)$$

donde $\phi(1 + 2\mathbb{Z})(k) = k^{-1}\ \forall k \in \mathbb{Z}_3 \times \mathbb{Z}_3$.

Por último, si $ord\,(Fix(\phi)) = 3$ y consideramos ϕ como una acción sobre K, se deduce de la proposición 5.4 que existen tres órbitas de cardinal dos, de manera que $\{a, b\}$ es una órbita si y sólo si $\alpha(a) = b$ y $\alpha(b) = a$. De este modo, si $\{a, b\}$ es una órbita y $b \neq a^{-1}$, entonces $\{a^{-1}, b^{-1}\}$ consituye otra órbita. Así, en el caso en el que no hubiese ninguna órbita formada por un elemento y su inverso, el número de órbitas de orden 2 sería par, lo cual no es cierto. Por tanto, $\exists x \in K$ tal que $\alpha(x) = x^{-1}$.

Sean $\phi_1, \phi_2 : H \to Aut(K)$ tales que $ord(Fix(\phi_1)) = ord(Fix(\phi_2)) = 3$ y denotamos $\alpha_1 = \phi_1(h)$ y $\alpha_2 = \phi_2(h)$. Sean a_1 y a_2 generadores de $Fix(\phi_1)$ y $Fix(\phi_2)$, respectivamente. Sean también $b_1, b_2 \in K$ tales que $\alpha_1(b_1) = b_1^{-1}$ y $\alpha_2(b_2) = b_2^{-1}$. Como $b_i \in K \setminus \langle a_i \rangle$, podemos considerar el automorfismo θ tal que $\theta(a_1) = a_2$ y $\theta(b_1) = b_2$. Dicho automorfismo verifica que $\theta \circ \alpha_1 = \alpha_2 \circ \theta$, deduciéndose de la proposición 4.9 que $H \ltimes_{\phi_1} K \cong H \ltimes_{\phi_2} K$. Por tanto, todos los productos semidirectos que verifican que $ord\,(Fix(\phi)) = 3$ son isomorfos. De este modo, únicamente falta por considerar un grupo:

$$G_5^{(18)} \cong \mathbb{Z}_2 \ltimes_\phi (\mathbb{Z}_3 \times \mathbb{Z}_3)$$

donde $\phi(1 + 2\mathbb{Z})(m + 3\mathbb{Z}, n + 3\mathbb{Z}) = (m + 3\mathbb{Z}, -n + 3\mathbb{Z})\ \forall m, n \in \mathbb{Z}_3$.

En todos los casos, como $\ker \phi = \{1_{\mathbb{Z}_2}\}$, el corolario 4.11 implica que $\mathcal{Z}(G) \cong Fix(\phi)$. De este modo, ningún par de $G_3^{(18)}$, $G_4^{(18)}$ y $G_5^{(18)}$ son isomorfos.

8.4. Grupos de orden 24

El objetivo de esta sección es realizar una clasificación salvo isomorfismo de los grupos de orden $24 = 2^3 \cdot 3$. Según hemos visto en el corolario 5.10 al primer teorema de Sylow, todo grupo G de orden 24 contiene al menos un 2-subgrupo de Sylow H, cuyo orden será 8, y un subgrupo K de orden 3.

Además, debido al segundo teorema de Sylow 5.11, todos los subgrupos de orden 8 de G son subgrupos conjugados, es decir, son isomorfos. De este modo, un método para la clasificación de los grupos de orden 24 será ver a qué grupo de orden 8 son isomorfos sus 2-subgrupos de Sylow.

Este razonamiento también es válido para los 3-subgrupos de Sylow pero, sin embargo, no aporta ninguna información extra puesto que dos grupos cualesquiera de orden 3 son isomorfos.

Por último, según el tercer teorema de Sylow 5.13, podemos sacar algunas conclusiones acerca del número de subgrupos de Sylow de G. En cuanto a $p = 2$, dicho teorema implica que $n_2|3 \Rightarrow n_2 = 1$ ó 3. Por otro lado, $n_3|8$ y, además, $n_3 \equiv 1 \mod 3$. Por tanto, los únicos posibles valores de n_3 son 1 y 4.

Vamos a empezar a clasificar los grupos de orden 24 según la cantidad de subgrupos de Sylow que tengan, es decir, según los valores de n_2 y n_3.

8.4.1. $\boxed{n_2(G) = 1,\ n_3(G) = 1}$

En este caso G posee un único subgrupo H de orden 8 y un único subgrupo K de orden 3 que, por el teorema 5.13, son subgrupos normales. Como, además, los órdenes de H y K son primos entre

sí, $H \cap K = \{1_G\}$ por el corolario 3.9. De este modo, la proposición 3.4 implica que $|HK| = 24$, es decir, $HK = G$. De esta manera, por el corolario 4.7, $G \cong H \times K$.

Según la proposición 7.2, $K \cong \mathbb{Z}_3$ por el hecho de tener orden 3. Por otro lado, por la observación 7.8 y la proposición 7.11, H ha de ser isomorfo a una de las siguientes opciones:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathcal{D}_4, \quad \mathcal{Q}_8.$$

Así, según a que grupo sea isomorfo H, G será isomorfo a una de las siguientes opciones:

1. $G_1^{(24)} \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \cong \mathbb{Z}_{24}$.
2. $G_2^{(24)} \cong (\mathbb{Z}_4 \times \mathbb{Z}_2) \times \mathbb{Z}_3 \cong \mathbb{Z}_{12} \times \mathbb{Z}_2$.
3. $G_3^{(24)} \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3 = \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
4. $G_4^{(24)} \cong \mathcal{D}_4 \times \mathbb{Z}_3$.
5. $G_5^{(24)} \cong \mathcal{Q}_8 \times \mathbb{Z}_3$.

Estos grupos no son isomorfos entre sí puesto que entonces también lo serían sus 2-subgrupos de Sylow, y esto no ocurre.

Otra observación importante es que el teorema 6.6 implica los grupos G_1, G_2 y G_3 son los únicos grupos abelianos de orden 24.

8.4.2. $\boxed{n_2(G) = 3,\ n_3(G) = 1}$

En este caso, G tiene tres subgrupos de orden 8 y un subgrupo normal K de orden 3. Tomamos un subgrupo H de orden 8 arbitrario. Análogamente al caso anterior, se verifica que $H \cap K = \{1_G\}$ y que $HK = G$. Entonces, por la proposición 4.6, se verifica que $G \cong H \ltimes_\phi K$ para algún homomorfismo $\phi : H \to Aut(K)$.

La forma de proceder en este caso va a ser la siguiente: para cada tipo de isomorfía de H como grupo de orden 8 se van a calcular los posibles homomorfismos ϕ que generen productos semidirectos.

Para ello, resulta útil estudiar el grupo de automorfismos $Aut(K) \cong Aut(\mathbb{Z}_3)$. Este grupo está compuesto por dos elementos: uno de ellos es la identidad y el otro, ψ, viene dado por $\psi(x) = x^2$.

Por tanto, los homomorfismos ϕ vendrán determinados por qué elementos de H verifican que $\widetilde{h}$ es la identidad o el automorfismo ψ, es decir, ϕ queda perfectamente determinada por el subgrupo $\ker\phi \subset H$.

En este momento resulta conveniente descartar los casos en los que $\ker\phi = H$, pues en dicho caso el producto semidirecto coincide con el directo y estaríamos en los supuestos de la sección anterior (se verificaría que $n_2 = 1$, en contra de lo que se está suponiendo en esta sección).

De este modo, como el teorema 2.5 implica que $G/\ker\phi \cong im\ \phi \subset Aut(K)$, ha de verificarse que $ord(\ker\phi)$ vale 4 u 8. En el segundo caso ϕ sería el homomorfismo nulo, que no se considera por lo comentado anteriormente. Así, se considerarán únicamente los casos en los que $ord(\ker\phi) = 4$.

En esta situación, resulta interesante presentar la siguiente proposición que nos permitirá ver cuándo dos productos semidirectos son isomorfos.

Proposición 8.2. Sean H y K dos subgrupos tales que $K \cong \mathbb{Z}_3$, de modo que $Aut(K) = \{Id, \psi\}$. Considérense los productos semidirectos $H \ltimes_{\phi_1} K$ y $H \ltimes_{\phi_2} K$. Si existe un automorfismo $\theta \in Aut(H)$ tal que $\theta(\ker\phi_1) = \ker\phi_2$, entonces $H \ltimes_{\phi_1} K \cong H \ltimes_{\phi_2} K$.

Demostración. La condición $\theta(\ker\phi_1) = \ker\phi_2$ se escribe como:

$$\ker\phi_1 = \theta^{-1}(\ker\phi_2) = \theta^{-1}\left(\phi_2^{-1}(Id_K)\right) = (\phi_2\circ\theta)^{-1}(Id_K) = \ker(\phi_2\circ\theta)$$

Entonces ϕ_1 y $\phi_2\circ\theta$ son homomorfismos $H \to Aut(K)$ con el mismo núcleo. Como $Aut(K)$ tiene sólo dos elementos, concluimos que $\phi_1 = \phi_2\circ\theta$. De este modo, la proposición 4.8 implica que

$$H \ltimes_{\phi_1} K \cong H \ltimes_{\phi_2} K$$

□

Ahora vamos a considerar los posibles grupos de orden 24 clasificados en esta sección según el tipo de isomorfía de H como grupo de orden 8. Cabe destacar de nuevo que en ningún caso dos grupos de orden 24 serán isomorfos si no lo son sus 2-subgrupos de Sylow.

- Supongamos en primer lugar que $H \cong \mathbb{Z}_8$. El único subgrupo de orden 4 de H es $\langle a^2\rangle$, donde a es un generador del grupo. Así, obtenemos un sexto grupo

  $$G_6^{(24)} \cong \mathbb{Z}_8 \ltimes_\phi \mathbb{Z}_3$$

  donde $\phi(n+8\mathbb{Z}) = \psi^n$.

- Supóngase ahora que $H \cong \mathbb{Z}_4\times\mathbb{Z}_2$, de modo que contiene 3 subgrupos de orden 4: dos de ellos, M_1 y M_2, isomorfos a $\mathbb{Z}_4$ y el otro, M_3, isomorfo a $\mathbb{Z}_2\times\mathbb{Z}_2$. De este modo, existen 3 homomorfismos $\phi_1,\phi_2,\phi_3 : H \to Aut(K)$ cuyos núcleos son los subgrupos mencionados anteriormente, respectivamente.

  Veamos primero que los subgrupos $H\ltimes_{\phi_1}K$ y $H\ltimes_{\phi_2}K$ son isomorfos. Para ello, sean $a=(1,0)$ y $b=(1,1)$ generadores de $M_1 = \ker\phi_1$ y $M_2 = \ker\phi_2$, respectivamente. Consideramos el isomorfismo

  $$\theta : \mathbb{Z}_4\times\mathbb{Z}_2 \to \mathbb{Z}_4\times\mathbb{Z}_2, (m+4\mathbb{Z}, n+2\mathbb{Z}) \mapsto (m+4\mathbb{Z}, m+n+2\mathbb{Z})$$

  que verifica que $\theta(a) = b$, de modo que $\theta(\ker\phi_1) = \ker\phi_2$, luego por la proposicion 8.2, $H\ltimes_{\phi_1}K \cong H\ltimes_{\phi_2}K$.

  Así, en este caso tenemos únicamente dos grupos. En primer lugar,

  $$G_7^{(24)} = (\mathbb{Z}_4\times\mathbb{Z}_2)\ltimes_{\phi_1}\mathbb{Z}_3$$

  donde $\phi_1 : \mathbb{Z}_4\times\mathbb{Z}_2 \to Aut(\mathbb{Z}_3)$ queda definido por $\phi(m+4\mathbb{Z}, n+2\mathbb{Z}) = \psi^n\ \forall m\in\mathbb{Z}_4,\ \forall n\in\mathbb{Z}_2$.

  Por otro lado, está el grupo

  $$G_8^{(24)} = (\mathbb{Z}_4\times\mathbb{Z}_2)\ltimes_{\phi_3}\mathbb{Z}_3$$

  donde $\phi_3(m+4\mathbb{Z}, n+2\mathbb{Z}) = \psi^m\ \forall m\in\mathbb{Z}_4,\ \forall n\in\mathbb{Z}_2$.

  Por el corolario 4.11, $\mathcal{Z}(G_7^{(24)}) \cong \ker\phi_1 \cong \mathbb{Z}_4$ y $\mathcal{Z}(G_8^{(24)}) \cong \ker\phi_3 \cong \mathbb{Z}_2\times\mathbb{Z}_2$, de modo que los grupos $G_7^{(24)}$ y $G_8^{(24)}$ no son isomorfos.

- Ahora se considera el caso en el que $H \cong \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$. Entonces, H tiene 7 subgrupos de orden 4, todos ellos isomorfos a $\mathbb{Z}_2\times\mathbb{Z}_2$. Vamos a ver que si tomamos dos de ellos M_1 y M_2, existe $\theta\in Aut(H)$ tales que $\theta(M_1) = M_2$. Para ello, sean (a,b,c) y (d,e,f) ternas de generadores de H tales que $M_1 = \langle a,b\rangle$ y $M_2 = \langle d,e\rangle$. Entonces, la aplicación dada por $\theta(xa+yb+zc) := xd+ye+zf\ \forall x,y,z\in\mathbb{Z}_2$ es un isomorfismo bien definido tal que $\theta(M_1) = M_2$, como queríamos. Por tanto, en este caso existe un único subgrupo de orden 24, que se escribe

  $$G_9^{(24)} = (\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2)\ltimes_\phi\mathbb{Z}_3$$

  donde $\phi(a+2\mathbb{Z}, b+2\mathbb{Z}, c+2\mathbb{Z}) = \psi^c\ \forall a,b,c\in\mathbb{Z}_2$

- Ahora suponemos que $H \cong \mathcal{D}_4$. Entonces, H tiene un subgrupo M_1 homeomorfo a $\mathbb{Z}_4$, que se identifica con $\langle\rho\rangle$ y dos subgrupos, M_2 y M_3, identificados con $\langle\rho^2, \tau\rangle$ y $\langle\rho^2, \tau\rho\rangle$, respectivamente.

  Según hemos visto, cada uno de estos subgrupos genera un único homomorfismo $\phi_i : H \to Aut(K)$ tal que $\ker\phi_i = M_i$. De este modo, tenemos tres productos semidirectos $H \ltimes_{\phi_i} K$ que son isomorfos a todos los posibles grupos de orden 24 con un subgrupo normal de orden 3 y tres subgrupos de orden 8 isomorfos a $\mathcal{D}_4$.

  Sin embargo, el automorfismo de H definido por $\theta\left(\tau^j\rho^i\right) := \tau^j\rho^{j+i}$, donde $j \in \{0,1\}$ e $i \in \mathbb{Z}$, verifica que $\theta(M_2) = M_3$, luego por la proposición 8.2, los dos últimos productos semidirectos son isomorfos.

  De este modo, tenemos dos nuevos grupos, salvo isomorfía:

  $$G_{10}^{(24)} = \mathcal{D}_4 \ltimes_{\phi_1} \mathbb{Z}_3$$

  donde $\phi_1\left(\tau^j\rho^i\right) = \psi^j \ \forall j, i \in \mathbb{Z}$.

  Y, además,

  $$G_{11}^{(24)} = \mathcal{D}_4 \ltimes_{\phi_2} \mathbb{Z}_3$$

  donde $\phi_2\left(\tau^j\rho^i\right) = \psi^i \ \forall i, j \in \mathbb{Z}$.

  Por el corolario 4.11, $\mathcal{Z}\left(G_{10}^{(24)}\right) \cong \mathbb{Z}_4$ y $\mathcal{Z}\left(G_{11}^{(24)}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Por tanto, $G_{10}^{(24)}$ y $G_{11}^{(24)}$ no son isomorfos.

- Por último, considérese el caso en el que $H \cong \mathcal{Q}_8$, de modo que H tiene tres subgrupos, M_1, M_2 y M_3 de orden 4, todos ellos isomorfos a $\mathbb{Z}_4$. En la notación habitual $\mathcal{Q}_8 = \{\pm1, \pm i, \pm j, \pm k\}$, i, j y k son los generadores de M_1, M_2 y M_3, respectivamente. Entonces, el automorfismo de $\mathcal{Q}_8$ dado por:

  $$\theta(-1) = -1, \quad \theta(i) = j, \quad \theta(j) = k, \quad \theta(k) = i.$$

  verifica que $\theta(M_1) = M_2$. Por otro lado, también se verifica que $\theta(M_2) = M_3$, de modo que, por la proposición 8.2, los tres productos semidirectos obtenidos a partir de los homomorfismos ϕ_i tales que $\ker\phi_i = M_i$ son isomorfos. De esta manera, en estas condiciones, únicamente se tiene un nuevo grupo.

  $$G_{12}^{(24)} = \mathcal{Q}_8 \ltimes_{\phi} \mathbb{Z}_3$$

  donde $\phi(x) = Id_{\mathbb{Z}_3} \ \forall x \in M_1 = \{\pm1, \pm i\}$ y $\phi(x) = \psi \ \forall x \notin M_1$.

8.4.3. $\boxed{n_2(G) = 1,\ n_3(G) = 4}$

En este caso, el 2-subgrupo de Sylow, de orden 8, es un subgrupo normal de G. Entonces, igual que en los casos anteriores, si tomamos un 3-subgrupo de Sylow, K, verificará que $H \cap K = \{1_G\}$, por ser los órdenes de H y K primos entre sí. Además, por la proposición 3.4, $ord(HK) = 24$, luego $HK = G$. Por tanto, estamos dentro de las hipótesis de la proposición 4.6, de modo que $G = K \ltimes_{\phi} H$, donde $\phi : K \to Aut(H)$ es un homomorfismo de grupos.

Entonces, si k genera el grupo K, $\phi(k) \in Aut(K)$ ha de tener orden 1 ó 3. En el primer caso, $\phi(k)$ sería la identidad, de modo que ϕ sería el homomorfismo nulo y el producto semidirecto en cuestión coincidiría con el producto directo, volviendo al caso considerado anteriormente en el que $n_3 = 1$. Por tanto, en adelante, buscaremos $\phi \in Aut(H)$ tales que $o(\phi(k)) = 3$.

- En primer lugar, si $H \cong \mathbb{Z}_8$, veamos que no existen automorfismos de H de orden 3. Razonando por reducción al absurdo, supongamos que existe tal ϕ. En este contexto, $\exists m \in \mathbb{N}$ tal que $\phi(a) = a^m \ \forall a \in \mathbb{Z}_8$. Entonces, como $\phi^3 = Id_H$, se verifica que:

$$a = \phi^3(a) = a^{m^3} \Rightarrow m^3 \equiv 1 \mod 8 \Rightarrow m \equiv 1 \mod 8$$

  donde la última implicación puede verse estudiando las diferentes clases de equivalencia. De este modo, $\phi(a) = a \ \forall a \in \mathbb{Z}_8$, luego $\phi = Id_H$, que tiene orden 1.

  Lo que se acaba de probar es que si $H \cong \mathbb{Z}_8$, entonces el único producto semidirecto que verifica estas condiciones es el producto directo, grupo ya considerado en la primera sección.

- Sea ahora $H \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ y sean a y b elementos de órdenes 4 y 2, respectivamente, que generan H. Sea $\phi \in Aut(H)$ de orden 3. Por ser un isomorfismo, se tiene que $\phi(a)$ ha de ser un elemento de orden 4, luego $\phi(a) \in \{a, a^3, ba, ba^3\}$.

  Veamos que $\phi(a) = a$. Si $\phi(a) = a^3$, se tendría que $\phi^3(a) = a^{27} = a^3 \neq a$, luego ϕ no tendría orden 3. Por otro lado, si $\phi(a) = ba$, entonces $\phi(a^3) = ba^3$. Por tanto $\phi^2(a) = \phi(ba) \in \{a, a^3\}$ por tener que tener orden 4 y ser ϕ inyectiva. Así, $\phi^3(a) \in \{\phi(a), \phi(a^3)\} = \{ba, ba^3\} \Rightarrow \phi^3(a) \neq a$, de modo que ϕ no tendría orden 3. Algo análogo ocurre cuando $\phi(a) = ba^3$, de modo que la única posibilidad que queda es que $\phi(a) = a$.

  Este razonamiento se puede aplicar a todos los elementos de orden 4, perteneciendo todos ellos a $Fix(\phi)$.

  Además, $\phi(a^2) = \phi(a)^2 = a^2$, de modo que $\phi(b) \in \{b, ba^2\}$. Sin embargo, $\phi(b) = ba^2 \Rightarrow \phi^2(b) = \phi(ba^2) = \phi(b)\phi(a)^2 = ba^4 = b \Rightarrow \phi^3(b) = \phi(b) \neq b$.

  Así, la única posibilidad es que $\phi(b) = b$, luego (por ser $\phi(a) = a$ y generar a y b el grupo) ϕ es la identidad, que tiene orden 1.

  De este modo, el único automorfismo de $\mathbb{Z}_4 \times \mathbb{Z}_2$ cuyo orden divide a 3 es la identidad, de modo que no existen grupos de orden 24 tales que $n_2 = 1$, $n_3 = 4$ y que el 2-subgrupo de Sylow sea isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$.

- En el caso en el que $H \cong \mathcal{D}_4$, tampoco existe ningún automorfismo de $\mathcal{D}_4$ de orden 3. En efecto, supongamos que existe uno, ϕ. Entonces $\phi(\rho) \in \{\rho, \rho^3\}$ por tener que tener orden 4. Sin embargo, en el caso de que $\phi(\rho) = \rho^3$, se tendría que $\phi^3(\rho) = \rho^{27} \neq \rho$, lo que contradice el supuesto de que $o(\phi) = 3$. Por tanto, $\phi(\rho) = \rho$.

  En este caso, $\phi(\tau) \in \mathcal{D}_4 \setminus \langle\rho\rangle$, luego existe $n \in \mathbb{N}$ tal que $\phi(\tau) = \tau\rho^n$. Así, $\phi^3(\tau) = \tau\rho^{3n} = \tau$, de modo que $3n \equiv 0 \mod 4$ y, como $mcd(3, 4) = 1$, también $n \equiv 0 \mod 4$.

  Por tanto, $o(\phi)|3 \Rightarrow \phi = Id_{\mathcal{D}_4}$, de modo que no tenemos que considerar nuevos grupos en esta sección, por el mismo motivo que en los casos de $H \cong \mathbb{Z}_8$ y $H \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

- Cuando $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, vamos a ver que sí que existe un producto semidirecto no trivial. Además, vamos a ver que es único utilizando la proposicion 4.9.

  En efecto, sea el homomorfismo $\phi : K \to Aut(H) \subset Biy(H)$, es decir, que puede considerarse como una acción del grupo K sobre H, entendido como conjunto. De este modo, dado un generador k del grupo K, denotaremos $\alpha := \phi(k)$. Entonces, por la proposición 5.4, el cardinal de cada órbita ha de ser 1 ó 3, siendo las órbitas de cardinal 1 las formadas por los elementos $x \in H$ tales que $\alpha(x) = x$, es decir, los puntos fijos de α. Es trivial ver que dicho conjunto de puntos fijos es un subgrupo de H, luego, por el corolario 3.8, tiene cardinal 1, 2, 4 ó 8. De este modo, la única posibilidad (obviando el caso en el que α sea la identidad, donde todas las

órbitas tienen cardinal uno) es que esta acción tenga dos puntos fijos y dos órbitas formadas por tres elementos.

Sean $\mathcal{O}_1$ y $\mathcal{O}_2$ las dos órbitas de cardinal 3. Al menos uno de los dos conjuntos $\mathcal{O}_1 \cup \{1_G\}$, $\mathcal{O}_2 \cup \{1_G\}$ no es un subgrupo. En efecto, si los dos conjuntos fueran subgrupos, por la proposición 3.4 y el hecho de que el producto está contenido en H, la intersección tendría orden mayor o igual que 2, lo que contradice el hecho de que las órbitas sean disjuntas. De este modo, existe una órbita $\mathcal{O}$ tal que $\mathcal{O} \cup \{1_G\}$ no es un subgrupo. Por la estructura de $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, los elementos de $\mathcal{O}$ generan H.

Sean ahora dos homomorfismos $\phi_1, \phi_2 : K \to Aut(H)$. Dado k generador de K, denotamos $\alpha_1 := \phi_1(k)$ y $\alpha_2 := \phi_2(k)$. Sean entonces $\mathcal{O}_1 = \{a, b, c\}$ y $\mathcal{O}_2 = \{x, y, z\}$ las órbitas, bajo las respectivas acciones dadas por ϕ_1 y ϕ_2, que generan H. En ellas, puede suponerse, renombrando los elementos, que $\alpha_1(a) = b$ y que $\alpha_2(x) = y$. Se considera el automorfismo de H dado por

$$\theta : H \to H,\ a^l b^m c^n \mapsto x^l y^m c^n\ \forall l, m, n \in \mathbb{Z}_2$$

que está bien definido y es un isomorfismo por ser $\{a, b, c\}$ y $\{x, y, z\}$ generadores del grupo y ser $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Además, verifica que

$$\theta \circ \phi_1(k) = \theta \circ \alpha_1 = \alpha_2 \circ \theta = \phi_2(k) \circ \theta$$

Y este resultado también implica que

$$\theta \circ \phi_1(k^2) = \theta \circ \phi_1(k) \circ \phi_1(k) = \phi_2(k) \circ \theta \circ \phi_1(k) = \phi_2(k) \circ \phi_2(k) \circ \theta = \phi_2(k^2) \circ \theta$$

Por tanto, la proposición 4.9 implica que todos los productos semidirectos de la forma $K \ltimes_\phi H$ son isomorfos.

De este modo, únicamente hay que considerar un nuevo grupo, dado por

$$G_{13}^{(24)} = \mathbb{Z}_3 \ltimes_\phi (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$$

donde $\phi(1 + 3\mathbb{Z})(l + 2\mathbb{Z}, m + 2\mathbb{Z}, n + 2\mathbb{Z}) = (m + 2\mathbb{Z}, n + 2\mathbb{Z}, l + 2\mathbb{Z})\ \forall l, m, n \in \mathbb{Z}_2$

- Por último, está el caso en el que $H \cong \mathcal{Q}_8$. Análogamente al caso anterior, la acción asociada a cada producto semidirecto tiene dos puntos fijos y dos órbitas de cardinal 3. En este caso, el único elemento de orden 2 de H es el punto fijo distinto de la identidad. Además, ningún elemento de orden 4 puede pertenecer a la misma órbita que su inverso, puesto que en este caso, existiría $x \in \mathcal{Q}_8$ (el elemento en cuestión o su inverso) tal que $\alpha(x) = x^{-1}$, siendo α el automorfismo imagen de un generador de K. Así, $\alpha^2(x) = x$ y $\alpha^3(x) = x^{-1}$, de modo que se contradiría el hecho de que el orden de α ha de dividir a 3.

  En la notación habitual de $\mathcal{Q}_8$, hay dos puntos fijos, 1 y -1, y dos órbitas $\{a, b, c\}$ y $\{a^{-1}, b^{-1}, c^{-1}\}$ formadas por elementos de orden 4.

  Sean ahora dos homomorfismos $\phi_1, \phi_2 : K \to Aut(H)$ que definen productos semidirectos y sean $\alpha_1 := \phi_1(k)$ y $\alpha_2 := \phi_2(k)$, donde k es un generador de K. Tomamos órbitas de ϕ_1 y ϕ_2, $\{a, b, c\}$ y $\{x, y, z\}$, respectivamente, tales que $\alpha_1(a) = b$ y $\alpha_2(x) = y$. Por la estructura de $\mathcal{Q}_8$, ab es c o c^{-1}. En el segundo caso, renombramos a, b y c por a^{-1}, b^{-1} y c^{-1}, respectivamente. Hacemos lo propio con la órbita $\{x, y, z\}$. Entonces, se verifica que $ab = c$ y que $xy = z$. Entonces, existe un homomorfismo θ verificando:

$$\theta : H \to H;\ a \mapsto x,\ b \mapsto y,\ c \mapsto z$$

de modo que $\theta \circ \alpha_1 = \alpha_2 \circ \theta$. Así, como ϕ_1 y ϕ_2 son arbitrarios, la proposición 4.9 implica que todos los productos semidirectos de esta forma son isomorfos, por lo que tenemos que considerar un único grupo en esta sección.

$$G_{14}^{(24)} = \mathbb{Z}_3 \ltimes_\phi \mathcal{Q}_8$$

donde $\phi(1 + 3\mathbb{Z})$ es el automorfismo de $\mathcal{Q}_8$ que verifica que:

$$i \mapsto j, \quad j \mapsto k, \quad k \mapsto i.$$

8.4.4. $\boxed{n_2(G) = 3,\ n_3(G) = 4}$

Antes de estudiar este caso, necesitamos considerar una serie de resultados.

Proposición 8.3. Dado un grupo G y un subgrupo suyo $H \subset G$, el grupo

$$core_G(H) = \bigcap_{g \in G} g^{-1} H g$$

es un subgrupo normal contenido en H.

Demostración. $core_G(H)$ es un subgrupo por ser la intersección de todos los subgrupos conjugados de H. Además, es un subgrupo normal porque para cada $x \in G$,

$$x^{-1} core_G(H) x = \bigcap_{g \in G} x^{-1} \left(g^{-1} H g\right) x = \bigcap_{g \in G} (gx)^{-1} H (gx) = \bigcap_{y \in G} y^{-1} H y = core_G(H)$$

□

Teorema 8.4. Dado un grupo G y un subgrupo $H \subset G$, sea $\Omega := \{Hx : x \in G\}$ el conjunto de clases laterales por la derecha. Entonces $G/core_G(H)$ es isomorfo a un subgrupo de $Biy(\Omega)$. En particular si $[G : H] = n$, entonces $G/core_G(H)$ es isomorfo a un subgrupo de $\mathcal{S}_n$.

Demostración. Considérese la acción de G sobre Ω dada por $\psi : G \to Biy(\Omega),\ g \mapsto \widetilde{g}$, donde

$$\widetilde{g} : \Omega \to \Omega,\ Hx \mapsto Hxg$$

Se comprueba trivialmente que $\widetilde{g_1 g_2} = \widetilde{g_1}\widetilde{g_2}\ \forall g_1, g_2 \in G$, luego ψ está bien definido como acción. El núcleo de la acción es

$$\ker \psi = \{g \in G : \widetilde{g} = Id_\Omega\} = \{g \in G : Hxg = Hx\ \forall x \in G\} = \{g \in G : xgx^{-1} \in H\ \forall x \in G\} =$$
$$\{g \in G : g \in x^{-1} H x\ \forall x \in G\} = core_G(H)$$

Por lo tanto, por el primer teorema de isomorfía 2.5, $G/core_G(H)$ es isomorfo a $\operatorname{Im} \psi$, que es un subgrupo de $Biy(\Omega)$.

□

Vamos a introducir ahora un nuevo tipo de subgrupo cuya definición es más fuerte que la de subgrupo normal.

Definición 8.5. Dado un grupo G, un subgrupo suyo $H \subset G$ se dice *característico* si $\theta(H) = H$ para cada $\theta \in Aut(G)$

Evidentemente, todo subgrupo característico es normal, puesto que la conjugación es un automorfismo de G. Algunas otras propiedades de los grupos característicos quedan expuestas en las siguientes proposiciones.

Proposición 8.6. Sea G un grupo y sea $H \subset G$ un subgrupo finito de orden n de modo que no existe ningún otro subgrupo del mismo orden. Entonces, H es un subgrupo característico.

Demostración. Para cada $\theta \in Aut(G)$, $\theta(H)$ es un subgrupo de orden n de G, luego es H. Así, H es un subgrupo característico. □

Proposición 8.7. Dado un grupo G y dos subgrupos suyos $H \subset N$ tales que $N \triangleleft G$ y H es característico en N. Entonces, H es subgrupo normal de G.

Demostración. Dado $g \in G$, se tiene que $g^{-1}Ng = N$, luego la conjugación por g es un automorfismo de N. Por tanto, como H es característico en N, se verifica que $g^{-1}Hg = H$, luego H es subgrupo normal de G. □

Queremos ver ahora que un grupo G de orden 24 tal que ninguno de sus grupos de Sylow es normal, es isomorfo al grupo de permutationes $\mathcal{S}_4$. Para ello, utilizamos el siguiente desarrollo, que puede verse más detallado en [5].

Sea K un subgrupo de Sylow de orden 3, cuyo normalizador $N := N_G(K)$, por el tercer teorema de Sylow 5.13, verifica que $[G : N] = n_3(G) = 4$. Entonces, denotando por $P := core_G(N)$, el teorema 8.4, implica que G/P es isomorfo a un subgrupo de $\mathcal{S}_4$.

Como $P = \bigcap_{g \in G} g^{-1}Ng \subset N$, se tiene que $K \triangleleft KP$ (cabe destacar que KP es subgrupo de G por ser P subgrupo normal, en virtud del corolario 3.3). Además, $KP \subset G$, luego $ord(KP)|ord(G) = 24$, de modo que K es un 3-subgrupo de Sylow normal de KP. Entonces, por el teorema 5.13, es el único subgrupo de orden 3 de KP, luego por la proposición 8.6, es característico. De aquí se concluye que KP no puede ser normal en G, pues en tal caso, la proposición 8.7 implicaría que $K \triangleleft G$, lo que no es cierto.

No obstante, $K \cap P = \{1_G\}$ puesto que, en caso contrario, P contendría a K y, por ser subgrupo normal, haría lo mismo con todos los 3-subgrupos de Sylow, siendo su orden mayor o igual que $9 > 6 = ord(N)$, contradiciendo el hecho de que $P \subset N$. Así, por la proposición 3.4, $ord(KP) = ord(K)ord(P) = 3ord(P)$, luego KP/P es un 3-subgrupo de Sylow de G/P que no es normal por no serlo KP en G, en virtud de la proposición 2.9. Por tanto, $n_3(G/P) > 1$. En particular, se deduce que $ord(G/P)$ es múltiplo de 3, luego $ord(P)$ no es divisible por 3.

Como P es un subgrupo de N, el corolario 3.8 implica que

$$ord(P)|ord(N) = \frac{ord(G)}{[G : N]} = \frac{24}{4} = 6$$

de modo que el orden de P solo puede ser 1 ó 2. En el caso en el que $ord(P) = 2$, el corolario 3.8 implica que $ord(G/P) = 12$. Así, según la proposición 8.1, ha de verificarse que $n_2(G/P) = 1$ o que $n_3(G/P) = 1$. Como hemos visto que $n_3(G/P) > 1$, ha de ser que $n_2(G/P) = 1$, existiendo un único subgrupo normal de orden 4. Por el teorema 2.8 y la proposición 2.9, existe un subgrupo normal S de orden 8 tal que $S/P \triangleleft G/P$. De esta manera, $n_2(G) = 1$, lo que contradice la hipótesis de esta sección.

Por tanto, $P = \{1_G\}$, luego $G \cong P$ es isomorfo a un subgrupo de $\mathcal{S}_4$. Pero como $ord(G) = 24 = ord(\mathcal{S}_4)$, se cumple que $G \cong \mathcal{S}_4$.

Así, el último grupo de orden 24 que queda por considerar es:

$$G_{15}^{(24)} = \mathcal{S}_4$$

8.5. Grupos de orden 30

Por el tercer teorema de Sylow 5.13, todo grupo G de orden 30 verifica que $n_3(G) \in \{1, 10\}$ y que $n_5(G) \in \{1, 6\}$. En el caso en el que $n_3(G) = 10$, G contendría 20 elementos de orden 3, mientras que si $n_5(G) = 6$, habría 24 elementos de orden 5. Como $ord(G) = 30$ es imposible que se den simultáneamente que $n_3(G) = 10$ y que $n_5(G) = 6$.

Entonces, bien $n_3(G) = 1$ o bien $n_5(G) = 1$, de modo que si escogemos subgrupos de Sylow H y K de órdenes 3 y 5, al menos uno de ellos es normal. Entonces, por el corolario 3.3, HK es un subgrupo. Nuevamente, el corolario 3.9 implica que $H \cap K = \{1_G\}$, de modo que, por la proposición 3.4, $ord(HK) = 15$. Así, todo grupo de orden 30 contiene un subgrupo N de orden 15, que es cíclico por la proposición 7.20. Además, N es normal por el lema 7.10.

Por otro lado, el teorema de Cauchy 5.7 implica la existencia de un subgrupo P de orden 2. Así, por el corolario 3.9, $P \cap N = \{1_G\}$, luego la proposición 3.4 implica que $|PN| = 30$, es decir, $PN = G$. Por tanto, estamos en las condiciones de la proposición 4.6 y $G \cong P \ltimes_\phi N$ para algún homomorfismo $\phi : P \to Aut(N)$.

Sean $a \in P$ y $b \in N$ generadores de los respectivos subgrupos. Denotando $\alpha := \phi(a)$, el hecho de que N sea cíclico implica que $\alpha(b) = b^n$ para algún $n \in \mathbb{N}$. Como α es la imagen de a por ϕ, su orden ha de dividir a dos, es decir, que $\alpha^2 = Id$. De este modo,

$$b = \alpha^2(b) = \alpha(b^n) = b^{n^2} \Rightarrow n^2 \equiv 1 \quad \text{mód } 15 \Rightarrow \alpha(b) = \{b, b^4, b^{11}, b^{14}\}$$

De este modo, tenemos 4 homomorfismos $\phi_1, \phi_2, \phi_3, \phi_4 : P \to Aut(N)$ distintos que verifican que $\phi_1(a)(b) = b$, $\phi_2(a)(b) = b^4$, $\phi_3(a)(b) = b^{11}$ y $\phi_4(a)(b) = b^{14}$; que generan cuatro grupos de orden 30 mediante productos semidirectos, los cuales se denotan por $G_1^{(30)} \cong \mathbb{Z}_{30}$, $G_2^{(30)} \cong \mathbb{Z}_3 \times \mathcal{D}_5$, $G_3^{(30)} \cong \mathbb{Z}_5 \times \mathcal{D}_3$, $G_4^{(30)} \cong \mathcal{D}_{15}$, respectivamente. Por el corolario 4.11: $\mathcal{Z}(G_1^{(30)}) = G_1^{(30)}$, $\mathcal{Z}(G_2^{(30)}) \cong \mathbb{Z}_3$, $\mathcal{Z}(G_3^{(30)}) \cong \mathbb{Z}_5$ y $\mathcal{Z}(G_4^{(30)}) = 1_{G_4^{(30)}}$. Por tanto, ningún par de estos grupos son isomorfos.

Referencias

[1] D. Clausen. *Classifying All Groups of Order 16.* Undergraduate thesis. University of Puget Sound, 2012.

[2] J. F. Fernando, J. M. Gamboa. *Estructuras Algebraicas:Teoría Elemental de Grupos.* Ed. Sanz y Torres, 2017.

[3] M. Hall Jr. *The Theory of Groups.* The Macmillan Company, 1959

[4] G.M. Hardy, E.M. Wright. *An introduction to the theory of numbers.* Oxford University Press, 1938.

[5] I.M. Isaacs. *Finite Group theory.* American Mathematical Society, 2008.

[6] G. A. Miller. *The regular substitution groups whose orders are less than 48.* Quart J. Math **28** (1896) 232-284.