UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

RUMBO A LA CLASIFICACION DE LOS GRUPOS METACICLICOS FINITOS

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C A

P R E S E N T A :

NADIA ROMERO ROMERO

DIRECTOR DE TESIS:
DR. FRANCISCO MARMOLEJO RIVAS

FACULTAD DE CIENCIAS
UNAM

2004

FACULTAD DE CIENCIAS
SECCION ESCOLAR

UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

ACT. MAURICIO AGUILAR GONZÁLEZ
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:

Rumbo a la clasificación de los grupos metacíclicos finitos

realizado por Nadia Romero Romero

con número de cuenta 9622414-0 **, quien cubrió los créditos de la carrera de:**

Matemáticas.

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Dr. Francisco Marmolejo Rivas
Propietario

Propietario Dr. Francisco González Acuña

Propietario Dr. Juan Morales Rodríguez

Suplente Dra. Martha Takane Imay

Suplente Dr. Alejandro Javier Díaz Barriga Casales

Consejo Departamental de
Matemáticas

M. en C. Alejandro Bravo Mojica

FACULTAD DE CIENCIAS
CONSEJO DEPARTAMENTAL
DE
MATEMATICAS

RUMBO A LA CLASIFICACIÓN DE LOS GRUPOS METACÍCLICOS FINITOS

Nadia Romero Romero

A María Fernanda y Santiago

Contenido

Agradecimientos

Mi primer agradecimiento es a la profesora Josefina Toledo M. de la Facultad de Química, por construir esa ventana que me llevaría más tarde a abrir la puerta del maravilloso mundo de las Matemáticas. Gracias a todos mis profesores y compañeros de la Facultad de Ciencias, pero especialmente a mis profesores de primer semestre Alejandro Díaz-Barriga, Rocío Vite y Pablo Barrera por mostrarme tres enfoques de las Matemáticas que ahora conforman uno solo.

A Jean-Paul Rosas y Ramón Zárate por su invaluable amistad y todos sus consejos, los matemáticos y los no matemáticos; a Pedro '*el wassa*' Valencia y Cristóbal Falconi no sólo por su amistad, sino también por ayudarme a ver que la Variable Compleja es hermosa. A Irina Gato Azul, Conchis Aqualung y Betty por aguantarme tanto y a todos mis amigos por existir.

Finalmente y de manera muy especial, al '*doc*' Francisco Marmolejo por todas sus enseñanzas, su disponibilidad, incansable optimismo y la paciencia que me tuvo en los momentos difíciles. A mis queridos padres por todo su apoyo y a Nidia, Fernanda y Santiago por los millones de sonrisas.

Introducción

En la sección III del libro *The Theory of Groups*, Hans Zassenhaus trata "el problema de la extensión" propuesto por Otto Schreir, que dice: Dados dos grupos abstractos, K y F, encontrar todos los grupos que contienen a K como subgrupo normal con grupo cociente isomorfo a F. Como caso particular de este problema, Zassenhaus menciona los grupos que tienen un subgrupo normal cíclico con grupo cociente cíclico. Un grupo con estas características es llamado metacíclico y su estructura resulta sorprendentemente compleja. Como el título lo indica, sólo trataremos grupos metacíclicos finitos, así que, en el futuro, al referirnos a un grupo metacíclico, supondremos que es finito. Un grupo metacíclico G puede ser escrito $G = SK$ con $S \leqslant G$, $K \trianglelefteq G$ y ambos cíclicos, este producto es llamado una factorización metacíclica de G. Si G tiene una factorización metacíclica tal que $S \cap K = 1$, entonces decimos que G se escinde. Como ejemplos de grupos metacíclicos tenemos a los grupos cíclicos, productos semidirectos de éstos y los cuaterniones.

La mayor parte de este trabajo está basada en el artículo *Metacyclic groups of odd order* [8] de Hyo-Seob Sim, publicado en 1994 y que, según Sim, presenta una determinación de los tipos de isomorfismo de grupos metacíclicos de orden impar en términos de presentaciones. Nuestro objetivo será describir detalladamente el proceso seguido por Sim para llegar a estas presentaciones y a la solución del problema de isomorfismo. Los resultados preliminares están enfocados a este objetivo, y por ello podrán parecer un poco extraños o desligados unos de otros, mas su función quedará clara conforme avancemos. Aquí incluimos también, los resultados que C. E. Hempel, en su artículo *Metacyclic groups* [4] de 2000, considera necesarios para clasificar los 2-grupos metacíclicos. En la primera sección del capítulo 2 construimos una factorización metacíclica para p-grupos metacíclicos con p primo impar que resultará muy conveniente para la clasificación de los grupos metacíclicos de orden impar. La segunda parte de este capítulo trata la clasificación de los 2-grupos metacíclicos.

En el Capítulo 3 construimos la descomposición de Hall estándar para un grupo metacíclico finito G. Para hacer esto, llamamos N a la intersección de todos los complementos de Sylow normales en G, como veremos, el complemento de Sylow correspondiente al primo más pequeño que divide el orden de G debe ser normal, por lo que esta definición tiene sentido. N será minimal entre los subgrupos de Hall de G normales con grupo factor nilpotente. En el Teorema 3.6 probamos que N se escinde. Así, en el Capítulo 4 construimos la presentación estándar para grupos metacíclicos de orden impar tomando un generador por cada factor cíclico en una descomposición semidirecta de N como 2 elementos en un conjunto generador de 4 elementos para G. Los otros dos elementos de este conjunto son escogidos de tal forma que generen un subgrupo de Hall nilpotente, H, que sea un complemento semidirecto de N en G. Con esta construcción, Sim asegura que todas las dificultades que arriban cuando G no se escinde sean localizadas en el subgrupo nilpotente H. El Teorema 4.2 asegura que todo grupo metacíclico no cíclico de orden impar tiene una presentación estándar.

Para combinar nuestro entendimiento de H y N en un resultado con respecto a G, requerimos conocimiento de las posibles acciones de H en N que resulten en un producto semidirecto $H \ltimes N$ que sea metacíclico, y del efecto que la elección de esta acción tiene en el tipo de isomorfismo de G, así que, en el Capítulo 5 tratamos cuestiones concernientes a los automorfismos de p-grupos metacíclicos con p impar y, finalmente, el Teorema 6.6 nos da una prueba para decidir cuando dos grupos definidos por presentaciones estándar son isomorfos.

Capítulo 1

Resultados preliminares

1.1. Generales

Si G es un grupo, escribiremos $Z(G)$ para su **centro**. Si K y Y son subgrupos de G, el **centralizador** de K en Y será denotado por $\mathbb{C}_K(Y)$ y el **conmutador** por $[X,\ Y]$, para el conmutador de G escribiremos G'. La conjugación $x^{-1}yx$ de un elemento y por x, sera representada por y^x. El neutro será denotado por 1.

Definición 1.1. Un grupo G es llamado **metacíclico** si tiene un subgrupo normal cíclico K tal que G/K también es cíclico. Llamaremos a K un **núcleo** de G.

Si G es un grupo metacíclico y $K = \langle y \rangle$ es un núcleo de G, entonces existe $x \in G$ tal que xK genera a G/K. Para cualquier $g \in G$ tenemos $gK = x^sK$, $s \in \mathbb{Z}$, luego $x^{-s}g \in K$. Es decir $g = x^sy^t$, $t \in \mathbb{Z}$ y $G = SK$ con $S = \langle x \rangle$, como se dijo en la Introducción, este producto es llamado una **factorización metacíclica** de G.

Lema 1.2. *Un grupo G es metacíclico con un subgrupo normal cíclico de orden m y grupo cociente cíclico de orden k si, y sólo si, tiene la siguiente presentación:*

$$\langle x,\ y \mid x^k = y^l,\ y^m = 1,\ y^x = y^n \rangle,$$

donde k, l, m y n son enteros positivos tales que $m \mid (n^k - 1)$ y $m \mid l(n-1)$.

Prueba. Sea G un grupo con una factorización metacíclica $G = SK$. G tiene dos generadores $x,\ y$, $\langle x \rangle = S$ y $\langle y \rangle = K$. Si el orden de K es m, entonces tenemos $y^m = 1$, ahora, si el índice de K en G es k, entonces $x^k = y^l$ p. a. l entero positivo, y claramente tenemos $y^x = y^n$, p.a. n entero positivo. Así obtenemos las igualdades

$y = y^{x^k} = y^{n^k}$ y $y^l = y^{lx} = y^{ln}$ y por lo tanto, $m \mid (n^k - 1)$ y $m \mid l(n-1)$. Con esto tenemos que G es una imagen homomórfica del grupo descrito por las tres relaciones de la presentación de arriba, pero el grupo descrito por ésta tiene orden a lo más mk, es decir, estos grupos son isomorfos y por lo tanto, esta es una presentación para G.

Ahora supongamos k, l, m, n enteros positivos tales que $m \mid (n^k - 1)$ y $m \mid l(n-1)$. Consideremos el conjunto A de los km elementos $x^i y^j$, i módulo k y j módulo m, con el siguiente producto:

$$x^i y^j \cdot x^s y^t = \begin{cases} x^{i+s} y^h & \text{si} \quad i+s < k \\ x^a y^{h+l} & \text{si} \quad i+s = k+a, \end{cases}$$

donde $[h] = [jn^s + t]$ en los enteros módulo m. Como $i + s < 2k$ tenemos $0 \leq a < k$ y de ser necesario, tomaremos el representante de la clase $[h + l]$ en los enteros módulo m. Verificaremos que $(A, \cdot)$ es un grupo. Para la asociatividad tenemos que probar:

$$(x^i y^j \cdot x^s y^t) \cdot x^u y^v = x^i y^j \cdot (x^s y^t \cdot x^u y^v).$$

Observemos

$$x^i y^j \cdot x^s y^t = \begin{cases} x^{i+s} y^{jn^s+t} & \text{si} \quad i+s < k \\ x^{a_0} y^{jn^s+t+l} & \text{si} \quad i+s = k+a_0 \end{cases}$$

y su producto por la derecha con $x^u y^v$ depende de si $i + s + u < k$, $i + s + u \geq k$, $u + a_0 < k$ ó $u + a_0 \geq k$. Por otro lado

$$x^s y^t \cdot x^u y^v = \begin{cases} x^{s+u} y^{tn^u+v} & \text{si} \quad s+u < k \\ x^{b_0} y^{tn^u+v+l} & \text{si} \quad s+u = k+b_0 \end{cases}$$

y el producto $x^i y^j \cdot (x^s y^t \cdot x^u y^v)$ depende de si $i + s + u < k$, $i + s + u \geq k$, $u + b_0 < k$ ó $u + b_0 \geq k$. Haciendo todas las posibles combinaciones de estas condiciones obtenemos el resultado.

Ahora obtendremos el inverso de un elemento $x^i y^j$ en A. Tomemos $s = k - i$ y t el representante de la clase en los enteros módulo m inversa aditiva a $[jn^s + l]$. Por la definición de producto tenemos $x^i y^j \cdot x^s y^t = 1$.

Así que $(A, \cdot)$ es un grupo que cumple las relaciones de la presentación de arriba y por lo tanto, es una imagen homomórfica del grupo que ésta genera, cuyo orden es menor o igual que km y entonces, es igual a A. La presentación del grupo cociente $A/\langle y \rangle$, es $\langle x \mid x^k = 1 \rangle$, luego el grupo generado por y es normal y tiene orden m y su grupo cociente tiene orden k.

En el futuro, denotaremos por $\mathsf{C}(n)$ al grupo cíclico de orden n.

Lema 1.3. *Subgrupos y grupos cociente de grupos metacíclicos son metacíclicos.*

Prueba. Sean G un grupo metacíclico y H un subgrupo de G. Si G tiene una factorización metacíclica $G = SK$, tomamos $K_1 = H \cap K \leqslant K$. Entonces K_1 es un subgrupo normal cíclico de H y por el Segundo Teorema de Isomorfismo, $H/K_1 \cong HK/K \leqslant G/K$ que es cíclico.

Ahora supongamos T un subgrupo normal de G, KT/T es cíclico y por el Tercer Teorema de Isomorfismo, KT/T es normal en G/T y

$$\frac{G/T}{KT/T} \cong \frac{G}{KT} \cong \frac{G/K}{TK/K}$$

y este último es cíclico. Es decir, KT/T es un subgrupo normal cíclico de G/T tal que su cociente es cíclico.

Continuamos enlistando varios resultados de la teoría de grupos a los que recurriremos constantemente para alcanzar nuestro objetivo. En las secciones siguientes omitiremos la demostración de algunas afirmaciones por ser resultados conocidos de la teoría de grupos, o porque su demostración es muy larga y se utilizará sólo en puntos particulares de algunas pruebas. Sin embargo, en todos los casos acompañamos la afirmación con una referencia bibliográfica en la que se encuentra una prueba.

Lema 1.4 (5.42 en [7]). *Sean x, y elementos de un grupo G y supongamos que ambos conmutan con $[x, y]$. Entonces:*

(i) $[x, y]^n = [x^n, y] = [x, y^n]$ *para todo* $0 \leq n \in \mathbb{Z}$; *y*

(ii) $x^n y^n = (xy)^n [x, y]^{n(n-1)/2}$ *para todo* $0 \leq n \in \mathbb{Z}$.

Prueba. (i)La prueba es por inducción sobre n. Claramente es verdad para $n = 0$. Para el paso inductivo observemos que

$$\begin{aligned} [x,y]^n[x,y] &= x^{-1}[x,y]^n y^{-1}xy, \quad \text{por hipótesis} \\ &= x^{-1}[x^n,y]y^{-1}xy, \quad \text{por inducción} \\ &= x^{-1}(x^{-n}y^{-1}x^n y)y^{-1}xy \\ &= [x^{n+1},y]. \end{aligned}$$

Análogamente para la otra igualdad.

(ii)También haremos la prueba por inducción sobre n, claramente es verdad para $n = 0$. Para el paso inductivo observemos que

$$\begin{aligned} xx^n y^n y &= x(xy)^n[x,\ y]^{n(n-1)/2}y, \quad \text{por inducción} \\ &= x(xy)^n y[x,\ y]^{n(n-1)/2}, \quad \text{por hipótesis} \\ &= xy(xy)^n[(xy)^n,\ y][x,\ y]^{n(n-1)/2} \\ &= (xy)^{n+1}[x,\ y]^n[x,\ y]^{n(n-1)/2}, \quad \text{por hipótesis y (i)} \\ &= (xy)^{n+1}[x,\ y]^{n(n+1)/2}. \end{aligned}$$

Definición 1.5. Decimos que un grupo G tiene **exponente** $n > 0$, si $x^n = 1$ para toda x en G. Si el grupo es finito, su exponente minimal será denotado por $\mathbf{exp\,G}$.

Lema 1.6 (2.2 en [8]). *Sea A un grupo abeliano finito con un subgrupo cíclico C, tal que $|C| = \exp A$. Entonces C es un factor directo de A.*

Prueba. Sea $C = \langle y \rangle$. A/C es abeliano finito, luego es la suma directa de, digamos r, subgrupos cíclicos $D_k = \langle x_k C \rangle$ con $|D_k| = s_k$. Observemos que para cada D_k podemos encontrar un elemento de la forma $x_k y^l$ en A cuyo orden sea s_k:

Sabemos que, bajo el mapeo natural, $\psi : A \to A/C$, $x_k C$ es la imagen de x_k. Así que $s_k | o(x_k)$ y $o(x_k)n = \exp A = o(y)$ p.a. entero n, luego

$$o(x_k^{s_k})n = \frac{o(x_k)n}{s_k} = \frac{o(y)}{s_k} = o(y^{s_k})$$

Concluimos $\langle x_k^{s_k} \rangle \leqslant \langle y^{s_k} \rangle$, es decir $x_k^{s_k} = (y^{s_k})^j$, $j \in \mathbb{Z}$. Así que $(x_k y^{-j})^{s_k} = 1$, pero la imagen de $x_k y^{-j}$ bajo ψ es $x_k C$, cuyo orden es s_k, por tanto el orden de $x_k y^{-j}$ es s_k. Podemos, entonces, definir un homomorfismo $f_k : D_k \to A$, $f_k(x_k C) = x_k y^{-j}$.

Con esto tenemos un grupo abeliano A y una familia de homomorfismos $\{f_k : D_k \to A,\ k = 1, \ldots, r\}$, por lo que existe un único homomorfismo $\varphi : A/C \to A$ tal que que si i_k es la inclusión de cada D_k en A/C entonces $\varphi i_k = f_k$ para toda $k = 1, \ldots r$. Luego $\psi\varphi = id_{A/C}$, de donde se sigue el resultado.

Lema 1.7 (2.3 en [8]). *Sean H y K subgrupos de un grupo finito G tales que $G = H \times K$. Supongamos que*

$$H_2 \trianglelefteq H_1 \leqslant H, \quad K_2 \trianglelefteq K_1 \leqslant K, \quad H_1/H_2 \cong K_1/K_2.$$

Sean θ un isomorfismo de H_1/H_2 en K_1/K_2 y

$$L := \{hk : \theta(hH_2) = kK_2,\ h \in H_1,\ k \in K_1\}.$$

Entonces L es un subgrupo de orden $|H_1K_2|$ tal que

$$H \cap L = H_2,\ K \cap L = K_2 \text{ y } H_1L = H_1K_1 = LK_1.$$

Además, el mapeo

$$(H_1,\ H_2,\ K_1,\ K_2,\ \theta) \mapsto L$$

es una biyección del conjunto de todos los 'quintetos' $(H_1,\ H_2,\ K_1,\ K_2,\ \theta)$ con tales características al conjunto de todos los subgrupos de G.

El grupo L es llamado la ***diagonal*** *definida por θ.*

Prueba. La imagen de L bajo la proyección en H es H_1 y su kernel es K_2, por lo tanto, $|L| = |H_1K_2|$.

Ahora sea g en $H \cap L$, $g = h_1k_1$, $h_1 \in H_1$, $k_1 \in K_1$ y $\theta(h_1H_2) = k_1K_2$. Como g está en H, entonces $k_1 \in H$ así que $k_1 = 1$, luego g está en H_2 y $H \cap L = H_2$. Análogamente $K \cap L = K_2$.

Claramente H_1L está contenido en H_1K_1 y

$$|H_1L| = \frac{|H_1||L|}{|H_1 \cap L|} = \frac{|H_1||K_1||H_2|}{|H_2|} = |H_1K_1|.$$

Análogamente el otro caso, es decir $H_1L = H_1K_1 = LK_1$.

En la última afirmación es claro que el mapeo está bien definido. Para ver que es inyectivo supongamos $L = L'$ donde

$$L := \{hk \mid \theta(hH_2) = kK_2,\ h \in H_1,\ k \in K_1\} \text{ y}$$

$$L' := \{h'k' \mid \theta'(h'H_2') = k'K_2',\ h' \in H_1',\ k' \in K_1'\}.$$

Tomemos $hk \in L$, $h \in H_1$, $k \in K_1$, luego $hk = h'k'$, con $h' \in H_1'$ y $k' \in K_1'$; obtenemos $h = h'$, $k = k'$ y podemos concluir $H_1 = H_1'$ y $K_1 = K_1'$. Además $L \cap H_1 = H_2$ y $L' \cap H_1' = H_2'$, entonces $H_2 = H_2'$. Análogamente y $K_2 = K_2'$. Con esto claramente $\theta = \theta'$.

Para ver que es suprayectivo tomemos $M \leqslant G$. Sean H_1 y K_2 la imagen y el kernel de la proyección sobre H de M; K_1 y H_2 la imagen y el kernel de la proyección sobre K del mismo. Tenemos entonces

$$\frac{M}{H_2 \times K_2} \cong \frac{M/H_2}{(H_2 \times K_2)/H_2}, \text{ luego}$$

$$\frac{M}{H_2 \times K_2} \cong \frac{K_1}{K_2}, \text{ análogamente } \frac{M}{H_2 \times K_2} \cong \frac{H_1}{H_2}.$$

Si $hk(H_2K_2) \mapsto kK_2$ es el primer isomorfismo y $hk(H_2K_2) \mapsto hH_2$ es el segundo, entonces $\theta(kK_2) = hH_2$ es un isomorfismo entre H_1/H_2 y K_1/K_2. Así, L la imagen de $(H_1,\ H_2,\ K_1,\ K_2,\ \theta)$, es un grupo de orden $|H_1K_2| = |M|$ y $L \leqslant M$, luego $L = M$.

Notación 1.8. Denotaremos por $|m \bmod n|$ al entero positivo más pequeño i tal que $m^i \equiv 1 \bmod n$, este es llamado ***el orden multiplicativo de*** **m** ***módulo*** **n** y no está definido a menos que $(m,\ n) = 1$.

Sean p un primo y a un entero, escribiremos $p^r \parallel a$ si $p^r \mid a$ y $p^{r+1} \nmid a$.

Los siguientes resultados de carácter técnico nos serán de mucha utilidad en el tratamiento de los p-grupos metacíclicos.

Proposición 1.9 (2.1 en [8]). *Sean p primo impar, m y n enteros no negativos, y r un entero.*

(i) Si $r \equiv 1$ mod p, entonces $|r \bmod p^n| = \frac{p^n}{(p^n,\ r-1)}$.

(ii) Si $r^{p^m} \equiv 1$ mod p^n, entonces $1 + r + \cdots + r^{p^m-1} \equiv p^m$ mod p^n.

Prueba. La prueba de esta proposición se divide en varios lemas.

Lema 1.9.1. *Sea p un primo y supongamos $r \equiv 1$ mod p. Si $p^\alpha \mid (r-1)$, $\alpha \geq 1$, entonces $p^{\alpha+1} \mid (r^p - 1)$.*

Prueba. Tenemos $r = p^\alpha k + 1$ p.a. $k \in \mathbf{Z}$, entonces $r^p = (p^\alpha k + 1)^p = \sum_{i=0}^{p} \binom{p}{i} p^{\alpha i} k^i$, luego:

$$r^p - 1 = \binom{p}{1} p^\alpha k + \cdots + \binom{p}{p} p^{\alpha p} k^p.$$

Claramente $p^{\alpha+1}$ divide cada sumando, de donde obtenemos el resultado.

Corolario 1.9.2. *Sea p un primo y supongamos $r \equiv 1$ mod p. Si $p^\alpha \mid (r-1)$, $\alpha \geq 1$, entonces $p^{\alpha+s} \mid (r^{p^s} - 1)$, para todo s entero positivo.*

Lema 1.9.3. *Sea $p \neq 2$ un primo y supongamos $r \equiv 1$ mod p. Si $p^\alpha \parallel (r-1)$, $\alpha \geq 1$, entonces $p^{\alpha+1} \parallel (r^p - 1)$.*

Prueba. Sabemos que $r^p - 1 = \sum_{i=1}^{p} \binom{p}{i} p^{\alpha i} k^i$, ahora con $(p,\ k) = 1$.

Para $i = 1$, $p^{\alpha+2} \nmid \binom{p}{1} p^\alpha k$.

Para $1 < i < p$, $p \mid \binom{p}{i}$ y $p^{\alpha+1} \mid p^{\alpha i} k^i$ luego $p^{\alpha+2} \mid \binom{p}{i} p^{\alpha i} k^i$.

Para $i = p$, $p^{\alpha+2} \mid \binom{p}{p} p^{\alpha p} k^p$, ya que $\alpha p \geq \alpha 3 \geq \alpha + 2$. Por lo tanto $p^{\alpha+2} \nmid r^p - 1$.

Corolario 1.9.4. *Sea $p \neq 2$ un primo y supongamos $r \equiv 1$ mod p. Si $p^\alpha \parallel (r-1)$, $\alpha \geq 1$, entonces $p^{\alpha+s} \parallel (r^{p^s}-1)$, para todo s entero positivo.*

Prueba de 1.9(i). Si $p^n \mid (r-1)$, entonces $\mid r \bmod p^n \mid = 1$.
Supongamos ahora $p^\alpha = (p^n,\ r-1)$, con $1 \leq \alpha < n$, entonces $p^\alpha \parallel r-1$, luego:

$$p^n = p^{\alpha+(n-\alpha)} \parallel (r^{p^{n-\alpha}}-1) \quad \Rightarrow \quad \mid r \bmod p^n \mid = p^{n-\alpha} = \frac{p^n}{(p^n,\ r-1)}.$$

Lema 1.9.5. *Sean p primo y l un entero tales que $(p,l)=1$ y $p^r l < p^m$, entonces $p^{m-r} \mid \binom{p^m}{p^r l}$.*

Prueba.

$$\binom{p^m}{p^r l} = \frac{p^m!}{(p^r l)!(p^m - p^r l)!} = p^{m-r}\frac{(p^m-1)!}{l(p^r l-1)!(p^m-p^r l)!} =$$

$$p^{m-r}\frac{(p^m-1)(p^m-2)\cdots(p^m-(p^r l-1))}{l(p^r l-1)(p^r l-2)\cdots(p^r l-(p^r l-1))} =$$

$$p^{m-r}\frac{p^m-(p^r l-1)}{l(p^r l-1)}\cdot\frac{p^m-(p^r l-2)}{p^r l-2}\cdots\frac{p^m-(p^r l-(p^r l-1))}{p^r l-(p^r l-1)}.$$

Ahora, si $p^\alpha \mid p^r l - i$, entonces $p^\alpha \mid p^m - (p^r l - i)$, por lo tanto p^{m-r} divide a $\binom{p^m}{p^r l}$.

Prueba de 1.9(ii). Observemos primero que $r^{p^m} \equiv 1 \bmod p^n \Rightarrow r^{p^m} \equiv 1 \bmod p$, luego por el pequeño teorema de Fermat $r \equiv 1 \bmod p$.

Supongamos entonces $p \neq 2$, $r \equiv 1 \bmod p$ y $r^{p^m} \equiv 1 \bmod p^n$. Si $p^n \mid r-1$, entonces p^n divide cada uno de los sumandos de:

$$(1-1)+(r-1)+\cdots+(r^{p^m-1}-1) =$$

$$1\cdots+r^{p^m-1}-p^m.$$

Supongamos $p^\alpha \parallel r-1$, con $1 \leq \alpha < n$, por 1.9(i), $\mid r \bmod p^n \mid = p^{n-\alpha}$, y como $r^{p^m} \equiv 1 \bmod p^n$, entonces $p^{n-\alpha} \mid p^m$, es decir $n \leq m+\alpha$. Ahora como $r = p^\alpha k + 1$ con $(k,\ p)=1$, entonces:

$$r^{p^m} = (p^\alpha k+1)^{p^m} = 1 + \sum_{i=1}^{p^m}\binom{p^m}{i}p^{\alpha i}k^i$$

luego:

$$1 + r + \cdots + r^{p^m-1} = \frac{r^{p^m-1}}{r-1} = \frac{r^{p^m-1}}{p^\alpha k} =$$

$$\sum_{i=1}^{p^m} \binom{p^m}{i} p^{\alpha(i-1)} k^{(i-1)},$$

y tenemos $1 + r + \cdots + r^{p^m-1} - p^m = \sum_{i=2}^{p^m} \binom{p^m}{i} p^{\alpha(i-1)} k^{(i-1)}$.

Como $n \leq m + \alpha$, basta probar que $p^{m+\alpha} \mid \sum_{i=2}^{p^m} \binom{p^m}{i} p^{\alpha(i-1)} k^{(i-1)}$, es decir basta que $p^m \mid \binom{p^m}{i} p^{i-2}$ para todo $i = 2, \ldots, p^m$. Sea $i \in \{2, \ldots, p^m\}$, supongamos $i = p^r l$ con $(l,\ p) = 1$, entonces $p^{m-r} \mid \binom{p^m}{p^r l}$, por el Lema 1.9.5, y $p^r \mid p^{p^r l - 2}$ porque $r \leq p^r l - 2$ de donde se sigue el resultado.

Lema 1.10. *Si n es un número natural y p es un primo, entonces el exponente de la máxima potencia de p que divide a $n!$ es*

$$\frac{n - (a_0 + \cdots + a_k)}{p-1},$$

donde $n = a_0 + a_1 p + \cdots + a_k p^k$, con $p > a_i \geq 0$.

Prueba. La prueba es por inducción sobre n. El resultado es claramente cierto si $n = 0$. Supongámos que es cierto para $n - 1$ y demostrémoslo para n.

$$n = a_0 + a_1 p + \cdots + a_k p^k, \text{ con } p > a_i \geq 0,$$

Además, $n! = n(n-1)!$. Así que, debemos calcular la máxima potencia de p que divide a n y la máxima potencia de p que divide a $(n-1)!$. Si $a_0 \neq 0$, entonces $p \nmid n$ y la máxima potencia de p que divide a $n!$ es la máxima potencia de p que divide a $(n-1)!$. Por otro lado, $n - 1 = (a_0 - 1) + a_1 p + \cdots + a_k p^k$, luego, esta es:

$$\frac{n - 1 - ((a_0 - 1) + a_1 + \cdots + a_k)}{p-1} = \frac{n - (a_0 + \cdots + a_k)}{p-1}.$$

Supongamos ahora que $a_0 = 0$ y sea a_i el primer coeficiente tal que $a_i \neq 0$. Entonces la máxima potencia de p que divide a n es i, mientras que

$$\begin{aligned} n - 1 &= a_k p^k + \cdots + a_i p^i - 1 = a_k p^k + \cdots (a_i - 1) p^i + p^i - 1 \\ &= a_k p^k + \cdots + a_{i+1} p^{i+1} + (a_i - 1) p^i + (p-1) p^{i-1} + \cdots + (p-1). \end{aligned}$$

Por inducción, la máxima potencia de p que divide a $(n-1)!$ es

$$\frac{n-1-((a_k+\cdots+a_{i+1}+(a_i-1)+i(p-1))}{p-1}.$$

Por lo que la máxima potencia de p que divide a $n!$ es

$$i+\frac{n-1-((a_k+\cdots+a_{i+1}+(a_i-1)+i(p-1))}{p-1}=\frac{n-(a_i+\cdots+a_k)}{p-1}.$$

Lema 1.11 (4.2 en[4]). *Sean m y n números naturales y p un primo. Supongamos que m y n se expresan en base p-aritmética como*

$$n=a_0+a_1p+\cdots+a_kp^k,\quad m=b_0+b_1p+\cdots+b_kp^k,$$

con $p>a_i,\ b_i\geq 0$. Entonces el exponente de la máxima potencia de p que divide a $\binom{m+n}{n}$ es $\varepsilon_0+\cdots+\varepsilon_k$, donde

$$\begin{aligned} a_0+b_0 &= \varepsilon_0p+c_0,\\ \varepsilon_0+a_1+b_1 &= \varepsilon_1p+c_1,\\ \varepsilon_1+a_2+b_2 &= \varepsilon_2p+c_2,\\ &\cdots\\ \varepsilon_{k-1}+a_k+b_k &= \varepsilon_kp+c_k. \end{aligned}$$

Prueba. Dado que $0\leq a_i,\ b_i<p$, por el algoritmo de la división, tenemos que $0\leq c_i<p$ y los enteros ε_i valen 1 ó 0. Multiplicando la primera igualdad por 1, la segunda por p, la tercera por p^2, etc., y sumándolas, obtenemos:

$$m+n=c_0+c_1p+c_2p^2+\cdots+c_kp^k+\varepsilon_kp^{k+1}.$$

Denotemos por A a la cantidad de veces que el factor p aparece en el coeficiente binomial $(m+n)!/(m!n!)$. Sabemos que A es igual a

$$\frac{m+n-(c_0+\cdots+c_k+\varepsilon_k)}{p-1}-\frac{m-(b_0+\cdots+b_k)}{p-1}-\frac{n-(a_0+\cdots+a_k)}{p-1},$$

simplificando

$$A=\frac{a_0+\cdots+a_k+b_0+\cdots+b_k-c_0-\cdots-c_k-\varepsilon_k}{p-1},$$

de la adición y desarrollo del sistema de igualdades se obtiene:

$$a_0 + \cdots + a_k + b_0 + \cdots + b_k - c_0 - \cdots - c_k = (p-1)(\varepsilon_0 + \cdots + \varepsilon_{k-1}) + \varepsilon_k p.$$

Finalmente

$$A = \varepsilon_0 + \cdots + \varepsilon_k.$$

Lema 1.12 (4.3 en [4]). *Si a, b y c son números naturales, $a \geq 1$ y p es un primo, entonces $(\pm 1 + p^a)^{p^b c}$ es congruente con*

$$(\pm 1)^{p^b c} + (\pm 1)^{p^b c - 1} p^{a+b} c + (\pm 1)^{p^b c} \delta(p,\ 2)(1 - \delta(b,\ 0)) p^{2a+b-1} c$$

módulo p^{2a+b}, donde δ es la función delta de Kronecker.

Prueba.

$$(\pm 1 + p^a)^{p^b c} = \sum_{i=0}^{p^b c} \binom{p^b c}{i} (\pm 1)^{p^b c - i} p^{ai}$$

Analizemos los tres primeros sumandos, es decir:

$$\begin{array}{ll} \text{para } i = 0 & (\pm 1)^{p^b c}, \\ \text{para } i = 1 & (\pm 1)^{p^b c - 1} p^{a+b} c, \\ \text{para } i = 2 & (\pm 1)^{p^b c - 2} (\frac{p^{2a+b} c (p^b c - 1)}{2}). \end{array}$$

Si p es impar, entonces esta última fracción es un múltiplo de p^{2a+b}, $\delta(p,\ 2) = 0$ y tenemos que $\binom{p^b c}{2} p^{2a}$ es congruente con $\delta(p,\ 2)(1 - \delta(b,\ 0)) p^{2a+b-1} c$ módulo p^{2a+b}. Veamos que esto también se cumple para $p = 2$. Tenemos dos casos: $b = 0$ ó $b \neq 0$. Si $b = 0$,

$$\frac{p^{2a+b} c (p^b c - 1)}{2} = p^{2a} \frac{c(c-1)}{2}.$$

Si $b \neq 0$,

$$\frac{p^{2a+b} c (p^b c - 1)}{2} - p^{2a+b-1} c = p^{2a+b-1} c (p^b c - 1) - p^{2a+b-1} c = p^{2a+b} (p^{b-1} c^2 - c).$$

En ambos casos tenemos $\binom{p^b c}{2} p^{2a}$ congruente con $\delta(p,\ 2)(1 - \delta(b,\ 0)) p^{2a+b-1} c$ módulo p^{2a+b}. Luego, basta demostrar que si $d \geq 3$, entonces $\binom{p^b c}{d} p^{ad}$ es divisible por p^{2a+b}.

Como $p^{ad} = p^{2a+(d-2)a}$ y $d \geq 3$, basta que $\binom{p^b c}{d}$ sea divisible por p^{b+2-d}, suponiendo $b+2-d \geq 0$ (con $d \geq 3$), ya que $p^{b+2-d+2a+(d-2)a} = p^{2a+b+(d-2)(a-1)}$ y $a \geq 1$. Sea e el entero más grande tal que $p^e \leq d$. No es difícil ver que si $d \geq 3$, entonces para cualquier primo p, $e \leq d-2$, y como $0 \leq 2-d+b$, entonces $0 \leq b-e$. Al sumar $p^b c - d$ con d en base p-aritmética, como el resultado es $p^b c$, se llevan, al menos, $b-e$ elementos. Luego, por el Lema 1.11, $\binom{p^b c}{d}$ es divisible por p^{b-e}, esto es suficiente ya que $b+2-d \leq b-e$.

Corolario 1.13 (4.4 en [8]). *Si $m \geq n \geq 1$, p es un primo, $n+p \geq 4$ y $r \geq 1$, entonces cada una de las afirmaciones*

$$(1+p^n)^{p^r} \equiv 1 \bmod p^m$$

$$(-1+2^n)^{2^r} \equiv 1 \bmod 2^m$$

es equivalente a $r \geq m-n$.

Prueba. Del Lema 1.12 tenemos

$$(1+p^n)^{p^r} \equiv 1 + p^{n+r} + \delta(p,\ 2)p^{2n+r-1} \bmod p^{2n+r}.$$

Si $p = 2$, entonces, de esta congruencia y nuestras hipótesis, tenemos:

$$\begin{aligned}(1+2^n)^{2^r} - 1 &= 2^{n+r}(1 + 2^{n-1} + 2^n y) \\ &= 2^m x,\end{aligned}$$

para algunos enteros x, y. Si $r < m-n$, entonces $2^{m-(r+n)}x = 1 + 2^{n-1} + 2^n y$. Como $n+p \geq 4$, entonces $n \geq 2$, luego $1 + 2^{n-1} + 2^n y$ es impar, lo que contradice la última igualdad. El regreso es inmediato de $(1+2^n)^{2^r} - 1 = 2^{n+r}(1 + 2^{n-1} + 2^n y)$.

La prueba para $(-1+2^n)^{2^r} \equiv 1 \bmod 2^m$ es análoga a ésta. Ahora, si p es impar, entonces $\delta(p,\ 2) = 0$, luego

$$(1+p^n)^{p^r} \equiv 1 + p^{n+r} \bmod p^{2n+r}.$$

Si suponemos $(1+p^n)^{p^r} \equiv 1 \bmod p^m$, lo primero que observamos es que $m \leq 2n+r$, ya que si $m > 2n+r$, entonces $(1+p^n)^{p^r} \equiv 1 \bmod p^{2n+r}$, y tenemos p^{n+r} congruente con 0 módulo p^{2n+r}, lo que es contradictorio. Así, $m \leq 2n+r$ implica $(1+p^n)^{p^r} \equiv 1+p^{n+r} \bmod p^m$ y obtenemos p^{n+r} congruente con 0 módulo p^m, de donde concluimos el resultado.

1.2. p-grupos

Para abordar la clasificación de los p-grupos metacíclicos necesitamos considerar diversas propiedades de los p-grupos, por ejemplo el Teorema 1.17 y su Corolario 1.18. Los siguientes resultados sobre p-grupos serán utilizados en éste y los siguientes capítulos.

Teorema 1.14 (4.6 en [7]). *Sea G un p-grupo finito. Todo subgrupo maximal es normal y tiene índice p.*

Definición 1.15. Sea p un primo y G un p-grupo finito. Decimos que G es **abeliano elemental** si G isomorfo a $\mathsf{C}(p) \times \cdots \times \mathsf{C}(p)$.

Lema 1.16 (Ejercicio 2.78 en [7]). *Sea G un p-grupo abeliano finito. G es abeliano elemental si y sólo si, G tiene exponente p.*

Lema 1.17 (5.3.4 en [6]). *Un grupo de orden p^n tiene un subgrupo maximal cíclico si, y sólo si, es uno de los siguientes tipos:*

(i) un grupo cíclico de orden p^n,

(ii) el producto directo de un grupo cíclico de orden p^{n-1} y uno de orden p,

(iii) $M_n(p) := \langle x,\ a \mid x^p = a^{p^{n-1}} = 1,\ a^x = a^{1+p^{n-2}} \rangle$, $n \geq 3$,

(iv) el dihédrico de orden 2^n, $n \geq 3$:

$$D_n = \langle x,\ y \mid x^2 = y^{2^{n-1}} = 1,\ y^x = y^{-1} \rangle,$$

(v) los cuaterniones generalizados de orden 2^n, $n \geq 3$:

$$Q_n = \langle x,\ y \mid x^2 = y^{2^{n-2}},\ y^{2^{n-1}} = 1,\ y^x = y^{-1} \rangle,$$

(vi) el semidihédrico de orden 2^n, $n \geq 3$:

$$S_n = \langle x,\ y \mid x^2 = y^{2^{n-1}} = 1,\ y^x = y^{-1+2^{n-2}} \rangle.$$

Prueba. Sea $|G| = p^n$. Supongamos que $N = \langle a \rangle$ es un subgrupo maximal cíclico, entonces $N \lhd G$ y $|G/N| = p$. Si $G/N = \langle xN \rangle$, entonces $G = \langle x,\ a \rangle$, $|a| = p^{n-1}$ y $x^p \in N$. Si G es abeliano y $x^p = b^p$ con $b \in N$, entonces $(xb^{-1})^p = 1$ y $G = \langle xb^{-1} \rangle \times N$;

de lo contrario $x^p = a^i$ donde $(i,\ p) = 1$, y $G = \langle x \rangle$. Por lo tanto, G es del tipo (i) o del tipo (ii). A partir de ahora podemos suponer que G no es abeliano, entonces $n > 2$.

El elemento x induce un automorfismo en N que debe tener orden p; por lo tanto, $a^x = a^m$ donde $m^p \equiv 1 \bmod p^{n-1}$ y $1 < m < p^{n-1}$. Ahora, por el Pequeño Teorema de Fermat, $m^{p-1} \equiv 1 \bmod p$, luego tenemos $m \equiv 1 \bmod p$.

Por el momento, supongamos que p es impar. Escribimos $m = 1 + kp^i$ donde $(p,\ k) = 1$ y, desde luego, $0 < i < n - 1$. Ahora, los dos primeros sumandos de $m^p = (1 + kp^i)^p$ son 1 y kp^{i+1} y, como p es impar, el resto de los sumandos son divisibles por p^{i+2}, luego $m^p \equiv 1 + kp^{i+1} \bmod p^{i+2}$. Pero $m^p \equiv 1 \bmod p^{n-1}$, luego $kp^{i+1} + lp^{i+2} = l'p^{n-1}$ con enteros $l,\ l'$. De esta igualdad y, dado que $i + 1 \leq n - 1$ y $(p,\ k) = 1$, concluimos que $i + 1 = n - 1$ e $i = n - 2$. Por lo tanto, $m = 1 + kp^{n-2}$. Ahora, existe un entero k' tal que $kk' \equiv 1 \bmod p$, entonces, los dos primeros sumandos de $(1 + kp^{n-2})^{k'}$, es decir $1 + kk'p^{n-2}$, es congruente con $1 + p^{n-2}$ módulo p^{n-1} y como éste divide al resto de los sumandos, entonces $(1 + kp^{n-2})^{k'} \equiv 1 + p^{n-2} \bmod p^{n-1}$, luego $a^{x^{k'}} = a^{(1+kp^{n-2})^{k'}} = a^{1+p^{n-2}}$, y podemos reemplazar x por $x^{k'}$ y suponer que $m = 1 + p^{n-2}$. Resta entonces, discutir la posición de x^p en N. Ahora, $x^p \in \langle a^p \rangle$, ya que si $x^p \notin \langle a^p \rangle$, entonces $o(x) = p^n$ y G sería cíclico, así $x^p = b^p$, $b \in N$. Además $[a,\ x] = a^{p^{n-2}}$ y $p^{n-2}m \equiv p^{n-2} \bmod p^{n-1}$, por lo que $[a,\ x]$ conmuta con todos los elementos de G y podemos utilizar la igualdad

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

demostrada en el Lema 1.4, de la que obtenemos $(xb^{-1})^p = x^p b^{-p} = 1$, ya que $[x,\ b]$ tiene orden menor o igual a p. Reemplazando x por xb^{-1} podemos suponer $x^p = 1$ y, por lo tanto, G es de tipo (iii).

Ahora supongamos $p = 2$. Ciertamente m es impar, digamos $m = 2k + 1$. Dado que $m^2 \equiv 1 \bmod 2^{n-1}$, tenemos $k(k+1) \equiv 0 \bmod 2^{n-3}$ y k es congruente con 0 ó con -1 módulo 2^{n-3}. Ahora, como $m < p^{n-1}$, en el primer caso $m = 2^{n-2}l + 1$ con l impar. Podemos, de la misma forma en que lo hicimos unas líneas arriba, reemplazar x por una potencia adecuada y suponer $m = 2^{n-2} + 1$. En el segundo caso tenemos $m = 2^{n-2}l - 1$, si l es par $m = 2^{n-1} - 1$; mientras que si l es impar podemos, nuevamente, suponer $m = 2^{n-2} - 1$. Examinemos, entonces, estos tres casos.

Si $m = 2^{n-1} - 1$, entonces $a^x = a^{-1}$. Ahora, para alguna t, $a^t = x^2 = (x^2)^x = a^{tx} = a^{-t}$, luego el elemento x^2 tiene orden 1 ó 2 en N, lo que muestra que x^2 es igual a 1 ó a $a^{2^{n-2}}$ y G es isomorfo a D_{2^n} o a Q_{2^n}, respectivamente. Ahora supongamos que $m = 2^{n-2} + 1$. Como x^2 no genera N, ya que en este caso x tendría orden 2^n y G sería

cíclico, entonces $x^2 = a^{2r}$ para algún entero r. Sea $b = a^{r(2^{n-3}-1)}$, observamos que

$$(xb)^2 = x^2b^2[b,\ x] = a^{2r}a^{r(2^{n-2}-2)}a^{r(2^{n-3}-1)2^{n-2}} = a^{r2^{2n-5}}.$$

Como $2n-5 = n-1+n-4$, si $n \geq 4$ entonces esta potencia de a es igual a 1, y sustituyendo x por xb tenemos que G es de tipo (iii). Si $n = 3$, entonces $a^x = a^{-1}$ y x^2 es igual a 1 ó a a^2, por lo tanto, G es isomorfo a D_8 o a Q_8.

Finalmente, sea $m = 2^{n-2} - 1$. Si $x^2 = a^{2r}$, entonces $a^{2r} = (a^{2r})^x = a^{2r(2^{n-2}-1)} = a^{-2r}$, y x^2 es igual a 1 ó a $a^{2^{n-2}}$. Si $x^2 \neq 1$, entonces $(xa^{-1})^2 = a^{2^{n-2}}a^{-2}a^{-(2^{n-2}-2)} = 1$ y G es de tipo (vi).

Corolario 1.18. *Sea G un p-grupo finito con p impar. Si G tiene un único subgrupo de orden p, entonces es cíclico.*

Prueba. Supongamos p impar y $\mid G \mid = p^n$. La prueba es por inducción sobre n; claramente el teorema es cierto si $n = 1$. Si $n > 1$, entonces G tiene un subgrupo H de índice p, H es cíclico por inducción y G es uno de los tres primeros grupos enlistados en el lema anterior, pero los grupos de tipo (ii) y (iii) tienen más de un subgrupo de orden p, luego G es cíclico.

Teorema 1.19 (7.3 en [7]). *Si p es un primo impar, entonces $Aut\mathsf{C}(p^m) \cong \mathsf{C}(l)$ donde $l = (p-1)p^{m-1}$.*

Teorema 1.20 (5.44 en [7]). *Sea $U(\mathsf{C}(2^m))$ el grupo de unidades del anillo $\mathsf{C}(2^m)$, es decir:*

$$U(\mathsf{C}(2^m)) = \{[a] \in \mathsf{C}(2^m) \mid a \text{ es impar}\}.$$

Si $m \geq 3$, entonces

$$U(\mathsf{C}(2^m)) = \langle [-1],\ [5] \rangle \cong \mathsf{C}(2) \times \mathsf{C}(2^{m-2}).$$

Lema 1.21. *Si C es un subgrupo cíclico de $U(\mathsf{C}(2^m))$ $(m \geq 3)$, entonces existe l, $2 \leq l \leq m$, tal que*

$$C = \langle [1+2^l] \rangle \quad \acute{o} \quad C = \langle [-1+2^l] \rangle.$$

Prueba. Del Teorema anterior sabemos que cada elemento de $U(\mathsf{C}(2^m))$ es de la forma $(\pm 1)[5]^a$ donde $1 \leq a \leq 2^{m-2}$. Observemos que $\langle [-1] \rangle$ y $\langle [5]^{2^{m-3}} \rangle$ son subgrupos cíclicos de orden 2 y si $a \neq 2^{m-3}$, entonces $\langle [5]^a \rangle \neq \langle -[5]^a \rangle$. Así, $U(\mathsf{C}(2^m))$ tiene $2 + 2(m-2) = 2(m-1)$ subgrupos cíclicos distintos. Por otro lado, hay $m-1$ naturales desde 2 hasta m. Es decir, los grupos cíclicos de la forma $\langle [\pm 1 + 2^l] \rangle$ son $2(m-1)$. Probaremos que todos son distintos.

Por el Corolario 1.13, $|1+2^l \bmod 2^m| = 2^{m-l}$ para toda $2 \leq l \leq m$ y

$$|-1+2^l \bmod 2^m| = \begin{cases} 2^{m-l} & \text{si } l < m \\ 2 & \text{si } l = m. \end{cases}$$

Luego, si $l_1,\ l_2 \in \{2, \ldots m\}$ y $l_1 \neq l_2$, tenemos

$$\langle [1+2^{l_1}] \rangle \neq \langle [1+2^{l_2}] \rangle, \quad \langle [-1+2^{l_1}] \rangle \neq \langle [-1+2^{l_2}] \rangle \quad \text{y}$$

$$\langle [1+2^{l_1}] \rangle \neq \langle [-1+2^{l_2}] \rangle.$$

Para probar $\langle [1+2^l] \rangle \neq \langle [-1+2^l] \rangle$ con $2 \leq l \leq m$, basta probar que la congruencia $(1+2^l)^k \equiv -1+2^l \bmod 2^m$, con $k < 2^{m-1}$ impar, no tiene solución. Supongamos que la tiene:

$$\begin{array}{rcll} 1+\sum_{i=1}^{k} 2^{il} & \equiv & -1+2^l & \bmod 2^m \Rightarrow \\ \sum_{i=1}^{k} 2^{il} & \equiv & -2+2^l & \bmod 2^m \Rightarrow \\ \sum_{i=1}^{k} 2^{il} & \equiv & 2(2^{l-1}-1) & \bmod 2^m. \end{array}$$

Entonces $\sum_{i=1}^{k} 2^{il-1} - 2^{l-1} + 1 = 2^{m-1}x$, p. a. $x \in \mathbb{Z}$, mas

$$\sum_{i=1}^{k} 2^{il-1} - 2^{l-1} + 1 = \sum_{i=2}^{k} 2^{il-1} + 1,$$

que es impar, por lo tanto la congruencia no tiene solución y concluimos la afirmación.

1.3. Regularidad

Definición 1.22. Si G es un p-grupo finito, $\mathbf{\Omega_n(G)}$ denota el subgrupo generado por todos los elementos de orden p^n y $\mathbf{\mho_n(G)}$ denota el subgrupo generado por las potencias p^n-ésimas de los elementos de G.

Un p-grupo G es **regular** si para cualesquiera dos elementos x y y de G, existe un elemento c en $\mho_1(H')$, $(H = \langle x,\ y \rangle)$ tal que $x^p y^p = (xy)^p c$.

No es difícil verificar que subgrupos y grupos cociente de un p-grupo regular son regulares.

Para entrar en materia debemos, desde luego, recordar la siguiente fórmula de P. Hall. Definimos, de manera inductiva, los ***conmutadores superiores*** $C_1(G) = G$ y $C_{i+1}(G) = [C_i(G),\ G]$.

Teorema 1.23 (4.3.5 en [9]). *Si x y y son elementos de un grupo G y $n \geq 2$ un entero, entonces*

$$x^n y^n = (xy)^n c_2^{e_2} \cdots c_n^{e_n}.$$

Donde c_r es un elemento de $C_r(\langle x, y\rangle)$ y el exponenete e_r es el $r-$ésimo coeficiente binomial

$$e_r = n(n-1)\cdots(n-r+1)/r!$$

El siguiente lema nos permitirá concluir que todo p-grupo metacíclico con p impar es regular.

Lema 1.24 (4.3.13 en [9]). *Sea G un p-grupo. Si $C_{p-1}(G)$ es cíclico, entonces G es regular. Si $p > 2$ y $C_2(G)$ es cíclico, entonces G es regular.*

Prueba. Sea G un p-grupo con $C_{p-1}(G)$ cíclico. Si p=2, entonces $G = C_1(G)$ es cíclico por hipótesis y por tanto regular. Supongamos $p>2$. Sean x y y dos elementos de G y sea $H = \langle x, y\rangle$. Entonces $C_{p-1}(H) \subset C_{p-1}(G)$ y por lo tanto $C_{p-1}(H)$ es cíclico. Si $C_{p-1}(H) \neq 1$, como G es nilpotente, entonces $C_p(H)$ es un subgrupo propio de $C_{p-1}(H)$. Luego, un generador de $C_p(H)$ pertenece a $\mho_1(H')$.

Para terminar, aplicamos la fórmula 1.23 a x y y con $n=p$ obteniendo

$$x^p y^p = (xy)^p c_2^{e_2} \cdots c_p^{e_p}, \quad c_r \in C_r(H) \text{ y}$$

$$e_r = p(p-1)\cdots(p-r+1)/r!$$

Así que los exponentes $e_2, \ldots e_{p-1}$ son divisibles por p y no importa que $e_p = 1$, ya que $c_p \in C_p(H) \subset \mho_1(H')$. Esto prueba que G es regular.

Si suponemos $p > 2$ y $C_2(G)$ cíclico, entonces $C_{p-1}(G) \subset C_2(G)$ de donde se sigue el resultado.

Corolario 1.25. *Si P es un p-grupo metacíclico con p impar, entonces P es regular.*

Lema 1.26 (4.3.14 en [9]). *Sea G un p-grupo regular, entonces para todo x, y en G y todo entero no negativo n tenemos:*

$$(x^{-1}y)^{p^n} = 1 \Leftrightarrow x^{p^n} = y^{p^n}$$

Prueba. Sea (R_n) la proposición

$$(R_n) : x^{p^n} = y^{p^n} \Rightarrow (x^{-1}y)^{p^n} = 1.$$

Probaremos (R_n) por inducción sobre n.

Base de inducción:

Usamos inducción sobre $|G|$. Supongamos $x^p = y^p$, que G no es abeliano y que $\langle x,\ y\rangle = G$.

Sea M un subgrupo maximal de G que contenga a x. Por 1.14, M es normal en G y de índice p. Como $x^p = y^p$ tenemos:

$$1 = [y^p,\ y] = [x^p,\ y] = x^{-p}(x^p)^y = x^{-p}(x^y)^p.$$

Es decir, x y x^y son elementos de M tales que $x^p = (x^y)^p$. Por hipótesis inductiva, (R_1) se satisface en M, entonces tenemos $(x^{-1}x^y)^p = 1$, concluyendo que $[x,\ y]$ tiene orden p. Como $G = \langle x,\ y\rangle$, entonces un elemento $b \neq 1$ en $G' \leqslant M$ es el producto de elementos de la forma $[x,\ y]^u$ con $u \in G$, pero $([x,\ y]^u)^p = ([x,\ y]^p)^u = 1$, entonces b es el producto de elementos de orden p. Dado que R_1 se satisface en M, entonces b tiene orden p . En particular, $\mho_1(G') = 1$. Pero, por hipótesis, G es regular, luego $x^{-p}y^p = (x^{-1}y)^p c$ donde c es un elemento de $\mho_1(G')$, por tanto $c = 1$ y $(x^{-1}y)^p = x^{-p}y^p = 1$. Con lo que terminamos la base inductiva.

Supongamos ahora $x^{p^n} = y^{p^n}$. Como la hipótesis inductiva es (R_{n-1}), tenemos $(x^{-p}y^p)^{p^{n-1}} = 1$, es decir, $x^{-p}y^p$ pertenece a $\Omega_{n-1}(G)$. El grupo cociente $G/\Omega_{n-1}(G)$ es regular, aplicando R_1 a este obtenemos que $(x^{-1}y)^p$ está en $\Omega_{n-1}(G)$.

Pero, como (R_{n-1}) se satisface, el grupo $\Omega_{n-1}(G)$ consiste de elementos cuyo orden es, a lo más, p^{n-1}, lo que nos lleva a

$$((x^{-1}y)^p)^{p^{n-1}} = (x^{-1}y)^{p^n} = 1.$$

Esto prueba que (R_n) se satisface en G.

Sea (S_n) la proposición

$$(S_n) : (x^{-1}y)^{p^n} = 1 \ \Rightarrow\ x^{p^n} = y^{p^n}.$$

Probamos primero que (S_1) se cumple.

Supongamos $(x^{-1}y)^p = 1$. Entonces

$$(xy^{-1})^{-p} = (yy^{-1}xy^{-1})^{-p} = y(x^{-1}y)^p y^{-1}$$

Luego, por (R_1), tenemos

$$1 = (xy^{-1}x^{-1}y)^p = [x^{-1},\ y]^p$$

Como en la prueba de (R_1), observamos que los elementos del conmutador de $\langle x,\ y\rangle$ tienen orden, a lo más, p. Luego, por la regularidad de G, $x^{-p}y^p = (x^{-1}y)^p = 1$.

Supongamos ahora que $(x^{-1}y)^{p^n} = 1$. Entonces $(x^{-1}y)^p \in \Omega_{n-1}(G)$. Como en el grupo cociente $G/\Omega_{n-1}(G)$ se cumple (S_1), tenemos que $x^{-p}y^p$ pertenece a $\Omega_{n-1}(G)$. Por (R_{n-1}), los elementos del subgrupo $\Omega_{n-1}(G)$ tienen orden, a lo más, p^{n-1}. Luego $(x^{-p}y^p)^{p^{n-1}} = 1$, y por (S_{n-1}), $(x^p)^{p^{n-1}} = (y^p)^{p^{n-1}}$. Es decir, (S_n) se cumple en G.

1.4. Solubilidad

Sea π un conjunto no vacío de primos. Un **π-número** es un entero positivo cuyos primos divisores pertenecen a π y un π'-número es aquel cuyos primos divisores no pertenecen a π. Un elemento de un grupo es llamado un **π-elemento** si su orden es un π-número. Si todo elemento es un π-elemento, el grupo es llamado un **π-grupo**, análogamente podemos definir π'-elemento y π'-grupo.

Si H y K son π-subgrupos de un grupo G y K es normal, entonces claramente HK es un π-grupo. Consecuentemente el subgrupo generado por todos los π-subgrupos normales de G es un π-grupo.

Definición 1.27. Dados π un conjunto no vacío de primos y G un grupo, el subgrupo generado por todos los π-subgrupos normales de G será denotado por $\mathbb{O}_\pi(G)$. Éste es el único π-subgrupo de G que es maximal normal.

Un **π-subgrupo de Sylow** se define como un π-subgrupo maximal. Los π-subgrupos de Sylow siempre existen pero, usualmente, no son conjugados si π contiene más de un primo, paga grupos finitos solubles es más conveniente considerar la siguiente definición.

Definición 1.28. Sea G un grupo finito y H un π-subgrupo tal que $[G : H]$ es un π'-número, llamaremos a H un **π-subgrupo de Hall** de G.

Es claro que todo π-subgrupo de Hall es un π-subgrupo de Sylow, sin embargo, en general, G no necesariamente contiene un π-subgrupo de Hall.

Lema 1.29 (9.1.1 en [6]). *Sean G un grupo y π un conjunto de primos, $\mathbb{O}_\pi(G)$ es la intersección de todos los π-subgrupos de Sylow de G.*

Teorema 1.30 (9.1.7 en [6]). *Si G es un grupo finito soluble, entonces todo π-subgrupo está contenido en un π-subgrupo de Hall de G. Más aún, todos los π-subgrupos de Hall de G son conjugados.*

Teorema 1.31 (9.1.8 en [6]). *Sea G un grupo finito y supongamos que para cada primo p hay un p'-subgrupo de Hall. Entonces G es soluble.*

Si tenemos $|G| = p_1^{e_1} \dots p_k^{e_k}$ y suponemos que Q_i es un p_i'-subgrupo de Hall de G, entonces llamamos al conjunto $\{Q_1, \dots, Q_k\}$ un **sistema de Sylow** de G. De los dos lemas anteriores se obtiene que un grupo finito tiene un sistema de Sylow si, y sólo si, es soluble.

Lema 1.32 (9.2.1 en [6]). *Sea $\{Q_1, \dots, Q_k\}$ un sistema de Sylow para un grupo finito soluble G. Si $\tau \neq \varnothing$ es un conjunto de primos, entonces $\bigcap_{p_i \notin \tau} Q_i$ es un τ-subgrupo de Hall de G.*

Prueba. Sea $M = \bigcap_{p_i \notin \tau} Q_i$. No es difícil verificar que el mapeo definido del conjunto de las clases laterales izquierdas de M en el producto cartesiano de los Q_i, $p_i \notin \tau$, $gM \mapsto (gQ_i)_{p_i \notin \tau}$, es inyectivo, luego

$$[G : M] \leq \prod_{p_i \notin \tau} [G : Q_i] = \prod_{p_i \notin \tau} p_i^{e_i}.$$

Sabemos que cada $[G : Q_i]$ divide a $[G : M]$. Como $[G : Q_i] = p_i^{e_i}$, entonces su producto divide a $[G : M]$ y tenemos $[G : M] = \prod_{p_i \notin \tau} p_i^{e_i}$, lo que muestra que M es un τ-subgrupo de Hall de G.

Teorema 1.33 (P. Hall, 9.2.3 en [6]). *En un grupo finito soluble G cualesquiera dos sistemas de Sylow son conjugados.*

Claramente un grupo metacíclico es soluble, de hecho tiene una serie normal cuyos elementos son subgrupos normales y cada grupo factor es cíclico, es decir, es **supersoluble**.

El siguiente lema muestra que, en un grupo metacíclico, el p'-subgrupo de Hall, también llamado complemento de Sylow, para p el primo divisor más pequeño del orden de G es normal. Esto nos permitirá, en el Capítulo 3, construir la descomposición de Hall estándar para grupos metacíclicos finitos.

Proposición 1.34 (2.6 en [8]). *Si $p_1 < p_2 < \cdots < p_r$ es la secuencia creciente de todos los primos divisores del orden de un grupo metacíclico G, entonces cada π_i-subgrupo de Hall de G es normal para $\pi_i = \{p_i, \dots, p_r\}$. En particular, el subgrupo de Sylow para el primo divisor más grande es normal.*

Prueba. Dividimos la prueba en un par de lemas.

Lema 1.34.1 (10.5.2 en [3]). *Un grupo finito supersoluble G tiene una serie normal $G = B_0 \geq \cdots \geq B_k = 1$ en la que cada B_i es normal en G y cada grupo factor B_{i-1}/B_i es cíclico de orden primo.*

Prueba. G tiene una serie normal $G = A_0 \geq \cdots \geq A_r = 1$ con $A_i \trianglelefteq G$ y cada A_{i-1}/A_i cíclico. Sean $p_1, \ldots, p_k$ los primos divisores del orden de G no necesariamente distintos. Si $|A_{i-1}/A_i| = p_1 \cdots p_s$, entonces A_{i-1}/A_i tiene un único subgrupo de orden $p_1, p_1p_2, \ldots, p_1 \cdots p_{s-1}$ y son subgrupos característicos. Como A_{i-1} es normal en G, la conjugación por un elemento de G define un automorfismo de A_{i-1}/A_i, luego, los $s-1$ subgrupos correspondientes entre A_{i-1} y A_i son normales en G.

Refinando de esta forma cada grupo factor A_{i-1}/A_i, obtenemos una serie normal en la que cada factor es cíclico de orden primo.

Lema 1.34.2 (10.5.3 en [3]). *Un grupo finito supersoluble G tiene una serie normal $G = C_0 \geq \cdots \geq C_k = 1$ ($C_i \trianglelefteq G$) en la que cada C_{i-1}/C_i es cíclico de orden primo y si C_{i-1}/C_i y C_i/C_{i+1} son de órdenes p_i y p_{i+1} tenemos $p_i \leqslant p_{i+1}$.*

Prueba. Por la proposición anterior, G tiene una serie normal $G = B_0 \geq \cdots \geq B_k = 1$ en la que $B_i \trianglelefteq G$ y para cada i, B_{i-1}/B_i y B_i/B_{i+1} son cíclicos de orden primo q y p respectivamente. Supongamos $q > p$, B_{i-1}/B_{i+1} tiene orden pq y por tanto tiene un subgrupo característico de orden q, sea éste B_i^*/B_{i+1}. Luego, como en el lema anterior, B_i^* es normal en G. Si remplazamos B_i por B_i^*, entonces $|\, B_{i-1}/B_i^* \,| = p$ y $|\, B_i^*/B_{i+1} \,| = q$. Continuando con este proceso, el cual no altera la longitud de la serie normal, llegaremos a una serie en la que los órdenes de grupos factores consecutivos son primos y no aumentan.

Supongamos ahora $|\, G \,| = p_1^{e_1} \cdots p_r^{e_r}$. Como G es supersoluble, por la proposición anterior, tiene una serie normal $G = C_0 \geq \cdots \geq C_k = 1$, ($B_i \trianglelefteq G$) con:

$$\left|\frac{C_0}{C_1}\right| = p_1, \ldots, \left|\frac{C_{a-1}}{C_a}\right| = p_1 \quad \text{y} \quad \left|\frac{C_a}{C_{a+1}}\right| = p_2,$$

y así sucesivamente, por lo que un elemento de la serie, digamos C_z es tal que $|C_0/C_z| = p_i^{e_i} \cdots p_r^{e_r}$, es decir, es un π_i-subgrupo de Hall de G.

Lema 1.35 (5.2.3 en [2]). *Sea A un p'-grupo de automorfismos del grupo abeliano G. Entonces tenemos*

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

Lema 1.36 (Corolario, p. 74 en [9]). *Sea p un primo impar. Supongamos que un p'-grupo Q actúa en un p-grupo P y que Q actúa trivialmente en $\Omega_1(P)$. Entonces la acción de Q en P es trivial.*

Capítulo 2

p-grupos metacíclicos

2.1. p-grupos metacíclicos con p primo impar

En el siguiente capítulo, dado un grupo metacíclico finito G, le construiremos una descomposición semidirecta que tendrá un factor nilpotente. Razón por la cual, explorar algunas propiedades de los p-grupos metacíclicos es de crucial importancia. Como consecuencia de este estudio, tendremos una forma canónica de presentación para los p-grupos metacíclicos con p impar.

Empezaremos estudiando los núcleos de los p-grupos metacíclicos. Desde luego, en esta sección nos interesaremos más por los núcleos de p-grupos metacíclicos con p impar, sin embargo, uno de nuestros resultados es aplicable a p-grupos metacílicos arbitrarios, y una muestra de su utilidad es el cálculo de $\exp G$.

Sobre los núcleos

Definición 2.1. El **subgrupo de Frattini** de un grupo arbitrario G es la intersección de todos los subgrupos maximales de G. Se denota por $\Phi(G)$. Si G no tiene subgrupos maximales, entonces $\Phi(G) := G$.

Un elemento g en G será llamado un **no generador** de G si $G = \langle g,\ X\rangle$ siempre implica $G = \langle X\rangle$.

El subgrupo de Frattini cumple la siguiente propiedad.

Lema 2.2 (5.2.12 en [6]). *En cualquier grupo G el subgrupo de Frattini es igual al conjunto de no generadores de G.*

Lema 2.3. *Sea G un grupo finito. Si N es un subgrupo normal de G entonces $\Phi(G)N/N \leqslant \Phi(G/N)$.*

Prueba. Si x es un elemento de $\Phi(G)$ entonces x pertenece a todo subgrupo maximal de G, en particular a aquellos que contienen a N, luego xN es un elemento de todo subgrupo maximal de G/N.

Lema 2.4 (2.10 en [8]). *Si P es un p-grupo metacíclico no cíclico, entonces:*

(i) $P/\Phi(P) \cong \mathsf{C}(p) \times \mathsf{C}(p)$.

(ii) $\Omega_1(P) \cong \mathsf{C}(p) \times \mathsf{C}(p)$, *para p impar.*

Prueba. (i) Si M es un subgrupo maximal de P, entonces M es normal en P y de índice p, luego P/M es abeliano, por lo que $P' \leqslant M$; más aún P/M tiene exponente p, esto es x^p está en M para todo x en P, luego $P'\mho_1(P) \leqslant \Phi(P)$.

Ahora observemos que $P/P'\mho_1(P)$ es un grupo abeliano de exponente p, por lo tanto, abeliano elemental. Claramente tenemos $\Phi(P/P'\mho_1(P)) = 1$ y, por 2.3,

$$\Phi(P/P'\mho_1(P)) \geqslant \Phi(P)P'\mho_1(P)/P'\mho_1(P),$$

luego $\Phi(P)P'\mho_1(P)/P'\mho_1(P) = 1$, así concluimos $P'\mho_1(P) = \Phi(P)$. Finalmente, como $P/\Phi(P)$ es un grupo metacíclico de exponente p entonces $|P/\Phi(P)| \leq p^2$. Supongamos $P/\Phi(P) \cong \mathsf{C}(p)$, con un generador $a\Phi(P)$. Como P no es cíclico, a pertenece a algún subgrupo maximal de P, digamos H. Entonces $H/\Phi(P)$ sería un subgrupo maximal de $P/\Phi(P)$ lo que es contradictorio. Por lo tanto $P/\Phi(P) \cong \mathsf{C}(p) \times \mathsf{C}(p)$.

(ii) Como P es regular, por el Lema 1.26, $\Omega_1(P)$ es en realidad el conjunto de todos los elementos de P de orden menor o igual que p. Como p es impar, si $\Omega_1(P)$ fuera cíclico, por el Corolario 1.18, P sería cíclico. Es decir, $\Omega_1(P)$ es un grupo metacíclico de exponenete p no cíclico, por tanto es de orden p^2, luego $\Omega_1(P) \cong \mathsf{C}(p) \times \mathsf{C}(p)$.

Lema 2.5 (2.11 en [8]). *Sea P un p-grupo metacíclico no cíclico y K un subgrupo de P. Entonces:*

(i) Si p es impar, K es cíclico si y sólo si K no contiene a $\Omega_1(P)$.

(ii) K es normal y P/K es cíclico si y sólo si K contiene a P' y K no está contenido en $\Phi(P)$.

Prueba. (i) Por el Lema 2.4, $\Omega_1(P)$ es isomorfo a $\mathsf{C}(p) \times \mathsf{C}(p)$. Supongamos que K no es cíclico. Entonces $\Omega_1(K)$ es también isomorfo a $\mathsf{C}(p) \times \mathsf{C}(p)$, es decir $\Omega_1(P) = \Omega_1(K)$, por lo tanto K contiene a $\Omega_1(P)$. Por otro lado, si K es cíclico, obviamente, no contiene a $\Omega_1(P)$.

(ii) '*sólo si*' Como K es normal y P/K es cíclico, obviamente K contiene a P'. Si K está contenido en $\Phi(P)$, entonces $P/\Phi(P)$, que es una imagen homomórfica del cíclico P/K, es cíclico, en contradicción con el Lema 2.4.

'*si*' Como K contiene a P', K es normal en P y como K no está contenido en $\Phi(P)$, $\Phi(P)$ está propiamente contenido en $\Phi(P)K$, es decir,

$$\frac{|P|}{|\Phi(P)K|} < \frac{|P|}{|\Phi(P)|} = p^2,$$

luego $P/\Phi(P)K$ es cíclico. Si $P = \Phi(P)K$, por 2.2, entonces P es cíclico, lo que no ocurre. Finalmente, ya que $\Phi(P/K)$ contiene a $\Phi(P)K/K$ y

$$\frac{|P/K|}{|\Phi(P)K/K|} = \frac{|P|}{|\Phi(P)K|} = p,$$

entonces $(P/K)/\Phi(P/K)$ es cíclico y, por el lema anterior, también P/K lo es.

Clasificación

Lema 2.6 (2.7 en [8]). *Sea G un grupo metacíclico con una factorización metacíclica $G = SK$. Sean $S = \langle x \rangle$, $K = \langle y \rangle$ y r un entero tal que $y^x = y^r$. Definimos $s := |r \bmod |K||$ y $t := |K| / (|K|,\ r-1)$. Entonces tenemos:*

$$G' = \langle y^{r-1} \rangle \cong \mathsf{C}(t), \quad Z(G) = \langle x^s,\ y^t \rangle \ \text{ y } \ S/\mathbb{C}_S(K) \cong \mathsf{C}(s).$$

Prueba. G' es generado por y^{r-1} y sus conjugados, mas $\langle y^{r-1} \rangle$ es un subgrupo característico de K, luego $G' = \langle y^{r-1} \rangle$ y claramente $|G'| = t$.

Como s es el mínimo entero positivo tal que $r^s \equiv 1 \bmod |K|$, entonces $\mathbb{C}_S(K) = \langle x^s \rangle$ y a su vez $\mathbb{C}_K(S) = \langle y^t \rangle$, luego $\langle x^s,\ y^t \rangle \leqslant Z(G)$. Por otro lado, si $x^i y^j \in Z(G)$ entonces

$$x^i y = (x^i y^j) y y^{-j} = y x^i, \quad x y^j = x^{-i} x (x^i y^j) = y^j x,$$

es decir $x^i \in \mathbb{C}_S(K)$ y $y^j \in \mathbb{C}_K(S)$, y concluimos $Z(G) = \langle x^s,\ y^t \rangle$. Finalmente tenemos $S/\mathbb{C}_S(K) = \langle x \rangle / \langle x^s \rangle \cong \mathsf{C}(s)$.

Corolario 2.7 (2.8 en [8]). *Sea P un p-grupo metacíclico con p impar y sea $P = SK$ una factorización metacíclica. Entonces $S/\mathbb{C}_S(K) \cong P'$.*

Prueba. Como S es un p-grupo finito, si $\langle x \rangle = S$, $x^{p^i} = 1$ para algún entero no negativo i, luego $r^{p^i} \equiv 1 \bmod p$, entonces por el Pequeño Teorema de Fermat $r \equiv 1 \bmod p$. Finalmente, por la Proposición 1.9(i), $s = t$.

Lema 2.8 (3.1 en [8]). *Sea P un p-grupo metacíclico con p impar. Si $K \trianglelefteq P$ y P/K son cíclicos, entonces existe un subgrupo cíclico S de P tal que $P = SK$ y $|S| = \exp P$.*

Prueba. Sea $P = S_0K$ una factorización metacíclica. Como P es regular, del Lema 1.26 obtenemos $\exp P = \max\{|S_0|, |K|\}$. Si $|K| \neq \exp P$, entonces $|S_0| = \exp P$. Así que supongamos $|K| = \exp P$ y $|S_0| < |K|$. También podemos suponer que P no es cíclico. Definimos $S = \langle ab^{-1} \rangle$, donde a y b son generadores de S_0 y K, respectivamente. Sea $|K| = p^{k+1}$. Como $|S_0| < |K|$, entonces $a^{p^k} = 1 \neq b^{p^k}$. De esto y la regularidad de P obtenemos $(ab^{-1})^{p^i} \neq 1$ para todo $i \leq k$, de donde se sigue $|S| = \exp P$. Sabemos que $SK = P$ porque a y b están contenidos en SK.

Si Y es un subgrupo de un grupo H, decimos que X es un **suplemento** para Y en H si $XY = H$. Si $Y \cap X = 1$, llamaremos a X un **complemento** de Y en H.

Corolario 2.9 (3.2 en [8]). *Sea H un grupo metacíclico nilpotente de orden impar. Si Y es un subgrupo normal cíclico de H tal que H/Y también es cíclico, entonces existe un suplemento cíclico X, para Y en H tal que $|X| = \exp H$.*

Prueba. Sean $p_1, \ldots, p_r$ los primos que dividen al orden de H. Definimos $Y_i = Y \cap H_i$ por cada H_i, p_i-subgrupo de Sylow de H. Como cada Y_i es un subgrupo característico de Y, entonces $Y_i \trianglelefteq G$ para toda $i = 1, \ldots, r$ y $H_i/Y_i \cong YH_i/Y \leqslant H/Y$, es decir H_i/Y_i es cíclico. Por el lema anterior, existe S_i subgrupo cíclico de H_i tal que $H_i = S_iY_i$ y $|S_i| = \exp H_i$. Entonces $H = P_1 \cdots P_r = S_1Y_1 \cdots S_rY_r$, así que $H = S_1 \cdots S_rY_1 \cdots Y_r$. Claramente $Y = Y_1 \cdots Y_r$ y $X := S_1 \cdots S_r$ es un subgrupo cíclico de H cuyo orden es $\exp H$.

Lema 2.10 (3.3 en [8]). *Sean p un primo y $P = SK$ una factorización metacíclica de un p-grupo P. Sea C un subgrupo propio de P que contiene a K. Entonces todo suplemento de C en P es un suplemento de K.*

Prueba. El resultado es obvio si P es cíclico, así que podemos suponer que P no es cíclico. Por el Lema 2.5(ii), K no está contenido en $\Phi(P)$ y $C\Phi(P)$ es un subgrupo propio de P, porque C lo es. Luego, por el Lema 2.4(i),

$$1 \neq \frac{|P|}{|C\Phi(P)|} = p^2 \frac{|C \cap \Phi(P)|}{|C|},$$

y tenemos $|C|/|C \cap \Phi(P)| = 1$ ó p, pero si $|C|/|C \cap \Phi(P)| = 1$ entonces K estaría contenido en $\Phi(P)$ lo cual no sucede. Entonces $|C|/|C \cap \Phi(P)| = p$, y por lo tanto $|P|/|C\Phi(P)| = p = |P|/|K\Phi(P)|$, por la prueba del Lema 2.5(ii). Así obtenemos que $K\Phi(P) = C\Phi(P)$. Entonces si X es un suplemento de C en P, $XK\Phi(P) = XC\Phi(P) = P$, y, por lo tanto, $XK = P$.

Definición 2.11. Sea P un p-grupo metacíclico con p impar. Para un subgrupo C de P, consideremos el conjunto

$$\{K : K \leqslant C,\ K \trianglelefteq P,\ K \text{ y } P/K \text{ cíclicos}\}.$$

Los grupos de orden mínimo en este conjunto serán llamados ***núcleos* C-*minimales***. Una factorización metacíclica $P = SK$ es llamada **C-*estándar*** si $|S| = \exp P$ y K es un núcleo C-minimal.

Del Lema 2.8, observamos que P tiene una factorización metacíclica C-estándar si el conjunto definido arriba es no vacío.

Lema 2.12 (3.4 en [8]). *Sea P un p-grupo con p primo impar, y $P = SK$ una factorización metacíclica. Definimos α, β, γ y δ como sigue:*

$$p^\alpha = [S : S \cap K],\ p^\beta = [K : S \cap K],\ p^\gamma = |K|,\ p^\delta = [K : P'].$$

Entonces

(i) $\gamma \geq \beta,\ \beta + \delta \geq \gamma \geq \delta$;

(ii) si $\delta = 0$, *entonces* $\beta = 0$.

Si $P = SK$ es C-estándar para un subgrupo C de índice p^κ conteniendo a K, entonces

(iii) $\alpha \geq \beta$;

(iv) si $\beta < \delta$, *entonces* $\alpha - \kappa < \beta$.

En cualquier caso, P tiene la siguiente presentación

$$\langle x,\ y \mid x^{p^\alpha} = y^{p^\beta},\ y^{p^\gamma} = 1,\ y^x = y^{1+p^\delta} \rangle.$$

Prueba. De la definición de los parámetros obtenemos

$$|P| = p^{\gamma+\alpha},\quad |P'| = p^{\gamma-\delta},\quad |S \cap K| = p^{\gamma-\beta},\quad |S| = p^{\alpha+\gamma-\beta}.$$

Probaremos la última relación de esta presentación suponiendo que P no es abeliano, ya que es obvia si lo es. Como $S/\mathbb{C}_S(K) \cong P'$ por el Corolario 2.7, S actúa en K como un grupo de automorfismos de orden $p^{\gamma-\delta}$. Por otro lado, de la Proposición 1.9(i), tenemos que $b \mapsto b^{1+p^\delta}$ define un automorfismo de orden $p^{\gamma-\delta}$. Por el Teorema 1.19, Aut K es cíclico, luego tiene un solo subgrupo de este orden, así que podemos elegir un x en S tal que $b^x = b^{1+p^\delta}$ para todo b en K, es decir $x\mathbb{C}_S(K)$ genera $S/\mathbb{C}_S(K)$. Como P no es abeliano, $|S/\mathbb{C}_S(K)| = p^t$ con $t > 0$. Si $\langle x_0 \rangle = S$, con $x = x_o^m$ entonces $(m,\ p^t) = 1$ es decir, $(m,\ p) = 1$ y tenemos $\langle x \rangle = S$. Claramente $\gamma \geq \beta$. Si $\gamma = \beta$, fácilmente observamos que $x^{p^\alpha} = y_0^{p^\beta}$ donde $\langle y_0 \rangle = K$. Si $\gamma - \beta > 0$, entonces $x^{p^\alpha} = (y_0^{p^\beta})^n$ y este último tiene orden $p^{\gamma-\beta}$ por lo que $(n,\ p^{\gamma-\beta}) = 1 \Rightarrow (n,\ p) = 1$ y $\langle y_0^n \rangle = K$. Así que, definiendo $y := y_0^n$ tenemos

$$x^{p^\alpha} = y^{p^\beta},\ y^{p^\gamma} = 1,\ y^x = y^{1+p^\delta}.$$

Entonces P es una imagen homomórfica del grupo presentado por

$$\langle x,\ y \mid x^{p^\alpha} = y^{p^\beta},\ y^{p^\gamma} = 1,\ y^x = y^{1+p^\delta} \rangle.$$

Pero esta presentación da origen a un grupo de orden menor o igual que $p^{\alpha+\gamma}$, así que P es isomorfo al grupo definido por ella.

$\gamma \geq \delta$ porque $P' \leqslant K$. Del hecho de que $y^{p^\beta} = (y^{p^\beta})^x = y^{p^\beta(1+p^\delta)}$, se sigue $\beta + \delta \geq \gamma$. Esto completa la prueba de (i). Para probar (ii), observamos primero que si $\delta = 0$ y P es cíclico, claramente tenemos $\beta = 0$. Supongamos entonces $\beta \geq 1$ y que P no es cíclico. El subgrupo de Frattini $\Phi(P)$ contiene al conmutador P', pero, por el Lema 2.5(ii), no contiene a K, así que P' es un subgrupo propio de K y por tanto $\delta \geq 1$.

Supongamos ahora que $P = SK$ es C-estándar. Como $\exp P = |S| = p^{\alpha+\gamma-\beta}$, entonces $p^{\alpha+\gamma} = \exp P\, p^\beta$, mas $\exp P$ es un múltiplo de p^γ, luego $\alpha \geq \beta$ y tenemos (iii). Supongamos $\beta < \delta$, es decir $P' \leqslant S \cap K$, queremos probar $\alpha - \kappa < \beta$.

Como $|K|$ divide a $|S|$, entonces $|S/P'|$ es un múltiplo de $|K/P'|$. Además P/P' es abeliano finito por lo que, si $p^r = |S/P'|$, para cualquier elemento zP' en P/P' tenemos $(zP')^{p^r} = P'$ y con ello $\exp(P/P') | p^r$, pero p^r es el orden de xP', luego $\exp(P/P') = |S/P'|$. Ahora podemos aplicar el Lema 1.6 a P/P' y obtenemos un subgrupo T de P, tal que $ST = P$ y $S \cap T = P'$. Más aún, S/P' y T/P' son cíclicos, el último por ser isomorfo a $K/(S \cap K)$, y como $|ST| = |SK|$, entonces $|T| = p^{\gamma-\delta+\beta} < p^\gamma$ ya que estamos suponiendo $\beta < \delta$.

Supongamos que T no es cíclico. Sea ϕ un isomorfismo de T/P' en un subgrupo de S/P', digamos W/P'. Definimos

$$Y = \{ts : \phi(tP') = sP',\ t \in T\}.$$

Aplicamos el Teorema 1.7 a $(T/P',\ 1,\ W/P',\ 1,\ \phi)$, entonces Y es un subgrupo tal que $S \cap Y = T \cap Y = P'$. Por el Lema 2.5(i), $P'\Omega_1(P) \leqslant T$, esto implica que Y no contiene a $\Omega_1(P)$ ya que de no ser así, $P'\Omega_1(P) \subseteq T \cap Y$ y P' no sería cíclico, lo que es contradictorio, por lo tanto Y es cíclico. Además Y es normal en P porque $P' \leqslant Y$. Nuevamente por el Lema 1.7 $|Y| = |T|$, luego $|Y| < |K|$. Con esto tenemos que $|P/P'| = |S/P'||Y/P'|$, y como $S \cap Y = P'$, entonces $P = SY$ y Y es un subgrupo normal cíclico de P tal que P/Y es cíclico.

Si T es cíclico, definimos $Y := T$, así que también se tiene $|Y| < |K|$. Por lo tanto, en cualquier caso tenemos un subgrupo cíclico normal Y tal que P/Y es cíclico, y $|Y| < |K|$. Finalmente, si suponemos $\alpha - \kappa \geq \beta$, entonces $|Y/P'| \leq |C/K|$, luego

$$\left|\frac{YK}{K}\right| = \left|\frac{Y}{Y \cap K}\right| \leq \left|\frac{Y}{P'}\right| \leq \left|\frac{C}{K}\right|.$$

Como P/K es cíclico, entonces $YK/K \leqslant C/K$, luego $Y \leqslant C$. Pero $P = SY$ es también una factorización metacíclica, esto contradice la C-minimalidad de K. Por lo tanto $\alpha - \kappa < \beta$.

Aplicaremos este lema con $C = P$, obteniendo un teorema de clasificación para p-grupos metacíclicos con p impar.

Teorema 2.13 (3.5 en [8]). *Con p impar, todo p-grupo metacíclico no cíclico P tiene una presentación de la forma*

$$P = \langle a,\ b \mid a^{p^\alpha} = b^{p^\beta},\ b^{p^{\beta+\delta}} = 1,\ b^a = b^{1+p^\gamma} \rangle,$$

donde α, β, γ, δ son enteros no negativos, tales que $\alpha \geq \beta \geq \gamma \geq \delta$, y $\gamma \geq 1$. Inversamente, cada presentación de este tipo define un p-grupo metacíclico no cíclico de orden $p^{\alpha+\beta+\delta}$, distintos valores para los parámetros α, β, γ, δ (con la condición de arriba) dan grupos no isomorfos.

Prueba. El Lema 2.8 nos garantiza que podemos escoger una factorización metacíclica $P = SK$ tal que el orden de S sea $\exp P$ y K tenga el menor orden posible. Aplicando el último lema con $\kappa = 0$ y redefiniendo $p^\delta := |S \cap K|$ y $p^\gamma := |K/P'|$, obtenemos la presentación deseada. Como $\kappa = 0$, de 2.12(iii) y 2.12(iv) obtenemos $\alpha \geq \beta \geq \gamma$ y de 2.12(i) tenemos $\gamma \geq \delta$. $\gamma \geq 1$ se obtiene de 2.12(ii) y del hecho de que P no es cíclico. Inversamente, si α, β, γ, δ son enteros no negativos tales que $\alpha \geq \beta \geq \gamma \geq \delta$ y $\gamma \geq 1$, entonces $p + \gamma \geq 4$ y $\alpha \geq \beta \geq \beta + \delta - \gamma$, con lo que podemos aplicar el Corolario 1.13 y obtenemos $(1 + p^\gamma)^{p^\alpha} \equiv 1 \bmod p^{\beta+\delta}$. Además $\beta + \delta \leq \beta + \gamma$, es decir $p^{\beta+\delta}$ divide a

$p^{\beta+\gamma}$, entonces, por el Lema 1.2 la presentación de arriba define un grupo metacíclico de orden $p^{\beta+\delta+\alpha}$.

Para la última afirmación, consideremos los grupos SP'/P' y K/P'. Dado que $\beta \geq \gamma$ tenemos $S \cap K \leqslant P'$, así que $S \cap P' = S \cap K$ y por tanto $|SP'/P'| = p^{\alpha}$, además por la Ley Modular de Dedekind tenemos $SP' \cap K = P'$, es decir

$$\frac{P}{P'} = \frac{SP'}{P'} \times \frac{K}{P'} \cong \mathsf{C}(p^{\alpha}) \times \mathsf{C}(p^{\gamma}),$$

así que α y γ son invariantes de P. Por otro lado, $\exp P = p^{\alpha+\delta}$ y $|P| = p^{\alpha+\beta+\delta}$ por lo que β y δ también son invariantes del grupo.

2.2. 2-grupos metacíclicos

Pero el dos no ha sido nunca un número
porque es una angustia y su sombra,
porque es la guitarra donde el amor se desespera,
porque es la demostración de otro infinito que no es suyo
y es las murallas del muerto
y es el castigo de la nueva resurrección sin finales.

Fragmento de 'Pequeño poema infinito', de Federico García Lorca.

Lema 2.14 (2.1 en [4]). *Sea G un grupo metacíclico con una presentación:*

$$\langle x,\ y \mid x^k = y^l,\ y^m = 1,\ y^x = y^r \rangle,$$

donde k, l, m y r son enteros positivos tales que $m|(r^k-1)$ y $m|l(r-1)$. Reemplazando y por una potencia adecuada del mismo, podemos suponer que $l|m$. Con tal l, tenemos $\exp G = m.c.m.(km/l,\ m)$.

Prueba. Sea $a = l/(m,\ l)$, claramente $(a,\ m) = 1$ por lo que $\langle y^a \rangle = \langle y \rangle$. Además $y^l = y^{a(m,\ l)}$ y $(m,\ l)$ divide a m. Remplazando y por y^a y l por $(m,\ l)$ tenemos la primera afirmación. Para la segunda tenemos $m.c.m.(km/l,\ m) = m.c.m.(|x|,\ |y|)$ y este múltiplo común divide a $\exp G$. Tomemos p el primo más pequeño que divide al orden de G y sea t el entero más grande tal que p^t divide a $m.c.m.(km/l,\ m)$. Como $\langle x \rangle \langle y \rangle$ es una factorización metacíclica de G, $\langle x \rangle_p \langle y \rangle_p$ es una factorización metacíclica de un p-subgrupo de Sylow P de G. Por la Proposición 1.34, $G = PN$ con N un p'-subgrupo de Hall normal. Por otro lado, si P es cíclico, claramente $(xy)^p = x^p y^p$ para todos $x,\ y \in P$. Sabemos que $\Phi(P)$ contiene a P', pero por 2.5(ii), si P no es cíclico; $\Phi(P)$ no contiene a K, luego P' es un subgrupo propio de K y $P' \leqslant \langle y \rangle_p^p$. Así que $P^p = \langle x \rangle_p^p \langle y \rangle_p^p$, y por inducción $P^{p^t} = 1$. Por lo tanto $G^{p^t} \leqslant N$. Repetimos este proceso para $N = P_0 N_0$, donde P_0 se define de manera análoga a P para q el primo divisor más pequeño del orden de N y N_0 es el respectivo complemento, obteniendo $G^{p^t q^{t_2}} \leqslant N^{q^{t_2}} \leqslant N_0$. Continuamos este procedimiento para primos progresivamente más grandes y tenemos

$$G^{m.c.m.(km/l,\ m)} \leqslant N^{m.c.m.(km/l,\ m)/p^t} \leqslant \cdots \leqslant 1.$$

Luego $(\exp G) \mid m.c.m.(km/l,\ m)$ y $(\exp G) = m.c.m.(km/l,\ m)$.

Lema 2.15 (4.5 en [4]). *Si P es el grupo presentado por*

$$\langle x,\ y \mid x^{p^k} = y^{p^l},\ y^{p^m} = 1,\ y^x = y^{1+p^n} \rangle,$$

donde $m-n \leq l \leq m$, $1 \leq n \leq m$ *y* $m-n \leq k$, *entonces* $Z(P) = \langle x^{p^{m-n}},\ y^{p^{m-n}} \rangle$. *Si* P *es el grupo presentado por*

$$\langle x,\ y \mid x^{2^k} = y^{2^l},\ y^{2^m} = 1,\ y^x = y^{-1+2^n} \rangle,$$

donde $m-1 \leq l \leq m$, $2 \leq n \leq m$ *y* $m-n \leq k$, *entonces* $Z(P) = \langle x^2,\ y^{2^{m-1}} \rangle$ *cuando* $m = n$, *en cualquier otro caso* $Z(P) = \langle x^{2^{m-n}},\ y^{2^{m-1}} \rangle$.

Prueba. Del Lema 2.14, sabemos que $Z(P) = \langle x^s, y^t \rangle$, con $s = |1+p^n \bmod p^m|$ y $t = p^m/(p^m,\ p^n)$. Para la primera presentación, claramente, $t = p^{m-n}$ y, por el Corolario 1.13, $s = p^{m-n}$, es decir, $Z(P) = \langle x^{p^{m-n}},\ y^{p^{m-n}} \rangle$. Para la segunda presentación, $t = 2^{m-1}$ y, por 1.13, $s = 2^{m-n}$, por lo que $Z(P) = \langle x^{2^{m-n}},\ y^{2^{m-1}} \rangle$, y si $m = n$, entonces $Z(P) = \langle x^2,\ y^{2^{m-1}} \rangle$.

Para la clasificación de los 2-grupos metacíclicos, Hempel dice haber tomado una clasificación no publicada de Newman y Xu que prefigura en [5], y la modifica un poco con miras a la clasificación de los grupos metacíclicos finitos. Para llegar a ella necesitaremos algunos lemas, el primero de ellos es parte del Teorema 5.4.3 en [2], en el que Gorenstein describe diversas propiedades de cuatro p-grupos metacíclicos; los dihédricos, cuaterniones generalizados, semidihédricos y los p-grupos $M_m(p)$.

Lema 2.16. *Los grupos de orden* 2^m*; dihédrico* D_m $(m \geq 2)$*, cuaterniones generalizados* Q_m $(m \geq 3)$*, semidihédrico* S_m $(m > 3)$ *y* $M_m(2)$ $(m > 3)$ *no son isomorfos.*

Prueba. Tomemos

$$M_m(2) = \langle x,\ y \mid x^2 = y^{2^{m-1}} = 1,\ y^x = y^{1+2^{m-2}} \rangle.$$

Si $z = [x,\ y] = y^{2^{m-2}}$, entonces

$$z^x = y^{(2^{m-2})(1+2^{m-2})} = y^{2^{2m-4}} y^{2^{m-2}} = z \quad \text{porque } m > 3,$$

luego, z conmuta con x y y. Del Lema 1.4 obtenemos

$$(xy^j)^2 = z^j y^{2j} = y^{2j+j2^{m-2}} = y^{2j(1+2^{m-3})},$$

luego xy^i tiene orden menor o igual a 2 si, y sólo si, $2j(1+2^{m-3}) \equiv 0 \bmod 2^{m-1}$, esto es, si y sólo si j es un múltiplo de 2^{m-2}. Por lo tanto $\Omega_1(M_m(2)) = \langle x,\ y^{2^{m-2}} \rangle \cong \mathsf{C}(2) \times \mathsf{C}(2)$. Ahora consideremos

$$D_m = \langle x,\ y \mid x^2 = y^{2^{m-1}} = 1,\ y^x = y^{-1} \rangle,$$

en este grupo tenemos $(xy)^2 = (xyx)y = y^{-1}y = 1$, así que xy y y tienen orden 2, luego $D_m = \langle x,\ y\rangle = \langle xy,\ y\rangle \subseteq \Omega_1(D_m)$, es decir $D_m = \Omega_1(D_m)$. Para

$$Q_m = \langle x,\ y \mid x^2 = y^{2^{m-2}},\ y^{2^{m-1}} = 1,\ y^x = y^{-1}\rangle$$

observamos

$$(xy^i)^2 = (xy^ix)y^i = y^{2^{m-2}}x^{-1}y^ixy^i = y^{2^{m-2}}$$

para toda i, luego xy^i nunca tiene orden 2. Entonces $\Omega_1(Q_m) = \langle y^{2^{m-2}}\rangle \cong \mathsf{C}(2)$. Finalmente, en

$$S_m = \langle x,\ y \mid x^2 = y^{2^{m-1}} = 1,\ y^x = y^{-1+2^{m-2}}\rangle$$

tenemos

$$(xy^i)^2 = (xy^ix)y^i = y^{i(-1+2^{m-2})}y^i = y^{i2^{m-2}},$$

así que xy^i tiene orden 2 si, y sólo si, i es par. Pero entonces $\Omega_1(S_m) = \langle xy^2,\ x\rangle = \langle y^2,\ x\rangle$. Si llamamos $y_1 = y^2$, entonces $o(y_1) = 2^{m-1}$ y

$$y_1^x = (y^2)^x = y^{2(-1+2^{m-2})} = y^{-2} = y_1^{-1},$$

es decir, $\Omega_1(S_m)$ es isomorfo a Q_{m-1}.

Tenemos entonces $|\Omega_1(D_m)| = 2^m$, $|\Omega_1(Q_m)| = 2$ y $|\Omega_1(S_m)| = 2^{m-1}$; así que, D_m, Q_m y S_m no son isomorfos. Por otro lado, $\Omega_1(M_m(2)) \cong \mathsf{C}(2)\times\mathsf{C}(2)$ por lo que $M_m(2)$ no es isomorfo a alguno de los otros tres grupos.

Lema 2.17 (4.1 en [4]). *Si m y n son enteros positivos, entonces*

$$\langle a,\ b \mid a^{2^m} = b^{2^{n+1}} = 1,\ b^a = b^{-1}\rangle \ncong \langle a,\ b \mid a^{2^m} = b^{2^{n+1}} = 1,\ b^a = b^{-1+2^n}\rangle.$$

Prueba. Escribiremos P_1 para el primer grupo y P_2 para el segundo. En $m = 1$, si $n = 1$, entonces P_2 es abeliano y P_1 no lo es. Si $n > 1$, entonces P_1 es dihédrico y P_2 es semidihédrico por lo que no son isomorfos. Supongamos entonces, $m \geq 2$. Para P_1, es claro que $2^{n+1}|((-1)^{2^m} - 1)$, luego, por el Lema 1.2, $|P_1| = 2^{m+n+1}$. Para P_2,

$$(-1+2^n)^{2^m} - 1 = \textstyle\sum_{i=1}^{2^m}\binom{2^m}{i}2^{ni}(-1)^{2^m-i},$$

y claramente 2^{n+1} divide a cada uno de estos sumandos, así que, por 1.2, P_2 también tiene orden 2^{m+n+1}. Para $i = 1,\ 2$, consideremos los conjuntos:

$$P_i^2 = \{g^2 \mid g \in P_i\}.$$

Sean i, j, enteros. En P_1 tenemos que si i es par, entonces $b^j a^i = a^i b^j$ y si i es impar, $b^j a^i = a^i b^{-j}$, luego

$$(a^i b^j)^2 = \begin{cases} a^{2i} b^{2j} & \text{si } 2|i \\ a^{2i} & \text{en cualquier otro caso.} \end{cases}$$

Claramente tenemos 2^{m-1} elementos a^k con k par y 2^n elementos b^r con r par, luego, 2^{m-2} elementos son de la forma a^{2i} con i par y 2^{m-2} lo son con i impar. Entonces $|P_1^2| = 2^{m+n-2} + 2^{m-2}$.

Ahora, en P_2 tenemos: Si i es par, desarrollando un binomio análogo al desarrollado al principio de esta prueba, $(-1+2^n)^i$ es congruente con 1 módulo 2^{n+1}, luego $b^j a^i = a^i b^j$; si i es impar y j es par, desarrollando ahora $j(-1+2^n)^i$ obtenemos que éste es congruente con $-j$ módulo 2^{n+1}, luego $b^j a^i = a^i b^{-j}$. Finalmente, si tanto i como j son impares, tenemos que los dos primeros sumandos del binomio $j(-1+2^n)^i$ son $-j$ y $2^n ij = 2^n(2r+1) = 2^{n+1}r + 2^n$, p. a. entero r, como el resto de lo sumandos es divisible por 2^{n+1}, entonces $j(-1+2^n)^i \equiv -j + 2^n \bmod 2^{n+1}$, y concluimos:

$$(a^i b^j)^2 = \begin{cases} a^{2i} b^{2j} & \text{si } 2|i \\ a^{2i} & \text{si } 2 \nmid i,\ y\ 2|j \\ a^{2i} b^{2^n} & \text{en cualquier otro caso.} \end{cases}$$

Entonces $|P_2^2| = 2^{m+n-2} + 2^{m-2} + 2^{m-2} > |P_1^2|$. Por lo tanto, $P_1 \ncong P_2$.

Lema 2.18. *Sea P un 2-grupo metacíclico que tiene la siguiente presentación*

$$\langle x,\ y \mid x^{2^k} = y^{2^l},\ y^{2^m} = 1,\ y^x = y^{1+2^n} \rangle,$$

con m, k, l y n enteros positivos, $2^m | 2^{n+l}$, $2^m | ((1+2^n)^{2^k} - 1)$ y $m > n \geq 2$. Para cualesquiera i, j enteros, tenemos:

$$(x^i y^j)^{2^{m-n}} = x^{i2^{m-n}} y^{j2^{m-n}} y^{ij2^{m-1}}.$$

Prueba. Del Teorema 1.23 obtenemos

$$x^{i2^{m-n}} y^{j2^{m-n}} = (x^i y^j)^{2^{m-n}} c_2^{e_2} \cdots c_{2^{m-n}}^{e_{2^{m-n}}},$$

donde c_r es un elemento de $C_r(\langle x^i,\ y^j \rangle)$ y el exponenete e_r es el $r-$ésimo coeficiente binomial $e_r = n(n-1)\cdots(n-(r-1))/r!$. Como P' es un subgrupo de $\langle y \rangle$, entonces $c_2 = [x^i,\ y^j]$ y $c_r = [c_{r-1},\ x^i]$ para toda $r = 3, \ldots, 2^{m-n}$, de hecho:

$$c_r = y^{j(1-(1+2^n)^i)^{r-1}} \text{ para toda } r = 2, \ldots, 2^{m-n}.$$

Entonces $c_2^{e_2} = y^{j(1-(1+2^n)^i)e_2}$ y

$$\begin{aligned} j(1-(1+2^n)^i)e_2 &= j(-\textstyle\sum_{\alpha=1}^{i}\binom{i}{\alpha}2^{n\alpha})2^{m-n-1}(2^{m-n}-1) \\ &= j(-\textstyle\sum_{\alpha=1}^{i}\binom{i}{\alpha}2^{m+(\alpha-1)n-1})(2^{m-n}-1) \\ &= -ij2^{m-1}(2^{m-n}-1) \\ &\quad +j(-\textstyle\sum_{\alpha=2}^{i}\binom{i}{\alpha}2^{m+(\alpha-1)n-1})(2^{m-n}-1) \\ &= ij2^{m-1}-ij2^{m+(m-n-1)} \\ &\quad +j(-\textstyle\sum_{\alpha=2}^{i}\binom{i}{\alpha}2^{m+(\alpha-1)n-1})(2^{m-n}-1) \\ &\equiv ij2^{m-1} \bmod 2^m \end{aligned}$$

y este último es congruente con $-ij2^{m-1}$ módulo 2^m, por lo que

$$(x^iy^j)^{2^{m-n}}c_3^{e_3}\cdots c_{2^{m-n}}^{e_{2^{m-n}}} = x^{i2^{m-n}}y^{j2^{m-n}}y^{ij2^{m-1}}.$$

Ahora, si $r \geq 3$

$$\begin{aligned} j(1-(1+2^n)^i)^{r-1} &= j(-\textstyle\sum_{\alpha=1}^{i}\binom{i}{\alpha}2^{n\alpha})^{r-1} \\ &= j(-\textstyle\sum_{\alpha=1}^{i}\binom{i}{\alpha}2^{n+(\alpha-1)n})^{r-1} \\ &= j2^{n(r-1)}(-\textstyle\sum_{\alpha=1}^{i}\binom{i}{\alpha}2^{(\alpha-1)n})^{r-1}. \end{aligned}$$

Llamemos a este resultado $j2^{n(r-1)}a$. Para el coeficiente binomial e_r, observamos que la máxima potencia de 2 que lo divide es $m-n-r_2$, donde r_2 es la máxima potencia de 2 que divide a r. Así, $e_r = 2^{m-n-r_2}b$ con b impar. Si r es impar, $r_2 = 0$ y

$$\begin{aligned} j(1-(1+2^n)^i)^{r-1}e_r &= j2^{n(r-1)+m-n}ab \\ &= j2^{n(r-2)+m}ab \\ &\equiv 0 \bmod 2^m. \end{aligned}$$

Por otro lado, si r es par, $r \geq 4$ y $r_2 \leq r-2 < n(r-2)$ porque $n \geq 2$. Luego

$$\begin{aligned} j(1-(1+2^n)^i)^{r-1}e_r &= j2^{n(r-1)+m-n-r_2}ab \\ &= j2^{n(r-2)-r_2+m}ab \\ &\equiv 0 \bmod 2^m. \end{aligned}$$

De donde obtenemos el resultado.

Teorema 2.19 (4.6 en [4] o '*two is the only odd prime*'). *Todo 2-grupo metacíclico tiene uno de los siguientes ocho tipos de presentaciones, en la cual los parámetros r, s, t, u, v y w son números naturales.*

(i) $\langle a \mid a^{2^r} = 1 \rangle$ *con* $r \geq 0$,

(ii) $\langle a,\ b \mid a^{2^r} = b^2 = 1,\ b^a = b \rangle$ *con* $r \geq 1$,

(iii) $\langle a,\ b \mid a^2 = b^{2^r} = 1,\ b^a = b^{-1} \rangle$ *con* $r \geq 2$,

(iv) $\langle a,\ b \mid a^2 = b^{2^r},\ b^{2^{r+1}} = 1,\ b^a = b^{-1} \rangle$ *con* $r \geq 1$,

(v) $\langle a,\ b \mid a^2 = b^{2^{r+1}} = 1,\ b^a = b^{1+2^r} \rangle$ *con* $r \geq 2$,

(vi) $\langle a,\ b \mid a^2 = b^{2^{r+1}} = 1,\ b^a = b^{-1+2^r} \rangle$ *con* $r \geq 2$,

(vii) $\langle a,\ b \mid a^{2^r} = b^{2^s},\ b^{2^{s+t}} = 1,\ b^a = b^{1+2^u} \rangle$ *con* $r \geq s \geq u \geq 2$ *y* $u \geq t$,

(viii) $\langle a,\ b \mid a^{2^{r+s+t}} = b^{2^{r+s+u+v}},\ b^{2^{r+s+u+v+w}} = 1,\ b^a = b^{-1+2^{r+u}} \rangle$ *donde* $r \geq 2$, $v \leq r$, $w \leq 1$, $su = tu = tv = 0$, *y si* $v \geq r - 1$, *entonces* $w = 0$.

Grupos de diferentes tipos o del mismo tipo pero con parámetros diferentes son no isomorfos.

Prueba. Sea P un 2-grupo metacíclico, claramente P es finito. Supongamos primero que P tiene un subgrupo cíclico maximal. Por el Teorema 1.17, P es isomorfo a uno de los primeros seis tipos enlistados.

Supongamos ahora que P no tiene subgrupo cíclico maximal. Por el Lema 1.2, P tiene una presentación de la forma

$$\langle x,\ y \mid x^a = y^b,\ y^c = 1,\ y^x = y^d \rangle,$$

donde c es una potencia de 2, como podemos tomar b tal que $b|c$ entonces b es una potencia de 2 y por lo tanto, a lo es también. Por el Lema 1.21, cambiando, si es necesario, los generadores x y y, podemos suponer que d es de la forma $\pm 1 + 2^\lambda$ para algún entero no negativo λ. Suponiendo que P no tiene subgrupos cíclicos maximales, concluimos que P tiene una presentación de la forma

$$\langle x,\ y \mid x^{2^k} = y^{2^l},\ y^{2^m} = 1,\ y^x = y^{\varepsilon + 2^n} \rangle, \tag{2.1}$$

donde $\varepsilon = \pm 1$, $m \geq n \geq 2$, $k \geq 2$, $m \geq l \geq 2$, $2^m | (\varepsilon + 2^n - 1)2^l$, $2^m | (\varepsilon + 2^n)^{2^k} - 1$ y $|P| = 2^{k+m}$. La primera condición de divisibilidad se puede expresar como

$$l \geq \begin{cases} m-n & \text{si } \varepsilon = 1 \\ m-1 & \text{si } \varepsilon = -1 \end{cases}$$

y por el Corolario 1.13, la segunda equivale a $k + n \geq m$.

Supongamos primero que $\varepsilon = 1$ y que $m > n$. Por el Lema 2.18 tenemos

$$\begin{aligned} (x^i y^j)^{2^{m-n}} &= x^{i2^{m-n}} y^{j2^{m-n}} y^{ij2^{m-1}} \\ &= \begin{cases} x^{i2^{m-n}} y^{j2^{m-n}} & \text{si } ij \text{ es par,} \\ x^{i2^{m-n}} y^{j2^{m-n}} y^{2^{m-1}} = x^{i2^{m-n}} y^{j2^{m-n}(1+2^{n-1})} & \text{si } ij \text{ es impar.} \end{cases} \end{aligned}$$

Este resultado será muy útil en los cálculos que siguen, de los cuales sólo el primero haremos con detalle. Tenemos cuatro casos: $k \geq l \geq n$, $l > k \geq n$, $l > k < n$ y $k \geq l < n$. En el primer caso, P es claramente de tipo (vii). En el segundo caso, observamos que si $a = xy^{1-2^{l-k}}$ y

$$b = \begin{cases} y^{1+2^{n-1}} & \text{si } k = m-n \\ y & \text{si } k > m-n, \end{cases}$$

entonces $x,\ y \in \langle a,\ b \rangle$, luego $\langle a,\ b \rangle = P$. Si $k > m-n$, entonces

$$\begin{aligned} a^{2^k} &= (xy^{1-2^{l-k}})^{2^k} \\ &= (xy^{1-2^{l-k}})^{2^{k-(m-n)}2^{m-n}} \\ &= (x^{2^{k-(m-n)}} y^{(1-2^{l-k})2^{k-(m-n)}+d2^n})^{2^{m-n}} && \text{para algún entero } d \text{ porque } P' = \langle y^{2^n} \rangle \\ &= x^{2^k} y^{(1-2^{l-k})2^k} && \text{por el resultado de arriba} \\ &= x^{2^k} y^{2^k - 2^l} \\ &= y^{2^k} \\ &= b^{2^k}. \end{aligned}$$

Si $k = m-n$, obtenemos rápidamente la misma conclusión. En ambos subcasos, también tenemos $b^{2^m} = 1$ y $b^a = b^{1+2^n}$. Por lo tanto, P es una imagen homomórfica del grupo definido por la presentación $\langle a,\ b \mid a^{2^k} = b^{2^k},\ b^{2^m} = 1,\ b^a = b^{1+2^n} \rangle$. Como el grupo definido por ésta tiene orden menor o igual a 2^{k+m}, debe ser isomorfo a P, luego P es de tipo (vii). Si $l > k < n$, entonces de una forma análoga, probamos que con $a = y^{-1}$ y $b = x^{-1}y^{(2^{l-k}-2^{n-k})(1-2^n)}$ tenemos

$$P \cong \langle a,\ b \mid a^{2^n} = b^{2^k},\ b^{2^{m+k-n}} = 1,\ b^a = b^{1+2^k} \rangle,$$

que también es un grupo de tipo (vii). Si $k \geq l < n$, entonces $\langle x \rangle \cap \langle y \rangle$ contiene a P', así que x y y conmutan con todo elemento de P'. Por 1.4 $(uv)^\alpha = u^\alpha v^\alpha [u,\ v]^{\binom{\alpha}{2}}$ para todo $u,\ v$ en P, $\alpha \geq 2$. Utilizando esta igualdad, observamos que con $a = x^{2^{k-l}} y^{-1}$ y $b = x$ tenemos

$$P \cong \langle a,\ b \mid a^{2^l} = b^{2^{k-l+m-t}},\ b^{2^{k-l+m}} = 1,\ b^a = b^{1+2^{k-l+n}} \rangle$$

donde

$$t = \begin{cases} 1 & \text{si } k+n = m, \\ 0 & \text{si } k+n > m. \end{cases}$$

Esto nos lleva de regreso a uno de los tres casos que consideramos anteriormente. Hemos mostrado que cuando $\varepsilon = 1$, P es de tipo (vii).

Ahora consideremos $\varepsilon = -1$, en este caso $l = m$ ó $l = m-1$. Primero supongamos $l = m$. Tomemos $a = x$ y $b = y$. Para llevar la presentación 2.1 a una de tipo (viii), tenemos que mostrar que el sistema de ecuaciones simultáneas

$$\begin{aligned} r+s+t &= k, \\ r+s+u+v &= r+s+u+v+w = m, \\ r+u &= n, \end{aligned}$$

tiene una solución que satisface las condiciones impuestas a los parámetros en (viii). Claramente, $w = 0$. Si $z = \min\{k,\ m\}$, entonces

$$(r,\ s,\ t,\ u,\ v) = \begin{cases} (n,\ z-n,\ k-z,\ 0,\ m-z) & \text{si } n \leq k, \\ (k,\ 0,\ 0,\ n-k,\ m-n) & \text{en otro caso} \end{cases}$$

es una solución.

Si $l = m-1$, entonces $m = l+1 \geq 3$. Primero supongamos que $n < m$. También podemos suponer que $k+n > m$, ya que de otra forma, con $x_1 = xy$,

$$P \cong \langle x_1, y \mid x_1^{2^k} = y^{2^m} = 1,\ y^{x_1} = y^{-1+2^n} \rangle,$$

que es el caso considerado en el párrafo anterior. Cuando $k+n > m > l \geq 2$, la presentación 2.1 puede ser llevada a una de tipo (viii) con $a = x$, $b = y$; verificando que el sistema de ecuaciones simultáneas

$$\begin{aligned} r+s+t &= k, \\ r+s+u+v &= r+s+u+v+w-1 = m-1, \\ r+u &= n, \end{aligned}$$

tiene una solución que satisface las condiciones impuestas a los parámetros en (viii). Análogamente al caso anterior, una solución es

$$(r,\ s,\ t,\ u,\ v) = \begin{cases} (n,\ z-n,\ k-z,\ 0,\ m-1-z) & \text{si } n \le k, \\ (k,\ 0,\ 0,\ n-k,\ m-1-n) & \text{en otro caso} \end{cases}$$

donde, en este caso, $z = \min\{k,\ m-1\}$.

Ahora supongamos $m = n$. Entonces $y^x = y^{-1}$ y $x^2 \in Z(P)$, entonces es fácil ver que con $y_1 = x^{2^{k-1}} y$,

$$P \cong \langle x,\ y_1 \mid x^{2^k} = y_1^{2^{m-1}} = 1,\ y_1^{2^m} = 1,\ y_1^x = y_1^{-1+2^{m-1}} \rangle,$$

que es el caso tratado en el párrafo anterior. Esto prueba que todo 2-grupo metacíclico tiene una presentación de las enlistadas aquí.

Del Lema 2.16, sabemos que los primeros seis tipos de grupos son no isomorfos entre ellos, y es claro que los parámetros son invariantes para cada uno. Como estos grupos tienen subgrupos cíclicos maximales, $|P|/\exp G \le 2$.

Supongamos que P es un grupo de tipo (vii). El Lema 1.2 muestra que $|P| = 2^{r+s+t}$, del Lema 2.14 tenemos que $\exp P = 2^{r+t}$ y sabemos que $P' = \langle b^{2^u} \rangle$. Entonces $P/P' \cong \mathsf{C}(2^r) \times \mathsf{C}(2^u)$. Tenemos entonces que, $r+s+t$, $r+t$, r y u son invariantes de P, por lo tanto, también lo son s y t. Como $|P|/\exp P = 2^s > 2$, P no es isomorfo a ninguno de los primeros seis tipos enlistados. Como $r \ge u \ge 2$, observamos también que $\mathsf{C}(4) \times \mathsf{C}(4)$ es una imagen homomórfica de P.

Ahora supongamos que P es un grupo de tipo (viii). Por el Lema 2.15

$$Z(P) = \begin{cases} \langle a^2,\ b^{2^{r+s+u+v+w-1}} \rangle & \text{si } s+v+w = 0, \\ \langle a^{2^{s+v+w}},\ b^{2^{r+s+u+v+w-1}} \rangle & \text{en otro caso,} \end{cases}$$

que es cíclico de orden mayor a 2 si $w = 1$, cíclico de orden 2 si $w = 0$ y $v = r$. Esto prueba que w es un invariante de P. Además $P' = \langle b^2 \rangle$ y $P/P' \cong \mathsf{C}(2) \times \mathsf{C}(2^{r+s+t})$. En particular, $\mathsf{C}(4) \times \mathsf{C}(4)$ no es una imagen homomórfica de P y por lo tanto, un grupo de tipo (viii) no es un grupo de tipo (vii). Por el Lema 2.14 tenemos

$$|P|/\exp P = 2^{2r+2s+t+u+v+w}/\max\{2^{r+s+t+w},\ 2^{r+s+u+v+w}\} \ge 2^r > 2,$$

por lo que un grupo de tipo (viii) no es un grupo de alguno de los primeros seis tipos.

Supongamos que $w = 0$ para un grupo de tipo (viii) P. Entonces $\exp P/P' = 2^{r+s+t}$ y los tres enunciados siguientes son verdaderos:

(a) $\exp P = \exp P/P' = |P|^{1/2}$ si, y sólo si $t = u = v = 0$;

(b) $\exp P = \exp P/P' > |P|^{1/2}$ si, y sólo si $t > 0$ y $u = v = 0$;

(c) $\exp P > \exp P/P'$ si, y sólo si $t = 0$ y $u + v > 0$.

En el caso (a) tenemos $P \cong \langle a,\ b \mid a^{2^{r+s}} = b^{2^{r+s}} = 1,\ b^a = b^{-1+2^r} \rangle$ donde $r \geq 2$ y $s \geq 0$. En este caso,

$$Z(P) \cong \begin{cases} \mathsf{C}(2) \times \mathsf{C}(2^{r-1}) & \text{si } s = 0, \\ \mathsf{C}(2) \times \mathsf{C}(2^r) & \text{en otro caso} \end{cases}$$

y $P/P' \cong \mathsf{C}(2) \times \mathsf{C}(2^{r+s})$, por lo tanto $|P/P'|/|Z(P)| = 2^{\max\{1,\ s\}}$. Si $|P/P'|/|Z(P)| > 2$, podemos concluir que los parámetros son invariantes. Cuando $|P/P'|/|Z(P)| = 2$, tendremos que distinguir los dos grupos obtenidos al hacer $(r,\ s)$ igual a $(q,\ 1)$ ó a $(q+1,\ 0)$, para cualquier $q \geq 2$. Ahora, por el Lema 2.17

$$\langle a,\ b \mid a^{2^{q+1}} = b^{2^{q+1}} = 1,\ b^a = b^{-1} \rangle \ncong \langle a,\ b \mid a^{2^{q+1}} = b^{2^{q+1}} = 1,\ b^a = b^{-1+2^q} \rangle.$$

Para el caso (b), tenemos $P \cong \langle a,\ b \mid a^{2^{r+s+t}} = b^{2^{r+s}} = 1,\ b^a = b^{-1+2^r} \rangle$ donde $r \geq 2$, $s \geq 0$ y $t \geq 1$. En este caso,

$$Z(P) \cong \begin{cases} \mathsf{C}(2) \times \mathsf{C}(2^{r+t-1}) & \text{si } s = 0, \\ \mathsf{C}(2) \times \mathsf{C}(2^{r+t}) & \text{en otro caso} \end{cases}$$

y $P/P' \cong \mathsf{C}(2) \times \mathsf{C}(2^{r+s+t})$. Tenemos $(\exp P)^2/|P| = 2^t$, luego t es un invariante de P. Además, $|P/P'|/|Z(P)| = 2^{\max\{1,\ s\}}$. Si $|P/P'|/|Z(P)| > 2$, podemos concluir que los parámetros son invariantes. Cuando $|P/P'|/|Z(P)| = 2$, tendremos que distinguir los dos grupos obtenidos al hacer $(r,\ s)$ igual a $(q,\ 1)$ ó a $(q+1,\ 0)$, para cualquier $q \geq 2$. Ahora, por el Lema 2.17

$$\langle a,\ b \mid a^{2^{q+t+1}} = b^{2^{q+1}} = 1,\ b^a = b^{-1} \rangle \ncong \langle a,\ b \mid a^{2^{q+t+1}} = b^{2^{q+1}} = 1,\ b^a = b^{-1+2^q} \rangle.$$

En el último caso, $P \cong \langle a,\ b \mid a^{2^{r+s}} = b^{2^{r+s+u+v}} = 1,\ b^a = b^{-1+2^{r+u}} \rangle$ donde $r \geq 2$, $v \leq r$, $su = 0$ y $u + v > 0$. En este caso,

$$Z(P) \cong \begin{cases} \mathsf{C}(2) \times \mathsf{C}(2^{r-1}) & \text{si } s = v = 0, \\ \mathsf{C}(2) \times \mathsf{C}(2^{r-v}) & \text{en otro caso} \end{cases}$$

y $P/P' \cong \mathsf{C}(2) \times \mathsf{C}(2^{r+s})$. También tenemos $|P/P'|/|Z(P)| = 2^{\max\{1,\ s+v\}}$. Como, en este caso, $\exp P = 2^{r+s+u+v}$, tenemos que $r+s$, $u+v$ y $\max\{1,\ s+v\}$ son invariantes de P. Si $s + v > 1$, entonces $s + v$ es un invariante, luego $us = 0$ implica que r, s, u

y v son invariantes de P. Supongamos que $s + v \leq 1$. Entonces $s = 0$ y $u > v = 0$ ó $v = 1$, resta entonces distinguir los dos grupos obtenidos al hacer $(u,\ v)$ igual a $(q+1,\ 0)$ ó a $(q,\ 1)$, para cualquier $q \geq 2$. Ahora, por el Lema 2.17

$$\langle a,\ b \mid a^{2^r} = b^{2^{r+q+1}} = 1,\ b^a = b^{-1} \rangle \ncong \langle a,\ b \mid a^{2^r} = b^{2^{r+q+1}} = 1,\ b^a = b^{-1+2^{r+q}} \rangle.$$

Si $w = 1$, entonces $P/\langle b^{2^{r+s+u+v}} \rangle$ es de tipo (viii) con $w = 0$ y los argumentos usados en los párrafos anteriores pueden ser usados para probar que los otros parámetros son invariantes. Con esto terminamos la prueba.

Capítulo 3

Descomposición de Hall estándar

Si H y N son grupos y $\phi: H \to \text{Aut } N$ es un homomorfismo, éste define un producto semidirecto de H y N que denotaremos por $H \ltimes_\phi N$, o simplemente por $H \ltimes N$. Consideraremos a H y N como subgrupos de $H \ltimes N$ por medio de las identificaciones naturales.

A continuación probaremos que todo grupo metacíclico finito se descompone canónicamente como el producto semidirecto de dos subgrupos de Hall, uno de ellos nilpotente. Además, el factor normal será construido de tal forma que resulte ser el más pequeño de los subgrupos de Hall normales con cociente nilpotente. Con esta descomposición procederemos a clasificar los grupos metacíclicos de orden impar.

Notación. Sea n un entero, $\pi(n)$ denotará el conjunto de los primos divisores de n. Extendiendo esta idea, si G es un grupo finito, escribiremos $\pi(G)$ para referirnos al conjunto de los primos divisores del orden de G. Si G es nilpotente, el único π-subgrupo de Hall será denotado por G_π para cada conjunto de primos π.

Lema 3.1 (5.3 en [8]). *Sea G un grupo con una factorización metacíclica $G = SK$. Para cada conjunto π de primos, el subgrupo $H = S_\pi K_\pi$ es el único π-subgrupo de Hall de G tal que $S_\pi = S \cap H$ y $K_\pi = K \cap H$, así $H = (S \cap H)(K \cap H)$.*

Prueba. Como S y K son cíclicos $S = S_\pi S_{\pi'}$ y $K = K_\pi K_{\pi'}$, es decir $G = S_\pi S_{\pi'} K_\pi K_{\pi'}$, pero K_π es normal en G, luego $G = S_\pi K_\pi S_{\pi'} K_{\pi'}$. Por otro lado $S_\pi K_\pi \cap S_{\pi'} K_{\pi'} = 1$, luego $|G| = |S_\pi K_\pi||S_{\pi'} K_{\pi'}|$. Entonces $H = S_\pi K_\pi$ es un π-subgrupo de Hall de G que, por la regla modular de Dedekind, satisface $S_\pi = S \cap H$ y $K_\pi = K \cap H$, por lo que la unicidad es obvia.

Definición 3.2 (5.4 en [8]). Sea G un grupo con una factorización metacíclica $G = SK$, en lo que resta de este capítulo, denotaremos por π al conjunto:

$$\pi := \{p \in \pi(G) \mid \text{ G tiene un } p'\text{-subgrupo de Hall normal}\},$$

por **H** al π-subgrupo de Hall $S_\pi K_\pi$ y por **N** al π'-subgrupo de Hall $S_{\pi'} K_{\pi'}$.

Lema 3.3 (5.5 en [8]). *Sean G un grupo con una factorización metacíclica $G = SK$, N y H definidos según 3.2, entonces $N = (S \cap N)(K \cap N)$ es un subgrupo normal de G y $H = (S \cap H)(K \cap H)$ es nilpotente.*

Prueba. Por el Lema 1.32 tenemos que N es la intersección de todos los p'-subgrupos de Hall normales para p en $\pi(G)$, entonces, por la prueba del Lema 3.1, $G = HN$ es una descomposición semidirecta de G. Si $p \in \pi$ y T/N es un p-subgrupo de Sylow de G/N entonces T es un $\pi' \cup \{p\}$-subgrupo de Hall de G. Nuevamente por 1.32, la intersección de los q'-subgrupos de Hall normales de G con $q \in \pi(G)$ y $q \neq p$ es un $(\pi - \{p\})'$-subgrupo de Hall de G, es decir es un $\pi' \cup \{p\}$-subgrupo de Hall de G que por ser normal es igual a T. Entonces T/N es un subgrupo normal de G/N, es decir $H \cong G/N$ es nilpotente.

$N = (S \cap N)(K \cap N)$ y $H = (S \cap H)(K \cap H)$ se siguen del Lema 3.1.

Como parte de la Definición 3.2, dado G grupo finito con una factorización metacíclica $G = SK$, $G = HN$ será llamada la **descomposición de Hall estándar** para la factorización metacíclica $G = SK$.

Los dos siguientes resultados serán utilizados en la prueba del Teorema 3.6, en el que abordamos importantes características de la descomposición de Hall estándar.

Lema 3.4 (5.2 en [8]). *Sean q un primo, G un grupo metacíclico con un q'-subgrupo H y Q un q-subgrupo de Sylow de G. Sea $G = SK$ una factorización metacíclica tal que:*

$$H = (S \cap H)(K \cap H) \quad \text{y} \quad Q = (S \cap Q)(K \cap Q).$$

Y sean

$$X = S \cap H, \quad Y = K \cap H, \quad U = S \cap Q \quad \text{y} \quad V = K \cap Q.$$

Si H normaliza Q, entonces $[H, Q] = 1$ ó

$$Y \leqslant \mathbb{C}_H(Q), \quad V = [H, Q], \quad U = \mathbb{C}_Q(H) \quad \text{y} \quad U \cap V = 1.$$

Prueba. De las hipótesis observamos que $H = XY$ y $Q = UV$ son factorizaciones metacíclicas de H y Q respectivamente.
Como K es un subgrupo cíclico normal de G, Y es un q'-subgrupo normal de G que normaliza Q, pero $H \cap Q = 1$, ya que H es un q'-subgrupo de G y Q es un q-subgrupo de G, entonces si $x \in Q$ y $y \in Y$, $y^{-1}x^{-1}yx \in Q$ y $y^{-1}x^{-1}yx \in Y$ de lo que obtenemos $Y \leqslant \mathbb{C}_H(Q)$ y como U y X son subgrupos de S que es abeliano, entonces $U \leqslant \mathbb{C}_Q(H)$.

Ahora si $h \in H$ y $a \in Q$:

$$\begin{aligned} h^{-1}a^{-1}ha &= y^{-1}x^{-1}v^{-1}u^{-1}xyuv \\ &= y^{-1}x^{-1}v^{-1}xyv && \text{porque } U \leqslant \mathbb{C}_Q(H) \\ &= x^{-1}y'v^{-1}y'^{-1}xv && \text{porque } Y \trianglelefteq H \\ &= x^{-1}v^{-1}xv && \text{porque } Y \leqslant \mathbb{C}_H(Q), \end{aligned}$$

es decir, $[H,\ Q] = [X,\ V]$. Supongamos $[H,\ Q] \neq 1$, como V es normal en Q y $[X,\ V] \neq 1$, entonces X actúa en V de manera no trivial, luego $V = \mathbb{C}_V(X) \times [X,\ V]$ (Lema 1.35), pero al ser V cíclico y de orden primo, si se descompone como un producto directo, uno de los factores es igual a 1, así $\mathbb{C}_V(X) = 1$ y $V = [H,\ Q]$. Luego, si $v \in V \cap \mathbb{C}_Q(H)$ y $h \in H$ de $1 = h^{-1}v^{-1}hv = y^{-1}x^{-1}v^{-1}xyv = x^{-1}v^{-1}xv$ obtenemos $v = 1$, luego $V \cap \mathbb{C}_Q(H) = 1$ y, por lo tanto, $U \cap V = 1$. Finalmente, como $Q = UV$ y $U \leqslant \mathbb{C}_Q(H)$, por la regla modular de Dedekind $\mathbb{C}_Q(H) = Q \cap \mathbb{C}_Q(H) = U$.

Para un primo $q \in \pi'$, introducimos los conjuntos $\hat{q} := \{p \in \pi' \mid p < q\}$ y $\check{q} := \{p \in \pi' \mid p < q\}$ que nos serán útiles en la prueba de los dos siguientes resultados. Para cualquier subconjunto ω de π' definimos $N_\omega := S_\omega K_\omega$.

Lema 3.5 (5.6 en [8]).

(i) $K_{\pi'} = G' \cap N$;

(ii) $S_{\pi'} = \prod_{q \in \pi'} \mathbb{C}_{N_q}(HN_{\hat{q}}) \leqslant \mathbb{C}_N(H)$;

(iii) $K_{\pi'} \cap S_{\pi'} = 1$.

Prueba. Si G es nilpotente, entonces $\pi(N)$ es vacío y, por lo tanto, los resultados también.

Si G no es nilpotente, entonces N no es trivial. Sea q en $\pi(N)$, por el Lema 3.1 $S \cap N_q = S_q$ y $K \cap N_q = K_q$. Como K_π es un π-subgrupo normal de G, está contenido en $\mathbb{O}_\pi(G)$, por otro lado, como G es soluble y H es π-subgrupo de Hall, $\mathbb{O}_\pi(G) \leqslant H$, más aún, si $o \in \mathbb{O}_\pi(G)$ y $n \in N$, tenemos $n^{-1}o^{-1}n \in \mathbb{O}_\pi(G)$ y $o^{-1}no \in N$, luego

$n^{-1}o^{-1}no \in \mathbb{O}_\pi(G) \cap N = 1$, es decir $\mathbb{O}_\pi(G)$ está contenido en $\mathbb{C}_H(N)$. Por lo tanto, $K_\pi \leqslant \mathbb{O}_\pi(G) \leqslant \mathbb{C}_H(N)$. Probaremos ahora que H normaliza N_q. Como $H = S_\pi K_\pi$, basta conjugar por $s \in S_\pi$ y tenemos:

$$s^{-1}N_q s = s^{-1}S_q K_q s = s^{-1}S_q s K_q = N_q$$

Consideremos ahora $S_{\hat{q}}S_q \leqslant S$ y $K_{\hat{q}}K_q \trianglelefteq G$, su producto es subgrupo de G y, como $K_{\hat{q}}$ es normal en G:

$$S_{\hat{q}}S_q K_{\hat{q}}K_q = S_{\hat{q}}K_{\hat{q}}S_q K_q = N_{\hat{q}}N_q$$

Esto es: $N_{\hat{q}}N_q$ es un subgrupo de G, y su orden tiene como primo divisor más grande a q, luego por la Proposición 1.34 el q-subgrupo de Sylow de $N_{\hat{q}}N_q$ es normal en $N_{\hat{q}}N_q$, por lo tanto $N_{\hat{q}}$ normaliza N_q, y $HN_{\hat{q}}$ también.

Este último resultado completa las hipótesis del lema anterior, por lo que si probamos $[HN_{\hat{q}},\ N_q] \neq 1$ podremos conluir (ii) y (iii).

Supongamos $[HN_{\hat{q}},\ N_q] = 1$, probaremos que $HN_{\hat{q}}N_{\tilde{q}}$ es un q'-subgrupo de Hall de G normal para llegar a una contradicción. Procediendo igual que para $N_{\hat{q}}N_q$ arriba, $HN_{\hat{q}}N_{\tilde{q}}$ es un subgrupo de G. Observemos que $N = N_{\hat{q}}N_q N_{\tilde{q}}$, así que, basta conjugar $HN_{\hat{q}}N_{\tilde{q}}$ por $n \in N_q$ arbitrario. Sea hm_1m_2 en $HN_{\hat{q}}N_{\tilde{q}}$, tenemos:

$$\begin{aligned} n^{-1}hm_1m_2n &= n^{-1}hm_1nm_2' \text{ con } m_2' \in N_{\tilde{q}} \text{ porque } N_{\tilde{q}} \trianglelefteq N \\ &= hm_1m_2' \end{aligned}$$

que es un elemento de $HN_{\hat{q}}N_{\tilde{q}}$, esto contradice el hecho de que $q \in \pi'$. Así, por el Lema 3.4, $S_q = \mathbb{C}_{N_q}(HN_{\hat{q}}) \leqslant \mathbb{C}_N(H)$, $K_q = [HN_{\hat{q}},\ N_q]$ y $S_q \cap K_q = 1$ para toda $q \in \pi(N)$, por lo tanto (ii) se sigue inmediatamente. Para (iii), tomemos a en $K_{\pi'} \cap S_{\pi'}$ entonces $a = \Pi_{i=1}^r k_i = \Pi_{i=1}^r s_i$ con k_i y s_i en el q_i-subgrupo de Sylow K_{q_i} de K y S_{q_i} de S, respectivamente. Entonces $k_1^{-1}s_1 = \Pi_{i=2}^r k_i s_r^{-1} \cdots s_2^{-1} \in K_{q_2} \cdots K_{q_r} S_{q_2} \cdots S_{q_r}$. Por lo tanto $k_1^{-1}s_1 = 1$, mas $S_{q_1} \cap K_{q_1} = 1$, luego $k_1 = s_1 = 1$ y $\Pi_{i=2}^r k_i = \Pi_{i=2}^r s_i$, continuamos con este proceso y concluimos (iii).

Finalmente, para probar (i), observemos que de $K_q = [HN_{\hat{q}},\ N_q]$ concluimos $K_{\pi'} \leqslant G'$, es decir $K_{\pi'} \leqslant G' \cap N$, y como $G' \leqslant K$ también tenemos $G' \cap N \leqslant K \cap N = K_{\pi'}$, por lo tanto $K_{\pi'} = G' \cap N$.

Teorema 3.6 (5.7 en [8]). *Si G es un grupo con una factorización metacíclica $G = SK$ y $G = HN$ es la descomposición de Hall estándar para la misma, entonces $N = (S \cap N)(K \cap N)$ es una factorización metacíclica que se escinde, con $S \cap N \leqslant \mathbb{C}_N(H)$. El subgrupo $K \cap N$ y la clase de conjugación de $S \cap N$ son independientes de la elección de la factorización metacíclica.*

Prueba. La factorización metacíclica $N = (S \cap N)(K \cap N)$ se escinde por (iii) del lema anterior, $S \cap N \leqslant \mathbb{C}_N(H)$ por (ii). Para probar la última afirmación, sea S^*K^* otra factorización metacíclica de G con descomposición de Hall estándar H^*N^*, como N es un π'-subgrupo de Hall normal, $N = N^*$. Por el Lema 1.32, para cualquier $p \in \pi'$, $\bigcap_{p \leq q \in \pi'} HN_{\hat{q}}N_{\check{q}}$ es un $(\{p\} \cup \check{p})'$-subgrupo de Hall de G, luego

$$|HN_{\hat{q}}| = |\textstyle\bigcap_{p \leq q \in \pi'} HN_{\hat{q}}N_{\check{q}}|.$$

Además, para todo $q \in \pi'$ tal que $p \leq q$ tenemos $K \cap N_{\hat{p}} \trianglelefteq K \cap N_{\hat{q}}N_{\check{q}}$ y $S \cap N_{\hat{p}} \trianglelefteq S \cap N_{\hat{q}}N_{\check{q}}$, por lo tanto $N_{\hat{p}} \leqslant N_{\hat{q}}N_{\check{q}}$, luego

$$HN_{\hat{p}} = \textstyle\bigcap_{p \leq q \in \pi'} HN_{\hat{q}}N_{\check{q}} \quad \text{y análogamente,} \quad H^*N^*_{\hat{p}} = \bigcap_{p \leq q \in \pi'} H^*N^*_{\hat{q}}N_{\check{q}}.$$

También tenemos

$$|HN_p| = |\textstyle\bigcap_{p \neq q \in \pi'} HN_{\hat{q}}N_{\check{q}}| \quad \text{y} \quad N_p \leqslant N_{\hat{q}}N_{\check{q}} \text{ para toda } p \neq q \in \pi',$$

y de manera análoga para $H^*N^*_p$, esto es

$$HN_p = \textstyle\bigcap_{p \neq q \in \pi'} HN_{\hat{q}}N_{\check{q}} \quad \text{y} \quad H^*N^*_p = \bigcap_{p \neq q \in \pi'} H^*N^*_{\hat{q}}N^*_{\check{q}}.$$

Además, $N_p = (H \cap N)N_p = HN_p \cap N$ y $N^*_p = H^*N^*_p \cap N$. Por el Teorema 1.33, existe $g \in G$ tal que $(H^*N^*_{\hat{q}}N^*_{\check{q}})^g = HN_{\hat{q}}N_{\check{q}}$ para toda $q \in \pi'$, entonces

$$\begin{aligned} HN_p \cap N &= \textstyle\bigcap_{p \neq q \in \pi'} HN_{\hat{q}}N_{\check{q}} \cap N \\ &= \textstyle\bigcap_{p \neq q \in \pi'} (H^*N^*_{\hat{q}}N^*_{\check{q}})^g \cap N \\ &= (\textstyle\bigcap_{p \neq q \in \pi'} H^*N^*_{\hat{q}}N^*_{\check{q}})^g \cap N \\ &= (\textstyle\bigcap_{p \neq q \in \pi'} H^*N^*_{\hat{q}}N^*_{\check{q}} \cap N)^g \quad = (H^*N^*_p \cap N)^g, \end{aligned}$$

es decir $N_p = (N^*_p)^g$. Por otro lado, si A es un grupo y R, $B \leqslant A$, para todo $a \in A$ tenemos $\mathbb{C}_R(B^a) = (\mathbb{C}_{(R^{a^{-1}})}(B))^a$, luego

$$\begin{aligned} S \cap N &= \textstyle\prod_{p \in \pi'} \mathbb{C}_{N_p}(HN_{\hat{p}}) \\ &= \textstyle\prod_{p \in \pi'} \mathbb{C}_{N_p}(\bigcap_{p \leq q \in \pi'} HN_{\hat{q}}N_{\check{q}}) \\ &= \textstyle\prod_{q \in \pi'} \mathbb{C}_{N_p}(\bigcap_{p \leq q \in \pi'} (H^*N^*_{\hat{q}}N^*_{\check{q}})^g) \\ &= \textstyle\prod_{q \in \pi'} \mathbb{C}_{N_p}((\bigcap_{p \leq q \in \pi'} H^*N^*_{\hat{q}}N^*_{\check{q}})^g) \\ &= \textstyle\prod_{q \in \pi'} (\mathbb{C}_{(N_p^{g^{-1}})}(\bigcap_{p \leq q \in \pi'} H^*N^*_{\hat{q}}N^*_{\check{q}}))^g \\ &= \textstyle\prod_{q \in \pi'} (\mathbb{C}_{N^*_p}(H^*N^*_{\hat{p}}))^g \\ &= (\textstyle\prod_{q \in \pi'} \mathbb{C}_{N^*_p}(H^*N^*_{\hat{p}}))^g \\ &= (S^* \cap N)^g. \end{aligned}$$

Para la independencia de $K \cap N$, tenemos

$$\frac{|N|}{|K \cap N|} = |S \cap N| = |(S^* \cap N)^g|, \quad \text{luego} \quad \frac{|N|}{|(S^* \cap N)^g|} = |K \cap N| \quad \text{y}$$

$$|K^* \cap N| = \frac{|N|}{|S^* \cap N|} = |K \cap N|.$$

Es decir $K^* \cap N$ y $K \cap N$ tienen el mismo orden y por (i) del lema anterior son subgrupos de G' que es cíclico, por lo tanto son iguales.

Definición 3.7. Una factorización metacíclica $G = SK$ es **estándar** si $|S| \geq |X|$ y $|K| \leq |Y|$ para toda factorización metacíclica $G = XY$. Si $G = SK$ es una factorización metacíclica estándar con descomposición de Hall estándar $G = HN$, entonces la factorización $G = (S \cap H)(K \cap H)(S \cap N)(K \cap N)$ es llamada una **factorización estándar** de G.

Como parte final de este capítulo probaremos la existencia de las factorizaciones metacíclicas estándar para grupos metacíclicos de orden impar y daremos una condición de suficiencia y necesidad para que una factorización metacíclica sea estándar.

Lema 3.8 (5.1 en [8]). *Sea $G = H \ltimes N$ un grupo finito con $(|H|, |N|) = 1$. Si $H = XY$ $(Y \trianglelefteq H)$ y $N = UV$ $(V \trianglelefteq N)$ son factorizaciones metacíclicas tales que $X \leqslant \mathbb{N}_H(V)$, $Y \leqslant \mathbb{C}_H(N)$ y $U \leqslant \mathbb{C}_N(H)$, entonces $G = (XU)(YV)$ es una factorización metacíclica de G.*

Prueba. De las hipótesis tenemos $G = (XU)(YV)$. Sean x, y, u, v los generadores de X, Y, U, V respectivamente. Como x y u conmutan y $(|X|, |U|) = 1$, tenemos $XU = \langle xu \rangle \leqslant G$, análogamente $YV = \langle yv \rangle \leqslant G$. Ahora, si tomamos hn en G y $y^a v^a$ en YV y conjugamos, nuestras hipótesis implican:

$$n^{-1}\boldsymbol{h}^{-1}y^a v^a hn = n^{-1}h^{-1}y^a v^a x^k y^c n = n^{-1}y^{-c}x^{-k}y^a x^{\boldsymbol{k}} y^c v^b n = n^{-1}y^l v^b n = y^l v^m$$

Por lo tanto YV es un subgrupo normal de G.

Lema 3.9 (5.9 en [8]). *Todo grupo metacíclico de orden impar tiene una factorización metacíclica estándar.*

Prueba. Sea G un grupo metacíclico de orden impar y $G = SK$ una factorización metacíclica con la descomposición de Hall estándar $G = HN$. Denotemos por $\mathscr{K}$ el conjunto de todos los subgrupos normales cíclicos de H tales que H/Y sea cíclico

y $Y \leqslant \mathbb{O}_\pi(G)$. $K \cap H$ pertenece a $\mathscr{K}$, así que el conjunto es no vacío. Tomemos Y en $\mathscr{K}$ con el menor orden posible en el conjunto. Por el Corolario 2.9, existe un subgrupo cíclico X de H tal que $H = XY$ y $|X| = \exp H$. Definimos $S^* := X(S \cap N)$ y $K^* := Y(K \cap N)$. Por 3.5 tenemos

$$X \leqslant \mathbb{N}_H(K \cap N) \text{ porque } K \cap N \trianglelefteq G; \quad Y \leqslant \mathbb{C}_H(N) \quad \text{y} \quad S \cap N \leqslant \mathbb{C}_N(H),$$

así que por 3.8, $G = S^*K^*$ es una factorización metacíclica de G. Ahora tomemos otra factorización metacíclica $G = S'K'$ con descomposición de Hall estándar $G = H'N$. Como $H = H'^g$ p. a. $g \in G$, entonces $\exp H = \exp H'$ y por el Teorema 3.6, $|S \cap N| = |S' \cap N|$, así que

$$|S^*| = (\exp H)|S \cap N| \geq |S' \cap H'||S' \cap N| = |S'|.$$

Por otro lado, si Y' es un subgrupo cíclico de H' cuyo cociente es cíclico, entonces Y'^g es un subgrupo cíclico de $H'^g = H$ cuyo cociente es cíclico, es decir $Y'^g \in \mathscr{K}$ y $|Y'| = |Y'^g| \geq |Y|$. Por el Teorema 3.6 $|K \cap N| = |K' \cap N|$, luego

$$|K^*| = |Y||K \cap N| \leq |K' \cap H'||K' \cap N| = |K'|.$$

Por lo tanto, $G = S^*K^*$ es una factorización metacíclica estándar. Más aún, $S^* \cap H = X$, $K^* \cap H = Y$, $S^* \cap N = S \cap N$ y $K^* \cap N = K \cap N$.

Lema 3.10 (5.10 en [8]). *Una factorización metacíclica $G = SK$ de un grupo metacíclico de orden impar es estándar si y sólo si para cada p en π, $H_p = S_pK_p$ es una factorización metacíclica $\mathbb{O}_p(G)$-estándar.*

Prueba. Sea G un grupo metacíclico de orden impar con una factorización metacíclica $G = SK$. Supongamos primero que es estándar, como en el lema anterior, sabemos que existen X y Y tales que $H = XY$, $|X| = \exp H$ y $|Y|$ es de orden minimal en $\mathscr{K}$. También sabemos que si $S^* := X(S \cap N)$ y $K^* := Y(K \cap N)$, entonces $G = S^*K^*$ es una factorización metacíclica estándar, luego

$$|S \cap H||S \cap N| = |S| = |S^*| = |X||S \cap N)| \quad \text{y}$$
$$|K \cap H||K \cap N| = |K| = |K^*| = |Y||K \cap N)|$$

Así que $|S \cap H| = \exp H$ y $|K \cap H|$ es de orden minimal en $\mathscr{K}$. Para cada $p \in \pi$, sean n_p la máxima potencia de p que divide a $\exp H$ y m_p la máxima potencia de p que divide a $|K \cap H|$. Como $|K \cap H|$ divide a $|S \cap H|$, entonces $n_p \geq m_p$, es decir $|S_p| = p^{n_p} \geq p^{m_p} = |K_p|$. Por otro lado, H_p es regular, por lo tanto $\exp H_p = \max\{|S_p|, |K_p|\} = |S_p|$.

Ahora, es claro que, para cada $p \in \pi$, K_p es un núcleo de H_p contenido en $\mathbb{O}_p(G)$, podemos entonces tomar B_p un núcleo $\mathbb{O}_p(G)$-minimal de H_p y $B := \prod_{p\in\pi} B_p$ está en $\mathscr{K}$. Así que $|B| \geq |K \cap H|$. Si $|B| > |K \cap H|$, entonces $|B_p| > p^{m_p} = |K_p|$ p. a. $p \in \pi$, lo que contradice la $\mathbb{O}_p(G)$-minimalidad de B_p, luego $|B| = |K \cap H|$ y $|B_p| = |K_p|$. Por lo tanto $H_p = S_pK_p$ es una factorización metacíclica $\mathbb{O}_p(G)$-estándar.

Ahora sea $H_p = S_pK_p$ una factorización metacíclica $\mathbb{O}_p(G)$-estándar para cada $p \in \pi$. Tomemos $G = S'K'$ otra factorización metacíclica de G con descomposición de Hall estándar $G = H'N$. Como H es un conjugado de H', entonces para cada $p \in \pi$, $|S'_p|$ divide a $\exp H'_p = \exp H_p = |S_p|$, luego

$$|S \cap H| = \prod_{p\in\pi} |S_p| \geq \prod_{p\in\pi} |S'_p| = |S' \cap H'|.$$

De 3.6 sabemos que $|S\cap N| = |S'\cap N|$ y $|S| = |S\cap H||S\cap N| \geq |S'\cap H'||S'\cap N| = |S'|$. Como H es un conjugado de H', análogamente al lema anterior, observamos que $|K_p| \leq |K'_p|$ para todo $p \in \pi$, así que

$$|K \cap H| = \prod_{p\in\pi} |K_p| \leq \prod_{p\in\pi} |K'_p| = |K' \cap H'|.$$

Del Teorema 3.6, sabemos que $K \cap N = K' \cap N$ y $|K| = |K \cap H||K \cap N| \leq |K' \cap H'||K' \cap N| = |K'|$. Por lo tanto $G = SK$ es una factorización metacíclica estándar.

Capítulo 4

Presentación estándar para grupos metacíclicos de orden impar

Ahora construiremos la presentación para grupos metacíclicos de orden impar propuesta por Hyo-Seob Sim, basándonos en los principales resultados de los dos capítulos anteriores. Probaremos que la mayoría de los parámetros involucrados son invariantes de los tipos de isomorfismo de los grupos definidos por éstas.

Notación. Sean m y n enteros positivos y p un número primo. Denotaremos por $\mathbf{m(p)}$ al entero más grande i tal que p^i divide a m. El conjunto $\{p \mid p \text{ primo}, m(p) > n(p)\}$ será denotado por $\pi(\mathbf{m/n})$.

Llamaremos $\mathbf{\Omega}$ al conjunto de todos los *'octetos'* $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$ de enteros positivos tales que para $\kappa := |\theta \bmod \zeta|$, se satisfacen las siguientes condiciones:

$$\begin{gathered}
\beta|\alpha,\ \beta|\gamma,\ \delta|\gamma,\ \gamma|\beta\delta, \\
\pi(\beta) \subseteq \pi(\delta), \\
\pi(\varepsilon) \subseteq \pi(\zeta), \\
\pi(\delta/\beta) \subseteq \pi(\beta\kappa/\alpha), \\
\pi(\alpha\gamma) \cap \pi(\zeta) = \varnothing, \\
\eta^{\varepsilon} \equiv 1 \bmod \zeta, \\
\theta^{\alpha} \equiv 1 \bmod \zeta, \\
(\theta\eta - 1,\ \zeta) = 1,
\end{gathered}$$

En el artículo *Metacyclic groups of odd order* [8], encontramos una última condición. Para $\mu := \text{m.c.m}\{q - 1 : q \in \pi(\zeta)\}$, (cuando $\zeta = 1$, $\mu := 1$), Sim considera también $\theta^{\mu} \equiv 1 \bmod \zeta$, mas el siguiente lema de Hempel prueba que no es necesaria.

Lema 4.1 (6.1 en [4]). *Sean α, ζ y θ enteros con $(\alpha, \zeta) = 1$. Si μ está definido como arriba y $\theta^\alpha \equiv 1 \bmod \zeta$, entonces $\theta^\mu \equiv 1 \bmod \zeta$.*

Prueba. Tomemos q en $\pi(\zeta)$. Como $(\alpha, \zeta) = 1$ tenemos $q \nmid \alpha$. Además $|\theta \bmod \zeta|$ divide a α por lo que q no divide a $|\theta \bmod \zeta|$. Por otro lado, $|\theta \bmod q^{\zeta(q)}|$ divide a $|\theta \bmod \zeta|$, luego q no divide a $|\theta \bmod q^{\zeta(q)}|$. Sabemos que el grupo de las unidades de los residuos reducidos módulo $q^{\zeta(q)}$ tiene tamaño $q^{\zeta(q)-1}(q-1)$, luego $|\theta \bmod q^{\zeta(q)}|$ divide a $q-1$. Pero $(q-1)|\mu$, luego $\theta^\mu \equiv 1 \bmod q^{\zeta(q)}$, con esto obtenemos el resultado.

Notación. Dados dos enteros positivos m y n el número $(\mathbf{m}|\mathbf{n})$, denota la solución no negativa más pequeña del sistema de congruencias simultáneas

$$x \equiv p^{m(p)} \bmod p^{n(p)}, \quad p \in \pi(n).$$

Observamos que si m divide a n, entonces para todo primo $p \in \pi(n)$, $(m|n) = p^{n(p)}a + p^{m(p)} = p^{m(p)}(1 + ap^k)$ con a y k enteros. Si $k > 0$, el máximo exponente de p que divide a $(m|n)$ es precisamente $m(p)$. Ahora, si $k = 0$, entonces $(m|n)$ es un múltiplo de $p^{n(p)} = p^{m(p)}$, así que $m = ((m|n), n)$.

Sea $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$ un elemento fijo en Ω con α, β, γ, δ, ε, ζ números impares. Definimos una presentación con el conjunto generador $\{x, y, u, v\}$ y las relaciones:

$$\begin{array}{llll} x^\alpha = y^\beta, & & & \\ y^\gamma = 1, & y^x = y^{1+(\delta|\gamma)}, & & \\ u^\varepsilon = 1, & u^x = u, & u^y = u, & \\ v^\zeta = 1, & v^x = v^\theta, & v^y = v, & v^u = v^\eta. \end{array}$$

Denotamos esta presentación por $\wp(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$ y la llamaremos una **presentación estándar**. Manteniendo los otros parámetros fijos, algunas veces abreviaremos esta presentación como $\wp(\eta, \theta)$, $\wp(\eta)$, $\wp(\theta)$, o simplemente $\wp$.

Nuestro objetivo ahora es probar el siguiente teorema.

Teorema 4.2 (6.3 en [8]). *Todo grupo metacíclico de orden impar tienen una presentación estándar y cada presentación estándar define un grupo metacíclico de orden impar. Los parámetros α, β, γ, δ, ε, ζ y el orden multiplicativo, κ, de θ módulo ζ son determinados por el tipo de isomorfismo del grupo presentado por ésta.*

Dividimos la prueba de este teorema en tres lemas.

Lema 4.3 (6.4 en [8]). *Si G es un grupo metacíclico de orden impar con una factorización estándar $G = XYUV$, entonces G tiene una presentación estándar $\wp(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta)$ donde*

$$\alpha = \left|\frac{X}{X \cap Y}\right|, \quad \beta = \left|\frac{Y}{X \cap Y}\right|, \quad \gamma = |Y|, \quad \delta = \left|\frac{Y}{(XY)'}\right|, \quad \varepsilon = |U|, \quad \zeta = |V|.$$

Prueba. Sean $H := XY$, $N := UV$, $S := XU$ y $K := YV$. Recordemos que $G = HN$ es la descomposición de Hall estándar para la factorización metacíclica $G = SK$. Definamos π, ϖ como los conjuntos de todos los primos divisores de los órdenes de H y N respectivamente. Entonces $\pi = \pi(\alpha\gamma)$, ya que $|H| = \alpha\gamma$. Por otro lado, observamos que si $K_q = 1$ para algún q en ϖ, entonces $S_{q'}K_{q'}$ es un q'-subgrupo de Hall normal, ya que $G = S_qS_{q'}K_{q'}K_q = S_qS_{q'}K_{q'}$, así que conjugar por un elemento de G se reduce a conjugar por uno de S_q. Concluiríamos entonces que q está en π, pero esto no ocurre, así que para todo q en ϖ tenemos $K_q \neq 1$. Como $V = K_\varpi$, entonces $V = \prod_{q\in\varpi} K_q$ y, por lo tanto, $\varpi = \pi(\zeta)$. Tenemos entonces $\pi(\varepsilon) \subseteq \pi(\zeta)$, además como π y ϖ son disjuntos, $\pi(\alpha\gamma) \cap \pi(\zeta) = \varnothing$.

Para cada $p \in \pi$, por el Lema 3.10, $H_p = S_pK_p$ es una factorización metacíclica $\mathbb{O}_p(G)$-estándar. Además, $|K_p| = |Y_p|$ y K es cíclico, así que Y_p es el p-subgrupo de Sylow de K. Análogamente, X_p es el p-subgrupo de Sylow de S. Luego por el Lema 2.12(iii), $\beta|\alpha$, por 2.12(i) $\beta|\gamma$, $\delta|\gamma$, $\gamma|\beta\delta$ y por 2.12(ii) $\pi(\beta) \subseteq \pi(\delta)$. Por este mismo lema, cada H_p tiene la siguiente presentación:

$$\langle x_p,\ y_p \mid x_p^{p^{\alpha(p)}} = y_p^{p^{\beta(p)}},\ y_p^{p^{\gamma(p)}} = 1,\ y_p^{x_p} = y_p^{1+p^{\delta(p)}} \rangle.$$

Sean $x := \Pi_{p\in\pi} x_p$ y $y := (\Pi_{p\in\pi} y_p^{\alpha_{p'}})^s$ donde $\alpha_{p'}$ es la p'-componente de α y $s = (\beta|\gamma)/\beta$. Claramente $y_p^{\alpha_{p'}}$ genera Y_p y $((\beta|\gamma),\ \gamma) = \beta$, luego $(s,\ \gamma) = 1$, así que $\langle x \rangle = X$ y $\langle y \rangle = Y$. Además x y y satisfacen las siguientes relaciones:

$$x^\alpha = y^\beta, \quad y^\gamma = 1, \quad y^x = y^{1+(\delta|\gamma)},$$

ya que

$$y^\beta = (\Pi_{p\in\pi} y_p^{\alpha_{p'}})^{(\beta|\gamma)} = \Pi_{p\in\pi} y_p^{\alpha_{p'}p^{\beta(p)}} = \Pi_{p\in\pi} x_p^{p^{\alpha(p)}\alpha_{p'}} = x^\alpha;$$

$y^\gamma = 1$ es inmediata, y finalmente:

$$\begin{aligned} y^x &= x^{-1}(\Pi_{p\in\pi} y_p^{s\alpha_{p'}})x = \Pi_{p\in\pi} x_p^{-1}(\Pi_{p\in\pi} y_p^{s\alpha_{p'}})\Pi_{p\in\pi} x_p \\ &= \Pi_{p\in\pi} x_p^{-1} y_p^{s\alpha_{p'}} x_p \quad \text{porque } x_p y_q = y_q x_p \text{ si } p \neq q \\ &= \Pi_{p\in\pi}(x_p^{-1} y_p x_p)^{s\alpha_{p'}} \\ &= \Pi_{p\in\pi} y_p^{(1+p^{\delta(p)})s\alpha_{p'}} = (\Pi_{p\in\pi} y_p^{\alpha_{p'}})^{s(1+(\delta|\gamma))} \\ &= y^{1+(\delta|\gamma)}. \end{aligned}$$

Sean u y v generadores de U y V respectivamente, claramente tenemos $u^\varepsilon = 1$ y $v^\zeta = 1$. Sea θ un entero positivo tal que $v^x = v^\theta$, definimos $\kappa := |\theta \bmod \zeta|$. Probaremos $\kappa = [H : \mathbb{O}_\pi(G)]$. Claramente $Y \leqslant \mathbb{O}_\pi(G)$, por lo que basta probar que x^κ es la primera potencia de x en $\mathbb{O}_\pi(G)$. Como G es soluble y H es un π-subgrupo de Hall, cualquier otro π-subgrupo de Hall es conjugado de H, así que por 1.29, basta demostrar $x^\kappa \in g^{-1}Hg$ para toda $g \in G$ y que κ es la primera potencia. Como $Y \leqslant \mathbb{O}_\pi(G) \leqslant \mathbb{C}_H(N)$ y $X,\ U \leqslant S$, entonces basta conjugar x^κ por v, pero esto es precisamente x^κ y $\kappa = [H : \mathbb{O}_\pi(G)]$ porque es la primera potencia de x que conmuta con v. Como el orden de Y divide al orden de $\mathbb{O}_\pi(G)$, tenemos $\kappa|\alpha$, así que $\theta^\alpha \equiv 1 \bmod \zeta$. Como la factorización metacíclica $\langle x_p\rangle\langle y_p\rangle$ de cada H_p es $\mathbb{O}_p(G)$-estándar, del Lema 2.12(iv), tenemos que si $\beta(p) < \delta(p)$, entonces $\alpha(p) - \kappa(p) < \beta(p)$, por tanto $\pi(\delta/\beta) \subseteq \pi(\beta\kappa/\alpha)$.

Ahora sea η un entero positivo tal que $v^u = v^\eta$. Entonces $\eta^\varepsilon \equiv 1 \bmod \zeta$. Si G es nilpotente, $N = 1$, esto es $\zeta = 1$. Si G no es nilpotente, sea q un primo en ϖ. Como $G = HN$ es la descomposición de Hall estándar para $G = SK$, los q'-subgrupos de Hall no son normales. Por lo tanto $S_{q'}$ actúa de manera no trivial en K_q y, por el Lema 1.36, así mismo en $\Omega_1(K_q)$. Luego, S actúa no trivialmente en $\Omega_1(K_q) = \mathsf{C}(q)$ y $(\theta\eta - 1,\ q) = 1$. En cualquier caso, obtenemos $(\theta\eta - 1,\ \zeta) = 1$.

Hemos observado que los parámetros $\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta$ y θ satisfacen las condiciones para los parámetros de las presentaciones estándar, así que dan origen a una presentación estándar $\wp(\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta,\ \theta)$. Por otro lado el conjunto $\{x,\ y,\ u,\ v\}$ genera a G. Las relaciones $u^x = u$ y $v^y = v$ son obvias y $u^y = u$ se obtiene del Teorema 3.6, así que $\{x,\ y,\ u,\ v\}$ satisface las relaciones de $\wp$. Por lo tanto, G es una imagen homomórfica del grupo definido por la presentación estándar $\wp$. La presentación $\wp$ define un grupo de orden a lo más $\alpha\gamma\varepsilon\zeta$, así que $\wp$ es una presentación estándar para G.

Consideremos una presentación estándar $\wp(\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta,\ \theta)$, sea $G := \langle x,\ y,\ u,\ v\rangle$ el grupo definido por ella. En lo que resta de este capítulo, κ denota el orden multiplicativo $|\theta \bmod \zeta|$ y mantenemos la siguiente notación fija:

$$H := \langle x,\ y\rangle, \quad X := \langle x\rangle, \quad Y := \langle y\rangle, \quad S := XU, \quad \pi := \pi(H)$$

$$N := \langle u,\ v\rangle, \quad U := \langle u\rangle, \quad V := \langle v\rangle, \quad K := YV, \quad \varpi := \pi(N)$$

Lema 4.4 (6.5 en [8]).

(i) H es un subgrupo metacíclico nilpotente con una presentación:

$$\langle x,\ y \mid x^{\alpha} = y^{\beta},\ y^{\gamma} = 1,\ y^{x} = y^{1+(\delta|\gamma)} \rangle,$$

$|H| = \alpha\gamma$, $|H/H'| = \alpha\delta$ *y* $\exp H = \alpha\gamma/\beta$;

(ii) N es un subgrupo metacíclico normal de orden $\varepsilon\zeta$ con una presentación:

$$\langle u,\ v \mid u^{\varepsilon} = 1,\ v^{\zeta} = 1,\ v^{u} = v^{\eta} \rangle;$$

(iii) $G = SK$ es una factorización metacíclica y su descomposición de Hall estándar es $G = HN$;

(iv) $\mathbb{O}_{\pi}(G) = \langle x^{\kappa},\ y \rangle$ y por lo tanto, $[H : \mathbb{O}_{\pi}(G)] = \kappa$.

Prueba. Sean

$$\bar{H} := \langle a,\ b \mid a^{\alpha} = b^{\beta},\ b^{\gamma} = 1,\ b^{a} = b^{1+(\delta|\gamma)} \rangle \quad \text{y}$$

$$\bar{N} := \langle c,\ d \mid c^{\varepsilon} = 1,\ d^{\zeta} = 1,\ d^{c} = d^{\eta} \rangle.$$

Obviamente $|\bar{H}| \leq \alpha\gamma$. Consideremos el grupo presentado por:

$$\langle a_p,\ b_p \mid a_p^{p^{\alpha(p)}} = b_p^{p^{\beta(p)}},\ b_p^{p^{\gamma(p)}} = 1,\ b_p^{a_p} = b_p^{1+p^{\delta(p)}} \rangle.$$

Si $r_p := \alpha_{p'}/\beta_{p'}$, entonces $(r_p,\ p) = 1$ y por lo tanto, la pareja $a_p, b_p^{r_p}$ genera el grupo definido por esta última presentación. Ahora

$$a_p^{\alpha} = a_p^{p^{\alpha(p)}\alpha_{p'}} = b_p^{p^{\beta(p)}\alpha_{p'}} = (b_p^{r_p})^{\beta}, \quad (b_p^{r_p})^{\gamma} = 1 \text{ y}$$

$$(b_p^{r_p})^{a_p} = b_p^{(1+p^{\delta(p)})r_p} = (b_p^{r_p})^{1+(\delta|\gamma)}.$$

Es decir, $a_p, b_p^{r_p}$ satisfacen las relaciones de $\bar{H}$ y el grupo que generan es una imagen homomórfica de $\bar{H}$, supongamos que lo es bajo f_p. Sabemos que este grupo tiene orden $p^{\alpha(p)+\gamma(p)} = |\bar{H}/\ker f_p|$, luego, si p y q son primos distintos en $\pi(\alpha\gamma)$ tenemos $(|\bar{H}/\ker f_p|,\ |\bar{H}/\ker f_q|) = 1$. Entonces $|\bar{H}/\bigcap_{p\in\pi(\alpha\gamma)} \ker f_p| = \alpha\gamma$. Esto muestra que $|\bar{H}| = \alpha\gamma$ y que $\bar{H}$ es el producto directo de los p-grupos definidos por las presentaciones de arriba con p corriendo en $\pi(\alpha\gamma)$. En particular, estos p-grupos son los subgrupos de Sylow de $\bar{H}$, luego $\bar{H}$ es nilpotente. Por otro lado, $\bar{N}$ es un grupo metacíclico de orden $\varepsilon\zeta$. Como $\theta^{\alpha} \equiv 1 \bmod \zeta$, entonces $\kappa|\alpha$, luego el grupo $\langle a^{\kappa},\ b \rangle$ es

un subgrupo normal de índice κ en $\bar{H}$, mientras que en $\bar{N}$, el automorfismo $c \mapsto c$, $d \mapsto d^{\theta}$ tiene orden κ. Como consecuencia tenemos que

$$c^a = c, \quad d^a = d^{\theta}, \quad c^b = c, \quad d^b = d$$

definen una acción de $\bar{H}$ en $\bar{N}$ con kernel $H^* = \langle a^{\kappa}, b \rangle$ y podemos formar el producto semidirecto correspondiente $\bar{G} = \bar{H} \ltimes \bar{N}$. El conjunto $\{a, b, c, d\}$ genera a $\bar{G}$ y sus elementos satisfacen todas las relaciones de G. Luego $\bar{G}$ es una imagen homomórfica de G. Por otro lado, el subgrupo H de G es una imagen homomórfica de $\bar{H}$, al igual que el subgrupo N de G es una imagen homomórfica de $\bar{N}$. Además $G = HN$. Entonces

$$|\bar{G}| \leq |G| \leq |H||N| \leq |\bar{H}||\bar{N}| = |\bar{G}|.$$

Luego

$$|H| \leq |\bar{H}| = \frac{|\bar{G}|}{|\bar{N}|} = \frac{|G|}{|\bar{N}|} \leq \frac{|G|}{|N|} = |H|.$$

Es decir $H \cong \bar{H}$, $N \cong \bar{N}$ y $G \cong \bar{G}$. De esto tenemos $|G| = \alpha\gamma\varepsilon\zeta$. Del Lema 3.8, sabemos que $G = SK$ es una factorización metacíclica.

Verificaremos ahora que $G = HN$ es la descomposición de Hall estándar para $G = SK$. Supongamos que existe un primo q en ϖ tal que un q'-subgrupo de Hall es normal en G. Es decir, $S_{q'}K_{q'}$ es normal en G. Ahora

$$s \in S_{q'}, k \in K_q \Rightarrow s^{-1}k^{-1}s \in K_q \quad \text{y} \quad k^{-1}sk \in S_{q'}K_{q'}$$

Por lo tanto, $s^{-1}k^{-1}sk = 1$, es decir $[S_{q'},\ K_q] = 1$. Como $S = XU$ y $\pi(X) \cap \pi(U) = \varnothing$ entonces $|S_{q'}| = \varepsilon_{q'}|X|$. De aquí obtenemos que $\langle xu^{q^{\varepsilon(q)}} \rangle = S_{q'}$. Además, la condición $(\theta\eta - 1,\ \zeta) = 1$ implica $(\theta\eta - 1,\ q) = 1$ y $\eta^{q^{\varepsilon(q)}} \equiv \eta \bmod q$ por el Pequeño Teorema de Fermat. Así que $(\theta\eta^{q^{\varepsilon(q)}} - 1,\ q) = 1$, luego conjugar a los elementos de K_q por $xu^{q^{\varepsilon(q)}}$ define una acción no trivial, es decir $S_{q'}$ actúa de manera no trivial en K_q, contradiciendo $[S_{q'},\ K_q] = 1$. Concluimos

$$\pi = \{p \in \pi(G) \mid G \text{ tiene un } p'\text{-subgrupo de Hall normal}\}$$

Por lo tanto, $G = HN$ es la descomposición de Hall estándar para la factorización metacíclica $G = SK$. Como $\delta|\gamma$ tenemos $((\delta|\gamma),\ \gamma) = \delta$, así que $|H'| = \gamma/\delta$ y $|H/H'| = \alpha\delta$. Para cada $p \in \pi$, H_p es regular, luego $\exp H_p = max\{o(x),\ o(y)\} = p^{\alpha(p)+\gamma(p)-\beta(p)}$, por tanto $\exp H = \alpha\gamma/\beta$. Finalmente, de la prueba del lema anterior obtenemos $\mathbb{O}_{\pi}(G) = H^*$.

Lema 4.5 (6.6 en [8]). *Los parámetros α, β, γ, δ, ε, ζ y κ son invariantes de G.*

Prueba. Como N es la intersección de los complementos de Sylow normales, tenemos que $|N| = \varepsilon\zeta$ es un invariante de G, y, por lo tanto, $|H| = \alpha\gamma$ es también un invariante. Por el lema anterior $\exp H = \alpha\gamma/\beta$ y $[H : \mathbb{O}_\pi(G)] = \kappa$, así que β y κ son invariantes.

Como consecuencia, si para cada $p \in \pi$, definimos $g_p := p^{\beta(p)+\kappa(p)}$, éste también es un invariante. Para cada p-subgrupo de Sylow de H, H_p, $e_p :=\exp(H_p/H_p')$ y $f_p := |H_p|/\exp \mathbb{O}_p(G)$ son invariantes. Podemos calcular explícitamente e_p y f_p.

Como H_p es regular, $e_p = max\{o(a_pH_p'),\ o(b_pH_p')\}$. Si $\beta(p) > \delta(p)$, entonces $\alpha(p) \geq \beta(p) > \delta(p)$, por lo tanto $e_p = p^{\alpha(p)}$. Si $\delta(p) \geq \beta(p)$, entonces $o(a_pH_p') = p^{\alpha(p)+\delta(p)-\beta(p)}$, luego $e_p = p^{\alpha(p)+\delta(p)-\beta(p)}$. Esto es, $e_p = max\{p^{\alpha(p)},\ p^{\alpha(p)+\delta(p)-\beta(p)}\}$. Como $\mathbb{O}_p(G) = \langle a_p^{p^{\kappa(p)}},\ b_p\rangle$, tenemos $\exp \mathbb{O}_p(G) = max\{p^{\gamma(p)+\alpha(p)-\kappa(p)-\beta(p)},\ p^{\gamma(p)}\}$ y por lo tanto, $f_p = min\{p^{\beta(p)+\kappa(p)},\ p^{\alpha(p)}\}$. Sea π^* el conjunto $\{p \in \pi \mid f_p = g_p\}$. Como f_p y g_p son invariantes para cada $p \in \pi$, entonces π^* y $\pi \setminus \pi^*$ están determinados por el tipo de isomorfismo de G. Observamos que, cualquiera que sea el valor de $\exp \mathbb{O}_p(G)$, $f_p \leq g_p$. Si $f_p = g_p$, entonces $\alpha(p) \geq \beta(p) + \kappa(p)$ y, como $\pi(\delta/\beta) \subseteq \pi(\beta\kappa/\alpha)$, tenemos $\beta(p) \geq \delta(p)$, luego $e_p = p^{\alpha(p)}$. Si $f_p < g_p$, entonces $f_p = p^{\alpha(p)}$. Concluimos entonces $\alpha = \Pi_{p\in\pi^*} e_p \Pi_{p\in\pi\setminus\pi^*} f_p$, y, por lo tanto, es un invariante. Como $\exp H = \alpha\gamma/\delta$ y $|H/H'| = \alpha\delta$ son invariantes, entonces γ y δ también lo son.

Del Teorema 3.6, sabemos que $|U| = |S \cap N| = \varepsilon$ y $|V| = |K \cap N| = \zeta$ son invariantes de G.

Los tres lemas anteriores proporcionan una prueba del Teorema 4.2. Manteniendo la misma notación, de estos lemas tenemos también la siguiente consecuencia.

Corolario 4.6 (6.7 en [8]). *La factorización $G = XYUV$ es estándar.*

Prueba. Sea $G = S_0Y_0U_0V_0$ una factorización estándar. Como $|X_0| = \exp H = |X|$, entonces, por el Teorema 3.6, sólo tenemos que probar $|Y| = |Y_0|$. Por el Lema 4.3, G tiene una presentación estándar $\wp(\alpha_0,\ \beta_0,\ \gamma_0,\ \delta_0,\ \varepsilon_0,\ \zeta_0,\ \eta_0,\ \theta_0)$ con $|Y_0| = \gamma_0$, pero, por el Lema 4.5, $\gamma = \gamma_0$. Es decir $|Y| = \gamma = \gamma_0 = |Y_0|$.

Observación (6.2 en [8]). Una presentación metacíclica consistente para el grupo definido por una presentación estándar puede ser dada de la siguiente manera:

$$\langle a,\ b \mid a^{\alpha\varepsilon} = b^{\beta\zeta},\ b^{\gamma\zeta} = 1,\ b^a = b^n\rangle$$

Donde n es el entero no negativo más pequeño tal que

$$\begin{cases} n & \equiv & 1 + (\delta|\gamma) \bmod \gamma, \\ n & \equiv & \eta\theta \bmod \zeta, \end{cases}$$

ya que y^{ζ} es un generador de Y, entonces para algún entero d

$$x^{\varepsilon\alpha} = y^{\varepsilon\beta} = y^{d\zeta\beta}.$$

Como $x^{\varepsilon\alpha}$ tiene orden $p^{\gamma-\beta}$, entonces $(d,p) = 1$ y y^d genera Y. Así que $a := xu, b := y^d v$ son los generadores de la presentación de arriba.

Capítulo 5

Ciertos automorfismos de p-grupos metacíclicos con p impar

Hemos visto que seis de los ocho parámetros de una presentación estándar son invariantes del grupo. En el siguiente capítulo determinaremos cuándo dos grupos definidos por dos presentaciones estándar son isomorfos, claramente, esta determinación estará basada en los parámetros θ y η. Como veremos al principio del siguiente capítulo, podremos investigar este problema en dos partes, cada una con uno de estos parámetros fijo.

Siendo η el parámetro para la conjugación de v por u (utilizando la notación del capítulo anterior), el Teorema 3.6 nos permitirá resolver fácilmente el caso θ fijo. Para η fijo tendremos que investigar la acción de H en N. Recordemos que H es el producto directo de sus p-grupos de Sylow H_p y la presentación estándar está basada en una factorización $\mathbb{O}_p(G)$-estándar para H_p. Por este motivo, nuestro objeto de estudio en este capítulo será cierto subgrupo de $\mathrm{Aut}(P/C)$, donde P es un p-grupo metacíclico con p impar y una factorización metacíclica C-estándar para algún subgrupo C. Este capítulo tendrá como objetivo conocer, en términos de una factorización metacíclica C-estándar fija, el tamaño del subgrupo de $\mathrm{Aut}(P/C)$ cuyos elementos se han obtenido de todos los automorfismos de P que normalizan, es decir, fijan conjuntistamente a C. Como resultado de este estudio sabremos, dada una factorización metacíclica C-estándar, cuántos y cómo son todos los núcleos de P que dan origen a factorizaciones metacíclicas C-estándar.

Definición 5.1. Sean $Y \trianglelefteq X \leqslant P$ y N un grupo de automorfismos de P que normalizan a X y Y. Cada elemento de N define un automorfismo de X/Y de manera natural, el conjunto de todos estos automorfismos, será denotado por $N\downarrow_{X/Y}$.

Escribiremos $\mathbb{N}_{\mathrm{Aut}\,P}(C)$ para el subgrupo de automorfismos de P que normalizan C y $\mathbb{C}_{\mathrm{Aut}\,P}(P/C)$ denotará a los elementos de $\mathbb{N}_{\mathrm{Aut}\,P}(C)$ tales que al obtener de manera natural un automorfismo de P/C, éste es la función identidad.

Lema 5.2 (4.1 en [8]). *Sea $P = SK$ una factorización metacíclica de un p-grupo P para p un primo arbitrario. Supongamos que C es un subgrupo de P que contiene a K. Entonces*

(i) si P es abeliano, $\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C} = \mathrm{Aut}(P/C)$;

(ii) en cualquier caso, $\mathbb{N}_{\mathrm{Aut}\,P}(C) = [\mathbb{N}_{\mathrm{Aut}\,P}(S) \cap \mathbb{N}_{\mathrm{Aut}\,P}(C)]\mathbb{C}_{\mathrm{Aut}\,P}(P/C)$.

Prueba. Como P/C es cíclico, todo automorfismo suyo es de la forma $aC \mapsto a^sC$ para algún entero s con $(s,\ p) = 1$. Si P es abeliano, el mapeo $x \mapsto x^s$, $x \in P$ es inyectivo, ya que $x^s = 1$ implica $o(x)|s$, luego $x = 1$, así que éste es un automorfismo de P. Claramente, este mapeo normaliza todo subgrupo de P y por lo tanto,

$$\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C} \hookrightarrow \mathrm{Aut}(P/C) \text{ y}$$

$$[\mathbb{N}_{\mathrm{Aut}\,P}(S) \cap \mathbb{N}_{\mathrm{Aut}\,P}(C)]\downarrow_{P/C} \hookrightarrow \mathrm{Aut}(P/C)$$

son suprayectivos, obtenemos entonces

$$\mathrm{Aut}(P/C) = \mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C} = [\mathbb{N}_{\mathrm{Aut}\,P}(S) \cap \mathbb{N}_{\mathrm{Aut}\,P}(C)]\downarrow_{P/C}.$$

De esta última igualdad obtenemos también que, si $\sigma \in \mathbb{N}_{\mathrm{Aut}\,P}(C)$ entonces $\sigma\downarrow_{P/C} = \alpha\downarrow_{P/C}$ para algún $\alpha \in \mathbb{N}_{\mathrm{Aut}\,P}(S) \cap \mathbb{N}_{\mathrm{Aut}\,P}(C)$. Luego $\sigma = \alpha(\alpha^{-1}\sigma)$ y $\alpha^{-1}\sigma$ pertenece a $\mathbb{C}_{\mathrm{Aut}\,P}(P/C)$, obteniendo el segundo resultado para P abeliano.

Supongamos ahora P no abeliano. El resultado es obvio si $C = P$, así que supongamos C subgrupo propio de P. Sólo tenemos que demostrar

$$\mathbb{N}_{\mathrm{Aut}\,P}(C) \leqslant [\mathbb{N}_{\mathrm{Aut}\,P}(S) \cap \mathbb{N}_{\mathrm{Aut}\,P}(C)]\mathbb{C}_{\mathrm{Aut}\,P}(P/C),$$

ya que la otra inclusión es obvia.

Sea x un generador fijo de S. Sabemos que existe un entero m tal que $b^x = b^m$ para toda b en K. También podemos encontrar un generador y de K tal que $x^{|S/(S\cap K)|} = y^{|K/(S\cap K)|}$. Entonces P tiene una presentación en los generadores x, y con las relaciones

$$x^{|S/(S\cap K)|} = y^{|K/(S\cap K)|},\ y^{|K|} = 1,\ y^x = y^m.$$

En el futuro, si A es un grupo y α es un homomorfismo de grupos, denotaremos por A^α a la imagen de A bajo α. Tomemos entonces, σ un automorfismo en $\mathbb{N}_{\mathrm{Aut}\,P}(C)$. Así, $P = S^\sigma K^\sigma$, K^σ es cíclico normal y S^σ es cíclico, por lo que ésta es una factorización metacíclica para P con $K^\sigma \leqslant C$. Por el Lema 2.10, $P = S^\sigma K$. Supongamos $x = \bar{x}b$ p.a. $\bar{x} \in S^\sigma$, $b \in K$. Entonces $xC = \bar{x}C$ y $\langle \bar{x} \rangle$ es un suplemento de C en P, luego $\langle \bar{x} \rangle$ es un suplemento de K en P. Por la Ley Modular de Dedekind obtenemos $S^\sigma = \langle \bar{x} \rangle (S^\sigma \cap K)$. Como S^σ es cíclico, $S^\sigma \cap K \leqslant \langle \bar{x} \rangle$ ó $\langle \bar{x} \rangle < S^\sigma \cap K$, mas este último caso implicaría P cíclico, así que $\langle \bar{x} \rangle = S^\sigma$. Podemos encontrar un generador $\bar{y}$ de K tal que $\bar{x}^{|S^\sigma/(S^\sigma \cap K)|} = \bar{y}^{|K/(S^\sigma \cap K)|}$. Como $|S^\sigma| = |S|$ y $|S \cap K| = |S^\sigma \cap K|$, entonces $\bar{x}^{|S/(S \cap K)|} = \bar{y}^{|K/(S \cap K)|}$. Claramente $\bar{y}^{\bar{x}} = \bar{y}^m$ y $\bar{y}^{|K|} = 1$.

Hemos obtenido una presentación para P de la anterior remplazando x con $\bar{x}$ y y con $\bar{y}$. El mapeo $\bar{x} \mapsto x$, $\bar{y} \mapsto y$ define un automorfismo de P, al que llamaremos τ. Sabemos que C y C^τ son subgrupos de P del mismo orden conteniendo a K; como P/K es cíclico, entonces $C/K = C^\tau/K$, así que $C = C^\tau$. Claramente $(S^\sigma)^\tau = S$, así que $\tau\sigma \in \mathbb{N}_{\mathrm{Aut}\,P}(S) \cap \mathbb{N}_{\mathrm{Aut}\,P}(C)$. Por otro lado $\tau^{-1}xC = \bar{x}C = xC$, es decir $\tau \in \mathbb{C}_{\mathrm{Aut}\,P}(P/C)$. Por lo tanto $\sigma = \tau^{-1}(\tau\sigma) \in [\mathbb{N}_{\mathrm{Aut}\,P}(S) \cap \mathbb{N}_{\mathrm{Aut}\,P}(C)]\mathbb{C}_{\mathrm{Aut}\,P}(P/C)$.

Como hemos dicho, determinaremos el orden de $\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}$, esto resulta suficiente para *conocer* a este grupo, ya que $\mathrm{Aut}(P/C)$ es cíclico por el Teorema 1.19, así que tiene un único subgrupo de este orden. Para este fin será de gran ayuda recordar las siguientes nociones sobre G-conjuntos.

Definición 5.3. Si X es un conjunto y G es un grupo, entonces X es un **G-conjunto** si existe una función $G \times X \to X$ (llamada una **acción**), denotada por $(g,\ x) \mapsto gx$, tal que :

(i) $1x = x$ para toda x en X; y

(ii) $g(hx) = (gh)x$ para todos $g,\ h$ en G y x en X.

Si X es un G-conjunto y $x \in X$, entonces el conjunto $\{gx \mid g \in G\}$ es llamado la **G-órbita** de x.

Diremos que la acción es **transitiva** si X tiene una sola G-órbita y la llamaremos **regular** si es transitiva y $g \in G$, $gx = x$ implican $g = 1$ para toda $x \in X$.

Lema 5.4 (Lema de Burnside, 3.22 en [7]). *Si X es un G-conjunto finito y N es el número de G-órbitas, entonces*

$$N = (1/|G|)\textstyle\sum_{\tau \in G} F(\tau),$$

donde, para $\tau \in G$, $F(\tau)$ es el número de x en X tales que $\tau x = x$.

En lo sucesivo, P denotará un p-grupo metacíclico con p un primo impar y $P = XY$ será una factorización metacíclica C-estándar fija para C un subgrupo de P. Definimos α, β, γ, δ y κ como

$$p^{\alpha} = \left|\frac{X}{X \cap Y}\right|, \quad p^{\beta} = \left|\frac{Y}{X \cap Y}\right|, \quad p^{\gamma} = |Y|, \quad p^{\delta} = \left|\frac{Y}{P'}\right|, \quad p^{\kappa} = \left|\frac{P}{C}\right|.$$

Si $\kappa = 0$ ($C = P$), entonces el orden de $\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}$ es 1 ya que $\mathrm{Aut}(P/C) = 1$. Si $\kappa > 0$ y $\gamma = \delta$, P es abeliano, por el lema anterior $\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C} = \mathrm{Aut}(P/C)$ y su orden es $(p-1)p^{\kappa-1}$. Así que, podemos suponer $\kappa > 0$ y $\gamma > \delta$. Definimos los conjuntos:

$$\mathscr{K} := \{K \mid P = XK \text{ es una factorización metacíclica } C\text{-estándar}\},$$

para K en $\mathscr{K}$, $A(K) := \{a \in X \mid b^a = b^{1+p^{\delta}} \text{para toda } b \in K\}$ y $A := \bigcup_{K \in \mathscr{K}} A(K)$. Definimos también

$$N := \mathbb{N}_{\mathrm{Aut}\,P}(X) \cap \mathbb{N}_{\mathrm{Aut}\,P}(C),$$

$$U := X/\mathbb{C}_X(P), \qquad V := X/(X \cap C).$$

Lema 5.5.

(i) $N\downarrow_U$ *actúa regularmente en* $\{A(K) \mid K \in \mathscr{K}\}$.

(ii) $N\downarrow_V$ *actúa regularmente en* $\{(C \cap X)x \mid x \in A\}$.

Prueba. Dada $K \in \mathscr{K}$, probaremos que $A(K)$ es una clase lateral derecha de $\mathbb{C}_X(P)$ en X. Como la factorización metacíclica $P = XK$ es C-estándar, tenemos $|K| = |Y|$, luego $|K/P'| = |Y/P'|$, así que, de las primeras líneas del Lema 2.12, sabemos que podemos encontrar $x \in X$ tal que $b^x = b^{1+p^{\delta}}$ para todo $b \in K$, es decir, $A(K) \neq \varnothing$, y, de hecho, sabemos que $\langle x \rangle = X$. Si w es un elemento arbitrario de $A(K)$, entonces para todo $b \in K$ tenemos

$$b^{wx^{-1}} = b^{(1+p^{\delta})x^{-1}} = b.$$

Concluimos $wx^{-1} \in \mathbb{C}_X(P)$ y $w \in \mathbb{C}_X(P)x$. Para la otra inclusión, supongamos $z \in \mathbb{C}_X(P)x$, entonces $b^{zx^{-1}} = b$, luego $b^z = b^{(1+p^{\delta})}$. Es decir, $A(K)$ es una clase lateral derecha de $\mathbb{C}_X(P)$ en X. Ahora, si $v \in P$, $v = x^l b$, $(b \in K)$. Sea zx un elemento de $A(K)$, entonces

$$v = x^l b = (zx)^l z^{-l} b \quad \text{y} \quad z^{-l} \in \mathbb{C}_X(P) \leqslant \mathbb{C}_P(K),\ b \in \mathbb{C}_P(K),$$

por lo tanto, cada subgrupo generado por un elemento de $A(K)$ es un suplemento de $\mathbb{C}_P(K)$ en P, luego, por el Lema 2.10, es también un suplemento de K en P. Si $\bar{x} \in A(K)$, por la Ley Modular de Dedekind obtenemos $X = \langle \bar{x} \rangle (X \cap K)$, como X es cíclico y P no es abeliano, concluimos $\langle \bar{x} \rangle = X$.

Consideremos la acción natural de N en A: Sean $a \in A$ y $\rho \in N$, sabemos que $a \in A(K)$ p.a. $K \in \mathscr{K}$, luego $\rho a \in A(\rho K) \subseteq A$. Mostraremos que esta acción es transitiva. Sea $x \in A(Y)$, tomemos $y \in Y$ tal que $x^{p^\alpha} = y^{p^\beta}$. Entonces x y y son generadores de X y Y, respectivamente, y satisfacen las relaciones del Lema 2.12. Como cada K en $\mathscr{K}$ es un grupo cíclico de orden $|Y|$, tenemos $X \cap Y = X \cap K$.

Se sigue entonces que para cualquier a en $A(K)$ podemos escoger b en K con $a^{p^\alpha} = b^{p^\beta}$, y a y b son generadores de X y K, respectivamente, que también satisfacen las relaciones del Lema 2.12. Luego $x \mapsto a$, $y \mapsto b$ define un automorfismo ρ en $\operatorname{Aut} P$ que normaliza X y manda Y a K. Ahora $C = C \cap XY = (C \cap X)Y$, luego $\rho C = \rho(X \cap C)\rho Y = (X \cap C)K = C$, es decir, ρ normaliza C. Esto prueba que A tienen una sola N-órbita y por lo tanto, la acción es transitiva.

Veamos ahora que tenemos una acción de $N\downarrow_U$ en $\{A(K) \mid K \in \mathscr{K}\}$ que es regular. Si $\rho \in N$, escribiremos $\rho\downarrow_U$ para el automorfismo en $N\downarrow_U$ obtenido de ρ. Esta acción trabaja de la siguiente manera

$$\rho\downarrow_U A(K) = \rho\downarrow_U (\mathbb{C}_X(P)x) = \mathbb{C}_X(P)\rho x = A(\rho K),$$

por lo que hemos dicho, esta acción está bien definida y es transitiva. Como hemos visto, todo $A(K)$ es igual a un $\mathbb{C}_X(P)x$, donde x es un generador de X, luego $\langle \mathbb{C}_X(P)x \rangle = X/\mathbb{C}_X(P)$. Ahora, $\rho\downarrow_U A(K) = A(K)$ implica $\rho\downarrow_U(\mathbb{C}_X(P)x) = \mathbb{C}_X(P)x$, entonces $\rho\downarrow_U = 1$. Esto prueba que la acción es regular y tenemos (i).

Como N actúa en A transitivamente, el mapeo $(\rho,\ (C \cap X)x) \mapsto (C \cap X)\rho x$ define una acción transitiva de N en el conjunto $\{(C \cap X)x \mid x \in A\}$. Análogamente al párrafo anterior, $N\downarrow_V$ actúa regularmente en $\{(C \cap X)x \mid x \in A\}$.

Definimos

$$\mathscr{L} := \{K \in \mathscr{K} \mid A(K) = A(Y)\}.$$

Ahora podemos probar el siguiente teorema.

Teorema 5.6 (4.2 en [8]). *Si $\kappa > 0$ y $\gamma > \delta$, entonces*

$$|\mathbb{N}_{\operatorname{Aut} P}(C)\downarrow_{P/C}| = \begin{cases} m/(m,\ p^{\gamma-\delta-\kappa}) & \text{si } \kappa < \gamma - \delta \\ mp^{\kappa+\delta-\gamma} & \text{en cualquier otro caso,} \end{cases}$$

donde $m = |\mathscr{K}|/|\mathscr{L}|$.

Prueba. Del Lema 5.2(ii), sabemos que $\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C} = N\downarrow_{P/C}$. Existe un isomorfismo natural entre $X/(X\cap C)$ y P/C, digamos σ, luego si $\alpha \in N$, entonces $\alpha\downarrow_V \mapsto \sigma\alpha\downarrow_V \sigma^{-1}$ define un isomorfismo de $N\downarrow_V$ en $N\downarrow_{P/C}$. Por lo tanto $\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C} \cong N\downarrow_V$, así, sólo tenemos que investigar el orden de $N\downarrow_V$.

Definimos

$$W := \begin{cases} \mathbb{C}_X(P)/(X\cap C) & \text{si } \mathbb{C}_X(P) \geqslant (X\cap C) \\ (X\cap C)/\mathbb{C}_X(P) & \text{si } \mathbb{C}_X(P) < (X\cap C). \end{cases}$$

Supongamos $\mathbb{C}_X(P) \geqslant X\cap C$. Si $x \in A$, entonces $(X\cap C)x \subseteq \mathbb{C}_X(P)x \subseteq A$, luego,

$$\{(C\cap X)x \mid x \in A\} = \{(C\cap X)x \mid (C\cap X)x \subseteq A\}.$$

Por el Lema 5.5(ii), $N\downarrow_V$ actúa regularmente en este último, así que, por el Lema 5.4, basta conocer el tamaño del mismo para determinar el de $N\downarrow_V$. Asociar a cada $K \in \mathscr{K}$ el conjunto $A(K)$ es una función definida de $\mathscr{K}$ en $\{A(K) \mid K \in \mathscr{K}\}$ y el número de preimágenes de cada $A(K)$ es $|\mathscr{L}|$. Luego $|\{A(K) \mid K \in \mathscr{K}\}||\mathscr{L}| = |\mathscr{K}|$, es decir $|\{A(K) \mid K \in \mathscr{K}\}| = |\mathscr{K}|/|\mathscr{L}|$. Por otro lado, cada $A(K)$ se divide en $|W|$ clases laterales derechas distintas de $X\cap C$, por lo tanto $|\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}| = (\frac{|\mathscr{K}|}{|\mathscr{L}|})|W|$.

Ahora consideramos el caso $\mathbb{C}_X(P) < X\cap C$. Si tomamos un automorfismo α en N, observamos que el mapeo $\alpha\downarrow_U \mapsto \alpha\downarrow_V$ define un homomorfismo suprayectivo de $N\downarrow_U$ en $N\downarrow_V$. Está bien definido porque si $\alpha\downarrow_U = \beta\downarrow_U$, entonces $\mathbb{C}_X(P)\alpha(x) = \mathbb{C}_X(P)\beta(x)$, luego $\alpha(x)(\beta(x)^{-1}) \in X\cap C$, por lo tanto $\alpha\downarrow_V = \beta\downarrow_V$ y claramente es suprayectivo. El kernel de este homomorfismo son las $\alpha \in N\downarrow_U$ que satisfacen el siguiente diagrama:

$$\begin{array}{ccc} U & \xrightarrow{\alpha} & U \\ \downarrow & & \downarrow \\ V & \xrightarrow[1]{} & V \end{array}$$

Claramente, este conjunto es $\mathbb{C}_{N\downarrow_U}(V)$ y $\mathbb{C}_{N\downarrow_U}(V) = N\downarrow_U \cap \mathbb{C}_{\mathrm{Aut}\,U}(V)$. Además, como $V \cong U/W$, tenemos $\mathbb{C}_{\mathrm{Aut}\,U}(V) = \mathbb{C}_{\mathrm{Aut}\,U}(U/W)$. Por otro lado $W = (X\cap C)/\mathbb{C}_X(P)$ está propiamente contenido en $U = X/\mathbb{C}_X(P)$, ya que

$$\frac{X\cap C}{\mathbb{C}_X(P)} = \frac{X}{\mathbb{C}_X(P)} \Rightarrow X \leqslant C \Rightarrow P = C,$$

contradiciendo nuestras hipótesis. Esto implica que el mapeo $g(\sigma) := (\sigma u)u^{-1}$, donde $\sigma \in \mathbb{C}_{\mathrm{Aut}\,U}(U/W)$ y u es un generador fijo de U, sea una biyección entre $\mathbb{C}_{\mathrm{Aut}\,U}(U/W)$ y W. Como $\sigma\downarrow_{U/W}$ es la identidad en U/W, entonces $(\sigma u)u^{-1} \in W$, además, es fácil ver que este mapeo es una función inyectiva. Es suprayectiva porque si $|U/W| = p^a$,

entonces todo elemento de W es de la forma $w = u^{kp^a}$ donde $k = 1, \ldots, |U|/p^a$. Como $a > 0$ implica $(kp^a + 1,\ p) = 1$, entonces $\lambda(u) := u^{kp^a+1}$ define un automorfismo de U. Ahora, $u^{kp^a} \in W$, por lo que $Wu = Wu^{kp^a+1}$, es decir $\lambda \downarrow_V = 1$. Entonces, $\lambda \in \mathbb{C}_{\mathrm{Aut}\,U}(U/W)$ y $g(\lambda) = w$. Así que, $|\mathbb{C}_{\mathrm{Aut}\,U}(U/W)| = |W|$. Conlcuimos entonces

$$|\mathbb{C}_{N\downarrow_U}(V)| = (|N\downarrow_U|,\ |W|).$$

Como $N\downarrow_U$ actúa regularmente en $\{A(K) \mid K \in \mathscr{K}\}$, tenemos $|N\downarrow_U| = |\mathscr{K}|/|\mathscr{L}|$, por lo tanto,

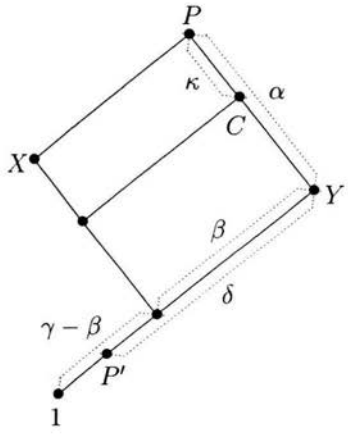
$$|N\downarrow_V| = \frac{|N\downarrow_U|}{|\mathbb{C}_{N\downarrow_U}(V)|} = \frac{|\mathscr{K}|/|\mathscr{L}|}{(|\mathscr{K}|/|\mathscr{L}|,\ |W|)}.$$

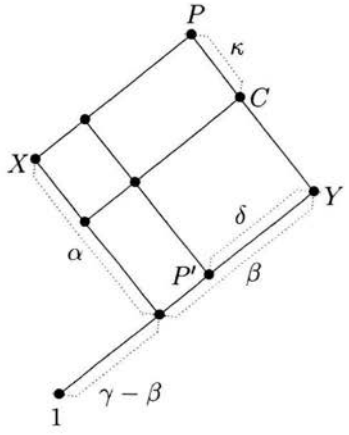
Sabemos que $|X/X\cap C| = p^\kappa$ y $|X/\mathbb{C}_X(P)| = |P'| = p^{\gamma-\delta}$, por lo que si $m = |\mathscr{K}|/|\mathscr{L}|$, entonces

$$|\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}| = \begin{cases} m/(m,\ p^{\gamma-\delta-\kappa}) & \text{si } \kappa < \gamma - \delta \\ mp^{\kappa+\delta-\gamma} & \text{en cualquier otro caso.} \end{cases}$$

Desde luego, ahora calcularemos los tamaños de $\mathscr{K}$ y $\mathscr{L}$. Comenzaremos por el de $\mathscr{K}$.

Como Y es un p-grupo cíclico, sabemos que $X \cap Y \leqslant P'$ ó $X \cap Y > P'$. Estas dos situaciones influirán de manera decisiva tanto en el tamaño de $\mathscr{K}$, en términos de la factorización metacíclica $P = XY$, como en la descripción de los posibles núcleos para factorizaciones metacíclicas C-estándar. Las siguientes figuras ilustran la situación que afrontaremos. La primera presenta el caso $\beta \leq \delta$, la segunda es para $\beta > \delta$.





Si K y N son grupos, $\mathrm{Hom}(K,\ N)$ denotará el conjunto de homomorfismos de K en N.

Lema 5.7 (2.4 en [1]). *Si $G = N \times K$ para un subgrupo abeliano N, entonces todo complemento de N es normal en G. El número de complementos de N en G es* $|\mathrm{Hom}(K,\ N)|$.

Este lema es un corolario al Teorema 2 del artículo *On semidirect products* de H. Bechtell. La prueba de este teorema no resulta complicada, por el contrario, el autor la desarrolla de manera natural. Si G cumple las condiciones de 5.7, del teorema se obtiene la biyección explícita entre $\mathrm{Hom}(K,\ N)$ y los complementos de N en G. Si $\phi \in \mathrm{Hom}(K,\ N)$, entonces ϕ se corresponde con $K^{1+\phi}$, donde $1+\phi : K \to G$ se define por $k \mapsto k\phi(k)$. En la prueba del siguiente lema veremos su aplicación.

Lema 5.8 (4.3 en[8]). *Si $\gamma > \delta$ entonces*

$$|\mathscr{K}| = \begin{cases} (p-1)p^{\beta-1} & \text{si } \alpha - \kappa \geq \beta \text{ y } \beta \leq \delta \\ \min(p^{\alpha-\kappa},\ p^{\delta}) & \text{en cualquier otro caso.} \end{cases}$$

Prueba. Sean x un elemento fijo de $A(Y)$ y y un elemento fijo en Y tal que $x^{p^\alpha} = y^{p^\beta}$. Sabemos que x y y son generadores de X y Y, respectivamente. Definimos $D := XP' \cap Y$ y $E := XP' \cap C$. Por la Ley Modular de Dedekind, tenemos

$$E = (X \cap C)P', \quad D = (X \cap Y)P', \quad EY = C, \quad \text{y} \quad E \cap Y = D.$$

Esto prueba que $C/D = Y/D \times E/D$. Como Y es cíclico, $X \cap Y \leqslant P'$ ó $X \cap Y > P'$, luego $Y/D \cong \mathsf{C}(\min\{p^\beta,\ p^\delta\})$, y de las dos últimas igualdades, obtenemos $E/D \cong \mathsf{C}(p^{\alpha-\kappa})$. A continuación probaremos que $K \in \mathscr{K}$ si, y sólo si, K es un subgrupo cíclico de C conteniendo D con K/D como complemento directo de E/D en C/D. Supongamos $P = XK$ una factorización metacíclica C-estándar. K es un grupo cíclico de orden $|Y|$, así que $X \cap K = X \cap Y$. Entonces

$$D = (X \cap Y)P' = (X \cap K)P' = XP' \cap K = E \cap K.$$

Por otro lado, $EK = (XP' \cap C)K = C$. Por lo tanto, K/D es un complemento directo de E/D en C/D. Ahora, sea K un subgrupo cíclico que contiene a D tal que K/D es un complemento directo de E/D en C/D. Entonces $K \geqslant P'$ y K es normal en P. Como $E = (X \cap C)P' \leqslant XK$, tenemos $XK = XKE = XC = P$. Además, $|K| = |Y|$, debido a que $|K/D| = |Y/D|$. Es decir, $K \in \mathscr{K}$.

Si definimos

$$\mathscr{K}^* := \{K \mid K/D \text{ es un complemento directo de } E/D \text{ en } C/D\};$$

entonces $\mathscr{K} = \{K \in \mathscr{K}^* \mid K \text{ es cíclico}\}$.

Como $C/D = Y/D \times E/D$, por el Lema 5.7, sabemos que existe una biyección entre los complementos directos de E/D en C/D y $\mathrm{Hom}(Y/D,\ E/D)$, ésta se encuentra dada por $\phi \mapsto (Y/D)^{1+\phi}$. Sabemos que existe un isomorfismo ϕ' entre $\phi(Y/D)$ y $(Y/D)/\ker\phi$ así que, según el Lema 1.7, cada $(Y/D)^{1+\phi}$ es la diagonal definida por $(Y/D,\ \ker\phi,\ \phi(Y/D),\ 1,\ \phi')$.

Tenemos, entonces, una biyección entre $\mathscr{K}^*$ y $\mathrm{Hom}(Y/D,\ E/D)$, el grupo correspondiente a ϕ será denotado por K_ϕ. Claramente $K_\phi = \{baD \mid \phi(bD) = aD, b \in Y\}$. Describiremos ahora la naturaleza de cada ϕ. Dado que Y/D y E/D son p-grupos cíclicos, el orden de $\mathrm{Hom}(Y/D,\ E/D)$ es $\min\{|Y/D|,\ |E/D|\}$, y $|Y/D| = \min\{p^\beta,\ p^\delta\}$ mientras que $|E/D| = p^{\alpha-\kappa}$, el orden es igual a $\min\{p^{\alpha-\kappa},\ p^\beta,\ p^\delta\}$. Como $\langle x^{p^\kappa}\rangle = (X \cap C)$, entonces $\langle x^{p^\kappa} D\rangle = E/D$. Supongamos $|E/D| < |Y/D|$. En este caso, ϕ está definido por $yD \mapsto x^{sp^\kappa} D$ con s un entero único tal que $0 \leq s < p^{\alpha-\kappa}$. Si $|Y/D| \leq |E/D|$, entonces E/D tiene un único subgrupo de orden $|Y/D|$, éste es $\langle x^{p^{\alpha-\beta}} D\rangle$, si $|Y/D| = p^\beta$; y es $\langle x^{p^{\alpha-\delta}} D\rangle$, si $|Y/D| = p^\delta$. Sea

$$\alpha^* := \max\{\kappa,\ \alpha - \beta,\ \alpha - \delta\}.$$

Entonces, dado $\phi \in \mathrm{Hom}(Y/D,\ E/D)$, ϕ está definido por $yD \mapsto x^{sp^{\alpha^*}} D$ con s un entero único tal que $0 \leq s < p^{\alpha-\alpha^*}$. Si escribimos K_s en lugar de K_ϕ, entonces $\mathscr{K}^* = \{K_s \mid 0 \leq s < p^{\alpha-\alpha^*}\}$. Lo que resta ahora es decidir cuántos K_s son cíclicos.

Para este fin, consideremos D^* el único subgrupo de Y de índice $p^{\alpha-\alpha^*}$, (en los tres casos posibles para α^* tenemos $\alpha - \alpha^* \leq \gamma$). Entonces

$$D^* = X \cap Y \ \Leftrightarrow\ \alpha - \alpha^* = \beta \ \Leftrightarrow\ (\alpha - \kappa \geq \beta \text{ y } \beta \leq \delta).$$

Nuestra discusión se divide en dos casos, que dependen de que $D^* = X \cap Y$ o no.

Caso I: $\alpha - \kappa \geq \beta$ y $\beta \leq \delta$. Esto es $D^* = D = X \cap Y$. La regularidad de P y $x^{p^\alpha} = y^{p^\beta}$ implican $(x^{p^{\alpha-1}} y^{-p^{\beta-1}})^p = 1$, es decir

$$\mathsf{C}(p) \times \mathsf{C}(p) \cong \langle y^{p^{\gamma-1}},\ x^{p^{\alpha-1}} y^{-p^{\beta-1}}\rangle = \Omega_1(P).$$

Como P no es abeliano $\beta \leq \delta < \gamma$, así que $\langle y^{p^{\gamma-1}}\rangle \leqslant \langle y^{p^\beta}\rangle$, entonces $D\Omega_1(P) = \langle y^{p^\beta},\ x^{p^{\alpha-1}} y^{-p^{\beta-1}}\rangle$ y tenemos

$$\frac{D\Omega_1(P)}{D} = \langle x^{p^{\alpha-1}} y^{-p^{\beta-1}} D\rangle.$$

Dado que $x^{p^{\alpha-1}}D$ y $y^{p^{\beta-1}}D$ tienen orden p y, bajo nuestras condiciones numéricas, $\alpha - 1 \geq \kappa$, entonces $x^{p^{\alpha-1}} \in \langle x^\kappa \rangle$ y

$$\Omega_1(E/D) = \langle x^{p^{\alpha-1}}D \rangle \quad \text{y} \quad \Omega_1(Y/D) = \langle y^{-p^{\beta-1}}D \rangle.$$

Por lo tanto, $\langle x^{p^{\alpha-1}}y^{-p^{\beta-1}}D \rangle$ es la diagonal definida por ψ, el isomorfismo definido por $y^{-p^{\beta-1}}D \mapsto x^{p^{\alpha-1}}D$ entre $\Omega_1(Y/D)$ y $\Omega_1(E/D)$. Observamos que K_ϕ es cíclico si, y sólo si, K_ϕ no contiene a $D\Omega_1(P)$. Ahora, dado K_ϕ, si ϕ restringido a $\Omega_1(Y/D)$ es igual a ψ, entonces $D\Omega_1(P)$ está contenido en K_ϕ. Por otro lado, si $D\Omega_1(P) \leqslant K_\phi$, entonces

$$\frac{D\Omega_1(P)}{D} \leqslant \frac{K_\phi}{D} = \{aD\phi(aD) \mid a \in Y\}.$$

Luego $x^{p^{\alpha-1}}y^{-p^{\beta-1}}D = aD\phi(aD)$ p. a. $a \in Y$ y tenemos $y^{-p^{\beta-1}}a^{-1}D = x^{-p^{\alpha-1}}D\phi(aD)$, el primer término de esta igualdad pertenece a Y/D y el segundo a E/D, luego $y^{-p^{\beta-1}}D = aD$ y $x^{p^{\alpha-1}}D = \phi(aD)$. Es decir,

$$\psi(aD) = \psi(y^{-p^{\beta-1}}D) = x^{p^{\alpha-1}}D = \phi(aD),$$

luego la restricción de ϕ a $\Omega_1(Y/D)$ es igual a ψ. Tenemos entonces, que K_ϕ es cíclico si y sólo si, $\phi|_{\Omega_1(Y/D)}$ no es igual a ψ.

Sea ϕ_0 en $\mathrm{Hom}(\mathsf{C}(p^\beta),\ \mathsf{C}(p^\beta))$ tal que $\phi_0|_{\mathsf{C}(p)} = \psi$. Si $\phi \in \mathrm{Hom}(\mathsf{C}(p^\beta),\ \mathsf{C}(p^\beta))$ y $\phi|_{\mathsf{C}(p)} = \psi$, entonces $\phi = \phi_0 + \phi - \phi_0$ y $\phi - \phi_0 \in \mathrm{Hom}(\mathsf{C}(p^\beta),\ \mathsf{C}(p^\beta))$ con $\ker\phi \geqslant \mathsf{C}(p)$.

Es decir

$$\{\phi \in \mathrm{Hom}(\mathsf{C}(p^\beta),\ \mathsf{C}(p^\beta)) \mid \phi|_{\mathsf{C}(p)} = \psi\}$$
$$= \{\phi_0 + \varphi \mid \varphi \in \mathrm{Hom}(\mathsf{C}(p^\beta),\ \mathsf{C}(p^\beta))\ \ker\varphi \geqslant \mathsf{C}(p)\}$$

y obtenemos una correspondencia biyectiva entre

$$\{\phi \in \mathrm{Hom}(\mathsf{C}(p^\beta),\ \mathsf{C}(p^\beta)) \mid \phi|_{\mathsf{C}(p)} = \psi\}$$

y $\mathrm{Hom}(\mathsf{C}(p^\beta)/\mathsf{C}(p),\ \mathsf{C}(p^\beta))$. Finalmente

$$|\mathscr{K}| = |\mathrm{Hom}(\mathsf{C}(p^\beta),\ \mathsf{C}(p^\beta))| - |\mathrm{Hom}(\mathsf{C}(p^{\beta-1}),\ \mathsf{C}(p^\beta))|.$$

Es decir, $|\mathscr{K}| = (p-1)p^{\beta-1}$ si $\alpha - \kappa \geq \beta$ y $\beta \leq \delta$.

Caso II: $\alpha - \kappa < \beta$ ó $\beta > \delta$. Esto es $\alpha^* > \alpha - \beta$, y por lo tanto $\beta > \alpha - \alpha^*$. Es decir, $X \cap Y$ es un subgrupo propio de D^*, luego $y^{p^{\beta-1}} \in D^*$. Si definimos $X^* := XD^*$, éste no es cíclico, ya que $\langle x,\ y^{p^{\beta-1}} \rangle/(X \cap Y) \cong \mathsf{C}(p^\alpha) \times \mathsf{C}(p)$. Así que, X^* contiene a

$\Omega_1(P)$. Ahora, si $\alpha - \alpha^* = \delta$, entonces $D^* = P' \leqslant K$. Por la ley Modular de Dedekind, tenemos $X^* \cap K = (X \cap K)D^* = D^*$ para toda $K \in \mathscr{K}^*$, luego, K no contiene a $\Omega_1(P)$. Si $\alpha - \alpha^* = \alpha - \kappa$, entonces

$$\frac{|Y|}{|D^*|} = \frac{|X|}{|X \cap Y|} \cdot \frac{|C|}{|P|}$$

y obtenemos $|D^*|(|C/YK|) = |Y \cap K|$. Es decir $|D^*| \leq |Y \cap K|$, como Y es cíclico, entonces $D^* \leqslant K$ y nuevamente, $X^* \cap K = D^*$. Concluimos K cíclico para toda K en $\mathscr{K}^*$. Por lo tanto $\mathscr{K} = \mathscr{K}^*$ y $|\mathscr{K}| = p^{\alpha - \alpha^*}$. Con esto terminamos la prueba.

Observemos que si $\alpha - \kappa \geq \beta$ y $\beta \leq \delta$, entonces el tamaño de $\mathscr{K}$ es la cantidad de números naturales menores que p^β y primos relativos a él. El siguiente lema muestra que, en este caso, cada s que determina a K_s es menor que p^β y $(s+1,\ p) = 1$.

Lema 5.9 (4.4 en [8]). *Suponiendo $\gamma > \delta$ tenemos:*

(i) Si $\alpha - \kappa \geq \beta$ y $\beta \leq \delta$, entonces $\mathscr{K} = \{\langle x^{sp^{\alpha-\beta}} y\rangle \mid 0 \leq s < p^\beta,\ (s+1,\ p) = 1\}$;

(ii) en cualquier otro caso, $\mathscr{K} = \{\langle x^{sp^{\alpha^*}} y\rangle \mid 0 \leq s < p^{\alpha - \alpha^*}\}$, donde α^* se reduce a $\max\{\kappa,\ \alpha - \delta\}$.

Prueba. De la regularidad de P y la definición de los parámentros tenemos

$$(x^{sp^{\alpha^*}} y)^{p^{\gamma-1}} = 1 \Leftrightarrow x^{sp^{\alpha^*+\gamma-1}} = y^{-p^{\gamma-1}} \Leftrightarrow \begin{cases} y^{-p^{\gamma-1}} = y^{-p^{\beta+\gamma-1-\beta}} \\ x^{sp^{\alpha^*+\gamma-1}} = x^{-p^{\alpha+\gamma-1-\beta}} \end{cases},$$

lo que ocurre, si, y sólo si

$$\begin{cases} \gamma > \beta, \\ sp^{\alpha^*+\gamma-1} \equiv -p^{\alpha+\gamma-1-\beta} \bmod p^{\alpha+\gamma-\beta} \end{cases} \Leftrightarrow \begin{cases} \gamma > \beta, \\ 1 + sp^{\alpha^*+\beta-\alpha} \equiv 0 \bmod p. \end{cases}$$

Es claro que $x^{sp^{\alpha^*}} y \in K_s$. Si s no es solución de $1 + sp^{\alpha^*+\beta-\alpha} \equiv 0 \bmod p$, entonces $x^{sp^{\alpha^*}} y$ tiene orden p^γ y $K_s = \langle x^{sp^{\alpha^*}} y\rangle$.

Si $\alpha - \kappa \geq \beta$ y $\beta \leq \delta$, entonces $\gamma > \beta$ porque $\gamma > \delta$. En este caso $\alpha^* = \alpha - \beta$ y, por lo tanto, las soluciones a dicha congruencia son aquellas s con $s \equiv -1 \bmod p$.

En el caso $\alpha^* > \alpha - \beta$ no hay solución para la congruencia. Por el Lema 4.3, hay exactamente $|\mathscr{K}|$ elecciones de s que no son soluciones de la congruencia y tenemos (ii).

Además de este lema, para determinar el tamaño de $\mathscr{L}$ también necesitamos lo siguiente.

Lema 5.10 (4.5 en [8]). *Si $\gamma > \delta$ entonces*

$$A(Y) = A(K_s) \quad \Leftrightarrow \quad sp^{\beta-\gamma+\delta} \equiv 0 \bmod p^{\alpha-\alpha^*},$$

donde $\alpha^* = \max\{\kappa,\ \alpha-\beta,\ \alpha-\delta\}$.

Prueba. Sean

$$B := (1+p^\delta)^{sp^{\alpha^*}} \quad \text{y} \quad B(p^\delta) := B^{p^{\delta-1}} + \cdots + B + 1.$$

Apoyados en el Lema 2.12, para los tres casos de α^* es fácil verificar $\alpha^* + 2\delta \geq \gamma$. Ahora

$$B = \sum_{i=0}^{sp^{\alpha^*}} \binom{sp^{\alpha^*}}{i} p^{i\delta} = 1 + tp^{\alpha^*+\delta},$$

donde t es un natural y $\alpha^* + \delta \geq 1$ porque $\alpha^* + \delta \geq \gamma - \delta > 0$. Así que $p^{\alpha^*+\delta} \leq (p^\gamma,\ B-1)$, entonces, por (i) de la Proposición 1.9

$$|B \bmod p^\gamma| = \frac{p^\gamma}{(p^\gamma,\ B-1)} \leq \frac{p^\gamma}{p^{\alpha^*+\delta}} = p^{\gamma-\alpha^*-\delta} \leq p^\delta.$$

Luego $B^{p^\delta} \equiv 1 \bmod p^\gamma$, y por 1.9(ii) $B(p^\delta) \equiv p^\delta \bmod p^\gamma$. Observemos también que, si a y c son enteros, entonces

$$(x^a y)^c = x^{ac} y^m, \quad m = (1+p^\delta)^{a(c-1)} + \cdots + (1+p^\delta)^{a(c-(c-1))} + 1.$$

De aquí desprendemos

$$\begin{aligned} A(Y) = A(K_s) &\Leftrightarrow (x^{sp^{\alpha^*}} y)^x = (x^{sp^{\alpha^*}} y)^{1+p^\delta} \\ &\Leftrightarrow x^{sp^{\alpha^*}} y^{1+p^\delta} = x^{(1+p^\delta)sp^{\alpha^*}} y^{B^{p^\delta}+B(p^\delta)} \\ &\Leftrightarrow x^{sp^{\alpha^*+\delta}} = 1 \\ &\Leftrightarrow sp^{\alpha^*+\delta} \equiv 0 \bmod p^{\alpha+\gamma-\beta} \\ &\Leftrightarrow sp^{\beta-\gamma+\delta} \equiv 0 \bmod p^{\alpha-\alpha^*}. \end{aligned}$$

Lema 5.11 (4.6 en [8]). *Si $\gamma > \delta$ entonces* $|\mathscr{L}| = \min\{p^{\beta-\gamma+\delta},\ p^{\alpha-\kappa}\}$.

Prueba. Observemos primero que $\beta-\gamma+\delta = 0$ y $K_s \in \mathscr{L}$, implican $s \equiv 0 \bmod p^{\alpha-\alpha^*}$. Mas s debe cumplir $0 \leq s < p^{\alpha-\alpha^*}$, por lo tanto, $s = 0$ y $\mathscr{L} = \{Y\}$.

Supongamos $\alpha - \kappa \geq \beta$ y $\beta \leq \delta$. Por los dos lemas anteriores, $K_s \in \mathscr{L}$ si, y sólo si, s es un múltiplo de $p^{\gamma-\delta}$ y $s < p^{\beta}$. Por otro lado $p^{\beta} = p^{\beta-(\gamma-\delta)+\gamma-\delta}$, si suponemos $\beta > \gamma - \delta$, entonces tenemos $p^{\beta-\gamma+\delta}$ posibilidades para s, es decir $|\mathscr{L}| = p^{\beta-\gamma+\delta}$. Si $\alpha - \alpha^* = \delta$ la situación es similar a la anterior y tenemos $|\mathscr{L}| = p^{\beta-\gamma+\delta}$. Si $\alpha - \alpha^* = \kappa$, seguimos nuevamente el razonamiento de arriba, mas en este ocasión tenemos dos casos, $\alpha - \kappa \geq \beta - \gamma + \delta$ ó $\alpha - \kappa < \beta - \gamma + \delta$ que nos llevan a $|\mathscr{L}| = \min\{p^{\beta-\gamma+\delta},\ p^{\alpha-\kappa}\}$.

En cualquier caso concluimos $|\mathscr{L}| = \min\{p^{\beta-\gamma+\delta},\ p^{\alpha-\kappa}\}$.

Corolario 5.12 (4.7 en [8]). *Sea ω el segundo término de la secuencia obtenida al arreglar $\alpha - \kappa$, $\beta - \kappa$, δ, $\beta - \gamma + \delta$ en orden no creciente. Si $\kappa > 0$ entonces*

$$|\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}| = \begin{cases} (p-1)p^{\kappa-1} & \text{si } \beta \leq \omega, \\ p^{\kappa-\beta+\omega} & \text{en cualquier otro caso.} \end{cases}$$

Prueba. Probamos primero que

$$(\gamma = \delta \text{ ó } (\alpha - \kappa \geq \beta \text{ y } \beta \leq \delta)) \Leftrightarrow \beta \leq \omega.$$

Si $\alpha - \kappa \geq \beta$ y $\delta \geq \beta$, entonces $\alpha - \kappa \geq \beta > \beta - \kappa$ y $\delta \geq \beta > \beta - \kappa$. Por lo tanto $\omega \geq \beta$. Supongamos ahora $\gamma = \delta$. Como $\delta \geq \delta + \beta - \gamma$, entonces $\omega \geq \beta - \gamma + \delta$ y tenemos $\omega \geq \beta$.

Para probar la otra implicación, supongamos $\omega \geq \beta$. Entonces $\omega = \alpha - \kappa$, $\omega = \delta$ o finalmente, $\omega = \beta - \gamma + \delta$. Supongamos $\omega = \alpha - \kappa$, es decir, $\alpha - \kappa$ es el segundo término de la secuencia mencionada. Como $\delta \geq \delta + \beta - \gamma$ y $\alpha - \kappa \geq \beta - \kappa$, entonces $\delta \geq \alpha - \kappa \geq \beta$. Si $\omega = \delta$, las desigualdades del caso anterior arrojan $\alpha - \kappa \geq \delta \geq \beta$. Finalmente observamos que $\beta - \gamma + \delta \leq \beta$, luego, si $\omega = \beta - \gamma + \delta$ entonces $\beta \leq \beta - \gamma + \delta \leq \beta$ y $\gamma = \delta$.

Ahora dividimos la prueba en dos casos.

(i) $\beta \leq \omega$. En este caso tenemos $\gamma = \delta$ ó $\alpha - \kappa \geq \beta$ y $\beta \leq \delta$. Cuando $\gamma = \delta$, por el Lema 5.2, $|\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}| = |\mathrm{Aut}(P/C)| = (p-1)p^{\kappa-1}$. Supongamos $\gamma > \delta$, $\alpha-\kappa \geq \beta$ y $\beta \leq \delta$. Por el Lema 5.8, $|\mathscr{K}| = (p-1)p^{\beta-1}$, y como $\alpha - \kappa \geq \beta > \beta - \gamma + \delta$, del Lema 5.11 obtenemos $|\mathscr{L}| = p^{\beta-\gamma+\delta}$. Así, $|\mathscr{K}|/|\mathscr{L}| = (p-1)p^{\gamma-\delta-1}$, ahora utilizamos el Teorema 5.6; de su primer caso obtenemos

$$|\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}| = \frac{(p-1)p^{\gamma-\delta-1}}{((p-1)p^{\gamma-\delta-1},\ p^{\gamma-\delta-\kappa})} = \frac{(p-1)p^{\gamma-\delta-1}}{p^{\gamma-\delta-\kappa}} = (p-1)p^{\kappa-1},$$

y del segundo obtenemos también

$$|\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}| = (p-1)p^{\gamma-\delta-1}p^{\kappa+\delta-\gamma} = (p-1)p^{\kappa-1}.$$

(ii) $\beta > \omega$. En este caso $\gamma > \beta$ y $\alpha-\kappa < \beta$ ó $\beta > \delta$. Entonces $|\mathscr{K}| = \min\{p^{\alpha-\kappa},\ p^{\delta}\}$ y $|\mathscr{L}| = \min\{p^{\alpha-\kappa},\ p^{\beta-\gamma+\delta}\}$. Sabemos que $\alpha-\kappa \geq \beta-\kappa$ y $\delta \geq \beta-\gamma+\delta$, entonces hay seis posibles formas de ordenar $\alpha-\kappa$, $\beta-\kappa$, δ, $\beta-\gamma+\delta$ en orden no creciente. Usando nuevamente las fórmulas del Teorema 5.6, cálculos similares a los de arriba muestran que $|\mathbb{N}_{\mathrm{Aut}\,P}(C)\downarrow_{P/C}| = p^{\kappa-\beta+\omega}$.

Capítulo 6

El problema de isomorfismo para presentaciones estándar

A continuación resolveremos el problema de isomorfismo para grupos definidos por presentaciones estándar $\wp(\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta,\ \theta)$. Sabemos ahora que los parámetros $\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon$ y ζ son invariantes del grupo, al igual que el orden multiplicativo de θ módulo ζ, que seguiremos denotando por κ. Así que, sólo necesitamos determinar cuales valores de η y θ originan grupos metacíclicos isomorfos con los parámetros $\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta$ y κ fijos.

Enunciamos primero un par de resultados sobre productos semidirectos que nos servirán en el tratamiento del problema.

Lema 6.1 (2.4 en [8]). *Sean P y Q grupos finitos y $\phi,\ \psi: P \to AutQ$ homomorfismos. Si γ es un isomorfismo de $P \ltimes_\phi Q$ en $P \ltimes_\psi Q$ que normaliza P y Q, entonces $\gamma((\phi x)y) = (\psi(\gamma x))(\gamma y)$, para todos $x \in P,\ y \in Q$.*

Prueba. Observemos

$$(\gamma x)\gamma((\phi x)y) = \gamma(x(\phi x)y) = (\gamma y)(\gamma x) \in P \ltimes_\psi Q,$$

por otro lado,

$$(\gamma x)(\psi(\gamma x))\gamma y = (\gamma x)(\gamma x)^{-1}\gamma(y)\gamma(x) = (\gamma y)(\gamma x).$$

De donde obtenemos la conclusión deseada.

Lema 6.2 (2.5 en [8]). *Sean P y Q grupos finitos solubles con $(|P|,\ |Q|) = 1$. Supongamos que ϕ y ψ son homomorfismos de P en $AutQ$. Entonces $P \ltimes_\phi Q \cong P \ltimes_\psi Q$*

si, y sólo si, existen $\alpha \in Aut\,P$ *y* $\beta \in Aut\,Q$ *tales que* $\beta(\phi(x)y) = (\psi(\alpha x))\beta y$, *para todos* $x \in P$, $y \in Q$.

Prueba. Sea $(x,\ y)$ la imagen de un elemento en Q bajo γ, un isomorfismo de $P \ltimes_\phi Q$ en $P \ltimes_\psi Q$ y supongamos que su orden es d, un divisor de $|Q|$. Observamos que $(x,\ y)^d = 1$ implica $x^d = 1$ y como $(|P|,\ |Q|) = 1$, entonces $x = 1$. Es decir, Q es un subgrupo característico, luego γ normaliza Q. Como γ es un isomorfismo, γP es un subgrupo de orden $|P|$ y ya que $(|P|,\ |Q|) = 1$, entonces γP y P son $\pi(P)$-subgrupos de Hall de $P \ltimes_\psi Q$ y, por lo tanto, son conjugados. Así que podemos suponer que γ normaliza P si la sustituimos con un automorfismo interior de $P \ltimes_\psi Q$. Tomamos las restricciones de γ a P y Q, sean éstas α y β, respectivamente. Entonces $\alpha \in \mathrm{Aut}\,P$ y $\beta \in \mathrm{Aut}\,Q$. La relación $\beta(\phi(x)y) = (\psi(\alpha x))\beta y$ se obtiene del Lema 6.1.

Supongamos que α y β son automorfismos que relacionan a ϕ y ψ en la forma mencionada. Definimos el mapeo γ de $P \ltimes_\phi Q$ en $P \ltimes_\psi Q$ como $\gamma(xy) = (\alpha x)(\beta y)$, que, se puede demostrar fácilmente, es un isomorfismo.

Cuando sea necesario, escribiremos $G(\eta)$, $G(\theta)$ ó $G(\eta,\ \theta)$ en lugar de G para indicar que el grupo depende de η, θ ó de ambos. Observemos que el rango relevante de (η, θ) es el conjunto

$$\{(\eta,\ \theta) \mid (\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta,\ \theta) \in \Omega,\ |\theta \bmod \zeta| = \kappa\}$$

para α, β, γ, δ, ε, ζ y κ enteros positivos fijos.

Lema 6.3 (7.1 en [8]).

$$G(\eta_1,\ \theta_1) \cong G(\eta_2,\ \theta_2) \ \Leftrightarrow\ G(\eta_1,\ \theta_1) \cong G(\eta_1,\ \theta_2),\ G(\eta_1,\ \theta_2) \cong G(\eta_2,\ \theta_2).$$

Prueba. Si $G(\eta_1,\ \theta_1) \cong G(\eta_2,\ \theta_2)$, entonces existe un grupo metacíclico G que tiene presentaciones estándar $\wp(\eta_1,\ \theta_1)$ y $\wp(\eta_2,\ \theta_2)$. Para $i = 1,\ 2$, sea $\{x_i,\ y_i,\ u_i,\ v_i\}$ un conjunto generador de G que satisface las relaciones de $\wp(\eta_i,\ \theta_i)$. Como $\langle u_i,\ v_i\rangle$ es un subgrupo de Hall normal en G, tenemos $\langle u_1,\ v_1\rangle = \langle u_2,\ v_2\rangle$, grupo al que denotaremos por N. Sabemos que $H := \langle x_1,\ y_1\rangle$ es un conjugado de $\langle x_2,\ y_2\rangle$. Cambiando los generadores de H por sus imágenes bajo esta conjugación, podemos suponer $H = \langle x_1,\ y_1\rangle = \langle x_2,\ y_2\rangle$. Por las relaciones que definen a la presentación estándar tenemos $[H,\ u_i] = 1$ y $[N,\ y_i] = 1$ para cada $i = 1,\ 2$. Además, por el Corolario 4.6, $G = \langle x_i\rangle\langle y_i\rangle\langle u_i\rangle\langle v_i\rangle$ es una factorización estándar, luego, por el Teorema 3.6 $\langle v_1\rangle = \langle v_2\rangle$. Entonces $v_1 = v_2^n$, y tenemos:

$$v_1^{\theta_2} = (v_2^{\theta_2})^n = (v_2^{x_2})^n = v_1^{x_2}.$$

Concluimos que el conjunto generador $\{x_2,\ y_2,\ u_1,\ v_1\}$ satisface las relaciones de $\wp(\eta_1,\ \theta_2)$, es decir $G(\eta_1,\ \theta_1) \cong G(\eta_1,\ \theta_2)$ y $G(\eta_1,\ \theta_2) \cong G(\eta_2,\ \theta_2)$. La otra dirección de nuestra afirmación es obvia.

Este resultado nos permite investigar el problema de isomorfismo en dos partes, una para η fija y otra con θ fija. Primero consideraremos el problema para θ fija. Veremos que este caso es mucho más sencillo que el otro.

Lema 6.4 (7.2 en [8]).

$$G(\eta_1) \cong G(\eta_2) \ \Leftrightarrow\ \exists s \in \mathbb{Z},\ s \geq 0 \text{ tal que } \eta_1 \equiv \eta_2^s \bmod \zeta,\ (s,\ \varepsilon) = 1.$$

Prueba. Sea G un grupo metacíclico con presentaciones estándar $\wp(\eta_1)$ y $\wp(\eta_2)$ y supongamos $G(\eta_1) \cong G(\eta_2)$. Para cada $i = 1,\ 2$, tomemos una factorización estándar $G = X_iY_iU_iV_i$ y generadores $x_i,\ y_i,\ u_i,\ v_i$ que satisfacen las relaciones de la presentación estándar $\wp(\eta_i)$. Recordemos que $V_1 = V_2$ y U_1 es un conjugado de U_2 por un elemento, digamos y, de V_2. Entonces existe un entero s, que podemos tomar no negativo, tal que $u_1 = (u_2^s)^y$ y $(s,\ \varepsilon) = 1$. Luego

$$v_1^{\eta_1} = v_1^{u_1} = y^{-1}u_2^{-s}yv_1y^{-1}u_2^sy = y^{-1}v_1^{\eta_2^s}y = v_1^{\eta_2^s}$$

Por lo tanto, $\eta_1 \equiv \eta_2^s \bmod \zeta$.

Para el regreso, es fácil observar que $\wp(\eta_1)$ se obtiene de $\wp(\eta_2)$ cambiando el generador u por u^s.

Ahora investigaremos el problema para η fija.

Definimos

$$H := \langle x,\ y \mid x^\alpha = y^\beta,\quad y^\gamma = 1,\quad y^x = y^{1+(\delta|\gamma)}\rangle \ \text{ y}$$

$$N := \langle u,\ v \mid u^\varepsilon = 1,\quad v^\zeta = 1,\quad v^u = v^\eta\rangle.$$

Escribimos $\bar{\theta}\colon H \to \operatorname{Aut} N$ para la acción de H en N definida por $\bar{\theta}x\colon u \mapsto u,\ v \mapsto v^\theta$ y $\bar{\theta}y = 1$. Podemos ver a $G(\theta)$ como $H \ltimes_{\bar{\theta}} N$. Obviamente, $\langle x^\kappa,\ y\rangle$ es el kernel común de las acciones definidas por $\bar{\theta}$ para todas los posibles valores de θ, llamaremos a este grupo H^*. Probaremos, entonces, el siguiente lema.

Lema 6.5 (7.3 en [8]).

$$H \ltimes_{\bar{\theta}_1} N \cong H \ltimes_{\bar{\theta}_2} N \ \Leftrightarrow\ \exists \rho \in \mathbb{N}_{\operatorname{Aut} H}(H^*) \text{ tal que } \theta_1 \equiv \theta_2^t \bmod \zeta$$

para algún entero t que satisface $(\rho x)H^* = x^tH^*$.

Prueba. Continuaremos escribiendo ϖ para $\pi(N)$ y π para $\pi(H)$.

Sea $G_i := H \ltimes_{\bar{\theta}_i} N$ para $i = 1, 2$. Supongamos que τ es un isomorfismo entre G_1 y G_2. Estos dos grupos se forman con el mismo conjunto de elementos; H, N y todos los subgrupos de ambos son subgrupos en G_1 y G_2. Como N es el único Hall ϖ-subgrupo de G_1 y G_2 tenemos $\mathbb{O}_\varpi(G_1) = N = \mathbb{O}_\varpi(G_2)$, y, por el Teorema 3.5, $G_1' \cap N = \langle v \rangle = G_2' \cap N$, tenemos entonces $\tau(N) = N$ y $\tau\langle v \rangle = \langle v \rangle$. Hemos visto ya que $\mathbb{O}_\pi(G_1) = H^* = \mathbb{O}_\pi(G_2)$, así que τ también manda H^* a H^*. Como H es un π-subgrupo de Hall, $\tau(H)$ lo es también y, por lo tanto, es un conjugado de H, luego, si es necesario, podemos remplazar τ por su composición con un automorfismo interior y suponer que τ normaliza H. En este caso, τ induce un automorfismo de H/H^*. Como H/H^* es generado por xH^*, tenemos

$$(\tau x)H^* = x^t H^*$$

para algún entero t, determinado por τ y que puede ser escogido con $0 < t < \kappa$. Del Lema 6.1 tenemos

$$\tau((\bar{\theta}_1 x)v) = (\bar{\theta}_2 \tau x)\tau v.$$

Por lo tanto

$$\begin{aligned} v^{\theta_1} &= (\bar{\theta}_1 x)v \\ &= \tau^{-1}((\bar{\theta}_2 \tau x)\tau v) \\ &= \tau^{-1}((\bar{\theta}_2 x^t)\tau v) \quad (\text{porque } \tau x \equiv x^t \bmod \ker \bar{\theta}_2) \\ &= v^{\theta_2^t}. \end{aligned}$$

La última igualdad es debida a que, como τ normaliza $\langle v \rangle$, la imagen de v bajo τ es una potencia de éste, es decir $(\bar{\theta}_2 x^t)\tau v = v^{r\theta_2^t}$ donde $\tau^{-1} v^r = v$. Esto prueba que

$$\theta_1 \equiv \theta_2^t \bmod \zeta,$$

y, como hemos observado, $\tau{\downarrow_H} \in \mathbb{N}_{\mathrm{Aut}\, H}(H^*)$ y $(\tau x)H^* = x^t H^*$.

Inversamente, supongamos que $\rho \in \mathbb{N}_{\mathrm{Aut}\, H}(H^*)$ con $(\rho x)H^* = x^t H^*$ para algún entero t tal que $\theta_1 \equiv \theta_2^t \bmod \zeta$. Consideremos la permutación $\tau : (h, n) \mapsto (\rho h, n)$ del conjunto común de elementos $H \times N$ de $H \ltimes_{\bar{\theta}_1} N$ y $H \ltimes_{\bar{\theta}_2} N$. τ fija a $H \times 1$ y a $1 \times N$ y sus restricciones a estos subgrupos son automorfismos. Para probar, usando el Lema 6.2, que τ es un isomorfismo de $H \ltimes_{\bar{\theta}_1} N$ en $H \ltimes_{\bar{\theta}_2} N$, tenemos que verificar $\tau((\bar{\theta}_1 h)n) = (\bar{\theta}_2 \tau h)\tau n$ cuando h y n corren sobre los conjuntos generadores de H y N, respectivamente. Con $h = y$, esto ocurre porque y y ρy se encuentran en el kernel común H^* de $\bar{\theta}_1$ y $\bar{\theta}_2$. Con $n = u$, se cumple porque u es un punto fijo de la imagen común de $\bar{\theta}_1$ y $\bar{\theta}_2$. El caso restante es $h = x$, $n = v$ y

$$\tau((\bar{\theta}_1 x)v) = \tau(v^{\theta_1}) = v^{\theta_1},$$

mientras que

$$\begin{aligned}(\bar{\theta}_2\tau x)\tau v &= (\bar{\theta}_2\rho x)v \\ &= (\bar{\theta}_2 x^t)v \\ &= v^{\theta_2^t} \\ &= v^{\theta_1}.\end{aligned}$$

Observamos que t puede ser determinada por el isomorfismo natural que existe entre $\mathrm{Aut}(H/H^*)$ y el grupo multiplicativo de unidades de los residuos reducidos módulo κ (los más pequeños representates no negativos de las clases de residuos módulo κ). Sea Φ la copia isomórfica del grupo $\mathbb{N}_{\mathrm{Aut}\,H}(H^*)\downarrow_{H/H^*}$ en el grupo multiplicativo de unidades de los residuos reducidos módulo κ. Podemos, entonces, concluir el siguiente resultado.

Teorema 6.6 (7.4 en [8]). *Las presentaciones estándar $\wp(\eta,\ \theta)$ y $\wp(\eta',\ \theta')$ definen grupos isomorfos si, y sólo si*

(i) existe un entero positivo s tal que $\eta' \equiv \eta^s \bmod \zeta$ y $(s,\ \varepsilon) = 1$, y

(ii) existe un entero t en Φ tal que $\theta' \equiv \theta^t \bmod \zeta$.

Ahora daremos una explícita descripción de Φ, basándonos en el último resultado del capítulo anterior.

Para cada entero positivo t y cada primo p, sea $t[p]$ el residuo obtenido al dividir t entre $p^{\kappa(p)}$, es decir, el único entero tal que

$$0 \leq t[p] < p^{\kappa(p)}, \quad t \equiv t[p] \bmod p^{\kappa(p)}.$$

Como H es nilpotente, es el producto directo $\prod_{p\in\pi} H_p$ de sus p-subgrupos de Sylow H_p, que son característicos en H, así que también tenemos $\mathrm{Aut}\,H = \prod_{p\in\pi}\mathrm{Aut}\,H_p$; más aún,

$$\mathbb{N}_{\mathrm{Aut}\,H}(H^*) = \prod_{p\in\pi}\mathbb{N}_{\mathrm{Aut}\,H_p}(H_p^*),$$

$$\mathbb{N}_{\mathrm{Aut}\,H}(H^*)\downarrow_{H/H^*} = \prod_{p\in\pi}\mathbb{N}_{\mathrm{Aut}\,H_p}(H_p^*)\downarrow_{H_p/H_p^*}.$$

En términos de los residuos reducidos módulo κ y módulo $p^{\kappa(p)}$, esto se traduce en lo siguiente. Si $\rho \in \mathbb{N}_{\mathrm{Aut}\,H}(H^*)$ y $(\rho x)H^* = x^t H^*$ con $0 < t < \kappa$, entonces $t[p]$ se corresponde con la componente de $\rho\downarrow_{H/H^*}$ indexada por p en su descomposición dada por la última igualdad, en el mismo sentido en que t se corresponde con $\rho\downarrow_{H/H^*}$. Ahora, dado $t[p]$ un elemento en, digamos $\Phi(p)$, el único subgrupo de orden $|\mathbb{N}_{\mathrm{Aut}\,H_p}(H_p^*)\downarrow_{H_p/H_p^*}|$

en el grupo cíclico de unidades de los residuos reducidos módulo $p^{\kappa(p)}$, por el Teorema Chino del Residuo, podemos recuperar t un elemento en Φ de los $t[p]$. Así, en base al Corolario 5.11, tenemos el siguiente teorema.

Para cualquier $p \in \pi$, definimos $\omega(p)$ como el segundo término de la secuencia obtenida al arreglar $\alpha(p) - \kappa(p)$, $\beta(p) - \kappa(p)$, $\delta(p)$, $\beta(p) - \gamma(p) + \delta(p)$ en orden no creciente.

Teorema 6.7 (7.5 en [8]). *Si* $\kappa(p) = 0$ *entonces* $\Phi(p) = 1$. *Supongamos* $\kappa(p) > 0$. *Si tenemos* $\beta(p) \leq \omega(p)$, *entonces*

$$\Phi(p) = \{t \in \mathbb{Z} \mid 0 < t < p^{\kappa(p)},\ (t,\ p) = 1\},$$

mientras que si $\beta(p) > \omega(p)$ *entonces*

$$\Phi(p) = \{t \in \mathbb{Z} \mid 0 < t < p^{\kappa(p)},\ t \equiv 1 \bmod p^{\beta(p)-\omega(p)}\}.$$

Más aún, $\Phi = \{t \in \mathbb{Z} \mid 0 < t < \kappa,\ t[p] \in \Phi(p)$ *para todo* $p \in \pi\}$.

Conclusiones

Con la descomposición de Hall estándar, la clasificación de los grupos metacíclicos finitos es inminente. Esta descomposición, que se puede encontrar para todo grupo metacíclico finito, no sólo nos da un producto semidirecto del mismo en el que los factores tienen órdenes que son primos relativos, sino que remonta el problema de expresar a un grupo metacíclico finito de una manera más conveniente que a través de la factorización metacíclica, cuando esta no se escinde. Esto es posible gracias a esa pequeña parte del trabajo de P. Hall que concierne a los Sistemas de Sylow.

Un grupo metacíclico finito G, no sólo tiene un Sistema de Sylow, sino que, al menos, uno de los subgrupos de Hall que lo conforman es normal. Esto nos permite definir N como la intersección de todos los elementos de algún Sistema de Sylow que sean normales y, por la solubilidad de G, únicos. N resulta ser un subgrupo de Hall de G con características que son de gran utilidad: N es de orden impar y es el más pequeño de los subgrupos de Hall de G con cociente nilpotente, así, $G = H \ltimes N$ con H un subgupo de Hall nilpotente; si $G = SK$ es una factorización metacíclica de G, la factorización metacíclica $N = (S \cap N)(K \cap N)$ se escinde y $K \cap N$ y la clase de conjugación de $S \cap N$ no dependen de la elección de la factorización metacíclica. Así, $|(S \cap N)|$ y $|(K \cap N)|$ son invariantes del grupo y las posibles accciones de $(S \cap N)$ en $(K \cap N)$ que redunden en grupos isomorfos a G se determinan fácilmente. Las pruebas de las afirmaciones de independencia descansan, principalmente, en el uso de los Sistemas de Sylow. Además, $S \cap N \leqslant \mathbb{C}_N(H)$ y $H = (S \cap H)(K \cap H)$, por lo que la acción de H en N se reduce a la acción de $(S \cap H)$ en $(K \cap N)$. Por otro lado, esta factorización metacíclica de H dependerá de la factorización metacíclica que tomemos para G.

Para los grupos metacíclicos de orden impar, Sim descubre que trabajar con una factorización metacíclica estándar, es decir, $G = SK$ con $|S| \geq |S'|$ y $|K| \leq |K'|$ para cualquier otra factorización metacíclica $G = S'K'$, produce condiciones numéricas

en la presentación de cada p-subgrupo de Sylow de H que desembocan en una presentación de G en la que los parámetros que corresponden a los generadores de H son invariantes. Con esto, el problema de isomorfismo depende sólo de las acciones de $(S \cap N)$ y $(S \cap H)$ en $(K \cap N)$.

Si G es un grupo metacíclico finito con una factorización metacíclica $G = SK$ y descomposición de Hall estandar $G = HN$, para encontrar una factorización metacíclica estándar basta con encontrar X, $Y \leqslant H$ tales que $H = XY$, $X = \exp H$ y Y sea un elemento con el menor orden posible en el conjunto

$$\mathscr{K} = \{Y \leqslant H \mid Y \text{ es un núcleo de } H \text{ con } Y \leqslant \mathbb{O}_{\pi(H)}(G)\}.$$

Sabemos que $K \cap N \in \mathscr{K}$, por lo que podemos tomar un elemento Y de $\mathscr{K}$ de tamaño mínimo. Esto basta, ya que definiendo $S^* = X(S \cap N)$ y $K^* = Y(K \cap N)$, por 3.8, $G = S^*K^*$ es una factorización metacíclica y por el Teorema 3.6 es estándar. Para G de orden impar, es la nilpotencia de H y la regularidad de cada H_p, lo que nos permite encontrar dicho X. Como H es nilpotente, encontrar una factorización metacíclica estándar es equivalente a encontrar una $\mathbb{O}_p(G)$-estándar para cada H_p p-subgrupo de Sylow de H. Si trataramos de seguir este camino para grupos metacíclicos de orden par, el primer paso sería encontrar una factorización $\mathbb{O}_2(G)$-estándar para H_2 el 2-subgrupo de Sylow de H.

Como vimos, existen ocho tipos de 2-grupos metacíclicos. Los que son abelianos son regulares y por lo tanto, para éstos tenemos una factorización metacíclica $\mathbb{O}_2(G)$-estándar, pero ¿para el resto?. Ahora bien, suponiendo que encontremos dicha factorización para todo 2-grupo metacíclico, la construcción de la presentación podría tornarse complicada ya que, en el caso de los grupos metacíclicos de orden impar, sabemos que todos los H_p tienen una presentación que tiene la misma forma, ver Lema 4.3. Entonces, también tendríamos que unificar las presentaciones de los 2-grupos metacíclicos en una sola forma general para presentarlos, distinguiéndolos en base a las condiciones numéricas, con el propósito de obtener los generadores de $S \cap H$ y $K \cap H$. Además, esta nueva presentación debería poder *combinarse* bien con la presentación que tenemos para los p-grupos metacíclicos con p impar. Esto tal vez, teniendo el mismo tipo de condiciones numéricas para los parámetros de ambas o aumentando las condiciones numéricas de la presentación para G. Y depués de esto, queda todavía la resolución del problema de isomorfismo, en el que ahora tenemos que investigar la acción de un 2-grupo metacíclico sobre $K \cap N$.

Sin embargo, ahora podemos ver el probema de los grupos metacíclicos de orden par de la siguiente forma: Para cualquier factorización metacíclica $G = SK$, no consideramos explícitamente $G = HN$, sino el producto $G = H_2 H_{2'} N$. $H_{2'} N$ es un subgrupo normal de G de orden impar, por lo tanto tiene una presentación estándar. Aún con esto, el camino a partir de aquí no deberá ser muy distinto al que describimos en el párrafo anterior. Deberemos combinar los ocho tipos de 2-grupos metacíclicos que existen con la presentación estándar para $H_{2'} N$. Esto podría cambiar drásticamente las condiciones numéricas de la presentación para G en relación a las consideradas en una presentación estándar. Además, la acción de H en N dependerá del tipo de 2-grupo metacíclico que tengamos en G.

Bibliografía

[1] H. Bechtell. On semidirect products. *Communications in Algebra*, 19(4):1151–1163, 1991.

[2] Daniel Gorenstein. *Finite Groups.* Harper & Row, New York, Evanston and London, 1968.

[3] Marshall Hall Jr. *The Theory of Groups.* Chelsea Publishing Company, New York, Second edition, 1976.

[4] C. E. Hempel. Metacyclic groups. *Communications in Algebra*, 28(8):3865–3897, 2000.

[5] M.F. Newman y M. Xu. Metacyclic groups of prime-power order. *Adv. in Math.(Beijing)*, 17:106–107, 1988.

[6] Derek J. S. Robinson. *A Course in the Theory of Groups.* Springer-Verlag, New York, 1982.

[7] Joseph J. Rotman. *An Introduction to the Theory of Groups.* Springer, New York, 1994.

[8] Hyo-Seob Sim. Metacyclic groups of odd order. *Proc. London Math. Soc.*, 69(3):47–71, 1994.

[9] Michio Suzuki. *Group Theory II.* Springer, New York, Berlin, Heidelberg and Tokyo, 1986.