Universidad de Valladolid

Facultad de Ciencias

TRABAJO FIN DE GRADO

GRADO EN MATEMÁTICAS

ALGUNAS FAMILIAS DE GRUPOS FINITOS NO CONMUTATIVOS

Autor:

M Mar Grima Bermell

Tutor:

José Enrique Marcos Naveira

Julio 2021

Índice general

Introducción

La Teoría de Grupos es una parte importante en el álgebra abstracta, siendo una base para esta. El álgebra abstracta es la parte de las matemáticas que se encarga del estudio de las estructuras algebraicas. Y, dentro de la misma, la Teoría de Grupos estudia la estructura algebraica denominada grupo; analizando, entre otras cosas, la clasificación de los grupos y sus propiedades.

Elegí el tema de Familia de Grupos Finitos porque siempre me ha gustado el Álgebra, y en concreto los grupos, al ser estos el pilar para construir otras estructuras, como los anillos o cuerpos; y he tenido interés muy a menudo por indagar más y ampliar mi conocimiento sobre este tema.

La Teoría de Grupos, cuyo origen está ligado al estudio de la resolución de ecuaciones algebraicas de grados arbitrarios, se aplica en la totalidad de las matemáticas, e incluso en otras ciencias como la Física. El objetivo de este trabajo es presentar una introdución a la Teoría de Grupos, profundizando más de lo que se hizo en clase. Analizaremos los teoremas de Sylow y cómo aplicarlos a la hora de estudiar y clasificar grupos finitos. También definiremos los conceptos de grupo resoluble y supersoluble, y de series derivadas de un grupo. Así mismo, expondremos los conceptos de grupo metacíclico y metabeliano. Todos ellos serán utilizados junto con el producto directo y, sobre todo, el producto semidirecto para construir varias familias de grupos finitos no abelianos, de las cuales estudiaremos sus propiedades detenidamente.

Este trabajo ha contribuido a refrescar y profundizar los conocimientos que estudié en la asignatura de Estructuras Algebraicas hace ya dos años. Elaborar este trabajo ha sido duro, por la cantidad de horas que hay que invertir en su realización, pero a su vez ha sido diferente e interesante por utilizar una metodología de estudio distinta a la empleada en clase. Personalmente, los tipos de grupos que considero más interesantes son los grupos metacíclicos y los metabelianos, porque me parece intrigante que un grupo pueda contener un subgrupo normal con cierta propiedad, y a la vez el cociente del grupo por este subgrupo posee la misma propiedad.

Procedemos a describir con más detalle el contenido del trabajo. Comenzaremos introduciendo algunas definiciones y conceptos fundamentales en la Teoría de Grupos. A continuación estudiaremos todo lo relacionado con acciones de grupos sobre conjuntos, dando varios resultados para caracterizar grupos finitos de órdenes concretos.

Seguidamente presentaremos los Teoremas de Sylow. Estos resultados nos ayudarán a determinar la cantidad y forma de los p-subgrupos de Sylow que contiene un grupo finito. Posteriormente mostraremos algunas de las posibles aplicaciones de los Teoremas de Sylow, acompañando estas reflexiones mediante varios ejemplos de estas aplicaciones.

Más adelante, definiremos los grupos resolubles, supersolubles, metacíclicos y metabelianos, estudiando sus principales propiedades. Inmediatamente después se analizará el producto semidirecto de grupos, con la intención de presentar esta herramienta para su consiguiente uso en la creación de ciertos grupos finitos.

Finalmente, aplicando todo lo visto con anterioridad podremos generalizar varios grupos ya conocidos y estudiar varias familias de grupos finitos, junto con sus propiedades más notables.

Inicialmente teníamos objetivos más ambiciosos: presentar más familias de grupos y sus propiedades. No obstante, circunstancias desfavorables y de salud lo han impedido.

El Trabajo Fin de Grado significa para mí el fin de una carrera de estudio totalmente vocacional, que por un lado me ha dado quebraderos de cabeza, y por otro me ha hecho disfrutar por poderme dedicar a unos estudios que me gustan.

Por último, me gustaría mostrar mi agradecimiento a mi tutor, el profesor José Enrique Marcos Naveira, quien me ha guiado y apoyado a lo largo de este proceso, ayudándome a materializar este trabajo.

Capítulo 1

Preliminares

En este capítulo fijaremos algunas notaciones y algunos conceptos que usaremos a lo largo de todo el trabajo. Introduciremos también algunos resultados básicos que siguen la línea de las definiciones.

1.1. Definiciones

Si G es un grupo, denotamos por 1 el elemento neutro de G si consideramos G con la multiplicación, mientras que si lo consideramos con la suma denotamos el elemento neutro de G como 0.

En primer lugar explicaremos algunos grupos importantes, posiblemente ya conocidos, que usaremos a lo largo de todo el trabajo.

Veamos la definición de grupo simétrico o de permutaciones.

Definición 1. *Sea X un conjunto, una biyección de X en él mismo es una permutación en X. El conjunto de permutaciones de X, que denotaremos $S(X)$, bajo la composición de funciones es un grupo. Si X es un conjunto finito de n elementos, es decir $|X| = n$, entonces consideramos X como el conjunto $\{1, 2, ..., n\}$, y denotamos $S(X)$ como $S(n)$. Un elemento π de $S(n)$, tal que $\pi(1) = a_1$, $\pi(2) = a_2$, ... $\pi(n) = a_n$, se representará de la siguiente manera:*

$$\begin{pmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{pmatrix}$$

Veamos ahora la definición de grupo diédrico, el cual es un subgrupo del grupo simétrico.

Definición 2. *Llamamos grupo diédrico, denotado por $D(n)$, al grupo de las simetrías de un polígono*

regular de n lados, para $n \geqslant 3$. Su orden es $2n$, es decir $|D(n)| = 2n$, y está generado por un elemento a de orden n y un elemento b de orden 2 tales que $ba = a^{-1}b$.

$$D(n) = \{a, b \mid \ a^n = 1 = b^2, \ ba = a^{-1}b\} \tag{1.1}$$

A continuación presentaremos la definición de grupo cuaternio.

Definición 3. *Llamamos grupo cuaternio, denotado por Q_8, al grupo generado por dos elementos, a y b, de orden 4 tales que $ba = a^{-1}b$ y $a^2 = b^2$.*

$$Q_8 = \langle a, b \mid \ a^4 = 1 = b^4, \ a^2 = b^2, \ ba = a^{-1}b \rangle$$

Los elementos de Q_8 son de la forma $a^k b^n$ donde k, n son enteros tales que $0 \leq k \leq 3$ y $0 \leq n \leq 1$, y la multiplicación de dos elementos es la siguiente:

$$(a^k b^n)(a^l b^m) = \begin{cases} a^{k+l}b^m, \ si \ n = 0 \\ a^{k-l}b^{n+m}, \ si \ n = 1 \end{cases}$$

Todo subgrupo propio de Q_8 es cíclico y se tiene que Q_8 es dicíclico.

Veamos la definición de producto directo, el cual es una herramienta muy útil para crear nuevos grupos a partir de otros más simples como comprobaremos.

Definición 4. *Dados dos grupos G, H, se define su producto directo $G \times H$ como el conjunto de pares (g, h) tal que $g \in G$ y $h \in H$, junto con la operación de multiplicación siguiente:*

$$(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$$

donde $g_1, g_2 \in G$ y $h_1, h_2 \in H$, $*$ es la operación en G y $\cdot$ es la operación en H.

Definición 5. *Sea G un grupo finito, G es simple si solo contiene dos subgrupos normales: el subgrupo trivial $\{1\}$, y él mismo.*

Definición 6. *Sea G un grupo y P, Q dos subgrupos de G. Entonces PQ es el siguiente subgrupo de*

G:

$$PQ = \{g \in G \,|g = pq \text{ con } p \in P, q \in Q\}$$

Definición 7. *Sea G un grupo y P, Q dos subgrupos de G. Entonces $\langle P, Q\rangle$ es el subgrupo resultado de la intersección de todos los subgrupos de G que contienen a P y a Q.*

1.2. Algunos resultados básicos

El primer resultado que vamos a mostrar está relacionado con los elementos conjugados y su orden.

Proposición 1. *Sea G un grupo, sea $x \in G$, los elementos conjugados de x tienen el mismo orden que x.*

`Demostración:` Para realizar esta demostración veamos que $(gxg^{-1})^n = gx^ng^{-1}$. Veremos esto por inducción sobre n. Para $n = 1$ es claro que es cierto. Supongamos que es cierto para $n = k$, observemos que también se cumple para $k + 1$:

$$(gxg^{-1})^{k+1} = ((gxg^{-1})^k)gxg^{-1} = (gx^kg^{-1})gxg^{-1} = gx^kxg^{-1} = gx^{k+1}g^{-1}$$

Sea x de orden n, entonces

$$(gxg^{-1})^n = gx^ng^{-1} = g \cdot 1 \cdot g^{-1} = gg^{-1} = 1$$

por lo que el orden de $(gxg^{-1})^n$ divide a n, y como

$$x = g^{-1}(gxg^{-1})g$$

se tiene que el orden de x, que es n, divide al orden de (gxg^{-1}), y por tanto el orden de (gxg^{-1}) es n. □

Proposición 2. *Sean $x, y \in G$ tales que $xy = yx$. Entonces, $\forall k \in \mathbb{Z}$, $(xy)^k = x^ky^k$.*

`Demostración:` Veámoslo por inducción sobre k. Para $k = 0$ es claro que se da la igualdad. Supongámoslo cierto para $k = n$ veamos que se cumple para $k = n + 1$.

$(xy)^{n+1} = (xy)^n(xy) = x^n y^n xy = x^n y^{n-1}(yx)y = x^n y^{n-1}(xy)y = x^n y^{n-2}(yx)y^2 = x^n y^{n-2}(xy)y^2 = x^n y^{n-3}(yx)y^3 = ... = x^n(yx)y^n = x^n(xy)y^n = x^{n+1}y^{n+1}$. □

Proposición 3. *Sea G un grupo. Si todo elemento de G es de orden 2, entonces G es abeliano.*

`Demostración:` Sean x, $y \in G$ cualesquiera, tenemos lo siguiente:

$$x(xy)y = x^2y^2 = 1 = (xy)(xy) = x(yx)y,$$

y por lo tanto $xy = yx$, por lo que G es abeliano. □

A continuación presentamos dos resultados básicos de teoría de grupos, relacionados con subgrupos normales.

Proposición 4. *Sea G un grupo. Si P, Q son dos subgrupos normales de G entonces PQ también lo es.*

`Demostración:` Sea $y \in PQ$, $x \in G$, se tiene que $y = pq$, entonces

$$xyx^{-1} = xpqx^{-1} = (xpx^{-1})(xqx^{-1})$$

y xpx^{-1} es un elemento de P por ser P normal y lo mismo ocurre con xqx^{-1}, luego $xyx^{-1} \in PQ$ por lo que es normal. □

Notación. Si H es un subgrupo normal de G se denota $H \triangleleft G$

Lema 1. *Sea G un grupo, Q un subgrupo de G y P un subgrupo normal de G, $P \triangleleft G$. Entonces $\langle P, Q\rangle = PQ$.*

`Demostración:` Es claro que $\langle P, Q\rangle$ contiene a PQ. Para demostrar la otra contención solo hace falta ver que PQ es un subgrupo de G y como PQ contiene a los subgrupos P y Q, el resultado es consecuencia de la definición de $\langle P, Q\rangle$. Es claro que $1 \in PQ$, y si $n_1, n_2 \in P$ y $h_1, h_2 \in Q$, entonces

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1}h_1)h_2 = n_1(h_1n_2h_1^{-1})(h_1h_2),$$

y como P es un subgrupo normal $h_1 n_2 h_1^{-1}$ es un elemento $n_3 \in P$ y entonces

$$(n_1 h_1)(n_2 h_2) = (n_1 n_3)(h_1 h_2) \in PQ.$$

Además

$$(nh)^{-1} = h^{-1} n^{-1} = (h^{-1} n^{-1} h) h^{-1} \in PQ$$

y por lo tanto PQ es un subgrupo de G y $\langle P, Q \rangle = PQ$. □

Vamos a mostrar dos resultados sobre el producto directo, subgrupos normales, y grupos abelianos.

Proposición 5. *Sea G un grupo, y H, K dos subgrupos normales de G, tales que*

$$H \cap K = \{e\} \quad y \quad G = HK$$

Entonces $G \cong H \times K$.

`Demostración:` Veamos que $hk = kh$ para todo $h \in H$ y para todo $k \in K$.Tenemos que

$$hkh^{-1} \in hKh^{-1} = K,$$

luego $hkh^{-1} = k'$ para algún $k' \in K$. Por el mismo razonamiento,

$$khk^{-1} \in kHk^{-1} = H,$$

luego $khk^{-1} = h'$ para algún $h' \in H$, luego deducimos que $hk = k'h$ y que $kh = h'k$, y por tanto $k'h = h'k$, luego $k'k^{-1} = h'h^{-1} \in H \cap K = \{e\}$, y tenemos que $k' = (k^{-1})^{-1} = k$, $h' = (h^{-1})^{-1} = h$ por lo que $hkh^{-1} = k$ y $hk = kh$, como queramos ver. Esto quiere decir que si $hk = h'k'$ con k, $k' \in K$ y h, $h' \in H$, entonces $k = k'$ y $h = h'$.
Observemos que la siguiente aplicación es isomorfismo de grupos

$$f : H \times K \longrightarrow G = HK$$
$$(h, k) \longrightarrow hk$$

Como $G = HK$ entonces todo $g \in G$ es de la forma hk con $h \in H$ y $k \in K$, y hemos visto que si existieran otros $k' \in K$ y $h' \in H$, entonces serían iguales a k y a h, luego es biyectiva, y su inversa es la aplicación que a cada $g \in G$ lo manda en (h, k) tales que $g = hk$. Veamos que $f((h,k)(n,m)) = f((h,k))f((n,m))$ para $h, n \in H$ y $k, m \in K$. Tenemos que

$$f((h,k)(n,m)) = f((hn,km)) = hnkm$$

y por otro lado tenemos que

$$f((h,k))f((n,m)) = (hk)(nm) = hnkm$$

por lo que son iguales y tenemos el un isomorfismo. □

Proposición 6. *Sean G y H dos grupos, $G \times H$ es abeliano si y solo si G y H son ambos abelianos.*

`Demostración:` Supongamos que $G \times H$ es abeliano, veamos que G y H son abeliano: dados g_1, $g_2 \in G$ tenemos que

$$(g_1 g_2, 1) = (g_1, 1)(g_2, 1) = (g_2, 1)(g_1, 1) = (g_2 g_1, 1)$$

y por lo tanto $g_1 g_2 = g_2 g_1$ y queda reflejado que G es abeliano. Con el mismo razonamiento se pone de manifiesto que H es abeliano.
Supongamos ahora que G y H son abelianos, veamos que $G \times H$ es abeliano: dados g_1, $g_2 \in G$, h_1, $h_2 \in H$, tenemos lo siguiente

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1) = (g_2, h_2)(g_1, h_1)$$

con lo que queda demostrada la proposición. □

Proposición 7. *Todo grupo de orden p, siendo p un número entero primo, es cíclico.*

`Demostración:` Sea G un grupo de orden p, sea g un elemento de G. Como el orden de g divide al orden de G, se tiene que g tiene orden o 1 o p. Si tiene orden 1, entonces es el elemento identidad; si g no es el elemento identidad entonces g tiene orden p, y por lo tanto el grupo cíclico generado por g, denotado por $\langle g \rangle$, es un subgrupo de G y tiene p elementos, y por lo tanto es igual a G. □

Proposición 8. *Cualquier subgrupo H de un grupo abeliano G es abeliano y es normal en G.*

`Demostración:` Sea G un subgrupo abeliano, y $H \subset G$ un subgrupo. Como $gm = mg$ para cualesquiera $g, m \in G$ se tiene también que para todo $h, k \in H \subset G$ $hk = kh$, por lo que H es abeliano, y dado $g \in G$,para cualquier $h \in H$ se tiene que $ghg^{-1} = gg^{-1}h = h \in H$ por lo que H es normal. □

La siguiente proposición será utilizada repetidamente a lo largo del documento.

Proposición 9. *Todo grupo cíclico es abeliano.*

`Demostración:` Sea G un grupo cíclico, esto quiere decir que existe un elemento $x \in G$ tal que $G = \langle x \rangle$. Sean $y, w \in G$ dos elementos cualesquiera, como x genera G entonces existen $n, m \in \mathbb{N}$ tal que $y = x^n$ y $w = x^m$. Comprobemos que y, w conmutan.

$$yw = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = wy,$$

y por lo tanto G es abeliano, como queríamos demostrar. □

Proposición 10. *Los grupos cíclicos de orden primo son los únicos grupos abelianos simples.*

`Demostración:` Veamos que un grupo cíclico de orden primo G es abeliano simple. Es abeliano pues, por la proposición 9. todo grupo cíclico es abeliano. G no tiene subgrupos, pues al ser de orden primo, éste no tiene divisores, y por lo tanto G no tiene subgrupos.
Veamos ahora que todo grupo abeliano simple es cíclico de orden primo (o isomorfo a uno cíclico de orden primo). Un grupo finito que contiene un solo subgrupo maximal es cíclico de orden primo. En un grupo abeliano G todo subgrupo es normal, por lo que si además es simple entonces G es cíclico de orden primo. □

Capítulo 2

Acciones de grupos sobre conjuntos

En este capítulo recurriremos repetidamente al estudio de las acciones sobre grupos, así como al de la órbita y el estabilizador de las mismas. Estos conceptos serán utilizados después para definir nuevos términos, como el centralizador, por ejemplo.
También estudiaremos lo que es el centro de un grupo, y algunos casos en los que un grupo es abeliano.

2.1. Primeras definiciones

Definimos ahora qué es una acción de un grupo sobre un conjunto. Usaremos este concepto en muchas de las definiciones posteriores, como en la de estabilizador de un elemento, o en la de la órbita de un elemento.

Definición 8. *Se dice que un grupo G actúa sobre un conjunto X si existe una aplicación de $G \times X$ en X definida por*

$$G \times X \to X$$
$$(g, x) \to g \cdot x$$

que cumple:

(a). Para todo $x \in X$, se cumple que $1_G \cdot x = x$, donde 1_G es el neutro de G.

(b). Para todo g_1 y g_2 en G y para todo x en X, $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

Veamos ahora un homomorfismo de un grupo G en $S(X)$, donde X es un conjunto sobre el que actúa el grupo G.

Definición 9. *Para todo $g \in G$ la aplicación $g \to \phi_g$, donde $\phi_g : X \to X$ está definida por $\phi_g(x) = g \cdot x$ para $x \in X$, donde $g \cdot x$ es una acción de G sobre el elemento x, es un homomorfismo de grupos de G en $S(X)$.*

Podemos definir, dada una acción de G sobre X, el estabilizador de un elemento del conjunto X como sigue:

Definición 10. *Dado un conjunto X y un grupo G con una acción sobre X, y dado $x \in X$, el estabilizador de x, que denotamos mediante G_x, es el conjunto de elementos de G que dejan fijo x, es decir,*

$$G_x = \{g \in G : g \cdot x = x\}$$

Es claro que G_x está contenido en G, pero es que además de estar contenido en G, es un subgrupo de G, como vamos a ver a continuación.

Proposición 11. *Para cualquier grupo G, que actúe sobre un conjunto X, y para cualquier elemento $x \in X$ el estabilizador G_x es un subgrupo de G.*

`Demostración:` Por la propiedad (a), se tiene que el elemento 1_G pertenece a G_x. Sean $g_1, g_2 \in G_x$ veamos que $g_1 g_2$ pertenece a G_x. Como $g_1, g_2 \in G_x$ se tiene que $g_1 \cdot x = x = g_2 \cdot x$, luego, por la propiedad (b),

$$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x$$

y por lo tanto $g_1 g_2 \in G_x$. Además, si $g \in G_x$ se tiene que

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1} g) \cdot x = 1_G \cdot x = x \tag{2.1}$$

y por lo tanto, el inverso de g pretenece a G_x. □

Podemos ahora definir la siguiente relación, que será una relación de equivalencia, la cual nos ayudará a definir la órbita de $x \in X$.

Definición 11. *Dado un grupo G, un conjunto X y una acción de G sobre X se define la relación R en X como sigue:*
x está relacionado con y, se denota xRy, si y solo si existe $g \in G$ tal que $y = g \cdot x$.

Proposición 12. *La relación R definida es, como adelantábamos, una relación de equivalencia.*

Demostración: Como para todo $x \in X$, se cumple que $1_G \cdot x = x$, se tiene que xRx. Veamos que si xRy entonces yRx: tenemos que $y = g \cdot x$ para algún $g \in G$ y entonces

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = x$$

y por lo tanto xRy. Notemos que es una acción transitiva, sean $x, y, z \in X$ tales que xRy y yRz, o sea $y = g \cdot x$ y $z = h \cdot y$ y por lo tanto $z = hg \cdot x$ por lo que xRz. □

La clase de equivalencia de esta relación es un conjunto que nos interesa, llamado órbita, y se define como sigue.

Definición 12. *La clase de equivalencia de x dada por la relación R se llama órbita de x y viene dada por:*

$$orb(x) = Gx = \{g \cdot x : g \in G\}$$

2.2. Relación órbita-estabilizador

Dado un grupo G con una acción sobre un conjunto X, observemos qué relación hay entre el estabilizador de un elemento $x \in X$, y su órbita a través del siguiente teorema.
En esta sección también presentaremos algunas propiedades que implican el carácter abeliano de un grupo,las cuales resultan útiles para clasificar los grupos finitos.

Teorema 1. Relación órbita-estabilizador
Sea G un grupo, X un conjunto y sea dada una acción de G sobre X. Entonces, para todo x en X se cumple que:

$$|Gx| = |G : G_x|.$$

Demostración: Dado $x \in X$ definimos la aplicación ψ que va de la órbita de x al conjunto cociente de G por el estabilizador de x,

$$\psi : Gx \to \{hG_x : h \in G\} = G/G_x$$
$$\psi(g \cdot x) = gG_x$$

Veamos que esta aplicación, que no es un homomorfismo pues Gx no es un grupo, está bien definida:
Supongamos que $g \cdot x = h \cdot x$ y por lo tanto $h^{-1}g \cdot x = x$, o sea $h^{-1}g \in G_x$ y por lo tanto $hG_x = gG_x$ y con esto hemos demostrado que no depende del representante que cojamos. Observemos que ψ es inyectiva:
Sea $\psi(g \cdot x) = \psi(h \cdot x)$, esto significa que $gG_x = hG_x$ y por lo tanto $h^{-1}g \in G_x$. Por la definición de G_x, esto implica que $h^{-1}g \cdot x = x$ y multiplicando por h en ambos lados de la ecuación se tiene que

$$hx = h \cdot (h^{-1}g \cdot x) = (hh^{-1}g) \cdot x = g \cdot x$$

y se tiene que ψ es inyectiva.Veamos que es sobreyectiva:
Dado $hG_x \in G/G_x$ se tiene que es imagen de $\psi(h \cdot x)$ y por lo tanto es sobreyectiva, con lo que queda demostrado que es una biyección. □

Contemplemos ahora el caso de una acción particular, la conjugación de un elemento $x \in X$ por un elemento g de G.

Proposición 13. *Sea G un grupo, X un subgrupo de G, la aplicación de $G \times X$ en X dada por $(g, x) \to g \cdot x$, con $g \cdot x = gxg^{-1}$ es una acción de G sobre X.*

`Demostración:` Sea e el elemento neutro de G, se tiene que $ex = x$ y que $xe^{-1} = x$ y por lo tanto $exe^{-1} = x$. Sean $g, h \in G$, se tiene entonces que $g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(h^{-1}g^{-1}) = (gh) \cdot x$, y por lo tanto sí es una acción. □

Definición 13. *Sea G un grupo, y sea $x \in G$. Se define el centralizador de x en G como*

$$C_G(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}.$$

Dado un elemento $g \in G$, el estabilizador de x (ver definición 10.) para la acción de conjugar por g, $g \cdot x = gxg^{-1}$, es lo mismo que el centralizador de x en G.

Proposición 14. *Sea H un subgrupo de G. Entonces para cada x en X se tiene que $C_H(x) \supseteq C_G(x) \cap H$.*

`Demostración:` Si $g \in C_G(x)$ y $g \in H$ se tiene que $g \in C_H(x) = \{h \in H : hxh^{-1} = x\}$, por lo que se tiene la contención. □

Definiremos ahora un subconjunto interesante dentro de un grupo G, su centro, sobre el que luego veremos varios resultados.

Definición 14. *Sea G un grupo, el centro de G se define por*

$$Z(G) = \{z \in G : zx = xz \quad \forall x \in G\}.$$

Es claro que $Z(G)$ es un grupo abeliano y normal en G, y si G es abeliano, este es igual a su centro.

Definición 15. *Sea G un grupo y H un subgrupo de G, se define el centralizador de H por $C_G(H) = \{g \in G : ghg^{-1} = h \; para \; todo \; h \in H\}$.*

Podemos relacionar esta definición con el centro de un grupo de la siguiente manera, se tiene que $C_G(G) = Z(G)$.

Definición 16. *Sea G un grupo y H un subgrupo de G, se define el normalizador de H en G por $N(H) = \{g \in G : gHg^{-1} = H\}$.*
Cuando hay lugar a confusión sobre de que grupo es subgrupo H se denota $N_G(H)$, siendo G el grupo del que H es subgrupo.

A continuación enunciaremos y demostraremos dos propiedades relacionadas con el centro de un grupo.

Proposición 15. *Sea $p \in \mathbb{Z}$ un número primo, y G un grupo finito con p^n elementos. Entonces $Z(G)$ tiene más de un elemento.*

`Demostración:` Sean $C_1, C_2, ..., C_r$ las clases de conjugación de G, es decir, las clases de equivalencia del espacio cociente de G entre R, siendo R la relación dada por la acción de conjugar $((g, x) \to gxg^{-1})$. Estas clases de equivalencia son una partición de G, y por lo tanto

$$|G| = |C_1| + |C_2| + ... + |C_r| \tag{2.2}$$

Numeramos las clases de forma que $C_1 = \{1\}$. Si x_i es un elemento de C_i, por la relación órbita-estabilizador se tiene que $|C_i| = |G|/|C_G(x_i)|$ dado que $Gx_i = C_i$ y $G_{x_i} = C_G(x_i)$, y por lo tanto $|C_i|$ es una potencia de p, siendo $1 = p^0$ si $C_G(x_i) = G$, como ocurre en el caso $i = 1$. No es posible que p divida a $|C_i|$ para $2 \leq i \leq r$, porque si lo hiciera el lado derecho de la ecuación 2.2 sería $\equiv 1$ (mód p) mientras que el lado izquierdo es divisible por p, lo cual es absurdo, y por lo tanto existe i tal que $2 \leq i \leq r$ tal que $C_G(x_i) = G$. En este caso $gx_i = x_i g$ para todo $g \in G$, y por lo tanto $x_i \in Z(G)$, demostrando que $Z(G)$ tiene más de un elemento. □

Proposición 16. *Sea G un grupo tal que $G/Z(G)$ es cíclico, entonces G es abeliano.*

`Demostración:` Que G sea abeliano significa que $G = Z(G)$.
Supongamos que $G/Z(G)$ es cíclico generado por $xZ(G)$, entonces todo elemento de G está en uno de los siguientes conjuntos $Z(G), xZ(G), x^2Z(G), ...$ Sean $x^i z,\ x^j w$ pertenecientes a G para algún par i, j y para z, w en $Z(G)$. Entonces

$$(x^i z)(x^j w) = x^i(zx^j)w = x^i(x^j z)w = x^{i+j}zw = x^{i+j}wz = x^{j+i}wz = (x^j w)(x^i z)$$

por lo que G es abeliano. □

El siguiente corolario se sigue de las dos proposiciones anteriores.

Corolario 1. *Sea p un número entero primo. Cualquier grupo con p^2 elementos es abeliano.*

`Demostración:` Por la proposición 15. sabemos que $Z(G)$ tiene más de un elemento, y como G tiene p^2 elementos, $|Z(G)|$ tiene que dividir a p^2, por lo que $|Z(G)|$ es o bien p o p^2. Si $|Z(G)| = p^2$, entonces $Z(G) = G$, y por lo tanto G es abeliano. Si $|Z(G)| = p$, entonces $G/Z(G)$ tiene p elementos y por lo tanto es cíclico, y por la proposición anterior entonces G es abeliano. □

Observemos una propiedad que sirve para clasificar grupos finitos de cierto orden.

Corolario 2. *Un grupo con p^2 elementos es, o bien cíclico, o bien isomorfo al grupo producto $C_p \times C_p$ donde C_p es el grupo cíclico de p elementos.*

`Demostración:` Si G tiene p^2 elementos, y uno de sus elementos tiene orden p^2, entonces G es cíclico. En otro caso podemos suponer que todo elemento distinto de la identidad de G tiene orden p. Sea x un elemento de esta forma, entonces $\langle x \rangle$ tiene p elementos. Elegimos un elemento y de G que no está en $\langle x \rangle$. Como $\langle x \rangle \cap \langle y \rangle = \{1\}$ y los dos tienen p elementos, entonces $\{x^i y^j \ : 0 \leq i, j \leq p-1\}$ tiene p^2 elementos distintos, es decir, este conjunto es G, y la aplicación $x^i y^j \to (x^i, y^j)$ es un isomorfismo entre G y el grupo producto de $\langle x \rangle$ y $\langle y \rangle$. □

Proposición 17. *Sea H un subgrupo de G. Entonces $C_G(H)$ es un subgrupo normal del grupo $N_G(H)$ y $N_G(H)/C_G(H)$ es isomorfo a un subgrupo de $Aut(H)$ (grupo de automorfismos de H).*

`Demostración:` Para cada $x \in N_G(H)$ definimos la aplicación υ_x en H definida por $\upsilon_x(h) = xhx^{-1}$. Esta aplicación es inyectica, pues si $xhx^{-1} = xgx^{-1}$ entonces $h = g$, y es sobreyectiva porque dado $k \in H$, $x^{-1}kx \in H$ por estar x conetenido en $N_G(H)$, y por lo tanto se tiene que $k = \upsilon_x(x^{-1}kx)$ con lo que se ve que es sobreyectiva. Además como $\upsilon_x(hg) = xhgx^{-1} = xhx^{-1}xgx^{-1} = \upsilon_x(h)\upsilon_x(g)$ se tiene que υ_x es un automorfismo y por lo tanto, la aplicación que va de $N_G(H)$ en $Aut(H)$ que lleva x en υ_x está bien definida. Veamos que es un homomorfismo: $\upsilon_x\upsilon_y(h) = \upsilon_x(yhy^{-1}) = xyhy^{-1}x^{-1} = (xy)h(xy)^{-1} = \upsilon_{xy}(h)$ y como el núcleo de esta aplicación es $C_G(H)$, por el primer teorema de isomorfía $N_G(H)/C_G(H)$ es isomorfo a la imagen de esta aplicación, que es un subgrupo de $Aut(H)$. □

Capítulo 3

Teoremas de Sylow

Peter Ludwig Mejdell Sylow fue un matemático noruego que en 1872 formuló y demostró una serie de teoremas ahora conocidos como teoremas de Sylow. Estos teoremas son una parte fundamental de la teora de grupos finitos, que se usan para analizar con mayor profundidad la estructura, y los p-subgrupos y los p-subgrupos de Sylow de un grupo.
En este capítulo los enunciaremos y probaremos.

3.1. p-subgrupos

En este capítulo p será un número entero positivo primo.
Primero veamos las definiciones de p-subgrupo y p-subgrupo de Sylow.

Definición 17. *Dado un número primo $p \in \mathbb{Z}$, un p-grupo es un grupo en el que cada elemento tiene como orden una potencia de p.*

Definición 18. *Dado un grupo G de orden $p^n k$, con $k \in \mathbb{Z}$ y p primo que no divide a k, un p-subgrupo de Sylow de G es un p-subgrupo maximal de G (maximal bajo la inclusión), es decir, un subgrupo con p^n elementos.*

Si p no divide el orden de un grupo G, el único p-subgrupo de Sylow de G es el constituido únicamente por la unidad, es decir $\{1\}$, mientras que si G es un p-subgrupo, su único p-subgrupo de Sylow será el total, es decir G.

Ejemplo 1 *Veamos cuáles son los ordenes de los subgrupos de Sylow de un grupo de orden* 1064800. *Como* $1064800 = 2^5 \times 5^2 \times 11^3$ *se tiene que los subgrupos de Sylow tendrán orden* $32, 25, 1331$.

Lema 2. *Sean $p, k \in \mathbb{Z}$, p primo y k no divisible por p. El número de formas de seleccionar un subconjunto con p^n elementos de un conjunto con $p^n k$ elementos es congruente con k módulo p.*

`Demostración:` Sabemos que el número de formas de seleccionar un subconjunto con p^n elementos de un conjunto con $p^n k$ elementos es el coeficiente de x^{p^n} en $(1+x)^{p^n k} = ((1+x)^{p^n})^k$.Además, tenemos que

$$(1+x)^{p^n} \equiv 1 + x^{p^n} \ (\mod p)$$

ya que todos los demás coeficientes de los demás monomios son divisibles por p. Por lo que el coeficiente de x^{p^n} en $(1+x)^{p^n k}$ es congruente módulo p con el coeficiente de x^{p^n} en $(1+x^{p^n})^k$, y por lo tanto es congruente con k módulo p. □

3.2. Teoremas de Sylow

En esta sección presentaremos todos los teoremas de Sylow y algunas propiedades de los p-subgrupos. Estos resultados hablan sobre el número de p-subgrupos de Sylow, o sobre p-subgrupos normales, entre otras cosas.

Veamos un primer enunciado. Esta primera parte de los teoremas de Sylow nos garantiza la existencia de p-subgrupos de Sylow en grupos finitos de orden $p^n k$.

Teorema 2. Primer teorema de Sylow
Sea $p, k \in \mathbb{Z}$ tales que p es primo y no divide a k, y G un grupo de orden $p^n k$. Entonces G tiene al menos un p-grupo de Sylow.

`Demostración:` Sea Σ el conjunto de todos los subconjuntos de G con p^n elementos, y por el lema anterior el número de elementos de Σ es congruente con k módulo p. Definimos una acción de G sobre Σ dada, para $g \in G$ y $S \in \Sigma$, por $g \cdot S = \{gs \ : \ s \in S\}$.
Sean $S_1, S_2, ..., S_r$ representantes de las órbitas de Σ bajo esta acción. Como cada miembro de Σ está en la órbita de uno de estos conjuntos $S_1, S_2, ..., S_r$, tenemos una unión disjunta

$$\Sigma = Orb(S_1) \cup Orb(S_2) \cup ... \cup Orb(S_r).$$

Si el cardinal de cada órbita es divisible por p entonces el número total de elementos de Σ es divisible por p, y por el lema anterior, se deduce que debe de haber al menos una órbita tal que el número de elementos de esta órbita, m, no es divisible por p. Sea esta órbita la órbita de $S \in \Sigma$. Por la relación

órbita-estabilizador (teorema 10) el número de elementos en el estabilizador G_S es de la forma kp^n/m, con m no divisible por p. Entonces $|G_S|$ es de la forma tp^n. Para cada g en G_S se tiene que $g \cdot S = S$ y por lo tanto para cualquier $s \in S, gs \in S$. Entonces $|G_S| = |(G_S)s| \leq |S| = p^n$. Y como $|G_S|$ es de la forma tp^n, y como mucho es p^n, deducimos que G_S tiene exactamente p^n elementos, y así llegamos la existencia de un p-subgrupo de Sylow de G, y hemos demostrado, además, que para cualquier $s \in S$, $(G_S)s = S$, donde $(G_S)s$ es la órbita de s por G_S . □

Veamos ahora que relación tiene el número de p-subgrupos de Sylow con p

Teorema 3. Segundo teorema de Sylow

Sea G un grupo finito de cardinal kp^n, el número de p-subgrupos de Sylow G es congruente con 1 módulo p.

`Demostración:` Sea Σ el conjunto de todos los subconjuntos de G con p^n elementos. Definimos una acción de G sobre Σ dada, para $g \in G$ y $S \in \Sigma$, por

$$g \cdot S = \{gs \ : \ s \in S\}.$$

Como hemos visto en el teorema anterior, si la órbita de un conjunto S de Σ tiene cardinal no divisible por p entonces para todo $s \in S$, $(G_S)s = S$ y por lo tanto $G_S = Ss^{-1}$ es un p-subgrupos de Sylow de G. Tenemos que $s^{-1}(G_S)s$ es un subgrupo de G con el mismo número de elementos que

$$s^{-1}(G_S)s = s^{-1}(Ss^{-1})s = s^{-1}S$$

es un p-subgrupo de Sylow de la órbita en cuestión. Notamos que la órbita de este grupo tiene k elementos ya que $|G_S| = p^n$. Luego, si una órbita tiene cardinal no divisible por p, entonces contiene un p-subgrupo de Sylow y el cardinal de la órbita es k.
Por otro lado, si una órbita contiene un p-subgrupo de Sylow de G, digamos P, y si g está en el estabilizador de G_P se tiene que $gP = P$. Como $g = g1 \in P$ se tiene que $G_P \subseteq P$, y como P está contenido en G_P deducimos que $G_P = P$. Por lo tanto G_P tiene cardinal p^n y la órbita de P tiene cardinal no divisible por p (de hecho, tiene cardinal k).
Hemos visto que toda órbita que contiene un p-subgrupo de Sylow tiene cardinal k, y toda órbita de cardinal no divisible por p contiene un p-subgrupo de Sylow.
Observemos que distintos p-subgrupos de Sylow están en órbitas distintas, pues si P_1, P_2 son p-

subgrupos de Sylow en la misma órbita, P_1 es igual al conjunto por la izquierda gP_2 para algún $g \in G$, y entonces $1 \in P_2 \cap gP_2$, y como dos clases laterales o son iguales o son disjuntos se tiene $P_1 = gP_2 = P_2$.
Por lo tanto, si n_p es el número de p-subgrupos de Sylow de G, por todo lo que acabamos de ver,

$$|\Sigma| \equiv kn_p \pmod{p}$$

Por el lema 2. tenemos que

$$k \equiv kn_p \pmod{p}$$

por lo que el número de p-subgrupos de Sylow es congruente con 1 módulo p. □

Proposición 18. *Si G es un p-grupo finito, el número de elementos de G es una potencia de p. Recíprocamente, cualquier grupo finito cuyo orden es una potencia de p es un p-grupo.*

En el siguiente enunciado hablaremos de p-subgrupos de Sylow dentro del normalizador de un p-subgrupo de Sylow de un grupo dado G.

Proposición 19. *Sea P un p-subgrupo de Sylow de un grupo finito G. Cualquier p-subgrupo de $N_G(P)$ está contenido en P y P es el único p-subgrupo de Sylow de $N_G(P)$.*

`Demostración:` Sea P un subgrupo de G de orden p^n, y Q un p-subgrupo de $N_G(P)$ de orden p^m. Como P es un subgrupo normal de $N_G(P)$, se tiene que $\langle P, Q\rangle = PQ$ por el lema 1. Como

$$|PQ| = \frac{|P||Q|}{|P \cap Q|}$$

tenemos que PQ es un subgrupo de G de orden p^{n+m-k} donde $|P \cap Q| = p^k$, y como p^n es la mayor potencia de p que divide a $|G|$, esto será posible solo si $m \leq k$, y al ser $P \cap Q$ un subgrupo de Q se tiene que $k \leq m$ y concluimos que $m = k$ y que $P \cap Q = Q$, por lo que se deduce que Q está contenido en P como queríamos ver. Y si Q es un p-subgrupo de Sylow de $N_G(P)$ se tiene que $P = Q$. □

Veamos la relación entre un p-subgrupo de Sylow y sus conjugados.

Teorema 4. Tercer teorema de Sylow

Si P es un p-subgrupo de Sylow de un grupo finito G y Q es un p-subgrupo de G, entonces Q está contenido en un conjugado de P.

Demostración: Consideramos el conjunto Π de los distintos conjugados de P, es decir,

$$\Pi = \{gPg^{-1} \ : g \in G\}.$$

Consideramos las órbitas de Π bajo la conjugación por elementos de P. Observamos que la órbita de P es $\{P\}$. Veamos que P es el único elemento de Π cuya órbita tiene cardinal 1. Si la órbita de gPg^{-1} contiene un único elemento , se tiene que para todo $x \in P$ ocurre que

$$x(gPg^{-1})x^{-1} = gPg^{-1}$$

luego para todo $x \in P$ tenemos que $g^{-1}xg$ es un elemento de $N_G(P)$ y el orden de $g^{-1}xg$ es el mismo que el orden de x. Se deduce que gPg^{-1} es un p-subgrupo en $N_G(P)$, de hecho, es un p-subgrupo de Sylow ya que gPg^{-1} tiene el mismo número de elementos que P. Por la proposición anterior $gPg^{-1} = P$ y esto prueba que P es el único elemento de Π cuya órbita tiene cardinal 1.
Por lo tanto, para cualquier g que no esté en P, el orden de la órbita de gPg^{-1} bajo la conjugación por elementos de P es mayor que 1. Por la relación órbita-estabilizador, estas órbitas tienen cardinal congruente con 0 módulo p y deducimos que

$$|\Pi| \equiv 1 \quad (\text{mód } p).$$

Consideramos ahora las órbitas de Π bajo la conjugación por elementos de Q. Como todas las órbitas tienen orden una potencia de p, lo que hemos visto antes nos muestra que hay al menos una órbita de cardinal 1, por lo que hay un elemento g tal que $\forall x \in Q$,

$$x(gPg^{-1})x^{-1} = gPg^{-1}$$

Como antes deducimos que gQg^{-1} está en $N_G(P)$, y por la proposición anterior $g^{-1}Qg \subseteq P$, o sea que $Q \subseteq gPg^{-1}$, que era lo que querámos demostrar. □

Tenemos el siguiente corolario, o cuarto teorema de Sylow.

Corolario 3. Cuarto teorema de Sylow

Todos los p-subgrupos de Sylow de un grupo finito son conjugados, así que el número de p-subgrupos de Sylow divide a $|G|$.

`Demostración:` Supongamos que P y Q son p-subgrupos de Sylow de G. Por el teorema anterior Q está contenido en un conjugado de P. Como P y Q tienen el mismo número de elementos la única posibilidad es que Q y el conjugado de P son iguales.
Por la relación órbita-estabilizador, el número de conjugados de P es igual al índice de $N_G(P)$, y por el teorema de Lagrange, el número de p-subgrupos de Sylow divide a $|G|$. □

Algunos resultados relacionados con subgrupos normales:

Corolario 4. *Sea G un grupo de orden kp^n con $mcd(p,k) = 1$. Si un p-subgrupo de Sylow es normal, entonces es el único p-subgrupo de Sylow de G*

Y tenemos también el contrarrecíproco de esta propiedad.

Proposición 20. *Sea G un grupo de orden kp^n con $mcd(p,k) = 1$. Si hay un único p-subgrupo de Sylow, este es un subgrupo normal.*

`Demostración:` Sea S el único subgrupo de orden p^n. Para todo $g \in G$ se cumple $|g^{-1}Sg| = |S| = p^n$, y $g^{-1}Sg$ es un subgrupo de G, luego $g^{-1}Sg = S$ para todo $g \in G$, pues S es el único subgrupo de orden p^n, y con esto queda demostrado que S es normal. □

Proposición 21. *Sea G un grupo finito. Sea P un p-subgrupo de Sylow de G y N un subgrupo normal de G.Entonces:*

(a). $P \cap N$ es un p-subgrupo de Sylow de N

(b). PN/N es es un p-subgrupo de Sylow de G/N

`Demostración:`

(a). Primero observemos que un subgrupo H de un grupo G es un p-subgrupo de Sylow si H es un p-subgrupo y el índice de H en G no es divisible por p. Como N es normal $\langle P, N\rangle = PN$

demostrado en el lema 1. y como $P \cap N$ es un subgrupo de P su orden es una potencia de p. Queremos ver que $|N : P \cap N|$ no es divisible por p. Tenemos que $|N : P \cap N| = |PN : P|$ y $|G : P| = |G : PN||PN : P|$, o sea que $|PN : P|$ divide a $|G : P|$, y por lo tanto $|PN : P|$ no es divisible por p, y $P \cap N$ es un subgrupo de N de índice no divisible por p. Por lo tanto, $P \cap N$ es un p-subgrupo de Sylow de N.

(b). Como $PN/N \cong P/(P \cap N)$, tenemos que PN/N es un subgrupo de G/N. Por la demostración en (a), $|G : PN|$ no es divisible por p, y entonces PN/N es un p-subgrupo de Sylow de G/N.

□

Capítulo 4

Aplicaciones de los teoremas de Sylow

En este capítulo aplicaremos lo enunciado en el capítulo anterior para estudiar la estructura de varios grupos de diferentes ordenes, en particular para ver si poseen p-subgrupos de Sylow y subgrupos normales. También trataremos cuándo algunos grupos de un orden concreto son cíclicos o isomorfos a otro tipo de grupo, como por ejemplo a un grupo diédrico.

4.1. Aplicaciones

Primero nos fijaremos en los grupos de orden pq con p, q primos y p mayor que q.

Proposición 22. *Sean $p, q \in \mathbb{Z}$ primos con $p > q$. Un grupo de orden pq tiene un p-subgrupo de Sylow normal.*

`Demostración:` Por el segundo teorema de Sylow el número de p-subgrupos de Sylow es congruente con 1 módulo p, y por el cuarto teorema el número de p-subgrupos de Sylow divide el cardinal del grupo, que en este caso es pq.
Los divisores de pq son 1,q, p y pq. De estos, p y pq tienen resto 0 al ser divididas por p, y q tiene resto q, ya que q es menor que p, y por lo tanto solo puede haber un p-subgrupo de Sylow, pues 1 es el único divisor de pq congruente con 1 módulo p. □

Esta propiedad la usaremos más adelante para ver el número de p-subgrupos de alguna familia en concreto.

Dado $n \in \mathbb{Z}$, $n \geq 3$, el grupo diédrico $D(n)$ es el dado por la siguiente relación

$$D(n) = \{a, b \mid \ a^n = 1 = b^2, \ ba = a^{-1}b\}, \tag{4.1}$$

siendo $2n$ el orden de $D(n)$.

Proposición 23. *El grupo diédrico $D(n)$ tiene al menos un 2-subgrupo de Sylow.*

Demostración: Por el primer teorema de Sylow, al ser $|D(n)| = 2n$, si n es impar se tiene que 2 es primo y no divide a n por lo que hay al menos un 2-subgrupo de Sylow de orden 2, mientras que si n es par, se tiene que $|D(n)| = 2^k m$ para algún $k, m \in \mathbb{Z}$ y también, por el primer teorema de Sylow, hay al menos un 2-subgrupo de Sylow pero de orden 2^k. □

Veamos un resultado particular de la proposición anterior, cuando $q = 2$, útil para clasificar grupos de índice par.

Corolario 5. Grupos de orden 2p

Sea p un número entero primo mayor que 2, y G un grupo con $2p$ elementos. Entonces G es o un grupo cíclico o isomorfo al grupo diédrico $D(p)$.

Demostración: Por la proposición 22. hay un p-subgrupo de Sylow de G normal, P, como P tiene p elementos es cíclico $P = \langle x \rangle$, luego x es un elemento de orden p. Por el teorema de Sylow, G tiene al menos un 2-subgrupo de Sylow, por lo que hay un elemento y de orden 2. Por lo tanto los elementos de G son $\{1, x, ..., x^{p-1}, y, yx, ..., yx^{p-1}\}$ luego G es o un grupo cíclico o isomorfo al grupo diédrico $D(p)$. □

Veamos ahora algo acerca los subgrupos normales de un grupo de orden p^2q.

Proposición 24. *Sean $p, q \in \mathbb{Z}$ primos distintos, entonces un grupo de orden p^2q tiene un subgrupo de Sylow normal.*

Demostración: El número de p-subgrupos de Sylow divide a p^2q y no es múltiplo de p, así que es o 1 o q.
Si $p > q$, entonces q no puede ser congruente con 1 módulo p por lo que el número de p-subgrupos de Sylow es 1, que es lo que queríamos.
Si $q > p$, puede haber q p-subgrupos de Sylow si $q \equiv 1(\mod p)$. En este caso, el número de q-subgrupos de Sylow divide a p^2q y no es múltiplo de q, luego es 1, p o p^2. Pero no puede ser p ya que no es congruente con 1 módulo q. Si el número de q-subgrupos de Sylow es p^2 tenemos que $p^2 \equiv 1(\mod q)$, por lo que q divide a $(p-1)(p+1)$ y esto ocurre solo si q divide a $(p-1)$ o a $(p+1)$, como $q > p$ q no puede dividir a $p-1$, la única posibilidad es que $q = p+1$, lo que implica que p y q

son primos consecutivos, luego $p = 2$ y $q = 3$, En este caso G tiene 12 elementos y el resultado se concluye del ejemplo anterior. □

Proposición 25. *Todo grupo G de 15 elementos es cíclico.*

Demostración: El número de 3-subgrupos de Sylow divide a 15 y es congruente con 1 módulo 3, luego hay un solo 3-sugrupo de Sylow. A su vez el número de 5-subgrupos de Sylow divide a 15 y es congruente con 1 módulo 5, luego también hay un solo 5-subgrupo de Sylow. Sea P el único 3-subgrupo y sea Q el único 5-subgrupo. Sea x un elemento de orden 3, luego (por la proposicion 4.11 de [Hump]) $\langle x \rangle$ tiene 3 elementos y por lo tanto es un 3-subgrupo de Sylow de G, luego $\langle x \rangle = P$, y x es uno de los dos elementos diferentes de la identidad de P. De igual forma, si y es un elemento de orden 5, entonces $\langle y \rangle = Q$, y y es uno de los cuatro elementos diferentes de la identidad de Q. Por tanto G tiene un elemento de orden 1 (la identidad), dos elementos de orden 3, y cuatro elementos de orden 5. (por el corolario 5.12 de [Hump]) el orden de cualquiera de los 8 elementos restantes divide 15, o sea será 1,3,5 o 15. Como ya hemos contado los elementos de orden 1,3 y 5, y no hay más, se tiene que estos 8 elementos restantes tienen orden 15, y por lo tanto G es cíclico. □

Veamos una clasificación de los grupos de orden 30.

Proposición 26. *Sea G un grupo con 30 elementos, entonces G tiene un subgrupo cíclico normal de 15 elemetos.*

Demostración: Todos los grupos de 15 elementos son cíclicos, así que solo tenemos que ver que tiene un subgrupo normal de 15 elementos.

Por el segundo teorema de Sylow el número de 3-subgrupos y 5-subgrupos de Sylow es congruente con 1 módulo 3 y congruente con 1 módulo 5 respectivamente, y por el cuarto teorema el número de 3-subgrupos y 5-subgrupos de Sylow divide el cardinal del grupo, que en este caso es 30. Luego hay uno o diez 3-subgrupos, y hay uno o seis 5-subgrupos.

Supongamos que solo hay un 3-subgrupo, P, y por lo tanto es normal, y podemos formar el espacio cociente G/P, que es tal que $|G/P| = 10 = 2 \cdot 5$. Por la proposición 22. el grupo G/P tiene un 5-subgrupo normal de Sylow de G, sea este grupo denotado por N/P, por el teorema de correspondencia, N es un subgrupo normal de G que contiene a H, y N tiene 15 elementos, y por lo tanto, es cíclico.

Si suponemos que hay diez 3-subgrupos de Sylow, $P_1, P_2, ..., P_{10}$. Por el teorema de Lagrange, para

$i, j \in \{1, 2, ..., 10\}$ con $i \neq j$, el número de elementos en $P_i \cap P_j$ divide a $|P_i| = 3$. Como P_i y P_j son distintos, se tiene que $P_i \cap P_j = \{1\}$. Como cada P_i tiene dos elementos de orden 3 que no está en ninguno de los otros P_j, significa que G tiene 20 elementos distintos de orden 3. Por lo tanto hay 30-(20+1)=9 elementos de G de orden diferente de 1 o 3. En este caso, si G tuviera seis 5-subgrupos de Sylow, $Q_1, ..., Q_6$, al ser estos diferentes se tiene que $Q_i \cap Q_j = \{1\}$ y cada Q_i tiene 4 elementos de orden 5, por lo que haría 24 elementos de orden 5, lo cual no es posible pues solo quedaban 9 elementos que no tuvieran orden 1 o 3. Por lo que si G tiene diez 3-subgrupos de Sylow, solo puede tener un único 5-subgrupos de Sylow, al que llamaremos Q. El subgrupo Q resulta ser normal, y el grupo cociente G/Q tiene orden $6 = 2 \cdot 3$ y por la proposición 22. el grupo G/Q tiene un subgrupo normal N/Q de cardinal 3. Por el teorema de correspondencia N es un subgrupo normal de G que contiene a Q, y $|N| = 15$ luego es cíclico, y queda demostrado que G tiene un subgrupo cíclico normal de 15 elementos en cualquier caso. □

Teorema 5. *Un grupo de cardinal 30 es o cíclico o diédrico o isomorfo a uno de los dos siguientes grupos* $\langle x, y : x^{15} = 1 = y^2, yxy^{-1} = x^4 \rangle$ *o* $\langle x, y : x^{15} = 1 = y^2, yxy^{-1} = x^{11} \rangle$.

`Demostración:` Por la proposición anterior, un grupo G de orden 30 tiene un subgrupo cíclico normal N de orden 15. Sea x el generador de dicho subgrupo N, y sea y el generador de un 2-subgrupo de Sylow de G. Como N es normal, $yxy^{-1} = x^i$ para algún $i \in \{1, 2, ..., 14\}$. Como $y^2 = 1$ $x = y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^iy^{-1} = x^{i^2}$, por lo que $i^2 \equiv 1(\mod 15)$. Los únicos i que cumplen esta congruencia son $i \equiv 1,\ 4,\ 11$ o $14(\mod 15)$. El caso $i \equiv 1(\mod 15)$ se da cuando G es cíclico, el caso $i \equiv -1(\mod 15)$ cuando G es un grupo diédrico, y los otros dos casos son cuando G es de la forma $\langle x, y : x^{15} = 1 = y^2, yxy^{-1} = x^4 \rangle$ o $\langle x, y : x^{15} = 1 = y^2, yxy^{-1} = x^{11} \rangle$. □

4.2. Ejemplos

En esta sección mostraremos algunos ejemplos en los que aplicaremos los resultados que hemos visto con anterioridad.

Ejemplo 2 *Un grupo de 12 elementos o bien tiene un 2-subgrupo de Sylow normal o bien tiene un 3-subgrupo de Sylow normal.*

Nótese que un 2-subgrupo de Sylow de un grupo de orden 12 tiene 4 elementos.

El númemro de 3-subgrupos de Sylow es, o 1, o 4. Veamos que si hay cuatro 3-subgrupo de Sylow el

número de 2-subgrupo de Sylow debe ser 1. Si G tiene cuatro 3-subgrupo de Sylow, $P_1,\ P_2,\ P_3,\ P_4$, cada intersección $P_i \cap P_j$ con $i \neq j$ es un subgrupo propio de P_i, donde P_i es un grupo con 3 elementos. Por lo que $P_i \cap P_j = \{1\}$ para $i \neq j$. Luego G contiene el elemento identidad junto con ocho elementos de orden 3, cada dos de ellos en un 3-subgrupo de Sylow. Además de estos nueve elementos hay otros tres elementos en el grupo G, y por lo tanto G tiene un único 2-subgrupo de Sylow compuesto por estos tres elementos y la identidad.

Ejemplo 3 *Sea G un grupo con 24 elementos, entonces G tiene, o un subgrupo normal de 8 elementos, o un subgrupo normal de 4 elementos.*
El número de 2-subgrupos de Sylow es, o 1, o 3. Si el número es 1 el 2-subgrupo de Sylow es un subgrupo normal de orden 8.
Si suponemos que G tiene tres 2-subgrupos de Sylow, P_1, P_2, P_3, cada uno con 8 elementos. Como

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

, el subconjunto P_1P_2 tiene $2^3 2^3/2^r$ elementos, donde $|P_1 \cap P_2| = 2^r$. Como P_1P_2 es un subconjunto de G, un grupo con 24 elementos, se tiene que $2^3 2^3 \leq |G| \cdot 2^r$, o sea, $2^6 = 64 \leq 24 \cdot 2^r$. Entonces $r \geq 2$. Y como $P_1 \cap P_2$ es un subgrupo propio de P_1 tiene, a lo sumo, 2^2 elementos y se deduce que si G tiene tres 2-subgrupos de Sylow, la intersección de cualquiera dos de ellos tiene orden 4.
Sea $T = P_1 \cap P_2$,o sea T tiene 4 elementos. Como T es un subgrupo de P_1 de índice 2, T es normal en P_1. De la misma forma T es un subgrupo normal de P_2. Como ambos P_1 y P_2 son subgrupos de $N_G(T)$, entonces $H = \langle P_1, P_2 \rangle$ es un subgrupo de $N_G(T)$, y por lo tanto T es un subgrupo normal de H. Como H es un subgrupo contiene a P_1P_2. Hemos visto que P_1P_2 tiene $\frac{2^3 2^3}{2^2} = 2^6/2^2 = 16$ elementos. Como el único subgrupo de G que tiene al menos 16 elementos es él mismo, se tiene que $H = G$ y por lo tanto T es un subgrupo normal de G de orden 4.

Ejemplo 4 *Veamos que un grupo G de orden 45 es abeliano. Como $45 = 3^2 \times 5$, G tieneun 3-subgrupo de Sylow, al que llamaremos H, de orden 9, y tiene un 5-subgrupo de Sylow, al que llamaremos K, de orden 5. Sea n el número de conjugados de H. Entonces $n = 1 + 3r$ con $r \geq 0$, y n divide a 45, y como los factores de 45 son $1, 3, 5, 9, 15, 45$, es claro que $n = 1$ y por lo tanto H es normal en G. De manera*

similar se ve que K es normal en G.Tenemos que $G = HK$ y como

$$|HK| = |HK||H \cap K| = |H||K| = 45$$

y por lo tanto G es isomorfo al producto directo de H por K, y como H es abeliano por la proposición 1. y como K es cíclico es por tanto abeliano, y por la proposición 6.

Capítulo 5

Grupos resolubles y supersolubles

En este capítulo mostraremos varias definiciones, y proposiciones sobre la estructura de grupos finitos, y algunos ejemplos sencillos. Por ejemplo, introduciremos el concepto de grupo resoluble y estableceremos algunas de las propiedades básicas de estos grupos.

5.1. Definiciones

Primero presentaremos las definiciones de serie subnormal y serie normal, que luego utilizaremos en las definiciones de grupo resoluble.

Definición 19. *Una serie subnormal de un grupo G es una cadena finita de subgrupos $\{G_i\}_{i=0}^{n}$, $G_i \subset G$ tal que :*

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_n = G$$

donde para cada $i = 0, 1, ..., n-1$ se cumple que G_i es un subgrupo normal de G_{i+1}.
Los factores de la serie son los grupos cocientes G_{i+1}/G_i. La longitud de la serie es el número de inclusiones estrictas, es decir, el número de factores no triviales.
Si además de esto cada G_i es normal en G, entonces se dice que es una serie normal.

Definición 20. *Un grupo G es resoluble si tiene una serie subnormal cuyos factores son grupos abelianos.*

Es claro que todo grupo abeliano es resoluble, pues $\{1\} \subset G$ y el conjunto $\{1\}$ es normal en G, ya que $g \cdot 1 \cdot g^{-1} \in \{1\}$ y se tiene que $G/\{1\} \simeq G$, que es abeliano.

Definición 21. *Un grupo G es supersoluble si tiene una serie normal cuyos factores son grupos ciclicos.*

Ejemplo 5 *Sea $G = \langle x \rangle$ el grupo cíclico de orden 6, entonces tenemos dos series normales:*

$$G \supseteq \langle x^2 \rangle \supseteq \{1\}$$

$$G \supseteq \langle x^3 \rangle \supseteq \{1\}$$

ya que cualquier subgrupo de un grupo abeliano es normal.
Además los factores son cíclicos, pues son $\langle x^2 \rangle / \{1\} \cong \langle x^2 \rangle$, $\langle x^3 \rangle / \{1\} \cong \langle x^3 \rangle$, $G/\langle x^2 \rangle \cong \langle x^3 \rangle$ *y* $G/\langle x^3 \rangle \cong \langle x^2 \rangle$, *que son cíclicos.*

El siguiente ejemplo es de un grupo no abeliano supersoluble.

Ejemplo 6 *El grupo cuaternio* Q_8, *de orden* 8 *no abeliano, tiene a* $\{1\}$ *y a* $\{1, -1\}$ *como subgrupos normales,* $\{1\} \triangleleft \{1, -1\} \triangleleft G$ *, y dado que todo subgrupo de* Q_8 *es cíclico, se tiene que* Q_8 *es supersoluble.*

Asociado al concepto de grupo resoluble viene el concepto de serie derivada.

Definición 22. *Sea* G *un grupo y* x, y *dos elementos cualesquiera de* G. *El conmutador de* x *e* y, *denotado por* $[x, y]$ *viene dado por* $[x, y] = xyx^{-1}y^{-1}$

A la hora de analizar un grupo G para ver si es abeliano o no, lo que buscamos es ver si dos elementos cualesquiera de este grupo conmutan o no; es decir, dados $x, y \in G$ queremos ver si $xy = yx$ o lo que es equivalente $(xy)(x^{-1}y^{-1}) = 1$, equivalente a su vez a que $[x, y] = 1$.

Definición 23. *El subgrupo derivado de* G, *denotado por* $[G, G]$ *o por* G', *es el subgrupo dado por*

$$[G, G] = G' = \langle [x, y] \ : \ x, y \in G \rangle$$

Es claro que un grupo G será abeliano si y solo si $G' = \{1\}$.

Definición 24. *Dado un grupo* G, *se define la serie derivada de* G *iterativamente por*

$$G^{(0)} = G; \ G^{(1)} = G'; \ G^{(2)} = [G', G']; \ ...G^{(r+1)} = [G^{(r)}, G^{(r)}].$$

5.2. Cuando un grupo es resoluble y otras propiedades

Veamos varias formas equivalentes de saber si un grupo G es resoluble.

La primera proposición que vamos a enunciar se deduce de las definiciones, ya que toda serie normal es subnormal, y todo grupo cíclico es abeliano.

Proposición 27. *Todo grupo supersoluble es resoluble*

Proposición 28. *Dado un grupo G, y $N \subseteq G$ un subgrupo normal de G, se tiene lo siguiente:*

(a). G' es normal en G.

(b). G/N es abeliano si y sólo si $G' \subseteq N$. En particular, G/G' es abeliano.

(c). G' es la intersección de todos los subgrupos N normales en G, $N \triangleleft G$, tales que el grupo cociente de G por N es abeliano.

(d). Si $S \subseteq G$, entonces $S' \subseteq G'$.

`Demostración:`

(a). Sea $x \in G$, y sea $y \in G'$, por definición de G' existen $z, w \in G$ tales que $y = [z, w] = zwz^{-1}w^{-1}$, y por lo tanto tenemos que $xyx^{-1} = xzwz^{-1}w^{-1}x^{-1} = xzwxx^{-1}z^{-1}w^{-1}x^{-1}$ que es otro elemento de G', por lo que G' es normal.

(b). G/N es abeliano si y sólo si $xNyN = yNxN$ para todo $x, y \in G$, y esto ocurre si y solo si $xyx^{-1}y^{-1}N = N$ para todo $x, y \in G$, es decir, si y solo si $[x, y]N = N$ lo cual ocurre si y solo si $[x, y] \in N$ para todo $x, y \in G$, si y solo si $G' \subseteq N$.

(c). Es consecuencia directa de (a) y (b).

(d). Es claro por la definición.

□

Proposición 29. *Cada $G^{(n+1)}$ es un subgrupo normal de $G^{(n)}$.*

`Demostración:` Si $n = 0$ tenemos que $G^{(0)} = G$ y el resultado es el apartado (a) de la proposición 28. Veamos que es cierto para n, es decir, $G^{(n+1)}$ es normal en $G^{(n)}$. Sea $g \in G^{(n)}$, tenemos que $G^{(n+1)} = [G^{(n)}, G^{(n)}] = \langle [x, y] \ : \ x, y \in G^{(n)} \rangle$ y dado $y \in G^{(n+1)}$ existen $z, w \in G^{(n)}$ tales que $y = [z, w]$ y por lo tanto $gyg^{-1} = g[z, w]g^{-1}$ y razonando como en la proposición 28. el apartado (a), vemos que este elemento pertenece a $[G^{(n)}, G^{(n)}] = G^{(n+1)}$, con lo que se tendría lo que queríamos probar. □

Hay un resultado un poco más fuerte, que dice que cada $G^{(n)}$ es un grupo normal de G.

Veamos una nueva definición de grupo resoluble, la cual en algunas circunstancias nos será más útil que la anterior definición.

Proposición 30. *Un grupo G es resoluble si y solo si $G^{(n)} = 1$ para algún $n \in \mathbb{N}$.*

Demostración: Supongamos que G es resoluble, entonces tiene una serie subnormal $\{1\} = G_n \subseteq G_{n-1} \subseteq ...G_1 \subseteq G_0 = G$, cuyos factores son abelianos. Por la proposición 28. apartado (b) se tiene que $G^{(k)} \subseteq G_k$ y por lo tanto $G^{(n)} = 1$ pues $G^{(n)} \subseteq G_n = 1$.
Por otro lado, si $G^{(n)} = 1$ tenemos que la serie derivada de G dada por

$$\{1\} = G^{(n)} \subseteq G^{(n-1)} \subseteq ...G^{(1)} \subseteq G^{(0)} = G$$

es una serie normal con factores abelianos. □

Recordamos que todo grupo cíclico es abeliano. Es decir, todo grupo cíclico es, por lo tanto, resoluble.
Otro resultado sobre grupos cíclicos de orden pq es el siguiente.

Y al ser cíclico es abeliano, y por lo tanto es resoluble.
A continuación vamos a mostrar una proposición que usaremos más adelante para demostrar otras proposiciones.

Proposición 31. *Sea G un grupo, H un subgrupo cualquiera de G y K un subgrupo normal de G, $K \triangleleft G$. Entonces $H \cap K$ es un subgrupo normal de H, es decir, $H \cap K \triangleleft H$.*

Demostración: Para cualquier x en $H \cap K$ y para cualquier $h \in H$ se tiene que hxh^{-1} está en H, por ser H un subgrupo de G. Además, como K es normal en G y x también está en K se tiene que hxh^{-1} pertenece a K, y por lo tanto hxh^{-1} está en $H \cap K$, por lo que es normal en H, como queríamos ver. □

Un ejemplo de esta propiedad es el siguiente:

Ejemplo 7 *Dado el grupo diédrico $D(6)$, el subgrupo $\mathbb{Z}_2$ es normal en $D(6)$, $\mathbb{Z}_2 \triangleleft D(6)$, y $\mathbb{Z}_6$ es un subgrupo de $D(6)$. Entonces $\mathbb{Z}_2 \cap \mathbb{Z}_6 = \mathbb{Z}_2$ es un subgrupo normal en $\mathbb{Z}_6$, $\mathbb{Z}_2 \triangleleft \mathbb{Z}_6$.*

Proposición 32. *Sea G un grupo resoluble. Entonces:*

(a). Cualquier subgrupo H de G es resoluble.

(b). El grupo cociente G/K es resoluble para cualquier subgrupo normal K de G.

`Demostración:`

(a). Como G es resoluble existe una cadena finita de subgrupos $\{G_i\}_{i=0}^n$, $G_i \subset G$ tal que $\{1\} = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$ y los grupos cocientes G_{i+1}/G_i para $i = 0, 1, ..., n-1$ son abelianos. Consideramos la cadena finita $\{H \cap G_i\}_{i=0}^n$. Se cumple la condición de normalidad por la proposición 31. por lo que tenemos que ver que $(H \cap G_{i+1})/(H \cap G_i)$ es abeliano para $i = 0, 1, ..., n-1$. Tenemos lo siguiente:

$$(H \cap G_{i+1})/(H \cap G_i) = (H \cap G_{i+1})/((H \cap G_{i+1}) \cap G_i) \cong (H \cap G_{i+1})G_i/G_i \subseteq G_{i+1}/G_i,$$

hemos usado el segundo teorema de isomorfía. Y como los subgrupos de grupos abelianos son abelianos se tiene que los grupos cocientes de la cadena finita considerada son abelianos, por lo que H es resoluble. □

(b). Para ver que G/K es resoluble, consideremos la cadena finita de subgrupos $\{G_iK/K\}_{i=0}^n$. Se tiene que G_iK/K es un subgrupo normal de $G_{i+1}K/K$, por lo que solo necesitamos ver que los grupos cociente son abelianos.

$$(G_{i+1}K/K)/(G_iK/K) \cong G_{i+1}K/G_iK = G_i(G_{i+1}K)/G_iK \cong G_{i+1}/(G_{i+1} \cap G_iK),$$

usamos el segundo y tercer teorema de isomorfía, por lo que

$$G_{i+1}/(G_{i+1} \cap G_iK) \cong (G_{i+1}/G_i)/((G_i \cap G_{i+1}K)/G_i)$$

Y como el grupo cociente de grupos abelianos es abeliano se tiene el resultado.

Vamos a ver un teorema de Feit y Thompson interesante sobre los grupos resolubles.

Teorema 6. de Feit-Thompson

Todo grupo finito de orden impar es resoluble.

Esta propiedad fue demostrada por Feit y Thompson en [Feit], siendo esta demostración una de gran extensión, cosa que era poco común entre las que se realizaban en de Teoría de Grupos. Este resultado es un resultado importante en clasificar los grupos simples finitos.

Veamos el "contrarrecíproco" de la proposición 32.

Proposición 33. *Un grupo G es resoluble si y solo si existe un subgrupo normal N de G, $N \triangleleft G$, tal que N y G/N son resolubles.*

`Demostración:` Una de las implicaciones nos la da la proposición 32.
Veamos la otra. Sean G/N y N resolubles, esto quiere decir que existen una serie normal de G/N, denotemosla $\{H_i\}_1^n$, con $H_i = M_i/N$, y una de N, denotada $\{N_j\}_1^m$, tales que

$$\{1\} = H_1 \triangleleft H_2 \triangleleft ...H_{n-1} = M_{n-1}/N \triangleleft H_n = M_n/N = G/N$$

$$\{1\} = N_1 \triangleleft N_2 \triangleleft ...N_{m-1} \triangleleft N_m = N$$

Entonces tenemos la cadena

$$\{1\} = N_1 \triangleleft N_2 \triangleleft ...N_m = N = M_1 \triangleleft M_2 \triangleleft ...M_n = G$$

es serie normal de factores N_{i+1}/N_i y $M_{i+1}/M_i \cong (M_{i+1}/N)/(M_i/N) = H_{i+1}/H_i$, luego G es resoluble. □

De esta proposición se deduce el siguiente corolario.

Corolario 6. *Sean H, K dos grupos resolubles. Entonces su producto directo $H \times K$ es resoluble.*

`Demostración:` Si consideramos el grupo dado por su producto directo $G = H \times K$ se tiene que H es normal en G, $H \triangleleft G$, y $G/H \cong K$ y por la proposición anterior se tiene el resultado. □

Teorema 7. *Sea p un número entero primo. Todo p-grupo finito es resoluble.*

`Demostración:` Ver el corolario 6.7 de [Milne].

Proposición 34. *Un grupo simple y resoluble es cíclico de orden primo.*

`Demostración:` Si es resoluble entonces es abeliano, y por ser simple y abeliano por la proposición 10. se tiene que es cíclico de orden primo, como queríamos. □

Se da también el recíproco, pues, de nuevo, por la proposición 10. todo grupo cíclico de orden primo es abeliano simple, y todo grupo abeliano es resoluble.

5.3. Grupos metacíclicos y metabelianos

En esta sección expondremos los grupos metacíclicos y metabelianos, y a través de algunos ejemplos analizaremos algunas de sus propiedades más notables.

Definición 25. *Un grupo G es metacíclico si contiene un subgrupo normal cíclico C de manera que el grupo cociente G/C es cíclico*

Más adelante comprobaremos que el producto semidirecto de dos grupos cíclicos, tales que se cumple cierta propiedad, es un grupo metacílico.

Definición 26. *Un grupo G es metabeliano si existe un subgrupo normal abeliano A, es decir $A \triangleleft G$, tal que el grupo cociente G/A es abeliano.*

Un grupo diédrico es metabeliano, pues tiene un subgrupo normal de orden n, y el cociente del grupo por este subgrupo es cíclico orden 2 y por lo tanto abeliano.

5.3.1. Algunos ejemplos

Veamos una propiedad importante de los grupos metacíclicos.

Proposición 35. *Todo grupo metacíclico G es supersoluble y metabeliano.*

`Demostración:` Si G es metacíclico entonces existe un subgrupo normal cíclico C contenido en G tal que el grupo cociente G/C es cclico, y entonces tenemos que $1 \triangleleft C \triangleleft G$ una cadena finita de subgrupos normales, tales que cada uno es normal en G y los grupos cocientes son cíclicos, pues $C/1 \simeq C$, que es cíclico por hipótesis, y G/C también es cíclico por hipótesis, luego G es supersoluble (y por lo tanto también es resoluble).

Por otro lado, todo grupo cíclico es abeliano, y por lo tanto se tiene que C es abeliano y normal en G, y también que G/C es abeliano, por lo que G es metabeliano. □

Proposición 36. *Todo grupo metabeliano es resoluble.*

Demostración: Sea G un grupo metabeliano y sea A el subgrupo normal abeliano de G tal que el grupo cociente G/A es abeiano. El subgrupo $\{1\}$ es normal en cualquier subgrupo de G, y por lo tanto es normal en A, y tenemos la serie $\{1\} \triangleleft A \triangleleft G$ en la que los factores son abelianos, pues $A/\{1\} \cong A$ que es abeliano, y G/A es abeliano por hipótesis. □

Proposición 37. *El producto directo de dos grupos cíclicos es un grupo metacíclico.*

Demostración: Sean G y H dos grupos cíclicos. Se tiene que el producto directo $G \times H$ tiene un subgrupo normal dado por $\{(g, 1) \ / \ g \in G \}$ donde 1 es la unidad en H, y este subgrupo es cíclico, pues es isomorfo a G, y el grupo cociente de $G \times H$ por este subgrupo es cíclico, pues es isomorfo a H, y por lo tanto es metacíclico. □

Cualquier grupo cíclcico es metabeliano, pues dado un grupo G cíclico se tiene que G es abeliano y que $\{1\}$ es un subgrupo normal en G, también abeliano, y el grupo cociente $G/\{1\} \cong G$ es abeliano.

En los próximos capítulos presentaremos abundantes ejemplos no triviales de grupos metabelianos y metacíclicos.

Capítulo 6

Producto semidirecto de grupos

En este capítulo definiremos y analizaremos las características del producto semidirecto, para poder utilizarlo posteriormente en el estudio de familias de grupos finitos.

6.1. Definición de semiproducto directo

Definición 27. *Dado un grupo G, el grupo de automorfismos de este grupo, denotado por $Aut(G)$, es el siguiente:*

$$Aut(G) = \{f : G \to G \ : \ f \text{ es endomorfismo y biyectiva}\}$$

La operación en $Aut(G)$ es la composición de automorfismos.

Definición 28. *Dados dos grupos H y K, y sea $\varphi : H \longrightarrow Aut(K)$ un homomorfismo de grupos. a la imagen de $h \in H$ por φ la denotaremos $\varphi(h) = \varphi_h$. Entonces tenemos la siguiente acción del grupo H en K:*

$$\begin{aligned} K \times H &\to K \\ (k, h) &\to hk = \varphi_h(k) \end{aligned}$$

Se denomina producto semidirecto de H y K respecto de φ, y se denota $H \rtimes K$ al grupo formado por los pares

$$K \rtimes H = \{(k, h) \ : \ h \in H, \ \ k \in K\}$$

con la siguiente operación, para $h_1, h_2 \in H$ y $k_1, k_2 \in K$:

$$(k_1, h_1)(k_2, h_2) = (k_1\varphi_{h_1}(k_2), h_1h_2)$$

Proposición 38. *Dado el grupo $K \rtimes H$, se tiene que el subgrupo $K \rtimes \{e\}$ es normal en $K \rtimes H$, donde*

e es el elemento neutro. Se cumple que el grupo cociente es isomorfo a H,

$$(K \rtimes H)/(K \rtimes \{e\}) \cong H.$$

6.2. Producto semidirecto de grupos cíclicos

En general si K, H son grupos cíclicos su producto semidirecto, $K \rtimes H$, es metacíclico, pues $(K \rtimes H)/(K \rtimes \{e\}) \cong H$.

Para ver que el producto semidirecto de dos grupos cíclicos (tales que el orden de uno divide el orden del otro menos una unidad) es un grupo metacíclico, veamos cual es el automorfismo que usamos en el producto semidirecto.

Denotamos $\mathbb{Z}_p = \mathbb{Z}/(p)$ y $\mathbb{Z}_q = \mathbb{Z}/(q)$ con p y q números enteros primos, (es decir, $\mathbb{Z}_p$ y $\mathbb{Z}_q$ son cíclicos) tales que $q < p$ y q divide a $p-1$. Como $\mathbb{Z}_p$ es un cuerpo con la suma y muliplicación módulo p que tiene p elementos, el grupo multiplicativo de $\mathbb{Z}_p$ tiene orden $p-1$, y como hay elementos de cualquier orden divisor de $p-1$, en particular hay de orden q. Sea α uno de estos elementos del grupo multiplicativo de $\mathbb{Z}_p$ de orden q. Dado el homomorfismo de grupos $\varphi : \mathbb{Z}_q \longrightarrow Aut(\mathbb{Z}_p)$, denotando $\varphi(k) = \varphi_k$ para todo $k \in \mathbb{Z}_q$, y dado $h \in \mathbb{Z}_p$, tenemos la siguiente acción

$$\begin{aligned} \mathbb{Z}_p \times \mathbb{Z}_q &\to \mathbb{Z}_p \\ (h, k) &\to \varphi_k(h) \end{aligned}$$

donde $\varphi_k(h) = \alpha^k h$.

Notación. El grupo multiplicativo de $\mathbb{Z}_p$ se denota por $(\mathbb{Z}_p^*, \cdot)$, y es un grupo cíclico con $p-1$ elementos.

Definición 29. *El producto semidirecto de $\mathbb{Z}_p$ y $\mathbb{Z}_q$, denotado $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, es el conjunto*

$$\{(a, b) : \ a \in \mathbb{Z}_p, \ b \in \mathbb{Z}_q \ \}$$

junto con la siguiente operación, $\oplus$, definida por :

$$(a, b) \oplus (c, d) = (a + \alpha^b c, b + d)$$

donde $a, c \in \mathbb{Z}_p$ y $b, d \in \mathbb{Z}_q$, y $\alpha \in \mathbb{Z}_p^*$ de orden q, donde las operaciones en la primera componente se realizan mdulo p y la suma en la segunda componente se hace mdulo q.

Lema 3. *Sean p, q dos números enteros primos tales que $q < p$ y q divide a $p-1$, entonces $(\mathbb{Z}_p \rtimes \mathbb{Z}_q, \oplus)$ es un grupo no conmutativo de orden pq.*

`Demostración:` Veamos que su orden es pq. Esto es claro, pues el conjunto $\{(a, b) : \ a \in H, \ b \in K \ \}$ tiene cardinal pq precisamente. Veamos que no es conmutativo. Sea α un elemento del grupo multiplicativo de $\mathbb{Z}_p$, diferente de la unidad, de orden q. Sean $(1, 1)$, $(0, 1) \in \mathbb{Z}_p \rtimes \mathbb{Z}_q$, se tiene que $(1, 1) \oplus (0, 1) = (0 + \alpha^1 1, 1 + 1) = (\alpha, 2)$ mientras que $(0, 1) \oplus (1, 1) = (1 + \alpha^1 0, 1 + 1) = (1, 2)$ y este es claramente diferente de $(\alpha, 2)$ con lo que queda demostrado que no es conmutativo. □

Ejemplo 8 *Veamos un ejemplo concreto en el que $q|(p-1)$. Para $q = 3$, $p = 7$ el grupo es*

$$\mathbb{Z}_7 \rtimes \mathbb{Z}_3 = \{(a, b) \mid a \in \mathbb{Z}_7, b \in \mathbb{Z}_3\}$$

Un elemento del grupo multiplicativo $(\mathbb{Z}_7^*, \cdot)$ de orden 3 es 2, ya que $2^3 = 8 = 1 \pmod 7$.
Luego la operación es la siguiente:

$$(a, b) \oplus (c, d) = (a + 2^b c, b + d).$$

Este grupo tiene los siguientes elementos:

- *El neutro $(0, 0)$ que es el único elemento de orden 1.*
- *Tiene 6 elementos de orden 7 de la forma $(a, 0)$ con $a \neq 0$.*
- *Contiene 14 elementos de orden 3, los cuales son (a, b) con $b \neq 0$.*

Notemos que estos últimos son de orden 3.

$$(a, b) \oplus (a, b) = (a + 2^b a, 2b),$$

$$(a,b)\oplus(a+2^b a,2b)=(a+2^b(a+2^b a),3b)=(a(1+2^b+2^{2b}),0)$$

y $1+2^b+2^{2b}=0$ *si* $b\neq 0$*:*

$$1+2^b+2^{2b}=\begin{cases}1+2+2^2, & si\ b=1\\ 1+2^2+2^4=1+4+16=21=0, & si\ b=2\end{cases}$$

Hay 7 *subgrupos de orden* 3*, uno en concreto es el subgrupo generado por* $(1,1)$*, es decir, el subgrupo*

$$\langle(1,1)\rangle=\{(1,1),(3,2),(0,0)\},$$

pues $(1,1)\oplus(1,1)=(1+2^1 1,1+1)=(3,2)$*, y* $(3,2)\oplus(1,1)=(3+2^2 1,2+1)=(3+4,3)=(7,3)=(0,0)$

Proposición 39. *Sean* $p,\ q$ *números enteros primos, tales que* p *es mayor que* q *y* q *no divide a* $p-1$*. Entonces todo grupo de orden orden* pq *es cíclico.*

`Demostración:` Como q no divide a $p-1$, p primo, entonces q no puede ser 2.
Sea G un grupo de orden pq. Sea n_p el número de p-subgrupos de Sylow de G y n_q el número de q-subgrupos de Sylow de G. Por la proposición 22. $n_p=1$, y además este subgrupo de orden p es normal. En cuanto a n_q, el número de q-subgrupos es congruente con 1 módulo q, y divide a pq, luego es 1 o p o q, pero q no puede ser por no ser congruente con 1 módulo q, y si p es congruente con 1 módulo q entonces q divide $p-1$, y esto no ocurre por hipótesis, luego $n_q=1$.
Sea H el subgrupo de Sylow de orden p de G, y sea K el subgrupo de Sylow de orden q de G. Por la proposición 20. tenemos que ambos son normales en G, y por ser H de orden p, por la proposición 7. todos sus elementos tienen orden p (salvo el elemento identidad) y por lo tanto no tiene ningún elemento de orden q, razonando igual, en K no hay ningun elemento de orden p, y por lo tanto $H\cap K=\{1\}$, donde 1 es el elemento identidad.Tenemos que

$$|HK|=\frac{|H||K|}{|H\cap K|}=|H||K|=pq$$

luego $G=HK$. Por la proposición 5. se tiene que $G=HK\simeq H\times K$.
Como H es cíclico de orden p, es isomorfo a $\frac{\mathbb{Z}}{(p)}$, $H\cong(\frac{\mathbb{Z}}{(p)},+)$, y como K es cíclico de orden q $K\cong(\frac{\mathbb{Z}}{(q)},+)$, luego $G=H\times K\cong(\frac{\mathbb{Z}}{(p)}\times\frac{\mathbb{Z}}{(q)},+)\cong(\frac{\mathbb{Z}}{(pq)},+)$, este último paso por ser p y q primos

distintos, luego G es cíclico. □

Comparando el lema 3. con la proposicíon 39. podemos apreciar la importancia de que $p-1$ sea divisible por q o no a la hora de comprobar si un grupo de orden pq es cíclico o no

Veamos qué subgrupos de Sylow tiene.

Proposición 40. $(\mathbb{Z}_p \rtimes \mathbb{Z}_q, \oplus)$ *tiene un p-subgrupo de Sylow y el número de q-subgrupos de Sylow es p.*

`Demostración:` Sean n_p, y n_q el número de p-subgrupos y q-subgrupos respectivamente. Se tiene que $n_p = 1$ por la proposición 22. Ahora, el número de q-subgrupos es congruente con 1 módulo q y divide a pq luego es o 1 o q o p, pero q no puede ser porque no es congruente con 1 módulo q, y no puede ser 1 porque si lo fuera, por la proposición 39. se tendría que $\mathbb{Z}_p \rtimes \mathbb{Z}_q \cong \mathbb{Z}_p \times \mathbb{Z}_q$ el cual es conmutativo, pero en el lema 3. hemos visto que esto no pasa, luego tiene p q-subgrupos de Sylow. □

Observación:
El grupo $\mathbb{Z}_q \rtimes \mathbb{Z}_p$ contiene al elemento neutro $(0,0)$, a $q-1$ elementos de orden q, los cuales son de la forma $(h,0)$ con $h \in \mathbb{Z}_q$, $h \neq 0$, y contiene $q(p-1)$ elementos de orden p, los cuales son de la forma (h,k) con $h \in \mathbb{Z}_q$ y $k \in \mathbb{Z}_p$, $k \neq 0$.

Proposición 41. *El grupo $G = \mathbb{Z}_p \rtimes \mathbb{Z}_q$ es un grupo metacíclico no conmutativo.*

`Demostración:` Tenemos que $\mathbb{Z}_p \rtimes \{0\}$ es un subgrupo de G normal, y cíclico, pues $\mathbb{Z}_p \rtimes \{0\} \cong \mathbb{Z}_p$ y además el grupo cociente $G/(\mathbb{Z}_p \rtimes \{0\}) \cong \mathbb{Z}_q$ es cíclico, con lo que se concluye que es un grupo metacíclico. □

Capítulo 7

Algunas familias de grupos metabelianos

En este capítulo presentaremos algunas familias de grupos metabelianos, junto con sus propiedades, usando todo lo visto hasta el momento.

Primero vamos a mostrar dos familias de grupos parecidas pero diferentes, no isomorfas, con las que veremos que el producto semidirecto de dos grupos abelianos no tiene por qué ser abeliano, al contrario de lo que pasa con el producto directo. Tras ello, veremos varios grupos metacíclicos con sus propiedades, y como generalizar estos grupos.

7.1. Producto semidirecto de grupos conmutativos

En esta sección veremos dos familias de grupos con las que comprobaremos que el producto semidirecto de grupos conmutativos no tiene por qué ser conmutativo.

En esta sección q denota un número entero primo. Denotamos $\mathbb{Z}_q = \mathbb{Z}/(q)$. Consideramos el grupo $\mathbb{Z}_q \times \mathbb{Z}_q$ con la suma componente a componente, es decir, $(\mathbb{Z}_q \times \mathbb{Z}_q,\ +)$; que es un grupo abeliano de orden q^2 no cíclico.

Proposición 42. *El grupo* $(\mathbb{Z}_q \times \mathbb{Z}_q,\ +)$ *de orden* q^2 *tiene un elemento de orden* 1*, y* $q^2 - 1$ *elementos de orden* q*.*

`Demostración:` Luego los elementos de este grupo tendrán orden o 1, o q o q^2. El único elemento que tiene orden 1 es el neutro $(0, 0)$, y ningún elemento tiene orden q^2 porque, en ese caso sería un grupo cíclico, lo cual es falso, por lo que los $q^2 - 1$ elementos restantes son de orden q. □

Sea p un número entero primo, menor que q, tal que p divide a $q - 1$. Sea α un elemento del grupo multiplicativo de $\mathbb{Z}_q$ de orden p, es decir, α es diferente de 1, y $\alpha^p = 1$.

Vamos a definir el siguiente grupo, como producto semidirecto de este grupo $\mathbb{Z}_q \times \mathbb{Z}_q$ y $\mathbb{Z}_p$.

Definición 30. *Sea $\alpha \in \mathbb{Z}_q^*$, con orden multiplicativo p. Definimos el grupo $(\mathbb{Z}_q \times \mathbb{Z}_q) \rtimes \mathbb{Z}_p$ como sigue:*

$$(\mathbb{Z}_q \times \mathbb{Z}_q) \rtimes \mathbb{Z}_p = \{(a, b, c) \mid a, b \in \mathbb{Z}_q,\ c \in \mathbb{Z}_p\},$$

con la operación $\oplus$ definida, para $(a, b, c), (d, e, f) \in (\mathbb{Z}_q \times \mathbb{Z}_q) \rtimes \mathbb{Z}_p$, de la siguiente forma:

$$(a, b, c) \oplus (d, e, f) = (a + \alpha^c d, b + \alpha^c e, c + f),$$

donde la primera y segunda suma son módulo q, y la tercera suma es módulo p.

Este grupo no es conmutativo y es de orden q^2p.

Proposición 43. *Los q-subgrupos de Sylow de este grupo son de orden q^2 y hay solamente 1, mientras que los p-subgrupos de Sylow tienen orden p y hay q^2.*

`Demostración:` El orden de los q-subgrupos y de los p-subgrupos de Sylow se obtienen a través de la definición de p-subgrupo de Sylow. Tenemos que el número de q-subgrupos de Sylow es congruente con 1 módulo q, y que el número de q-subgrupos de Sylow divide el cardinal del grupo, que es q^2p, luego puede haber $\{\ 1,\ p,\ q,\ q^2,\ pq\ \}$, y de estos q divide a $\{\ q,\ q^2,\ pq\ \}$, luego estos no pueden ser congruente con 1 módulo q, mientras que el número de q-subgrupos de Sylow no puede ser p, pues p no es congruente con 1 módulo q, por lo que solo hay un q-subgrupo.
Ahora bien, p divide a p y a pq, luego el número de p-subgrupos de Sylow puede ser 1, q o q^2,y como todos son congruentes con 1 módulo p el segundo teorema de Sylow no descarta ninguno. Veamos que el número de p-subgrupos de Sylow es q^2. Veamoslo primero para $p = 3$, y luego para un p cualquiera se ve de forma similar. Sea α un elemento del grupo multiplicativo de $\mathbb{Z}_q$ de orden 3, y diferente de la unidad. Entonces $\alpha^3 = 1$ es decir $\alpha^3 - 1 = 0$ que es lo mismo que:

$$(\alpha - 1)(\alpha^2 + \alpha + 1) = 0 \tag{7.1}$$

y como $\alpha \neq 1$ tenemos que $\alpha^2 + \alpha + 1 = 0$.

Por otro lado, veamos que el orden de (a, b, c) con $c \neq 0$ es 3.

$$(a, b, c) \oplus (a, b, c) = (a + \alpha^c a, b + \alpha^c b, 2c)$$

$$(a, b, c) \oplus (a, b, c) \oplus (a, b, c) = (a + \alpha^c a, b + \alpha^c b, 2c) \oplus (a, b, c) = (a + \alpha^c a + \alpha^{2c} a, b + \alpha^c b + \alpha^{2c} b, 3c)$$

siendo $c \in \mathbb{Z}_3$, $c \neq 0$ entonces $c \in \{1, 2\}$, y al ser la tercera suma módulo 3 se tiene que la tercera componente es nula, y que

$$1 + \alpha^c + \alpha^{2c} = \begin{cases} 1 + \alpha + \alpha^2, \ si \ c = 1 \\ 1 + \alpha^2 + \alpha^4, \ si \ c = 2 \end{cases}$$

y la primera expresión, cuando $c = 1$ es igual a 0, debido a lo visto inmdiatamente después de la ecuación (7.1), y en la segunda ecuación se tiene que $\alpha^4 = \alpha$, por lo que al final nos da la misma expresión que antes, que es nula, por lo que se tiene que la suma $(a, b, c) \oplus (a, b, c) \oplus (a, b, c) = (0, 0, 0)$, de lo cual concluimos que (a, b, c) es de orden 3 si $c \neq 0$.
Hay $q^2(p - 1) = q^2 2$ elementos de orden 3, y en cada subgrupo de orden 3, que es cíclico y tiene 3 elementos, uno de ellos la unidad, tiene 2 elementos de orden 3, por lo que hay $q^2 2/2 = q^2$ subgrupos de orden 3, con lo que se tiene el resultado.
Ahora, para un p cualquiera se tiene que $\alpha^p = 1$ es decir $\alpha^p - 1 = 0$, por lo que

$$(\alpha - 1)(\alpha^{p-1} + \alpha^{p-2} + ... + \alpha + 1) = 0$$

Por otro lado, el orden de (a, b, c), con $c \neq 0$, es p, lo cual se ve igual que hemos hecho antes:

$$(a, b, c) \oplus (a, b, c) = (a + \alpha^c a, b + \alpha^c b, 2c)$$

Y la suma de (a, b, c) un total de p veces es

$$(a, b, c) \oplus (a, b, c) \oplus ... \oplus (a, b, c) = (a + \alpha^c a + ... + \alpha^{(p-1)c} a, b + \alpha^c b + ... + \alpha^{(p-1)c} b, nc)$$

siendo $c \in \mathbb{Z}_q$ de orden p, $c \neq 0$ entonces $c \in \{1, 2, ..., p - 1\}$, y al ser la última suma módulo p se

tiene que la tercera componente es nula, y que

$$1+\alpha^c+...+\alpha^{(p-2)c}+\alpha^{(p-1)c}=\begin{cases}1+\alpha+...+\alpha^{(p-2)}+\alpha^{(p-1)}, & si\ c=1\\ 1+\alpha^2+...+\alpha^{2(p-2)}+\alpha^{2(p-1)}, & si\ c=2\\ ... & \\ 1+\alpha^{p-1}+...+\alpha^{(p-1)(p-2)}+\alpha^{(p-1)(p-1)}, & si\ c=p-1\end{cases}$$

y razonando de manera similar se llega a que (a,b,c) es de orden p. Y como hay $q^2(p-1)$ elementos de orden p, y dado un subgrupo de orden p este es cíclico por ser p primo, este grupo tiene p elementos, de los cuales uno es el neutro, y el resto es de orden p, luego cada subgrupo de orden p tiene $p-1$ elementos de orden p, con lo que se deduce que hay $q^2(p-1)/(p-1)=q^2$ subgrupos de orden p. Por lo tanto el número de p-subgrupos de Sylow es q^2. □

Observemos cuántos elementos hay en $(\mathbb{Z}_q\times\mathbb{Z}_q)\rtimes\mathbb{Z}_p$ de cada orden.

Proposición 44. *Este grupo tiene los siguientes elementos:*

- *Hay un elemento de orden* 1*, el neutro* $(0,0,0)$.
- *Tiene* q^2-1 *elementos de orden* q*, los cuales son de la forma* $(a,b,0)$ *con* $a,b\in\mathbb{Z}_q$*,* $(a,b)\neq(0,0)$.
- *Además hay* $q^2(p-1)$ *elementos de orden* p*, los cuales son de la forma* (a,b,c) *con* $a,b\in\mathbb{Z}_q$ *y* $c\in\mathbb{Z}_p$*,* $c\neq 0$.

Este grupo tiene varios subgrupos de orden pq, como por ejemplo el subgrupo generado por los elementos $(1,1,0)$ y $(1,1,1)$. Estos elementos son de orden q y p respectivamente y el subgrupo que generan, $\langle(1,1,0),(1,1,1)\rangle$ es de orden pq. Otro subgrupo de orden pq es el subgrupo $\langle(1,0,0),(1,1,1)\rangle$, por ejemplo.

Ejemplo 9 *Por ejemplo para* $q=5$ *y* $p=2$ *tenemos que la operación en* $(\mathbb{Z}_5\times\mathbb{Z}_5)\rtimes\mathbb{Z}_2$*, dado que* $-1=4\in\mathbb{Z}_5^*$ *es de orden multiplicativo* 2*, es la que sigue*

$$(a,b,c)\oplus(d,e,f)=(a+4^cd,b+4^ce,c+f),$$

y el subgrupo generado por $(1,1,0)$ *y* $(1,1,1)$ *es el siguiente:*

$$\langle(1,1,0),(1,1,1)\rangle = \{(0,0,0),(1,1,0),(2,2,0),(3,3,0),(4,4,0),(1,1,1),(2,2,1),(3,3,1),(4,4,1),(0,0,1)\}$$

Pues tenemos que

$$\begin{aligned}
&(1,1,0)\oplus(1,1,1) = (1+4^0 1, 1+4^0 1, 0+1) = (2,2,1),\\
&(2,2,0)\oplus(1,1,1) = (2+4^0 1, 2+4^0 1, 0+1) = (3,3,1)\\
&...\\
&(4,4,0)\oplus(1,1,1) = (4+4^0 1, 4+4^0 1, 0+1) = (5,5,1) = (0,0,1).
\end{aligned}$$

Se deja al lector comprobar que las sumas de cualesquiera dos elementos de este conjunto vuelve a ser un elemento de este conjunto. Además se tiene que el inverso de $(a,a,0)$ *es* $(b,b,0)$ *siendo* b *el inverso de* a *en* $\mathbb{Z}_5$*,* $a,b \neq 0$*, es decir* $a+b=0$*; y el inverso de* $(a,a,1)$ *es el mismo, para* $a = 0,1,...,4$*. Tenemos, por tanto, que* $\langle(1,1,0),(1,1,1)\rangle$ *es un subgrupo de orden* $pq = 2\cdot 5 = 10$ *de* $(\mathbb{Z}_5\times\mathbb{Z}_5)\rtimes\mathbb{Z}_2$*. Todos los elementos de este subgrupo son o bien de orden* 5*, y en este caso son de la forma* $(a,a,0)$ *con* $a\neq 0$*, o bien son de orden* 2 *y son de la forma* $(a,a,1)$*, y el neutro.*

Este grupo también contiene subgrupos de orden q^2, por ejemplo el generado por los elementos $(1,0,0)$ y $(0,1,0)$.

Proposición 45. *Sea* $G = (\mathbb{Z}_q\times\mathbb{Z}_q)\rtimes\mathbb{Z}_p$*. Se tiene que* $\mathbb{Z}_q\times\mathbb{Z}_q \cong \mathbb{Z}_q\times\mathbb{Z}_q\times\{0\} \triangleleft G$*, y tenemos que*

$$\frac{G}{\mathbb{Z}_q\times\mathbb{Z}_q} \cong \mathbb{Z}_p$$

que es cíclico, y por lo tanto abeliano. Se tiene entonces que G *es metabeliano, y por lo tanto es resoluble.*

De forma análoga podemos definir el grupo $(\mathbb{Z}_q\times\mathbb{Z}_q\times\mathbb{Z}_q)\rtimes\mathbb{Z}_p$, que es de orden q^3p, el cual tiene el siguiente número de elementos de cada orden:

Proposición 46. *Tenemos los siguientes elementos:*

- *Hay un elemento de orden* 1*, que es el neutro* $(0,0,0,0)$.

- *Tiene* $q^3 - 1$ *elementos de orden* q *los cuales son de la forma* $(a, b, c, 0)$*, con* $(a, b, c) \neq (0, 0, 0)$.
- *Hay* $q^3(p-1)$ *elementos de orden* p *los cuales son de la forma* (a, b, c, d)*, con* $d \neq 0$.

  Además hay un q*-subgrupo de Sylow de orden* q^3.

Y podemos definir sucesivamente de esta forma grupos de orden $q^n p$, con un elemento de orden 1, (el neutro), $q^n - 1$ elementos de orden q y $q^n(p-1)$ elementos de orden p.

La segunda familia de grupos es la siguiente.

Sean p y q números enteros primos, con $p < q$ y tales que p divide a $q - 1$. Consideramos el grupo $\mathbb{Z}_p \times \mathbb{Z}_p$ con la suma componente a componente.
Este grupo es un grupo abeliano de orden p^2 que no es cíclico. Tiene un elemento de orden 1, el neutro, y los $p^2 - 1$ elementos restantes son de orden p, pues al no ser cíclico no puede tener elementos de orden p^2.

Definición 31. *Defino el producto semidirecto de* $\mathbb{Z}_q$ *por este grupo como:*

$$\mathbb{Z}_q \rtimes (\mathbb{Z}_p \times \mathbb{Z}_p) = \{(a, b, c) \mid a \in \mathbb{Z}_q,\ b, c \in \mathbb{Z}_p\},$$

tal que dado $\alpha \in \mathbb{Z}_q^*$*, con* $\alpha \neq 1$*, y* $\alpha^p = 1$*, la operación está definida por*

$$(a, b, c) \oplus (d, e, f) = (a + \alpha^{b+c} d, b + e, c + f),$$

donde la primera suma es módulo q *y las otras dos son módulo* p.

Este grupo que acabamos de definir, $\mathbb{Z}_q \rtimes (\mathbb{Z}_p \times \mathbb{Z}_p)$, es un grupo no conmutativo de orden qp^2.

El grupo $\mathbb{Z}_q \rtimes (\mathbb{Z}_p \times \mathbb{Z}_p)$ no es isomorfo al grupo $(\mathbb{Z}_q \times \mathbb{Z}_q) \rtimes \mathbb{Z}_p$ definido al principio del capítulo.

Una razón por la que no son isomorfos es que tienen ordenes diferentes. Otra razón que se podría dar es que tienen diferente número de subgrupos de Sylow y de diferente orden, como vamos a ver en la siguiente proposición.

Proposición 47. *Los q-subgrupos de Sylow de este grupo son de orden q, y hay 1, mientras que los p-subgrupos de Sylow son de orden p^2*

Demostración: El numero de q-subgrupos de Sylow divide a qp^2, luego es un valor de $\{1,\ q,\ p,\ p^2,\ qp,\ qp^2\}$, y al ser congruente con 1 módulo q, se deduce que hay un q-subgrupo de Sylow.
Mientras que por un razonamiento similar al de la proposición 43. se llega a que el número de p-subgrupos de Sylow es q. □

Observación: En el grupo $(\mathbb{Z}_q \rtimes (\mathbb{Z}_p \times \mathbb{Z}_p), \oplus)$ hay

- Un elemento de orden 1, el elemento $(0,0,0)$.
- $q-1$ elementos de orden q, que son de la forma $(a,0,0)$ con $a \neq 0$.
- Hay $(q-1)(p-1)$ elementos de orden pq, los cuales son de la forma $(a,b,-b)$ con $a \neq 0$, $b \neq 0$.
- Hay $(qp+1)(p-1)$ elementos de orden p, que son de dos formas:
  - $(0,b,c)$, con $(b,c) \neq (0,0)$, de los que hay p^2-1.
  - hay $(q-1)p(p-1)$ elementos de orden p de la forma (a,b,c) con $a \neq 0$ y $b+c \neq 0$.

No hay elementos de orden p^2, o qp^2.

Al igual que el anterior, este subgrupo tiene varios subgrupos de orden pq, y también tiene subgrupos de orden p.

Lema 4. *Este grupo tiene $qp+1$ subgrupos de orden p.*

Demostración: Como hay $(qp+1)(p-1)$ elementos de orden p, y en cada subgrupo de orden p hay $p-1$ elementos de orden p diferentes del neutro, entonces el número de subgrupos de orden p es

$$\frac{(qp+1)(p-1)}{p-1} = qp+1.$$

□

Proposición 48. *Sea $J = \mathbb{Z}_q \rtimes (\mathbb{Z}_p \times \mathbb{Z}_p)$. Entonces J es metabeliano, y por lo tanto es resoluble.*

`Demostración:` Se tiene que $\mathbb{Z}_q \cong \mathbb{Z}_q \rtimes (\{0\} \times \{0\})$ que es normal en J, y tenemos que

$$\frac{J}{\mathbb{Z}_q} \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

que es abeliano por ser producto directo de grupos abelianos. □

De forma análoga a como hemos definido J definimos el grupo $\mathbb{Z}_q \rtimes (\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p)$, que ser de orden qp^3, el cual tiene:

- El elemento neutro $(0, 0, 0, 0)$, que es de orden 1.
- Y $q - 1$ elementos de orden q de la forma $(a, 0, 0, 0)$ donde $a \neq 0$.
- Los elementos de orden pq son de la forma (a, b, c, d), con $a \neq 0$, $(b, c, d) \neq (0, 0, 0)$ y $b + c + d = 0$.
- Los elementos de orden p de las dos formas siguientes:
  - $(0, b, c, d)$, con $(b, c, d) \neq (0, 0, 0)$
  - (a, b, c, d), con $a \neq 0$ y $b + c + d \neq 0$.

Este grupo, al igual que los anteriores, tiene varios subgrupos de orden pq, por ejemplo el subgrupo generado por los elementos $(0, 1, 1, 1)$ y $(1, 1, 1, 1)$. Tiene también subgrupos de orden p^2, o p^3. Un ejemplo de subgrupo de orden p^2 es el subgrupo $\langle (0, 1, 0, 0), (0, 0, 1, 0) \rangle$.

Podemos definir sucesivamente de esta forma grupos de orden qp^n.

Y con estos ejemplos se observa que aunque los grupos de salida son conmutativos el producto semidirecto no tiene porque serlo.
Con estas dos familias de grupos nos damos cuenta de la cantidad de grupos no conmutativos, que se pueden construir usando un sencillo producto semidirecto.

7.2. Generalización del grupo diédrico

En esta sección presentaremos una generalización del grupo diédrico.

Ya vimos que un grupo diédrico es metabeliano, y es además metacíclico, lo cual pondremos de manifiesto a continuación.

Consideramos ahora el producto semidirecto de $\mathbb{Z}_n$ y $\mathbb{Z}_2$

$$\mathbb{Z}_n \rtimes \mathbb{Z}_2 = \{(a, b) \mid a \in \mathbb{Z}_p,\ b \in \mathbb{Z}_2\}$$

con la siguiente operación

$$(a, b) \oplus (c, d) = (a + (-1)^b c, b + d)$$

Se tiene que $|\mathbb{Z}_n \rtimes \mathbb{Z}_2| = 2n$, y es un grupo no conmutativo para $n \geq 3$.
Además tiene un subgrupo cíclico de orden n, el subgrupo $\mathbb{Z}_n \rtimes \{0\} \cong \mathbb{Z}_n$, y como el cociente de $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ por este subgrupo es isomorfo a $\mathbb{Z}_2$, con lo que se tiene que $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ es metacíclico.

Proposición 49. *Hay un isomorfismo de grupos dado por:*

$$\begin{aligned} f : \mathbb{Z}_n \rtimes \mathbb{Z}_2 &\longrightarrow D(n) \\ (h, k) &\longrightarrow a^h b^k \end{aligned}$$

donde a, b son los elementos que generan el grupo diédrico $D(n)$.

Esto quiere decir que el grupo diédrico $D(n)$ es metacíclico, al igual que $\mathbb{Z}_n \rtimes \mathbb{Z}_2$.

Ahora vamos a mostrar un nuevo grupo que se obtiene de forma similar que este grupo isomorfo al grupo diédrico que hemos visto.

Definición 32. *Vamos a definir el grupo al que llamaremos generalización del grupo diédrico como el producto semidirecto de $\mathbb{Z}_n$ por $\mathbb{Z}_2 \times \mathbb{Z}_2 \times ... \times \mathbb{Z}_2$ que es el producto directo de $\mathbb{Z}_2$ un total de k veces.*

$$\mathbb{Z}_n \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2 \times ... \times \mathbb{Z}_2) = \{(a, b_1, b_2, ..., b_k) \mid a \in \mathbb{Z}_n,\ b : i \in \mathbb{Z}_2,\ i = 1, 2, ...k\ \}$$

Y este grupo tiene la siguiente operación:

$$(a, b_1, b_2, ..., b_k) \oplus (\alpha, c_1, c_2, ..., c_k) = (a + (-1)^{b_1+b_2+...+b_k}\alpha,\ b_1 + c_1, ...,\ b_k + c_k\}$$

Este grupo, $G = \mathbb{Z}_n \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2 \times ... \times \mathbb{Z}_2)$, tiene orden $2^k n$.
Además es metabeliano, pues tiene que $\mathbb{Z}_n \rtimes (\{0\} \times \{0\} \times ... \times \{0\}) \cong \mathbb{Z}_n$ es normal en G y es abeliano, y se tiene que el cociente es $\frac{G}{\mathbb{Z}_n \rtimes (\{0\}\times\{0\}\times...\times\{0\})} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times ... \times \mathbb{Z}_2$, que es abeliano por ser producto directo de grupos abelianos.

En el caso de que n sea un número primo impar el grupo G tiene $n-1$ elementos de orden n.

Veamos un ejemplo de $\mathbb{Z}_n \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ para n primo.

Ejemplo 10 *Un ejemplo curioso que generaliza al grupo diedrico, con $n = 5$, es el grupo $G = \mathbb{Z}_5 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$, un grupo de 20 elementos, que en este caso es metabeliano.*
La suma de dos elementos (a, b, c), (d, e, f) de G es

$$(a, b, c) \oplus (d, e, f) = (a + (-1)^{b+c}d, b + e, c + f).$$

El grupo G contiene los siguientes elementos:

(a). Hay un elemento de orden 1, el neutro $(0, 0, 0)$.

(b). Hay 4 elementos de orden 5 de la forma $(a, 0, 0)$ con $a \in \mathbb{Z}_5$, $a \neq 0$.

(c). Tiene 11 elementos de orden 2, los cuales son $(a, 1, 0)$, $(a, 0, 1)$ y $(0, 1, 1)$ con $a \in \mathbb{Z}_5$.

(d). Hay 4 elementos de orden 10 de la forma $(a, 1, 1)$ con $a \in \mathbb{Z}_5$, $a \neq 0$.

Veamos qué 5-subgrupos de Sylow y 2-subgrupos de Sylow tiene G.
Por el cuarto teorema de Sylow el número de 5-subgrupos de Sylow y 2-subgrupos de Sylow divide el cardinal de G, luego habrá o 1, 2, 4, 5, 10 o 20 subgrupos de cada tipo.
Por el segundo teorema de Sylow, el número de 5-subgrupos de Sylow es congruente con 1 módulo 5, por lo que solo hay un 5-subgrupos de Sylow, y este es el siguiente:

$$\{(0, 0, 0),\ (1, 0, 0),\ (2, 0, 0),\ (3, 0, 0),\ (4, 0, 0)\}.$$

Como el número de 2*-subgrupos de Sylow es congruente con* 1 *módulo* 2*, luego puede haber* 1 *o* 5*, y cada* 2*-subgrupo de Sylow tiene orden* 4*, es decir, tiene* 4 *elementos.*
Tras unos cálculos se llega a la conclusión de que el número de 2*-subgrupos de Sylow es* 5*, y estos son:*

$$\{(0,0,0),\ (0,1,0),\ (0,0,1),\ (0,1,1)\}$$
$$\{(0,0,0),\ (1,1,0),\ (1,0,1),\ (0,1,1)\}$$
$$\{(0,0,0),\ (2,1,0),\ (2,0,1),\ (0,1,1)\}$$
$$\{(0,0,0),\ (3,1,0),\ (3,0,1),\ (0,1,1)\}$$
$$\{(0,0,0),\ (4,1,0),\ (4,0,1),\ (0,1,1)\}$$

7.3. Familias de grupos metacíclicos

En esta sección mostraremos varias familias de grupos metacíclicos y alguna generalización de estas. Asimismo, estudiaremos el número de elementos de cierto orden de cada una y algunos subgrupos suyos.

En esta sección p denota un número primo impar.

Dado p denotamos el grupo cíclico $\mathbb{Z}/(p)$ por $\mathbb{Z}_p$ y $\mathbb{Z}/(4)$ por $\mathbb{Z}_4$. Sea el grupo $G = \mathbb{Z}_p \rtimes \mathbb{Z}_4$,

$$G = \{(a,b) \mid a \in \mathbb{Z}_p,\ b \in \mathbb{Z}_4\},$$

con la operación definida como sigue:

$$(a,b) \oplus (c,d) = (a + (-1)^b c, b + d),$$

donde la primera componente la suma es módulo p y en la segunda es módulo 4.

Propiedades: Esta operación tiene las siguientes propiedades:

(a). El neutro es el elemento $(0,0)$

(b). El inverso de (a,b) es $(-(-1)^b a, -b)$. Esto se comprueba fácilmente haciendo la suma.

(c). La operación es asociativa.

`Demostración:` Sean $(a,b),\ (c,d),\ (e,f) \in G$, tenemos que:

$$((a,b) \oplus (c,d)) \oplus (e,f) = (a + (-1)^b c, b + d) \oplus (e,f) = (a + (-1)^b c + (-1)^{b+d} e, b + d + f)$$

mientras que por otro lado tenemos lo siguiente:

$$(a,b) \oplus ((c,d) \oplus (e,f)) = (a,b) \oplus (c + (-1)^b e, d + f) = (a + (-1)^b (c + (-1)^b e), b + d + f) =$$
$$= (a + (-1)^b c + (-1)^b (-1)^d e, b + d + f)$$

con lo que vemos que es asociativo.

□

Se tiene que el orden del grupo G es $4p$.

Proposición 50. *El grupo G tiene un único p-subgrupo de Sylow. Este p-subgrupo de Sylow es de orden p. Además el total de 2-subgrupos de Sylow es p, y estos 2-subgrupos son de orden 4.*

El único p-subgrupo de Sylow de G es el subgrupo $\mathbb{Z}_p \rtimes \{0\}$, que es isomorfo a $\mathbb{Z}_p$, luego es cíclico. Se tiene además que el grupo cociente es $G/\mathbb{Z}_p \cong \mathbb{Z}_4$, luego es cíclico también, y por lo tanto G es metacíclico.
De hecho se llama grupo dicíclico porque es un ejemplo sencillo de grupo metacíclico.

Observemos el número de elementos de cada orden que contiene G.

Proposición 51. *El número de elementos de cada orden es el siguiente:*

(a). Hay un elemento de orden 1, el neutro $(0,0)$.

(b). Hay $p-1$ elementos de orden p de la forma $(a,0)$ con $a \in \mathbb{Z}_p$, $a \neq 0$.

(c). EL grupo G tiene $2p$ elementos de orden 4.

(d). El único elemento de orden 2 es $(0,2)$.

(e). Hay $p-1$ elementos de orden $2p$ de la forma $(a,2)$ con $a \in \mathbb{Z}_p$, $a \neq 0$.

Demostración:

(c) Se tiene que un subgrupo cíclico de orden 4 tiene dos elementos de orden 4, y en este caso se cumple que todos los subgrupos de orden 4 son cíclicos. Como el número de 2-subgrupos de Sylow es p entonces hay $2p$ elementos de orden 4, y estos son de la forma $(a,1)$ y $(a,3)$, con $a \in \mathbb{Z}_p$, $a \neq 0$.
(d) Veamos que el elemento $(0,2)$ es de orden 2. Tenemos que $(0,2) \oplus (0,2) = (0+(-1)^2 0, 2+2) = (0,4) = (0,0)$. Además es el único elemento de orden 2, pues para $(a,b) \in G$, $(a,b) \neq (0,2)$, se tiene que su suma es $(a,b) \oplus (a,b) = (a+(-1)^b a, b+b)$, donde la segunda componente es nula si y solo si $b = 2$, y en este caso la primera componente resulta ser $2a$, el cual es diferente de 0 para todo $a \in \mathbb{Z}_p$, $a \neq 0$.
(e) Veamos que $(a,2)$ tiene orden p. Tenemos que:

$$(a,2) \oplus (a,2) = (a+(-1)^2 a, 2+2) = (2a,0)$$
$$(a,2) \oplus (a,2) \oplus (a,2) = (2a,0) \oplus (a,2) = (3a,2)$$

y la suma k veces de $(a,2)$ es

$$(a,2) \oplus (a,2) \oplus ... \oplus (a,2) = \begin{cases} (ka,2), \text{ si } k \text{ es impar} \\ (ka,0), \text{ si } k \text{ es par} \end{cases}$$

y $ka = 0$ solo si k es múltiplo de p. Por ser p impar, el primer k tal que $ka = 0$ es $k = 2p$, luego este es su orden. □

Los 2-subgrupos de Sylow de G son $\langle (a,1) \rangle = \langle (a,3) \rangle = \{(0,0),(a,1),(0,2),(a,3)\}$. Como $(0,2)$ es el único elemento de orden 2 entonces debe estar en cada subgrupo de orden 4.

El siguiente resultado lo hemos comentado anteriormente.

Proposición 52. *G es metacíclico.*

Además del ejemplo que hemos puesto antes, otro subgrupo cíclico tal que el cociente de G por él es cíclico también es el siguiente grupo:

$$J = \langle (1,2) \rangle = \mathbb{Z}_p \times \{0,2\} \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}.$$

Como es un subgrupo de índice 2 es un subgrupo normal en G, y se tiene que $G/J \cong C_2$, el grupo

cíclico de orden 2.

7.3.1. Generalización: grupo dicíclico

Vamos a definir primero el grupo dicíclio.

Definición 33. *Definimos el grupo dicíclico como sigue*

$$Dic(n) = \{a, b \mid \ a^{2n} = 1, \ \ a^n = b^2, \ \ b^{-1}ab = a^{-1}\}$$

Nótese que el orden del grupo dicíclico es $4n$, es decir, $|Dic(n)| = 4n$.

El grupo G, definido anteriormente, pero con $n \in \mathbb{N}$, en vez de $n = p$ primo, es lo que hemos llamado grupo dicíclico, es decir, $Dic(n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_4$, donde

$$\mathbb{Z}_n \rtimes \mathbb{Z}_4 = \{(a, b) \mid a \in \mathbb{Z}_n, \ b \in \mathbb{Z}_4\},$$

y se tiene la misma operación que antes

$$(a, b) \oplus (c, d) = (a + (-1)^b c, b + d).$$

7.3.2. Generalizaciones del grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_4$

Tenemos la siguiente generalización del grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_4$.
Para p primo impar consideramos el grupo $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_4$ con la operación

$$(a, b, c) \oplus (d, e, f) = (a + (-1)^c d, b + (-1)^c e, c + f),$$

y así sucesivamente.

Proposición 53. *Si $p \geq 5$ primo el grupo $X = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_4$ tiene un único p-subgrupo de Sylow, el cual es de orden p^2.*

`Demostración:` Como el número de p-subgrupos de Sylow divide a $p^2 2^2$, luego el número de p-subgrupos de Sylow es o 1, 2, 4, p, $2p$, $4p$, p^2 o $2p^2$, pero como este número tiene que ser

congruente módulo 1 con p solo puede haber 1, 2 o 4; si $p > 5$ entonces solo hay un único p-subgrupo de Sylow. □

Conociendo los subgrupos es fácil deducir los órdenes de los elementos.

El grupo X contiene:

- Un elemento de orden 1, el neutro $(0, 0, 0)$.
- Tiene $p^2 - 1$ elementos de orden p y son de la forma $(a, b, 0)$ con $a, b \in \mathbb{Z}_p$, $(a, b) \neq (0, 0)$.
- Tiene $2p^2$ elementos de orden 4, los cuales son de la forma $(a, b, 1)$ y $(a, b, 3)$ con $a, b \in \mathbb{Z}_p$.
- Contiene $p^2 - 1$ elementos de orden $2p$ de la forma $(a, b, 2)$ con $a, b \in \mathbb{Z}_p$, $(a, b) \neq (0, 0)$.
- Y contiene al elemento $(0, 0, 2)$, que es el único de orden 2.

Proposición 54. *El grupo X es metabeliano.*

`Demostración:` X tiene un p-subgrupo de Sylow de orden p^2. Sea H este p-subgrupo, $H = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \{0\} \cong (\mathbb{Z}_p \times \mathbb{Z}_p)$, por lo que H es abeliano, y se tiene además que el grupo cociente G/H es abeliano, pues $G/H \cong \mathbb{Z}_4$. □

Se puede definir de esta forma un grupo $(\mathbb{Z}_p \times \mathbb{Z}_p \times ... \times \mathbb{Z}_p) \rtimes \mathbb{Z}_4$ de orden $4p^t$, siendo este grupo el resultado del producto semidirecto de el grupo producto de $\mathbb{Z}_p$ un total de t veces y $\mathbb{Z}_4$. Este grupo también es metabeliano.

Sea p primo impar. Otra generalización del grupo $\mathbb{Z}_p \rtimes \mathbb{Z}_4$ es el siguiente grupo

$$K = \mathbb{Z}_p \rtimes \mathbb{Z}_{2^n},$$

para $n \geq 1$, con la operación

$$(a, b) \oplus (c, d) = (a + (-1)^b c, b + d).$$

para $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_{2^n}$.

Proposición 55. *El grupo K tiene orden $2^n p$ y es no conmutativo.*

Proposición 56. *El grupo K tiene un único p-subgrupo de Sylow, de orden p. El número de 2-subgrupos de Sylow es p. Cada uno de estos 2-subgrupo de Sylow tiene orden 2^n y es cíclico.*

El p-subgrupo de Sylow es $H = \langle(a, 0)\rangle$ con $a \in \mathbb{Z}_p$, $a \neq 0$, y los 2-subgrupos son $H_0 = \langle(0, 1)\rangle$, $H_1 = \langle(1, 1)\rangle$, $H_2 = \langle(2, 1)\rangle$,...,$H_{p-1} = \langle(p - 1, 1)\rangle$.

Proposición 57. *El grupo K es metacíclico.*

`Demostración:` El p-subgrupo de Sylow H es normal en K , y es cíclico por ser de orden p, pues $H \cong \mathbb{Z}_p$, y se tiene que $K/H \cong \mathbb{Z}_{2^n}$, que es cíclico, y por lo tanto K es metacíclico.
Veamos que H es normal. Sea $(a, b) \in K$, y sea $(h, 0) \in H$, entonces, siendo $(-(-1)^b a, -b)$ el inverso de (a, b) tenemos que

$$\begin{aligned}(-(-1)^b a, -b) \oplus (h, 0) \oplus (a, b) = (-(-1)^b a + (-1)^{-b} h, -b) \oplus (a, b) = \\ = (-(-1)^b a + (-1)^{-b} h + (-1)^{-b} a, -b + b)\end{aligned}$$

y esto es un elemento de la forma $(c, -b + b) = (c, 0)$, con $c = -(-1)^b a + (-1)^{-b} h + (-1)^{-b} a$, es decir, $c \in \mathbb{Z}_p$, y por lo tanto es un elemento de H, con lo que H es normal. □

Esta generalización se puede hacer también para un $p \in \mathbb{N}$, p no necesariamente primo.

Tras ver las familias de grupos no conmutativos aquí expuestas, queda de manifiesto las múltiples posibilidades en esta materia.

Bibliografía

[Adem] A. Adem, R. J. Milgram, Cohomology of Groups, 2004 Springer-Verlag, Berlin.

[Axler] S. Axler, F.W. Gehring, y K.A. Ribet, The theory of finite group, 2004 Springer-Verlag New York, Inc.

[Baum] B. Baumslag, B. Chandler, Schaum's outline of theory and problems of group theory, 1968 McGraw-Hill, Inc.

[Coxeter] H.S.M Coxeter, W.O.J Moser, Generators and relations for discrete groups, 1972 Springer-Verlag Berlin Heidelberg New York.

[Feit] W. Feit, J. G. Thompson, Solvability of groups of odd order, 1963 Pacific J. Math. 13, páginas 775−1029.

[Gardi] Cyril F. Gardiner, A first course in group theory, 1980 Springer-Verlag, New York.

[Hump] J.F.Humphreys, A course in group theory, 1996 Oxford University Press Inc.

[Hungerford] T.W. Hungerford, Algebra, 1974 Springer-Verlag New York, Inc

[Machí] Antonio Machí, Groups an introduction to ideas and methods of the theory of groups, 2012 Springer-Verlag Italia.

[Milne] J.S. Milne, Group theory, 2009 https://www.jmilne.org/math/CourseNotes/gt.html.

[Robin] D.J.S. Robinson, A course in the theory of groups', 1993 Springer-Verlag New York, Inc.

[Roman] Steven Roman, Fundamentals of group theory, 2012 Springer Science+Business Media, Birkhuser Boston.

[Rotman] Joseph J. Rotman, An introduction to the theory of groups, 1995 Springer-Verlag New York Inc.

[Serre] J.P. Serre, Linear representations of finite groups, 1977 Springer-Verlag, New York Inc.

[Smith] Geoff Smith, Olga Tabachnikova, Topics in group theory, 2000 Springer -Verlag London.

[Wallace] D.A.R. Wallace, Groups, 1974 Allen and Unwin.