Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

P-GRUPOS FINITOS

Autora: Henar Martín Martín
Tutor: José Enrique Marcos Naveira
2025

Resumen:

En esta memoria se aborda el estudio de los p-grupos finitos. Se comienza con la clasificación completa del caso abeliano. A continuación, se aportan dos maneras diferentes para construir p-grupos no conmutativos: el uso del producto semidirecto y las construcciones matriciales, brindando en ambos casos gran cantidad de ejemplos. Posteriormente, se incluye un capítulo a nivel informativo de los últimos avances en el campo. Finalmente, se cierra el trabajo tratando los grupos extraespeciales.

Palabras clave: p-grupos, producto semidirecto, grupos extraespeciales.

Abstract:

The study of finite p-groups is addressed on this paper. It starts with the complete classification of the abelian case. It then presents two distinct methods for constructing non-commutative p-groups: semidirect product and matrix constructions, with numerous examples provided for each approach. Subsequently, an informative chapter outlines the latest developments in the field. The work concludes with a discussion of extraspecial groups.

Keywords: p-groups, semidirect product, extraspecial groups.

Índice general

1. Introducción **3**

2. Prelimiares de p-grupos **5**

3. Grupos abelianos de orden p^n **11**
3.1. Particiones 16

4. Producto semidirecto para la construcción de p-grupos no abelianos **19**
4.1. Un ejemplo de construcción de 2-grupos no abelianos 20
4.2. El p-grupo no abeliano $\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p)}$ 22
4.3. El p-grupo no abeliano $\left(\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)}\right) \rtimes \frac{\mathbb{Z}}{(p)}$ 24
4.4. El p-grupo no abeliano $\frac{\mathbb{Z}}{(p^2)} \rtimes \left(\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \cdots \times \frac{\mathbb{Z}}{(p)}\right)$ 25
4.5. Otros productos semidirectos 26

5. p-grupos de matrices **29**
5.1. El grupo lineal general y grupo lineal especial 29
5.2. $UT(n,p)$, un p-grupo de matrices triangulares dentro de $SL(n,p)$ 31
5.3. Exponente en $UT(n,p)$ 31
5.4. Subgrupos de $UT(n,p)$ 33
5.5. El grupo de Heisenberg 35
5.6. Otro ejemplo de producto semidirecto 36
5.7. p-grupos de matrices sobre $\frac{\mathbb{Z}}{(p^n)}$ 37

6. Sobre la clasificación de p-grupos finitos **39**
6.1. Grupos de orden 2^n 40
6.2. Grupos de orden 3^n 41
6.3. Grupos de orden p^3 con $p \geq 3$ 41
6.4. Grupos de orden 8 42

7. Grupos extraespeciales **43**
7.1. Producto central 44

Bibliografía **47**

Capítulo 1

Introducción

> Necesitamos unas supermatemáticas en las que las operaciones sean tan desconocidas como las cantidades sobre las que operan, y un supermatemático que no sepa qué está haciendo cuando realiza esas operaciones.
> Esas supermatemáticas son la teoría de grupos.
>
> *Sir Arthur Stanley Eddington*

Siempre me han llamado la atención los escritos que empiezan con alguna cita relacionada con el tema a tratar, y desde que leí esta del astrofísico y filósofo Sir Arthur Stanley Eddington supe que la necesitaba para introducir el trabajo. El motivo es que, precisamente, logra describir de una manera muy amena lo que significa estudiar teoría de grupos para mí.

Sería presuntuoso por mi parte dejar al lector la libertad de pensar que con ello me creo una supermatemática. No, estoy lejos de ser Lagrange, Cayley o cualquier matemático que sentó las bases de este campo. Reconozco mis limitaciones. Pero, en el segundo curso de la universidad, gracias a Estructuras Algebraicas (y también a Topología), comprendí la belleza de la abstracción matemática. Recuerdo bien la sensación de satisfacción al completar y comprender un trabajo de ampliación del temario que introducía a los p-grupos. De modo que la propuesta de acabar el grado profundizando en tal tema me resultó atractiva.

La pretensión de obtener clasificaciones es una ambición muy matemática. En este texto, sin embargo, no se pretende dar una clasificación cerrada de los p-grupos finitos, pues supera con creces mis posibilidades. De hecho, en el sexto capítulo se confirma que es, de manera general, un objetivo poco realista.

Uno de los resultados mencionados más llamativos está precisamente en el informativo capítulo 6 sobre la clasificación de los p-grupos finitos, que pone de manifiesto el superexponencial crecimiento del número de grupos con p^n elementos, que es de orden

$$p^{\left(\frac{2}{27}n^3+O\left(n^{\left(\frac{8}{3}\right)}\right)\right)}.$$

A lo largo de todo el trabajo se aportan numerosos ejemplos para la construcción de p-grupos que respaldan un orden tan sumamente alto como el mostrado previamente.

Resulta grato comprobar que a pesar de la saturación de p-grupos que existen, tan inmensa como para ser incapaces de abarcarlos actualmente, cuando se exigen ciertas propiedades el estudio se simplifica. El capítulo 3 es una buena muestra de ello, ya que en él se detallan todos los grupos abelianos que hay de orden p^n salvo isomorfismo.

La parte más compleja llega a la hora de abordar la construcción de p-grupos no abelianos. En este trabajo se muestran dos herramientas distintas en los capítulos 4 y 5. Cada una de ellas es enriquecedora por su cuenta, y también es interesante ver cómo se complementan la una a la otra. Además, al mismo tiempo, se muestra como ambos caminos, en ocasiones, pueden guiarnos al mismo lugar.

Concretamente, por un lado, el capítulo 4 nos introduce una nueva construcción que permite generalizar el producto de grupos con el que se trabaja en el grado: el producto semidirecto, dando un paso más en la abstracción.

Por otro lado, dedicando el capítulo 5 a los p-grupos de matrices enfatizamos el interés que tienen en las matemáticas estos elementos que nos resultan tan habituales desde el comienzo de la carrera. Un reconocimiento al hecho de que cada concepto aprendido desde los inicios es valioso.

Para acabar, en cambio, escogimos los grupos extraespeciales: un tema bastante específico dentro de la teoría de grupos. Es un contenido apropiado para remarcar que la materia aportada a lo largo de la memoria prepara de una manera muy gradual el camino para perimitirnos abordar algo tan particular.

Capítulo 2

Prelimiares de p-grupos

En esta sección se revisarán algunos conceptos de estructuras algebraicas. Se dan por conocidas definiciones fundamentales como la de grupo, de clases laterales o subgrupos normales, así como sus propiedades y resultados derivados elementales, como el Teorema de Lagrange. Algunos de los resultados que sí revisaremos no se demostraran, pues suelen ser materia vista en el grado.

Lo primero será definir nuestro objeto principal de estudio.

Definición 1. Sea p un primo. Un **p-grupo finito** es un grupo de orden p^n con $n \geq 1$.

En este texto nos centramos en el caso finito, pero la definición general de p-grupo merece igualmente una mención.

Definición 2. Sea p un primo. Un **p-grupo** es un grupo en el que cada elemento tiene como orden una potencia de p.

Observación. A lo largo de todo el texto la letra p queda reservada para los números primos.

Ahora damos paso a los conceptos de centro y centralizador por su peso en los primeros resultados que conseguiremos sobre p-grupos.

Definición 3. Dado un grupo G se define el **centro** del grupo como el conjunto

$$Z(G) = \{x \in G : xg = gx \text{ para todo } g \in G\}.$$

Esto es, el conjunto de los elementos de G que conmuntan con todos los elementos de G.

Definición 4. Sea $x \in G$. El **centralizador** de x en G es el conjunto

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

Esto es, los elementos de G que conmutan con x.

Notemos que el concepto de centralizador está estrechamente relacionado con el de centro. Además, ambos nacen de la misma idea que surge con la relación de conjugación y ligan con los subgrupos normales.

Fijamos que las **clases** de un elemento $x \in G$ por la relación de conjugación se escriben como $Cl(x)$, y recordamos que son precisamente

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

Repasamos algunos resultados importantes respecto a estos conceptos, comenzando por las propiedades del centro.

Lema 5. El centro $Z(G)$ es un subgrupo abeliano y normal de G.

Tal y como anticipamos, el centro está ligado a las clases de conjugación y los subgrupos normales. Veamos algunos resultados al respecto:

Lema 6. Un elemento x pertenece al centro si y solo si $Cl(x) = \{x\}$.
En particular, el elemento neutro e de G cumple $Cl(e) = \{e\}$.

Lema 7. Sea G un grupo y H un subgrupo suyo. Entonces H es normal en G si y solo si H es unión de clases de conjugación de G.

Demostración. Probaremos cada una de las implicaciones:
$\boxed{\Longrightarrow}$ Veremos que, de hecho,

$$H = \bigcup_{h \in H} Cl(h).$$

Obviamente $H \subset \cup_{h \in H} Cl(h)$. Aseguremos que la contención contraria también se da.
Resulta que, al asumir que H es normal, tenemos que $gHg^{-1} \subset H$. Y por tanto, para cada $h \in H$ se verifica que

$$Cl(h) = \{ghg^{-1} : g \in G\} \subset gHg^{-1} \subset H.$$

Entonces $Cl(h) \subset H$ para todo $h \in H$ y así $\bigcup_{h \in H} Cl(h) \subset H$. Al darse las dos contenciones se da la igualdad.
$\boxed{\Longleftarrow}$ Necesitamos ver que dado $g \in G$, $gHg^{-1} \subset H$.
Si H es unión de clases de conjugación, en particular

$$H = \bigcup_{h \in H} Cl(h).$$

Pero como las clases de conjugación son precisamente $Cl(h) = \{xhx^{-1} : x \in G\}$, se concluye que

$$H = \bigcup_{h \in H} Cl(h) = \bigcup_{h \in H} \{xhx^{-1} : x \in G\} \supset gHg^{-1}.$$

■

Respecto al centralizador, comenzamos por su propiedad más elemental.

Lema 8. Sea G un grupo y $g \in G$. El centralizador $C_G(g)$ es un subgrupo de G.

Ahora podemos continuar relacionando el centro y las clases de conjugación con el centralizador.

Lema 9. Sea G un grupo y $x \in G$. Las siguientes condiciones son equivalentes:

- $C_G(x) = G$.
- $x \in Z(G)$.

De hecho, entre el centro y las clases de conjugación, en cuestión de cardinalidad tenemos el siguiente resultado:

Lema 10. Sea G un grupo y $x \in G$. El cardinal de la clase de conjugación $Cl(x)$ es el índice del subgrupo centralizador. Es decir,

$$|Cl(x)| = [G : C_G(x)].$$

En particular, si G es finito, el cardinal de $Cl(x)$ divide al orden del grupo. Concretamente,

$$|Cl(x)| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

Demostración. Como el índice $[G : C_G(x)]$ es el cardinal del conjunto de clases por la izquierda respecto a $C_G(x)$ denotaremos por comodidad

$$A = \{\text{Clases por la izquierda respecto a } C_G(x)\}.$$

Si probamos que existe una biyección entre $Cl(x)$ y A habremos terminado. Definimos entonces

$$\begin{array}{rcl} \alpha : Cl(x) & \longrightarrow & A \\ gxg^{-1} & \longrightarrow & gC_G(x) \end{array}$$

Lo primero es asegurarnos de que esta aplicación está bien definida. Si suponemos que $g, h \in G$ verifican $gxg^{-1} = hxh^{-1}$, necesitamos probar que $\alpha(gxg^{-1}) = \alpha(hxh^{-1})$, vaya, que $gC_G(x) = hC_G(x)$. Pero notemos que multiplicando a $gxg^{-1} = hxh^{-1}$ por la izquierda por h^{-1} y por la derecha por g, se sigue que $h^{-1}gx = xh^{-1}g$. Y esto justamente quiere decir que $h^{-1}g \in C_G(x)$ y por tanto h y g están relacionados y su clase es la misma.

Para ver la sobreyectividad basta notar que un elemento de A es de la forma $gC_G(x)$ para algún $g \in G$. Así, tomando tal elemento g y eligiendo en $Cl(x)$ a gxg^{-1}, podemos concluir que $\alpha(gxg^{-1}) = gC_G(x)$.

Para ver la inyectividad, probemos que si $\alpha(gxg^{-1}) = \alpha(hxh^{-1})$, entonces $gxg^{-1} = hxh^{-1}$. Que $\alpha(gxg^{-1}) = \alpha(hxh^{-1})$ es exactamente lo mismo que decir que $gC_G(x) = hC_G(x)$. Por tanto $h^{-1}g \in C_G(x)$, es decir $(h^{-1}g)x = x(h^{-1}g)$. Entonces si multiplicamos tal igualdad por la izquierda por h y por la derecha por g^{-1}, se sigue que $gxg^{-1} = hxh^{-1}$.

Justo lo que necesitábamos ver.

Por último, las igualdades finales del enunciado son ciertas si G es finito a consecuencia del Teorema de Lagrange.

■

A consecuencia de que las clases de conjugación son una partición, del lema previo y del lema 6, tenemos que para un grupo finito G con $r = m+n$ clases de conjugación, siendo x_i un representante de cada clase para cada $i = 1, 2, \ldots, r$, y considerando además n como el número de clases unipuntuales y m aquellas con más de un elemento, se tiene la **ecuación de las clases de conjugación**:

$$|G| = \sum_{i=1}^{r} |Cl(x_i)| = |Z(G)| + \sum_{i=1}^{m} |Cl(x_i)| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)].$$

Con esta primera base, ya podemos dar unos primeros resultados interesantes sobre p-grupos:

Proposición 11. Sea G un p-grupo finito de p^n elementos. Entonces $Z(G)$ tiene más de un elemento.

Demostración. Sea r el número de clases de conjugación de G. Consideremos para cada $i \in \{1, 2, \ldots, r\}$ un elemento x_i representante de cada clase.

Por la ecuación de las clases de conjugación, tenemos que

$$|G| = |Cl(x_1)| + |Cl(x_2)| + \cdots + |Cl(x_r)|. \tag{2.1}$$

Notemos que la clase de conjugación del elemento neutro es unipuntual, es decir, $Cl(1) = \{1\}$.

Sin pérdida de generalidad podemos numerar las clases de manera que $x_1 = 1$, con lo que $|Cl(x_1)| = |Cl(1)| = |\{1\}| = 1$.

Por el lema 10, para todo $i \in \{1, 2, \ldots, r\}$ tenemos que

$$|G| = |Cl(x_i)||C_G(x_i)|. \tag{2.2}$$

Entonces para todo $i \in \{1, 2, \ldots, r\}$ tenemos que $|Cl(x_i)|$ divide a $|G|$, o dicho de otra manera y teniendo en cuenta que $|G| = p^n$, lo que deducimos es que $|Cl(x_i)|$ es potencia de p.

Como el centro es un subgrupo, $1 \in Z(G)$.

De modo que para probar que $Z(G)$ tiene más de un elemento, solo tenemos que justificar que existe algún elemento distinto de 1 que está en $Z(G)$. Para ello aprovecharemos de nuevo el lema 9. Razonaremos por reducción al absurdo suponiendo que 1 es el único elemento de $Z(G)$. Por el lema 9, esto se traduce en que $C_G(x_i) \neq G$ para todo $i \in \{2, 3, \ldots, r\}$, y por tanto $|Cl(x_i)| = p^{k_i}$ con k_i natural distinto de cero para todo $i \in \{2, 3, \ldots, r\}$, o lo que es lo mismo, p divide a cada $|Cl(x_i)|$ con $i \in \{2, 3, \ldots, r\}$. Pero bajo estas consideraciones volviendo a la igualdad (2.1) llegamos a dos conclusiones contradictorias:

- Por un lado, como $|Cl(x_1)| = 1$ y p divide a cada $|Cl(x_i)|$ con $i \in \{2, 3, \ldots, r\}$, tenemos que $|Cl(x_1)| + |Cl(x_2)| + \cdots + |Cl(x_r)| \equiv 1 \mod p$.
- Por otro lado de $|G| = p^n$ se deduce $|G| \equiv 0 \mod p$.

Llegamos al absurdo, y por tanto la hipótesis de que 1 es el único elemento de $Z(G)$ es falsa y ha de existir otro i distinto de 1 para el cual $C_G(x_i) = G$ y que por tanto x_i pertenezca a $Z(G)$.

■

Proposición 12. Sea G un grupo tal que $G/Z(G)$ es cíclico. Entonces G es abeliano, y por tanto $G = Z(G)$.

Demostración. Sea $G/Z(G)$ cíclico generado por $xZ(G)$. Por tanto para todo $g \in G$ se tiene que g está en una de las clases laterales de $Z(G), xZ(G), x^2Z(G), \ldots$ ya que las clases laterales forman una partición de G. Así pues, dados $g_1, g_2 \in G$ arbitrarios, se pueden escribir de la forma $g_1 = x^i z_1$, $g_2 = x^j z_2$ para ciertos exponentes i, j y algún $z_1, z_2 \in Z(G)$.

Como el objetivo es probar que G es abeliano, veamos que $g_1 g_2 = g_2 g_1$. Para ello solo hay que aprovechar adecuadamente la forma de escribir g_1 y g_2 y sus propiedades como potencias, la asociatividad y las propiedades del centro:

$$\begin{aligned} g_1 g_2 = (x^i z_1)(x^j z_2) = x^i (z_1 x^j) z_2 = x^i (x^j z_1) z_2 = (x^i x^j)(z_1 z_2) = (x^i x^j)(z_2 z_1) = (x^{i+j})(z_2 z_1) = \\ = (x^{j+i})(z_2 z_1) = (x^j x^i)(z_2 z_1) = x^j (x^i z_2) z_1 = x^j (z_2 x^i) z_1 = (x^j z_2)(x^i z_1) = g_2 g_1 \end{aligned}$$

■

Proposición 13. Cualquier grupo con p^2 elementos es abeliano.

Demostración. Sea G un grupo de cardinal $|G| = p^2$. Al ser por hipótesis G finito y ser conocido que $Z(G)$ es un subgrupo de G, el teorema de Lagrange nos dice que $Z(G)$ solo puede tener 1, p o p^2 elementos. Estudiemos entonces cada caso:

- Caso 1. Supongamos que $|Z(G)| = 1$.
  Es un caso que no puede darse por la proposición 11.
- Caso 2. Supongamos que $|Z(G)| = p$.
  Si $|Z(G)| = p$, del teorema de Lagrange se deduce que $|G| = p^2 = p \cdot |G/Z(G)| = |Z(G)| \cdot |G/Z(G)|$, y por tanto $|G/Z(G)| = p$, y al ser p primo tendríamos que $G/Z(G)$ es cíclico. Pero por la proposición 12 al ser $G/Z(G)$ cíclico obtendríamos que $G = Z(G)$ y en consecuencia $|Z(G)| = p^2$, lo cual es contrario a la hipóteis del caso. Por tanto no se puede dar que $|Z(G)| = p$.
- Caso 3. Supongamos que $|Z(G)| = p^2$.
  Si $|Z(G)| = p^2$ como $Z(G)$ está contenido en G, al tener los mismos elementos se deduce que $Z(G) = G$, y como el centro es abeliano, el grupo G lo será también.

Por tanto la única posibilidad viable es la del caso 3, ante la cual hemos probado que G es abeliano, y por tanto queda demostrada la proposición.

■

Una consecuencia inmediata del Teorema de Cauchy, el cual se puede consultar en *A course on Finite Groups* de Harvey E. Rose [12], es el siguiente resultado:

Corolario 14. Sea G un p-grupo abeliano finito de orden p^n. Entonces existe algún $b \in G$ tal que $orden(b) = p$.

Teorema 15. Sea G un p-grupo de orden p^n. Entonces el grupo G tiene algún subgrupo de orden p^s para cada $1 \leq s \leq n$.

Demostración. Lo demostraremos por inducción sobre n.

- Si $n = 1$ es obvio por el corolario anterior.
- Si se verifica para $1, 2, \ldots n-1$, veamos que es cierto para n.
  Por la ecuación de las clases de conjugación

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)],$$

siendo m el número de clases con más de un elemento y x_i un generador de cada una para cada $i \in \{1, 2, \ldots, m\}$.
Como p divide a G y a $[G : C_G(x_i)]$ para todo $i \in \{1, 2, \ldots, m\}$, se tiene que p divide a $|Z(G)|$. Entonces, por el Teorema de Cauchy, $Z(G)$ tiene algún subgrupo A con $|A| = p$, y además es cíclico por ser p primo. Como el centro es abeliano, el subgrupo A es normal.
Consideremos el cociente G/A, cuyo orden es p^{n-1}. Podemos aplicar la hipótesis de inducción a G/A y entonces tenemos que G/A tiene subgrupos de orden p^m para cada $1 \leq m \leq n-1$. Por la biyección existente entre los subgrupos de G/A y los subgrupos de G que contienen a A se sigue que G tiene subgrupos de orden p^m para $1 \leq m \leq n-1$. Como para n es evidentemente cierto porque el propio G lo verifica, hemos terminado.

■

Nota. El resultado previo es un caso particular del primer teorema de Sylow.

Cerramos la sección con la definición del exponente de un grupo.

Definición 16. Sea G un grupo. En caso de existir, el menor número natural r tal que $g^r = e$ para todo $g \in G$ se denomina **exponente** o **periodo** del grupo G.

Además de ser útil para algunas de las demostraciones de este texto, tiene interés en sí misma porque conocer el exponente de un grupo nos da información sobre su estructura interna.

Nota. Si un grupo es finito de orden n, obviamente el periodo divide a n.

Nota. En un p-grupo finito G de orden p^n, el exponente o periodo es un divisor de p^n.

Capítulo 3

Grupos abelianos de orden p^n

Una estrategia muy común en matemáticas es comenzar estudiando casos con propiedades más amables, para luego poco a poco ir extendiendo el estudio a situaciones más genéricas. Esa será nuestra manera de proceder, de modo que comenzaremos exigiendo a los grupos ser abelianos.

Definición 17. Sea $(G,+)$ un grupo conmutativo. Sean $H_1, H_2, \ldots, H_m$ subgrupos de G. Se define el **grupo suma** de $H_1, H_2, \ldots, H_m$ a

$$H_1 + H_2 + \cdots + H_m = \{a_1 + a_2 + \cdots + a_m \in G : a_1 \in H_1, a_2 \in H_2, \ldots, a_m \in H_m\}.$$

Definición 18. Sea $(G,+)$ un grupo conmutativo. Sean $H_1, H_2, \ldots, H_m$ subgrupos de G. Se dice que G es **suma directa** de $H_1, H_2, \ldots, H_m$, y se denota

$$H_1 \oplus H_2 \oplus \cdots \oplus H_m$$

si se cumplen las dos condiciones siguientes:

- $G = H_1 + H_2 + \cdots + H_m$.
- Para todo $b \in G$ existen $a_1 \in H_1, a_2 \in H_2, \ldots, a_m \in H_m$ únicos tales que $b = a_1 + a_2 + \cdots + a_m$.

Exponemos condiciones equivalentes para la suma directa en el siguiente resultado:

Lema 19. Sea G un grupo y sean $H_1, H_2, \ldots, H_m$ subgrupos de G tales que $G = H_1 + H_2 + \cdots + H_m$. Las cuatro condiciones siguientes son equivalentes:

1. G es suma directa de $H_1, H_2, \ldots, H_m$.
2. Si $0 = a_1 + a_2 + \cdots + a_m$ con $a_1 \in H_1, a_2 \in H_2, \ldots, a_m \in H_m$, entonces $a_1 = a_2 = \cdots = a_m = 0$.
3. El homomorfismo de grupos

$$\begin{aligned} \alpha : H_1 \times H_2 \times \cdots \times H_m &\longrightarrow H_1 + H_2 + \cdots + H_m \\ (a_1, a_2, \ldots, a_m) &\longrightarrow a_1 + a_2 + \cdots + a_m \end{aligned}$$

   es un isomorfismo.

4. Para cada $i = 1, 2, \ldots, m$ se cumple que

$$H_i \cap \sum_{j \neq i} H_j = \{0\}.$$

Demostración. Probaremos la cadena de implicaciones:

$\boxed{(1) \Longrightarrow (2)}$

Razonaremos por reducción al absurdo. Supongamos que se tiene que $0 = a_1 + a_2 + \cdots + a_m$ con cierto $j \in \{1, 2, \dots m\}$ tal que $a_j \neq 0$. Pero sabemos que también $0 = 0 + 0 + \cdots + 0$, por tanto se rompe la unicidad para la expresión de 0 y llegamos al absurdo.

$\boxed{(2) \Longrightarrow (3)}$

Para ver que es isomorfismo nos falta asegurar la biyectividad. Por tanto tenemos que ver que es sobreyectiva e inyectiva.

La sobreyectividad es sencilla, puesto que dado un elemento $g \in G = H_1 + H_2 + \cdots + H_m$ se puede escribir como $g = a_1 + a_2 + \cdots + a_m$ con $a_1 \in H_1, a_2 \in H_2, \dots, a_m \in H_m$, de modo que considerando $(a_1, a_2, \dots, a_m) \in H_1 \times H_2 \times \cdots \times H_m$, su imagen por el homomorfismo α es la deseada.

La inyectividad tampoco requiere un gran esfuerzo. Notemos que si $\alpha(a_1, a_2, \dots, a_m) = \alpha(b_1, b_2, \dots, b_m)$ tenemos que $\alpha(a_1, a_2, \dots, a_m) - \alpha(b_1, b_2, \dots, b_m) = 0$. Y al ser α homomorfismo se sigue que $\alpha(a_1 - b_1, a_2 - b_2, \dots, a_m - b_m) = 0$. Ahora bien, por como está definida α, esto es $(a_1 - b_1) + (a_2 - b_2) + \cdots + (a_m - b_m) = 0$, y la hipótesis (2) nos garantiza que esto solo sucede si $a_1 - b_1 = 0, a_2 - b_2 = 0, \dots, a_m - b_m = 0$. Vaya, si $a_1 = b_1, a_2 = b_2, \dots, a_m = b_m$, lo cual implica que $(a_1, a_2, \dots, a_m) = (b_1, b_2, \dots, b_m)$. Justo lo que nos aporta que es inyectiva.

$\boxed{(3) \Longrightarrow (4)}$

Recordemos que por ser $H_1, H_2, \dots, H_m$ subgrupos el elemento neutro 0 está en todos ellos. Ahora, para probar la implicación razonaremos por reducción al absurdo y suponemos que existe $i \in \{1, 2, \dots, m\}$ tal que

$$H_i \cap \sum_{j \neq i} H_j \neq \{0\}.$$

Sin pérdida de generalidad podemos asumir que $i = 1$. Tenemos que entonces existen $a \in H_1$, $b_j \in H_j$ para $j = 2, 3, \dots, m$ verificando $a = b_2 + b_3 + \cdots + b_m$.
Por tanto $\alpha(a, 0, \dots, 0) = \alpha(0, b_2, \dots, b_m)$, lo que está en contra de la inyectividad.

$\boxed{(4) \Longrightarrow (1)}$

Notemos que por hipótesis general, se asume que $G = H_1 + H_2 + \cdots + H_m$. Así, lo que tenemos que garantizar es que dado $b \in G$ existen $a_1 \in H_1, a_2 \in H_2, \dots, a_m \in H_m$ únicos tales que $b = a_1 + a_2 + \cdots + a_m$.

Si razonamos para ver el contrarecíproco y suponemos que existe $i \in \{1, 2, \dots, m\}$ tal que

$$H_i \cap \sum_{j \neq i} H_j \neq \{0\},$$

donde sin pérdida de generalidad podemos asumir que $i = 1$, tenemos que entonces existen $a \in H_1$, $b_j \in H_j$ para $j = 2, 3, \dots, m$ verificando $a = b_2 + b_3 + \cdots + b_m$.
Pero entonces tenemos al menos dos maneras distintas de expresar a, lo que implica que G no es suma directa de $H_1, H_2, \dots, H_m$.

■

Y pasamos ahora a introducir un nuevo término y algunos resultados al respecto que nos empiezan a acercar a la clasificación de los p-grupos abelianos finitos.

Definición 20. Sea $(G, +)$ un grupo abeliano no nulo. Decimos que G es **indescomponible** si, puesto como suma directa de dos subgrupos, entonces uno de los dos subgrupos es trivial.

Proporcionamos más información sobre los grupos indescomponibles, puesto que entenderlos nos permitirá comprender casos más complejos. El siguiente lema nos justifica precisamente en qué sentido nos ayudará a estudiar casos más complicados.

Lema 21. Todo grupo G abeliano finito no nulo se puede expresar como suma directa de subgrupos indescomponibles, admitiedo el caso de que el propio grupo de partida sea indescomponible.

Demostración. Se demuestra por inducción sobre $|G|$.

Si $|G| = 2$ es trivial.

Supongamos que es cierto para $|G| = 1, 2, \ldots, n-1$ y probémoslo para n. Tenemos dos posibilidades:

- Si G es indescomponible, es trivial.
- Si G no es indescomponible entonces existen subgrupos no triviales A y B tales que $G = A \oplus B$. Notemos que los cardinales de A y B son menores que el de G. Podemos entonces aplicar la hipótesis de inducción de modo que A y B son suma directa de indescomponibles. Así pues usamos esas dos descomposiciones para construir la de G y hemos terminado.

■

Lema 22. Sea G un p-grupo abeliano finito de orden p^n. Si p^m es el periodo de G, entonces existe $a \in G$ tal que $orden(a) = periodo(G)$.

Demostración. Como $|G| = p^n$ y el orden de un elemento de g debe dividir al orden del grupo, los órdenes de los elementos solo pueden ser potencias de p. Por tanto el periodo coincide con el orden del elemento b con mayor orden. Así, tenemos lo que deseábamos, $orden(a) = periodo(G) = p^m$, porque si no existiera un b con tales características el periodo sería menor.

■

Lema 23. Sea G un p-grupo abeliano de orden p^n. Sea $a \in G$ tal que $orden(a) = periodo(G) = p^m$. Consideramos el grupo cociente $G/\langle a \rangle$. Entonces para todo elemento $b \in G/\langle a \rangle$ existe $x \in G$ tal que $b = x + \langle a \rangle$ y $orden(b) = orden(x)$.

Demostración. Tomemos un representante de b: sea $y \in G$ tal que $b = y + \langle a \rangle$. Sean $orden(b) = p^k$ y $orden(y) = p^s$. Se tiene que $p^k \leq p^s \leq p^m$, lo que equivale a que $k \leq s \leq m$.

Si $k = s$, entonces ya hemos conseguido lo pedido.

Si $k < s$ hay que trabajar un poco más. Como el orden de b es p^k, tenemos que $p^k(y+\langle a \rangle) = p^k b = 0$ y vemos que $p^k y \in \langle a \rangle$. Es decir, $p^k y = qa$ para cierto $q \in \mathbb{Z}$. Podemos expresar q como el producto $q = rp^t$, donde p no divide a r.

Entonces,

$$p^{m+k-t}y = p^{m-t}p^k y = p^{m-t}qa = p^{m-t}rp^t a = rp^m a = 0 = p^s y,$$

y se deduce que $m + k - t \geq s$.

Pero por otro lado

$$p^{m+k-t-1}y = p^{m-t-1}p^k y = p^{m-t-1}qa = p^{m-t-1}rp^t a = rp^{m-1}a \neq 0,$$

y junto con lo anterior se concluye que $m + k - t = s$.

Consideremos el elemento $x = y - rp^{m-s}a$ de G y veamos que cumple lo las dos condiciones que necesitamos. Es obvio que $x + \langle a \rangle = y + \langle a \rangle = b$. Luego $orden(b) = p^k$ divide a $orden(x)$. Y como además $p^k x = p^k y - rp^{k+m-s}a = p^k y - rp^t a = p^k y - qa = p^k y - p^k y = 0$ concluimos que $orden(x) = p^k = orden(b)$.

■

Lema 24. Sea G un p-grupo abeliano de orden p^n. Son equivalentes los siguientes tres asertos:

1. G es indescomponible.
2. G es cíclico.
3. G es isomorfo a $\mathbb{Z}/(p^n)$.

Demostración. La equivalencia entre (2) y (3) es conocida, así que nos centramos en probar la equivalencia entre (1) y (2).

$\boxed{(1) \Longrightarrow (2)}$

Sea G indescomponible. Probaremos por inducción sobre n que entonces es cíclico.

- Si $n = 1$ entonces $|G| = p$ y es conocido que todo grupo de orden primo es cíclico.
- Supongamos que para $1, 2, \ldots, n-1$ es cierto y probemos que entonces también es cierto para n, cuando $|G| = p^n$.
  Por el lema 22 existe $a \in G$ tal que el orden de a es igual al periodo del grupo. Tenemos dos casos:
  - Si $orden(a) = p^n$ hemos terminado.
  - Si $orden(a) \neq p^n$ entonces considero el cociente $G/\langle a \rangle$.
    Por el lema 21 lo puedo expresar como suma directa de subgrupos indescomponibles:

$$G/\langle a \rangle = C_1 \oplus C_2 \oplus \cdots \oplus C_k \tag{3.1}$$

    Por hipótesis de inducción, cada C_i con $1 \leq i \leq k$ es cíclico, de modo que existen x_i tales que $C_i = \langle x_i + \langle a \rangle \rangle$ para cada $1 \leq i \leq k$. Además, por el lema 23 podemos suponer que $orden(x_i + \langle a \rangle) = orden(x_i)$ para cada $1 \leq i \leq k$.
    Vamos a comprobar que

$$G = \langle a \rangle \oplus \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \cdots \oplus \langle x_k \rangle,$$

    lo que contradice la hipótesis de ser indescomponible. Necesitamos asegurar que la suma es directa y para ello veremos una de las condiciones equivalentes vistas en el lema 19: si $b, m_1, m_2, \ldots, m_k \in \mathbb{Z}$ con $ba + m_1x_1 + m_2x_2 + \cdots + m_kx_k = 0$ entonces $ba = m_1x_1 = m_2x_2 = \cdots = m_kx_k = 0$.
    Notemos que $ba + m_1x_1 + m_2x_2 + \cdots + m_kx_k = 0$ implica que $0 = m_1(x_1 + \langle a \rangle) + m_2(x_2 + \langle a \rangle) + \cdots + m_k(x_k + \langle a \rangle)$. Por tanto, de la ecuación (3.1) seguimos que $m_i(x_i + \langle a \rangle) = 0$ para cada $1 \leq i \leq k$. Entonces m_i es múltipo de $orden(x_i)$ para cada $1 \leq i \leq k$. En consecuencia $m_ix_i = 0$ para todo $1 \leq i \leq k$ y también $ba = 0$.

$\boxed{(2) \Longrightarrow (1)}$

Razonaremos por reducción al absurdo. Supongamos que G es descomponible con $G = A \oplus B$. Entonces tenemos $|A| = p^s$ y $|B| = p^t$ de forma que $1 < p^s < p^n$ y $1 < p^t < p^n$. En esta situación, el exponente o periodo de G será

$$exp(G) = m.c.m(p^s, p^t) = \text{máx}\{p^s, p^t\} < p^n,$$

lo que contradice el hecho de que G es cíclico.

■

El siguiente resultado es clave, porque nos da una manera de describir cualquier p-grupo abeliano afirmando la invariancia respecto a los exponentes en el orden de los subgrupos implicados en la descomposición.

Teorema 25. Sea G un p-grupo abeliano de orden p^n. Entonces G es suma directa de subgrupos cíclicos de órdenes $p^{e_1}, p^{e_2}, \ldots, p^{e_r}$ donde los números $e_1 \geq e_2 \geq \cdots \geq e_r$ son únicos y cumplen $e_1 + e_2 + \cdots + e_r = n$.

Demostración. Se demuestra por inducción sobre n.

- Si $n = 1$ es obvio porque G es cíclico en sí mismo.

- Supongamos que es cierto para $1, 2, \ldots, n-1$ y veamos que es cierto para n.

  Consideremos un elemento $x \in G$ de máximo orden posible y sea $A = \langle x \rangle$. Lo que probaremos será que $G = A \times B$ para algún subgrupo B, porque aplicando a B la hipótesis de inducción tendríamos la descomposición deseada.

  La existencia de tal subgrupo B la probaremos precisamente construyéndolo.
  Consideremos el espacio cociente G/A. Por la hipótesis de inducción este espacio es producto interno de grupos cíclicos generados por las clases $\langle y_1A\rangle, \langle y_2A\rangle, \ldots, \langle y_sA\rangle$, siendo sus órdenes $p^{m_1}, p^{m_2}, \ldots, p^{m_s}$. Entonces tenemos que $(y_i)^{p^{m_i}} = x^{t_i}$ para algún t_i para cada $1 \leq i \leq s$.
  Para cada $1 \leq i \leq s$, podemos suponer además que p^{m_i} divide a t_i, obteniendo de ello que $(y_i)^{p^{m_i}} = (x_i)^{p^{m_i}}$ para algún $x_i = x^{t_i/p^{m_i}} \in A$.
  Notemos que tal suposición es lícita ya que en caso de que para algún valor de i se tuviera que p^{m_i} no divide a t_i se tendría que $t_i = k_i p^{r_i}$, donde p no divide a k_i y $r_i < m_i$. Lo que permitiría concluir que x^{k_i} genera A y que el orden de x^{t_i} es p^{m-r_i} siendo p^m el orden de x. Lo que implicaría que el orden de y_i es mayor que el orden de x, en contra de como habíamos tomado x.

  Escribimos ahora $z_i = y_i x_i^{-1}$ para cada $1 \leq i \leq s$ y consideremos el grupo B generado por $z_1, z_2, \ldots, z_s$.

  Notemos que como $z_i^{p^{m_i}} = 1$, el orden de cada z_i divide a p^{m_i} para cada $1 \leq i \leq s$. Además, $z_iA = y_iA$ siendo $ord(y_iA) = p^{m_i}$ para cada $1 \leq i \leq s$, así que el orden de z_i no puede ser menor que p^{m_i}. Por tanto el orden de z_i es concretamente p^{m_i}.

  Si vemos que finalmente G es producto interno de A y B habremos terminado. Para ello necesitamos probar dos propiedades:

  - Cada elemento de G se puede escribir como ab siendo $a \in A$ y $b \in b$.
    Como $z_iA = y_iA$ para $1 \leq i \leq s$, la clase puede escribirse como producto de potencias de $z_1A, z_2A, \ldots, z_sA$. Entonces g es producto de un elemento de A y otro de B.
  - $A \cap B = \{1\}$.
    Si $a \in A \cap B$, entonces por estar en B es de la forma $a = z_1^{k_1} z_2^{k_2} \ldots z_s^{k_s} = y_1^{k_1} y_2^{k_2} \ldots y_s^{k_s}$, y por tanto $aA = z_1^{k_1} A z_2^{k_2} A \ldots z_s^{k_s} A = y_1^{k_1} A y_2^{k_2} A \ldots y_s^{k_s} A$. Pero por estar a en A, esta clase es A.
    Al generar $y_1A, y_2A, \ldots, y_sA$ el cociente G/A tenemos que es isomorfo a $C_{p^{m_1}}, C_{p^{m_2}}, \ldots, C_{p^{m_r}}$ y concluimos que p^{m_i} divide a k_i para $1 \leq i \leq s$, de modo que $a = 1$.

  Con ello terminamos la prueba.

■

En esta situación, los números $p^{e_1}, p^{e_2}, , \ldots, p^{e_r}$ se denominan **factores invariantes** y también **divisores elementales**.

Gracias al teorema previo, podemos dar un ejemplo de todos los grupos abelianos de orden p^5 que existen, salvo isomorfismo:

$$\frac{\mathbb{Z}}{(p^5)}, \qquad \frac{\mathbb{Z}}{(p^4)} \times \frac{\mathbb{Z}}{(p)}, \qquad \frac{\mathbb{Z}}{(p^3)} \times \frac{\mathbb{Z}}{(p^2)}, \qquad \frac{\mathbb{Z}}{(p^3)} \times \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)}$$

$$\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p)}, \qquad \frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)}, \qquad \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)}.$$

Dentro de esta lista, sabemos que la primera posibilidad dada es un grupo cíclico. La última también tiene su terminología concreta, que es la siguiente:

Definición 26. Un ***p*-grupo elemental** es un p-grupo conmutativo finito de exponente o periodo exactamente p, en el que todo elemento distinto del neutro es de orden p.

Cada p-grupo elemental de orden p^n es isomorfo al grupo

$$\overbrace{\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \cdots \times \frac{\mathbb{Z}}{(p)}}^{n \text{ veces}} \qquad \text{dotado de la operación suma.}$$

3.1. Particiones

Para cerrar el capítulo, en esta sección vamos a demostrar cuántos p-grupos abelianos no isomorfos existen. Para ello, la unicidad de los factores invariantes es clave, al igual que recordar la función partición.

Definición 27. La **función partición** P asocia a cada entero no negativo n el número de posibles particiones de sí mismo, esto es, la cantidad de formas en las que n puede ser expresado como la suma de números enteros positivos sin importar el orden.

Por ejemplo, $P(5) = 7$ porque el número 5 tiene 7 particiones: 5, $4+1$, $3+2$, $3+1+1$, $2+2+1$, $2+1+1+1$ y $1+1+1+1+1$.

Nótese que tales particiones se corresponden con los grupos abelianos de orden p^5 indicados previamente.

Se incluyen a continuación también los datos de las primeras cuarenta evaluaciones de la función partición.

n	$P(n)$	n	$P(n)$	n	$P(n)$	n	$P(n)$
1	1	11	56	21	792	31	6842
2	2	12	77	22	1002	32	8349
3	3	13	101	23	1255	33	10143
4	5	14	135	24	1575	34	12310
5	7	15	176	25	1958	35	14883
6	11	16	231	26	2436	36	17977
7	15	17	297	27	3010	37	21637
8	22	18	385	28	3718	38	26015
9	30	19	490	29	4565	39	31185
10	42	20	627	30	5604	40	37338

Tabla 3.1: Número de particiones $P(n)$ para $n = 1$ a 40

Se puede dar mucha información interesante sobre la función partición, y hay teoría bastante complicada al respecto. Aunque en la página de OEIS (referencia [OEIS]) se puede encontrar mucho más contenido, no vamos a profundizar en ello. Lo que en nuestro contexto sí es relevante, es incluir la siguiente fórmula obtenida por los matemáticos G. H. Hardy y Ramanujan:

$$P(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right) \quad \text{cuando } n \to \infty. \tag{3.2}$$

Su demostración se sale de los objetivos del texto, pero es importante porque permite un cálculo aproximado mucho más rápido que las fórmulas exactas y aporta información valiosa sobre su crecimiento: es más veloz que cualquier función polinómica en n pero no tanto como la exponencial pura.

Con el teorema siguiente justificamos el interés de este trabajo por la función partición.

Teorema 28. Sea n un natural. Entonces hay exactamente $P(n)$ grupos abelianos no isomorfos de orden p^n.

Demostración. Por el teorema 25 sabemos que un p-grupo abeliano de orden p^n puede ser expresado como suma directa de subgrupos cíclicos cuyos órdenes son los factores invariantes.

La unicidad de los factores invariantes nos garantiza que, si al hacer tal descomposición dos grupos los tienen iguales, entonces son isomorfos.

Por tanto, como cada partición de n nos da unos factores invariantes distintos, se tiene que cada partición de n define una estructura única de un grupo abeliano.

■

Así pues, acudiendo a la tabla (3.1) podemos asegurar que, por ejemplo, tenemos 5604 grupos abelianos de orden p^{30}; y por la fórmula de Hardy y Ramanujan de la ecuación (3.2) conocemos el crecimiento asintótico del número de p-grupos abelianos no isomorfos.

Capítulo 4

Producto semidirecto para la construcción de p-grupos no abelianos

En este capítulo dejamos de exigir la conmutatividad y pasamos a los grupos no abelianos. Para ello nos enfocaremos en una manera de construir nuevos grupos basándonos en el producto semidirecto externo.

Antes, recordamos que dado un grupo $(G, *)$, el conjunto de sus automorfismos dotado de la operación "composición de automorfismos" tiene estructura de grupo . Lo denotamos $(Aut(G), \circ)$.

Definición 29. Sean dos grupos N y H, y sea ϕ un homomorfismo de grupos $\phi : H \longrightarrow Aut(N)$ para el que denotamos $\phi(h) := \phi_h$. El **producto semidirecto externo** de N y H, denotado por $N \rtimes_\phi H$, es la pareja constituida por $(N \times H, \bullet)$, donde $N \times H$ el conjunto dado por el producto cartesiano y $\bullet$ la operación dependiente de ϕ definida como sigue:

$$\begin{array}{rcl} \bullet : (N \times H) \times (N \times H) & \longrightarrow & N \times H \\ ((n_1, h_1), (n_2, h_2)) & \longrightarrow & (n_1, h_1) \bullet (n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2) \end{array}$$

Proposición 30. El producto semidirecto externo es un grupo.

Demostración. Sean H, N y ϕ como en la definición previa. Probemos que $N \rtimes_\phi H$ es un grupo, para lo que necesitamos asegurar las tres condiciones siguientes:

- Asociatividad.
  Dados $(n_j, h_j) \in N \times H$ para $j = 1, 2, 3$, veamos que $((n_1, h_1) \bullet (n_2, h_2)) \bullet (n_3, h_3) = (n_1, h_1) \bullet ((n_2, h_2) \bullet (n_3, h_3))$.

  Por un lado tenemos que
  $((n_1, h_1) \bullet (n_2, h_2)) \bullet (n_3, h_3) = (n_1 \phi_{h_1}(n_2), h_1 h_2) \bullet (n_3, h_3) = (n_1 \phi_{h_1}(n_2) \phi_{h_1 h_2}(n_3), (h_1 h_2) h_3)$.

  Por otro lado tenemos que
  $(n_1, h_1) \bullet ((n_2, h_2) \bullet (n_3, h_3)) = (n_1, h_1) \bullet (n_2 \phi_{h_2}(n_3), h_2 h_3) = (n_1 \phi_{h_1}(n_2 \phi_{h_2}(n_3)), h_1(h_2 h_3)) = (n_1 \phi_{h_1}(n_2) \phi_{h_1 h_2}(n_3), (h_1 h_2) h_3)$. Como de ambas formas obtenemos lo mismo, la asociatividad queda probada.

- Existe elemento neutro.
  Veamos que dado $(n, h) \in N \times H$ se verifica que $(1, 1) \bullet (n, h) = (n, h) = (n, h) \bullet (1, 1)$.
  Tenemos que $(1, 1) \bullet (n, h) = (1\phi_1(n), 1h) = (n, h)$.
  Y de igual modo tenemos que $(n, h) \bullet (1, 1) = (n\phi_h(1), h) = (n, h)$.

- Cada elemento tiene su inverso.
  Veamos que dado $(n, h) \in N \times H$ el elemento $(\phi_h^{-1}(n^{-1}), h^{-1})$ cumple la condición de ser su

inverso. Nótese que $(\phi_h)^{-1} = \phi_{h^{-1}}$, pues ϕ es homomorfismo de grupos. Teniéndolo en cuenta, se comprueba directamente operando:

$$(n,h) \bullet (\phi_h^{-1}(n^{-1}), h^{-1}) = (n\phi_h(\phi_h^{-1}(n^{-1})), hh^{-1}) = (1,1)$$

$$(\phi_h^{-1}(n^{-1}), h^{-1}) \bullet (n,h) = (\phi_h^{-1}(n^{-1})\phi_{h^{-1}}(n), h^{-1}h) = (1,1)$$

■

Nota. Al asegurar que el producto semidirecto externo, el par $(N \times H, \bullet) =: N \rtimes_\phi H$, es de hecho un grupo, notemos que podemos tomar la licencia habitual de escribir el conjunto subyacente con la misma notación que el propio grupo $N \rtimes_\phi H = (N \rtimes_\phi H, \bullet)$ sin perder de vista en qué contexto está cada uno.

Proposición 31. Dado un grupo $N \rtimes_\phi H$, producto semidirecto como el anterior, se cumple que $N \times \{1\}$ es un subgrupo normal suyo.

Cabe destacar que el producto semidirecto externo que hemos presentado no deja de ser una generalización del producto directo, ya que si el homomorfismo ϕ de la definición 29 es la aplicación constantemente igual a la identidad de $Aut(G)$, la operación $\bullet$ es exactamente el producto usual.

4.1. Un ejemplo de construcción de 2-grupos no abelianos

En esta sección vamos a introducir un primer ejemplo que nos permitirá obtener de un 2-grupo conmutativo no elemental, otro 2-grupo no conmutativo. Además, estableceremos la relación que tiene este procedimiento con los grupos diédricos.

La obtención del nuevo 2-grupo no conmutativo se buscará con la construcción de un producto semidirecto. Para ello necesitamos recordar algunos resultados que nos asegurarán la correción al definir el homomorfismo del que dependerá la operación. Los resultados no se demostrarán porque son sencillos y no aportan contenido de interés al texto.

Lema 32. Sea $(G,+)$ un grupo conmutativo. La aplicación

$$\begin{array}{rccc} \phi_{-1} : G & \longrightarrow & G \\ a & \longmapsto & -a \end{array}$$

es un automorfismo del grupo.

Observación. En esta sección consideraremos $C_2 = \{+1, -1\}$ el grupo cíclico de dos elementos con notación multiplicativa.

Observación. El grupo C_2 considerado previamente es isomorfo a $\left(\frac{\mathbb{Z}}{(2)}, +\right)$.

Lema 33. Sea $(G,+)$ un grupo conmutativo con algún elemento de orden mayor o igual que 3. Consideremos ϕ_1 la aplicación identidad y el automorfismo ϕ_{-1} del lema previo. La aplicación

$$\begin{array}{rccc} \phi : C_2 & \longrightarrow & Aut(G) \\ 1 & \longmapsto & \phi_1 \\ -1 & \longmapsto & \phi_{-1} \end{array}$$

es un homomorfismo de grupos inyectivo.

Observación. Nótese que la condición sobre el orden de G, que tenga al menos tres elementos, es necesaria para que en $Aut(G)$ haya algún homomorfismo distinto de la identidad. Si no lo hay, el producto semidirecto que podemos definir es, como dijimos, justamente el producto directo. Entonces, al estar construido a partir de dos grupos conmutativos, conseguiríamos otro grupo conmutativo, y ese no es el objetivo.

Una vez definido el homomorfismo ϕ, es inmediato el asegurar la posibilidad de la construcción de un producto semidirecto.

Lema 34. Sea $(G,+)$ un grupo conmutativo con algún elemento de orden mayor o igual que 3. Entonces tenemos definido un grupo producto semidirecto

$$G \rtimes_\phi C_2$$

con la operación de grupo dada por

$$(g,a) \bullet (h,b) = (g + \phi_a(h), a \cdot b).$$

Observación. Con una notación más compacta la operación se puede escribir como

$$(g,a) \bullet (h,b) = (g + a \cdot h, a \cdot b).$$

Proposición 35. Si $(G,+)$ es un 2-grupo conmutativo de orden 2^n con algún elemento de orden mayor o igual que 4, entonces el producto semidirecto definido en el lema previo,

$$G \rtimes_\phi C_2,$$

es un 2-grupo de orden 2^{n+1} y no conmutativo.

En esta situación,

$$G \cong G \times \{1\}$$

es un subgrupo normal de $G \rtimes_\phi C_2$.

Ya hemos detallado una manera de construir para cada 2-grupo conmutativo no elemental, otro 2-grupo no conmutativo. Así pues, finalizamos la sección detallando como se relaciona este caso con el grupo diédrico. Recordemos primero su definición:

Definición 36. El **grupo diédrico**, denotado por D_n es el grupo de simetrías de un polígono regular de n lados, incluyendo rotaciones y reflexiones.

Recordemos también que el grupo diédrico D_n tiene orden $|D_n| = 2n$, y que además se escribe usualmente como

$$D_n = \langle a, b | a^n = b^2 = e, bab = a^{n-1} \rangle,$$

siguiendo la representación con generadores y relaciones.

Ahora, nuestra construcción de 2-grupos no abelianos liga con el grupo diédrico porque

$$D_{2^n} \cong \frac{\mathbb{Z}}{(2^n)} \rtimes_\phi C_2.$$

De entrada podemos observar que $\frac{\mathbb{Z}}{(2^n)}$ cumple evidentemente las condiciones requeridas para ser el grupo G de la proposición 35, de modo que se sigue que

$$|D_{2^n}| = 2^{n+1} = \left| \frac{\mathbb{Z}}{(2^n)} \rtimes_\phi C_2 \right|.$$

Además, es sencillo encontrar en este producto semidirecto dos elementos que verifiquen las relaciones de a y b. Concretamente los elementos $(1,1)$ y $(0,-1)$, asignando respectivamente los roles de a y b, funcionan como indican .

4.2. El p-grupo no abeliano $\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p)}$

En esta sección vamos a introducir un ejemplo algo más elaborado que nos permitirá obtener a partir de $\frac{\mathbb{Z}}{(p^2)}$ y $\frac{\mathbb{Z}}{(p)}$, un p-grupo de orden p^3 no conmutativo.

La manera de proceder será análoga a la sección previa: se buscará su obtención con la construcción del producto semidirecto

$$\left(\frac{\mathbb{Z}}{(p^2)} \rtimes_\phi \frac{\mathbb{Z}}{(p)}, \oplus\right).$$

La clave vuelve a ser definir el homomorfismo ϕ adecuado del que dependerá la operación $\oplus$ del producto semidirecto, y se requerirán también algunos lemas auxiliares para garantizar su correcta definición. Los resultados tampoco se demostrarán porque son sencillos y no aportan contenido de interés al texto.

Lema 37. Sea $j \in \{0, 1, 2, \ldots, p-2, p-1\}$. La aplicación

$$\begin{array}{rccc} \phi_j : \dfrac{\mathbb{Z}}{(p^2)} & \longrightarrow & \dfrac{\mathbb{Z}}{(p^2)} \\ a & \longmapsto & (1+jp)a \end{array}$$

es un automorfismo del grupo $\left(\frac{\mathbb{Z}}{(p^2)}, +\right)$.

Observación. Nótese que con el producto $(1+jp)a$ escrito en la definición de la aplicación anterior, no nos referimos a otro que al producto usual del anillo $\left(\frac{\mathbb{Z}}{(p^2)}, +, \cdot\right)$.

A continuación detallamos algunas propiedades que verifican estos automorfismos:

- ϕ_0 es el automorfismo identidad.
- Dados ϕ_j y ϕ_k con $j \in \{0, 1, 2, \ldots, p-2, p-1\}$, la composición de ambos reulta ser $\phi_j \circ \phi_k = \phi_{j+k}$ donde $j+k$ se toma como su residuo módulo p, ya que $(1+jp)(1+kp) = 1 + (j+k)p + jkp^2 \equiv 1 + (j+k)p \mod (p^2)$.
- El punto previo nos asegura que el inverso de ϕ_j es ϕ_{p-j}.

Podemos poner un caso sencillo de como funcionan los inversos de este tipo de automorfismos, por ejemplo cuando $p = 5$. Si consideramos $\phi_2, \phi_3 : \frac{\mathbb{Z}}{(25)} \longrightarrow \frac{\mathbb{Z}}{(25)}$, notemos que $2+3 = 5$ y $(1+2\cdot5)(1+3\cdot5) = 1 + (2+3)\cdot 5 + 2\cdot 3 \cdot 5^2 \equiv 1 + 5^2 \equiv 1 \mod (5^2)$.

Lema 38. Consideremos ϕ_j para $j \in \{0, 1, 2, \ldots, p-2, p-1\}$ del lema previo.
La aplicación

$$\begin{array}{rccc} \phi : \left(\dfrac{\mathbb{Z}}{(p)}, +\right) & \longrightarrow & Aut\left(\left(\dfrac{\mathbb{Z}}{(p^2)}, +\right)\right) \\ j & \longmapsto & \phi_j \end{array}$$

es un homomorfismo de grupos inyectivo.

Nótese también que el homomorfismo ϕ previamente definido no es una biyección, puesto que hay otros automorfismos distintos de nuestros ϕ_j en $Aut((\frac{\mathbb{Z}}{(p^2)}, +))$.

Lema 39. Tenemos definido un grupo producto semidirecto

$$\frac{\mathbb{Z}}{(p^2)} \rtimes_\phi \frac{\mathbb{Z}}{(p)}$$

de los grupos

$$\left(\frac{\mathbb{Z}}{(p^2)},+\right) \quad \text{y} \quad \left(\frac{\mathbb{Z}}{(p)},+\right)$$

con la operación de grupo dada por

$$(g,a)\oplus(h,b)=(g+\phi_a(h),a+b).$$

Observación. Con una notación más compacta la operación se puede escribir como

$$(g,a)\oplus(h,b)=(g+(1+ap)h,a+b).$$

Proposición 40. El producto semidirecto definido en el lema previo,

$$\frac{\mathbb{Z}}{(p^2)}\rtimes_\phi \frac{\mathbb{Z}}{(p)},$$

es un p-grupo de orden p^3 y no conmutativo.

Para cerrar esta sección vamos a enunciar un par de propiedades de la construcción realizada:

1. Por un lado, notemos que podemos contabilizar cuantos elementos hay de cada orden posible. Para ello, recordemos que en $\left(\frac{\mathbb{Z}}{(p^2)},+\right)$ hay:

   - Un elemento de orden 1. Es el neutro, $\bar{0}$.
   - $p-1$ elementos de orden p. Son los elementos de la forma $j\bar{p}$ con $j\in\{1,2,\dots,p-1\}$.
   - p^2-p elementos de orden p^2. Son los elementos de la forma $\bar{h}$ con $mcd(h,p)=1$.

   Entonces con un simple razonamiento de combinatoria, volviendo a nuestro producto semidirecto $\frac{\mathbb{Z}}{(p^2)}\rtimes_\phi \frac{\mathbb{Z}}{(p)}$, podemos concluir que hay:

   - Un elemento de orden 1. Es el neutro, $(0,0)$.
   - $p(p-1)=p^2-p$ elementos de orden p^2. Son los elementos de la forma $(h,0)$ con $mcd(h,p)=1$.
   - $p^3-(p^2-p+1)=p^3-p^2+p-1$ elementos de orden p. Son los elementos de la forma:

   $$\begin{cases}(h,0) \text{ con } mcd(h,p)=p \text{ y } h\neq 0\\ (h,a) \text{ con } a\neq 0\end{cases}$$

2. Por otro lado, notemos que el centro de $\frac{\mathbb{Z}}{(p^2)}\rtimes_\phi \frac{\mathbb{Z}}{(p)}$ tiene necesariamente orden p. Esto se debe a que, de hecho, el centro de cualquier grupo no conmutativo de orden p^3 tiene necesariamente orden p. Tal afirmación es consecuencia de las proposiciones 11 y 12. Detallémoslo:

   Proposición 41. El centro de cualquier grupo G no conmutativo de orden p^3 tiene orden p.

   Demostración. Por la proposición 11 al ser $|G|=p^3$, el centro $Z(G)$ tiene más de un elemento.

   Como el centro es un subgrupo, y el orden de los subgrupos debe dividir al orden del grupo, solo puede ser que $|Z(G)|$ sea o p o p^2.

   Vamos a descartar la posibilidad de que sea p^2. Si $|Z(G)|=p^2$, entonces el cociente $G/Z(G)$ tendría orden

   $$|G/Z(G)|=\frac{|G|}{|Z(G)|}=\frac{p^3}{p^2}=p.$$

   Pero esto implicaría que $G/Z(G)$ fuera cíclico y abeliano, y entonces de la proposición 12 se deduciría que G es abeliano, algo que va en contra de nuestra hipótesis de que G era no abeliano.

   ■

En este caso, de hecho, el centro de $\frac{\mathbb{Z}}{(p^2)} \rtimes_\phi \frac{\mathbb{Z}}{(p)}$ es

$$Z\left(\frac{\mathbb{Z}}{(p^2)} \rtimes_\phi \frac{\mathbb{Z}}{(p)}\right) = \{(jp, 0) : j \in \{0, 1, \dots, p-1\}\} = \langle (p, 0) \rangle.$$

4.3. El p-grupo no abeliano $\left(\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)}\right) \rtimes \frac{\mathbb{Z}}{(p)}$

En esta sección nos vamos a centrar en una forma de generalizar la construcción de la anterior. Considerarmos, en lugar de $\frac{\mathbb{Z}}{(p^2)}$, su producto n veces, $\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)}$.

Los pasos que daremos serán los mismos, y las demostraciones no las detallaremos porque tampoco aportan contenido de interés. Primero, como hicimos con el lema 37, aseguraremos que las aplicaciones que nos interesan son automorfismos:

Lema 42. Sea $j \in \{0, 1, 2, \dots, p-2, p-1\}$. La aplicación

$$\begin{array}{rccc} \phi_j : \frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)} & \longrightarrow & \frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)} \\ (a_1, a_2, \dots, a_n) & \longmapsto & ((1+jp)a_1, (1+jp)a_2, \dots, (1+jp)a_n) \end{array}$$

es un automorfismo del grupo $\left(\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)}, +\right)$.

El segundo paso es garantizar la correcta definición del homomorfismo ϕ, como en el lema 38:

Lema 43. Consideremos ϕ_j para $j \in \{0, 1, 2, \dots, p-2, p-1\}$ del lema previo.
La aplicación

$$\begin{array}{rccc} \phi : \left(\frac{\mathbb{Z}}{(p)}, +\right) & \longrightarrow & Aut\left(\left(\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)}, +\right)\right) \\ j & \longmapsto & \phi_j \end{array}$$

es un homomorfismo de grupos inyectivo.

El tercer paso, análogamente al lema 39, se centra en construir el producto semidirecto:

Lema 44. Tenemos definido un grupo producto semidirecto

$$\left(\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)}\right) \rtimes_\phi \frac{\mathbb{Z}}{(p)}$$

de los grupos

$$\left(\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)}, +\right) \quad \text{y} \quad \left(\frac{\mathbb{Z}}{(p)}, +\right)$$

con la operación de grupo dada por

$$((g_1, g_2, \cdots, g_n), a) \oplus ((h_1, h_2, \cdots, h_n), b) = ((g_1, g_2, \cdots, g_n) + \phi_a(h), a + b).$$

Observación. Con una notación más compacta la operación se puede escribir como

$$((g_1, g_2, \cdots, g_n), a) \oplus ((h_1, h_2, \cdots, h_n), b) = ((g_1 + (1+ap)h, g_2 + (1+ap)h, \cdots, g_n + (1+ap)h), a + b).$$

Proposición 45. El producto semidirecto definido en el lema previo,

$$\left(\frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p^2)} \times \cdots \times \frac{\mathbb{Z}}{(p^2)}\right) \rtimes_\phi \frac{\mathbb{Z}}{(p)},$$

es un p-grupo de orden p^{2n+1} y no conmutativo cuyos elementos son todos de orden 1, p o p^2.

4.4. El p-grupo no abeliano $\frac{\mathbb{Z}}{(p^2)} \rtimes \left(\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \cdots \times \frac{\mathbb{Z}}{(p)}\right)$

En esta sección vamos a generalizar de nuevo la construcción $\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p)}$, pero esta vez modificando el segundo espacio. Considerarmos, en lugar de $\frac{\mathbb{Z}}{(p)}$, su producto n veces $\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \cdots \times \frac{\mathbb{Z}}{(p)}$.

La manera de proceder es similar, pero en este caso no podremos garantizar también la inyectividad del homomorfismo ϕ. Por otro lado, las aplicaciones que nos interesan vuelven a ser

$$\begin{array}{rccc} \phi_j : \dfrac{\mathbb{Z}}{(p^2)} & \longrightarrow & \dfrac{\mathbb{Z}}{(p^2)} \\ a & \longmapsto & (1+jp)a \end{array}$$

con $j \in \{0, 1, 2, \ldots, p-1\}$, las del lema 37, que, como habíamos enunciado ya, son automorfismos.

La carencia de inyectividad del homomorfismo ϕ viene de que ahora no tenemos la ventaja que nos otorgaba la cómoda inclusión de $\frac{\mathbb{Z}}{(p)}$ en $\frac{\mathbb{Z}}{(p^2)}$. En esta situación nos interesa más garantizar solamente el lema siguiente:

Lema 46. Consideremos ϕ_j para $j \in \{0, 1, 2, \ldots, p-1\}$ como indicamos anteriormente, las del lema 37. Entonces, la aplicación

$$\begin{array}{rccc} \phi : \left(\dfrac{\mathbb{Z}}{(p)} \times \dfrac{\mathbb{Z}}{(p)} \times \cdots \times \dfrac{\mathbb{Z}}{(p)}, +\right) & \longrightarrow & Aut\left(\dfrac{\mathbb{Z}}{(p^2)}, +\right) \\ \mathbf{j} = (j_1, j_2, \cdots, j_n) & \longmapsto & \phi_{j_1+j_2+\cdots+j_n} \end{array}$$

es un homomorfismo de grupos.

Nótese que $j_1 + j_2 + \cdots + j_n$ se refiere a $j_1 + j_2 + \cdots + j_n \mod p$.

A continuación, en el tercer paso, análogamente a los lemas 39 y 44, construimos el producto semidirecto.

Lema 47. Tenemos definido un grupo producto semidirecto

$$\frac{\mathbb{Z}}{(p^2)} \rtimes_\phi \left(\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \cdots \times \frac{\mathbb{Z}}{(p)}\right)$$

de los grupos

$$\left(\frac{\mathbb{Z}}{(p^2)}, +\right) \quad \text{y} \quad \left(\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \cdots \times \frac{\mathbb{Z}}{(p)}, +\right)$$

con la operación de grupo dada por

$$(g, (a_1, a_2, \ldots, a_n)) \oplus (h, (b_1, b_2, \ldots, b_n)) = (g + \phi_{(a_1,a_2,\ldots,a_n)}(h), (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)).$$

Observación. Con una notación más compacta la operación se puede escribir como

$$(g, (a_1, a_2, \ldots, a_n)) \oplus (h, (b_1, b_2, \ldots, b_n)) = (g + (1 + (a_1 + a_2 + \cdots + a_n)p)h, (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)).$$

Proposición 48. El producto semidirecto definido en el lema previo,

$$\frac{\mathbb{Z}}{(p^2)} \rtimes \left(\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \cdots \times \frac{\mathbb{Z}}{(p)}\right),$$

es un p-grupo de orden p^{2+n} y no conmutativo cuyos elementos son todos de orden 1, p o p^2.

4.5. Otros productos semidirectos

Como hemos podido ver en las secciones previas, el *modus operandi* para construir grupos utilizando el producto semidirecto no difiere mucho de unos a otros. Por ese motivo, citamos algunos casos más sin introducir los lemas y justificaciones que aseguran las condiciones que necesitamos.

Los primeros ejemplos que mencionaremos nacen de incrementar las potencias del primo en en las que basamos los grupos implicados.

Por ejemplo, modificando el primer factor se puede construir el producto semidirecto

$$\frac{\mathbb{Z}}{(p^3)} \rtimes \frac{\mathbb{Z}}{(p)}$$

considerando la operación $(g,a) \oplus (h,b) = (g + (1+ap^2)h, a+b)$.

En este caso el centro del grupo es

$$Z = \{(jp, 0) : j \in \{0, 1, \cdots, p^2 - 1\}\}.$$

$$\sim \sim \sim \sim \sim$$

En cambio, modificando el segundo factor se puede construir el producto semidirecto

$$\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p^2)}$$

considerando la operación $(g,a) \oplus (h,b) = (g + (1+ap)h, a+b)$.

En este caso el centro del grupo es

$$Z = \{(jp, kp) : j, k \in \{0, 1, \cdots, p - 1\}\}.$$

$$\sim \sim \sim \sim \sim$$

Además, si modificamos ambos, se puede construir el producto semidirecto

$$\frac{\mathbb{Z}}{(p^3)} \rtimes \frac{\mathbb{Z}}{(p^2)}$$

considerando la operación $(g,a) \oplus (h,b) = (g + (1+ap^2)h, a+b)$.

En este caso el centro del grupo es

$$Z = \{(jp, kp) : j \in \{0, 1, \cdots, p^2 - 1\}, k \in \{0, 1, \cdots, p - 1\}\}.$$

$$\sim \sim \sim \sim \sim$$

De hecho, de manera general se tiene que

$$\left(\frac{\mathbb{Z}}{(p^n)} \rtimes \frac{\mathbb{Z}}{(p^s)}, \oplus\right)$$

considerando la operación $(g,a) \oplus (h,b) = (g + (1+ap^{n-1})h, a+b)$, es también un producto semidirecto.

En este caso el centro del grupo es

$$Z = \{(jp, kp) : j \in \{0, 1, \cdots, p^{n-1} - 1\}, k \in \{0, 1, \cdots, p^{s-1} - 1\}.$$

$$\sim \sim \sim \sim \sim$$

Nótese que, además de la amplia gama de posibilidades que nos otorga la generalización previa, podemos conseguir aún más grupos definiendo una operación diferente. Por ejemplo,

$$\left(\frac{\mathbb{Z}}{(p^n)} \rtimes \frac{\mathbb{Z}}{(p^s)}, \boxplus\right)$$

cuando consideramos una nueva operación dada por $(g,a) \boxplus (h,b) = (g + (1 + ap^{n-s})h, a + b)$ es un producto semidirecto distinto de $\left(\frac{\mathbb{Z}}{(p^n)} \rtimes \frac{\mathbb{Z}}{(p^s)}, \oplus\right)$.

En este caso el centro del grupo es

$$Z = \{(jp^s, 0) : j \in \{0, 1, \cdots, p^{n-s} - 1\}\}.$$

$$\sim \sim \sim \sim \sim$$

Por último, cabe mencionar que una vez conocidos algunos ejemplos, se puede complicar un poco más la idea mezclando estas construcciones. Por ejemplo,

$$\left(\left(\frac{\mathbb{Z}}{(p^3)}\right) \rtimes \left(\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p^2)}\right), \odot\right)$$

con la operación $(a,(b,c)) \odot (\alpha,(\beta,\gamma)) = (a + (1 + p^2b + pc)\alpha, (b + \beta, c + \gamma))$ es otro producto semidirecto.

Capítulo 5

p-grupos de matrices

El teorema de Cayley nos asegura que cada grupo finito de orden n es isomorfo a un subgrupo del grupo simétrico. Teniendo en cuenta que las permutaciones pueden verse como transformaciones lineales, y que estas se pueden representar matricialmente, el interés en los grupos de matrices es natural.

Por desgracia, la construcción de estos subgrupos de matrices no es sencilla y se sale de los objetivos de este texto. Sin embargo, sí que resulta procedente detallar algunos ejemplos de p-grupos de matrices. Para ello introduciremos primero el grupo lineal general y el lineal especial, a pesar de que ellos mismos no son p-grupos, y detallaremos posteriormente como encontrar en ellos ciertos subgrupos que sí son p-grupos.

5.1. El grupo lineal general y grupo lineal especial

El **grupo lineal general** de grado n es el grupo constituido por el conjunto de las matrices invertibles de tamaño $n \times n$ con el producto usual de matrices. Las entradas de la matriz pueden fijarse en cualquier cuerpo o anillo, pero nosotros nos centraremos en aquellas con entradas en $\mathbb{F}_p$, los cuerpos finitos de p elementos. Así pues, consideraremos el conjunto

$$GL(n, \mathbb{F}_p) = \{A \in \mathfrak{M}_{n\times n}(\mathbb{F}_p) : det(A) \neq 0\}$$

con la operación producto de matrices habitual, trabajando así con el grupo

$$(GL(n, \mathbb{F}_p), \cdot).$$

Notación. A veces al conjunto $GL(n, \mathbb{F}_p)$ se le denota simplemente como $GL(n, p)$.

Proposición 49. El orden del grupo $GL(n, p)$ es $(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$.

Demostración. Necesitamos contar el número de matrices con determinante no nulo y entradas en el cuerpo F_p. Para ello la combinatoria será nuestra principal herramienta, ya que el procedimiento se basará en comprobar de cuantas formas podemos elegir la columna j una vez sabemos las opciones que teníamos en las previas de modo que continue sin ser dependiente de las anteriores.

La forma génerica de las matrices que nos interesan es la siguiente:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Si nos centramos en la primera columna, lo único que se exige es que no sea nula. Esto nos permite $p^n - 1$ opciones.

Pasando a la segunda columna, si esta fuera un múltiplo de la primera el determinante si sería nulo. Como es precisamente lo que deseamos evitar, se concluye que hay $p^n - p$ opciones para la segunda columna.

Del mismo modo, la tercera columna no puede ser combinación lineal de las dos anteriores, puesto que en tal caso el determinante se anularía. Eso nos deja con $p^n - p^2$ opciones para la tercera columna.

Con un razonamiento análogo para cada una de las columnas restantes se deduce que, de hecho, para cada $i \in \{1, 2, \ldots, n\}$ tenemos $p^n - p^{i-1}$ opciones para la i-ésima columna.

Por lo tanto, el número total de matrices invertibles, es decir, el orden de $GL(n, p)$ es el producto

$$(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}).$$

■

Notemos que la proposición previa nos asegura que $GL(n, p)$ no es un p-grupo.

Veamos entonces qué conclusiones podemos sacar si nos restringimos a un subgrupo suyo, al **grupo lineal especial** de grado n. El grupo lineal especial es el grupo

$$(SL(n, \mathbb{F}_p), \cdot),$$

constituido por el conjunto de las matrices de tamaño $n \times n$ con determinante 1, es decir,

$$SL(n, \mathbb{F}_p) = \{A \in \mathfrak{M}_{n\times n}(\mathbb{F}_p) : det(A) = 1\},$$

y considerando como operación el producto usual de matrices.

Las entradas de la matriz, al igual que antes, nos intersan en $\mathbb{F}_p$ y así lo describimos, pero de manera general también se podría considerar cualquier anillo o cuerpo.

Notación. A veces al conjunto $SL(n, \mathbb{F}_p)$ se le denota simplemente como $SL(n, p)$.

Proposición 50. El orden del grupo $SL(n, p)$ es

$$\frac{|GL(n, p)|}{p - 1}.$$

Demostración. Recurrimos a la aplicación determinante:

$$\begin{aligned} \det : GL(n, p) &\longrightarrow (\mathbb{F}_p^*, \cdot) \\ A &\longrightarrow \det(A) \end{aligned}$$

Notemos que det es un homomorfismo, porque es bien conocido que $\det(A \cdot B) = \det(A)\det(B)$. Además, al considerar el conjunto de llegada $\mathbb{F}_p^*$ donde ya no contamos con el cero, la aplicación es sobreyectiva, de modo que $\mathrm{Im}(\det) = \mathbb{F}_p^*$. Y también se puede observar que el núcleo de la aplicación es precisamente

$$\ker(\det) = \{A \in \mathfrak{M}_{n\times n} : det(A) = 1\} = SL(n, p).$$

Aplicando a det el teorema del homomorfismo, deducimos que

$$\frac{GL(n, p)}{\ker(\det)} \cong \mathrm{Im}(\det).$$

Y con lo que sabemos sobre el núcleo y la imagen de det, se puede escribir precisamente como

$$\frac{GL(n, p)}{SL(n, p)} \cong \mathbb{F}_p^*.$$

Por tanto, en cuestión de cardinalidad, se llega a

$$\frac{|GL(n, p)|}{|SL(n, p)|} = |\mathbb{F}_p^*|,$$

donde despejando $|SL(n, p)|$ se confirma la expresión para el orden de tal grupo que teníamos en el enunciado.

■

Notemos que la proposición previa nos asegura que $SL(n,p)$ tampoco es un p-grupo. Sin embargo, todo este estudio sí tiene cabida en el texto, y el sentido nos lo da la siguiente sección.

5.2. $UT(n,p)$, un p-grupo de matrices triangulares dentro de $SL(n,p)$

Entre las matrices, aquellas triangulares suelen ser de interés, puesto que es más sencillo trabajar con ellas. Por ejemplo, en la rama de numérico se suelen aprovechar para descomposiciones por el ahorro computacional que permiten.

En este texto vamos a quedarnos con el grupo que denotaremos

$$(UT(n,p),\cdot),$$

constituido por el conjunto $UT(n,p)$ de matrices triangulares superiores con diagonal de unos, de tamaño $n\times n$ y entradas en $\mathbb{F}_p$, es decir,

$$UT(n,p)=\left\{\begin{pmatrix}1 & a_{12} & a_{13} & \dots & a_{1n}\\ 0 & 1 & a_{23} & \dots & a_{2n}\\ 0 & 0 & 1 & \dots & a_{3n}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \dots & 1\end{pmatrix}\in\mathfrak{M}_{n\times n}(\mathbb{F}_p)\right\},$$

y la operación producto usual de matrices.

Recuérdese que el producto de matrices es no conmutativo, y nótese que si $n\geq 3$ este caso no es distinto.

Observemos también que las matrices de este grupo tienen todas determinante 1, de modo que $(UT(n,p),\cdot)$ es un subgrupo de $(SL(n,p),\cdot)$, y por tanto también de $(GL(n,p),\cdot)$. Además, el orden de $(UT(n,p),\cdot)$ es precisamente

$$|UT(n,p)|=p^{\frac{n(n-1)}{2}}.$$

Entonces, este grupo $(UT(n,p),\cdot)$ sí es un p-grupo, que además es no conmutativo si $n\geq 3$. Este hecho nos confirma que, **a pesar de que ni $GL(n,p)$, ni $SL(n,p)$ son p-grupos, siempre se puede encontrar un subgrupo suyo que sí lo es.**

En las siguientes secciones aportaremos más información respecto a este p-grupo.

5.3. Exponente en $UT(n,p)$

Por la información curiosa que aporta sobre la estructura interna de los grupos y las simplificaciones que permitirán después en las operaciones que nos requerirán algunos ejemplos, vamos a comenzar especificando algunos resultados que ligan con el concepto de exponente.

Lema 51. Si $p\geq 3$, entonces todo elemento distinto del neutro en $UT(3,p)$ tiene orden p. Es decir, el exponente del grupo es p.

Demostración. Tomamos una matriz M cualquiera de $UT(3,p)$ distinta de la identidad,

$$M=\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix},$$

y comprobaremos que multiplicancándola por sí misma, es a la p-ésima potencia la primera vez que llegamos a la matriz identidad. Notése que:

$$M^2 = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

$$M^3 = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix}$$

$$M^4 = \begin{pmatrix} 1 & 4a & 4b+6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{pmatrix}$$

$$M^5 = \begin{pmatrix} 1 & 5a & 5b+10ac \\ 0 & 1 & 5c \\ 0 & 0 & 1 \end{pmatrix}$$

Podemos observar que la recurrencia que se deduce para el cálculo de la j-ésima potencia para cada $j \in \mathbb{N}$ es precisamente:

$$M^j = \begin{pmatrix} 1 & ja & jb+\binom{j}{2}ac \\ 0 & 1 & jc \\ 0 & 0 & 1 \end{pmatrix}.$$

Notemos que el orden de M no puede ser estrictamente menor que p, porque como al menos una de las varibles a, b o c ha de ser no nula para que M no sea la identidad, se tiene que al menos $ja \neq 0$, o $jb \neq 0$, o $jc \neq 0$ para $j < p$ recordando que estamos trabajando en $\frac{\mathbb{Z}}{(p)}$.

Para asegurar que el orden es realmente p, confirmemos que pa, pc y $pb + \binom{p}{2}ac$ son cero. Ahora bien, es inmediato que $pa = pb = pc = 0$. Y como $\binom{p}{2} = \frac{p(p-1)}{2}$ es múltiplo de p, también se anula $\binom{p}{2}ac$.

Hemos comprobado entonces lo que necesitábamos y podemos asegurar que todos los elementos de $UT(3,p)$ son de orden p.

Además, el exponente de $UT(3,p)$ es p por la propia definición de exponente (definición 16).

■

Generalicemos el lema anterior a una condición que relacione el tamaño de las matrices para cualquier n con el orden del cuerpo en el que tienen las entradas. La naturaleza del resultado es la misma y por tanto el *modus operandi* también. Sin embargo, la detallaré porque las herramientas técnicas son distintas, aportando una bonita mezcla de combinatoria y álgebra básica.

Proposición 52. Sea $UT(n,p)$ con $p \geq n$. Entonces todo elemento distinto del neutro tiene orden p y por tanto se trata de un grupo de exponente p.

Demostración. Sea $A \in UT(n,p)$ distinta de la identidad. Entonces $A = I + N$ siendo I la matriz identidad y N triangular superior estricta no nula.

En esta ocasión recurriremos al binomio de Newton,

$$A^m = (I+N)^m = I + \sum_{k=1}^{m} \binom{m}{k} N^k.$$

Nótese que $\binom{m}{k} = \frac{m!}{k!(m-k)!}$, y se puede ver que si $m = p$, entonces $\binom{m}{k}$ es múltiplo de p para $0 < k < p$. Además, las matrices triangulares estrictamente superiores de tamaño n son nilpotentes, y $N^n = 0$. Así pues, como $p \geq n$ también $N^p = 0$. De modo que es $A^p = I$.

Veamos ahora que p es el primer natural para el que esto sucede. Asegurémoslo razonando por reducción al absurdo suponiendo que existe $j < p$ tal que $A^j = I$.
En esta situación tenemos que

$$I = A^j = (I+N)^j = I + \binom{j}{1}N + \binom{j}{2}N^2 + \binom{j}{3}N^3 + \cdots + \binom{j}{j-1}N^{j-1} + N^j,$$

equivalentemente,

$$0 = \binom{j}{1}N + \binom{j}{2}N^2 + \binom{j}{3}N^3 + \cdots + \binom{j}{j-1}N^{j-1} + N^j.$$

Sacando factor común N, esto se ve como

$$0 = N\left(\binom{j}{1}I + \binom{j}{2}N + \binom{j}{3}N^2 + \cdots + \binom{j}{j-1}N^{j-2} + N^{j-1}\right),$$

donde notemos que la expresión matricial del paréntesis ha de ser invertible. Esto es porque el producto de matrices estrictamente superiores es estrictamente superior, de modo que el primer sumando es el único que interviene en la diagonal y nos permite conocer fácilmente que su determinante es $\binom{j}{1}^n = j^n$, que no es nulo porque $0 < j < p$ y $n \leq p$. Que una matriz sea invertible equivale a que sea regular por la derecha, lo cual entra en contradicción con que N no es nula.

■

Por último, nos centramos en los 2-grupos. Nótese que la proposición previa no entra en conflicto con la siguiente.

Proposición 53. Sea G un 2-grupo en el que todo elemento distinto del neutro tiene orden 2 (grupo de exponente 2). Entonces G es un grupo conmutativo.

Demostración. Deseamos ver que dados $a, b \in G$ entonces $ab = ba$. Nótese que por ser un grupo, $ab \in G$. Por ser todos los elementos de orden dos, en particular $(ab)^2 = 1$. Es decir, $abab = 1$. Además, que cada elemento sea de orden dos, nos aporta que el inverso de cada elemento es él mismo. Entonces, si multiplicamos en ambos lados de la igualdad anterior por a por la izquierda y por b por la derecha, se sigue que $ba = ab$. Justo lo que deseábamos probar.

■

Recordando la definición 26, esto nos garantiza que simplemente con ser 2-grupo de exponente 2 se cumple la condición de conmutatividad y por tanto es un grupo elemental, que ya afirmamos que es isomorfo al grupo $\frac{\mathbb{Z}}{(2)} \times \frac{\mathbb{Z}}{(2)} \times \cdots \times \frac{\mathbb{Z}}{(2)}$ dotado de la operación suma.

5.4. Subgrupos de $UT(n,p)$

La mayor parte de esta sección se dedicará a dar ejemplos. Sin embargo, el primer resultado se centra en garantizar la relación de isomorfía entre grupos con matrices de distintos tamaños sobre el mismo cuerpo. El motivo es que esto nos permite conocer directamente subgrupos que son p-grupos para casos de grupos de orden mayor, lo que puede ser útil al estudiar la estructura de grupos más grandes.

Lema 54. Si $n < m$ se tiene que $UT(n,p)$ es isomorfo a un subgrupo de $UT(m,p)$

No lo demostraremos, pero podemos poner un ejemplo cuando $n = 3$ y $m = 4$ que ilustra claramente un modo constructivo de proceder. Basta con definir el isomorfismo siguiente:

$$\begin{array}{ccc} i : UT(3,p) & \longrightarrow & UT(4,p) \\ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & a & c & 0 \\ 0 & 1 & b & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{array}$$

Ahora ya sí pasamos a los ejemplos. Cabe remarcar primero que los grupos de $UT(n,p)$ tienen muchos subgrupos que son p-grupos.

Expongamos algunos ejemplos curiosos partiendo del grupo $UT(4,p)$. Consideraremos casos con $p \geq 4$, ya que por el lema 52 conocemos que el exponente de estos subgrupos es p. Como adelantamos al introducir la sección previa, esto simplificará partes tediosas y poco interesantes del estudio de estos ejemplos.

$$H_1 = \left\{ \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \in UT(4,p) \right\} \qquad H_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 1 & b & c \\ 0 & 0 & 1 & d \\ 0 & 0 & 0 & 1 \end{pmatrix} \in UT(4,p) \right\}$$

$$H_2 = \left\{ \begin{pmatrix} 1 & a & 0 & b \\ 0 & 1 & 0 & c \\ 0 & 0 & 1 & d \\ 0 & 0 & 0 & 1 \end{pmatrix} \in UT(4,p) \right\}$$

Nótese que:
$|H_1| = p^5$
$|H_2| = p^4$
$|H_3| = p^4$.

La matriz identidad pertenece evidentemente a todos los conjuntos. Así pues, para asegurar que realmente son subgrupos es suficiente con ver que dadas dos matrices cualesquiera en el conjunto, su producto continúa siendo una matriz del conjunto. Como es una sencilla comprobación ver que cada H_1, H_2, H_3 es cerrado para el producto, no lo detallaremos.

Nótese que ver la clausura para el producto es suficiente, porque en particular esto obliga a que las potencias de un elemento estén en el conjunto, y como el exponente es p tenemos garantizada la pertenencia del inverso al conjunto.

Además, aunque gracias a la proposición 52 ya sabemos que si $p \geq 5$ el exponente es p y hemos contado con las ventajas que esto ofrece, por reafirmar el interés que puede tener la manera de trabajar del lema 51, nótese que es sencillo asegurar que el orden de cualquier elemento es p si se conoce la forma de la j-ésima potencia.

Tomemos una matriz $M = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \in H_1 \setminus I$ y calculemos algunas potencias:

$$M^2 = \begin{pmatrix} 1 & 2a & 2b & 2c + ad + be \\ 0 & 1 & 0 & 2d \\ 0 & 0 & 1 & 2e \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M^4 = \begin{pmatrix} 1 & 4a & 4b & 4c + 6ad + 6be \\ 0 & 1 & 0 & 4d \\ 0 & 0 & 1 & 4e \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M^3 = \begin{pmatrix} 1 & 3a & 3b & 3c + 3ad + 3be \\ 0 & 1 & 0 & 3d \\ 0 & 0 & 1 & 3e \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M^5 = \begin{pmatrix} 1 & 5a & 5b & 5c + 10ad + 10be \\ 0 & 1 & 0 & 5d \\ 0 & 0 & 1 & 5e \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Esto nos permite reconocer la recurrencia para la j-ésima potencia,

$$M^j = \begin{pmatrix} 1 & ja & jb & jc + \binom{j}{2} ad + \binom{j}{2} be \\ 0 & 1 & 0 & jd \\ 0 & 0 & 1 & je \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

y argumentando análogamente al lema 51 se concluye de igual forma que el exponente es p.

Exponemos también algunos ejemplos partiendo del grupo $UT(5,p)$ con $p \geq 5$, que nos permite dar subgrupos de mayor orden manteniendo que p sea el exponente del grupo:

$$B_1 = \left\{ \begin{pmatrix} 1 & a & b & 0 & c \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & d \\ 0 & 0 & 0 & 1 & e \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in UT(5,p) \right\} \qquad B_3 = \left\{ \begin{pmatrix} 1 & a & b & c & d \\ 0 & 1 & 0 & e & f \\ 0 & 0 & 1 & 0 & g \\ 0 & 0 & 0 & 1 & h \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in UT(5,p) \right\}$$

$$B_2 = \left\{ \begin{pmatrix} 1 & a & b & c & d \\ 0 & 1 & 0 & 0 & e \\ 0 & 0 & 1 & 0 & f \\ 0 & 0 & 0 & 1 & g \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in UT(5,p) \right\}$$

Nótese que:
$|B_1| = p^5$
$|B_2| = p^7$
$|B_3| = p^8$.

Por razonamientos análogos a los realizados para los ejemplos de $UT(4,p)$, para asegurar que realmente son subgrupos basta ver que son conjuntos cerrados para la operación. Tampoco lo detallaremos, porque comprobar que cada B_1, B_2, B_3 es cerrado para el producto es sencillo.

Nótese que, como hemos ilustrado, esta es una manera bastante mécanica de trabajar para construir gran cantidad de p-grupos. De todos modos, obsérvese que no hemos asegurado en ningún momento que no nos conduzcan a grupos no isomorfos. No hay mayor problema, es parte de lo que augurábamos en la introducción, se puede llegar al mismo lugar por varios caminos.

5.5. El grupo de Heisenberg

Dentro de estos grupos de matrices $UT(n,p)$ con el producto matricial usual, hacemos una mención especial a

$$\mathbb{H}_p = UT(3,p) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{3\times 3}(\mathbb{F}_p) \right\}.$$

A este grupo $(\mathbb{H}_p, \cdot)$ de orden p^3 se le denota de manera especial y se le llama grupo de Heisenberg en honor al físico Werner Heisenberg, ya que esta estructura está estrechamente relacionada con la mecánica cuántica a la que él se dedicaba.

Para este texto el caso de interés es el discreto por ser el que liga con los p-grupos, pero realmente en física el que tiene más importancia es el caso continuo con coeficientes en $\mathbb{R}$. Aún así, el estudio de unos invita al estudio de los otros y por su peso en la ciencia el grupo de Heisenberg merece destacarse, además de que nos será de utilidad en capítulos posteriores.

Ya hemos adelantado en la sección 5.3 que si $p \geq 3$ el exponente de $\mathbb{H}_p$ es p, y cerraremos el contenido sobre este grupo describiendo su centro:

$$Z(\mathbb{H}_p) = Z(UT(3,p)) = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{3\times 3}(\mathbb{F}_p) \right\}.$$

5.6. Otro ejemplo de producto semidirecto

En esta sección mezclaremos las ideas propias de este capítulo con las del capítulo 4. Vamos a definir un producto semidirecto

$$\left(\left(\frac{\mathbb{Z}}{(3)}\right)^3 \rtimes_\phi \frac{\mathbb{Z}}{(3)}, \bullet\right).$$

Nótese que en esta situación el homomorfismo ϕ va de $\frac{\mathbb{Z}}{(3)}$ a $Aut\left(\left(\frac{\mathbb{Z}}{(3)}\right)^3\right)$, y recuérdese que los automorfismos de $\left(\frac{\mathbb{Z}}{(3)}\right)^3$ se pueden escribir como matrices 3×3. De este modo la operación de la pareja que forma el producto semidirecto se pude definir de la siguiente forma:

$$((a_1,a_2,a_3),b) \bullet ((c_1,c_2,c_3),d) = \left((a_1,a_2,a_3) + (c_1,c_2,c_3)\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}^b, b+d\right).$$

Con la notación que hemos estado utilizando para las cuestiones sobre el producto semidirecto se identifica claramente que

$$\begin{array}{rcl}\phi : \dfrac{\mathbb{Z}}{(3)} & \longrightarrow & Aut\left(\left(\dfrac{\mathbb{Z}}{(3)}\right)^3\right)\\ b & \longmapsto & \phi_b\end{array}$$

siendo ϕ_b el homomorfismo

$$\begin{array}{rcl}\phi_b : \left(\dfrac{\mathbb{Z}}{(3)}\right)^3 & \longrightarrow & \left(\dfrac{\mathbb{Z}}{(3)}\right)^3\\ (a_1,a_2,a_3) & \longmapsto & (a_1,a_2,a_3)\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}^b.\end{array}$$

Obsérvese que en el caso $b = 0$ tenemos el homomorfismo identidad.

Notése que esta misma construcción es válida para cada primo $p \geq 3$.

Además, la construcción previa también puede generalizarse a otras dimensiones. Si p es un primo tal que $p \geq 5$, entonces se puede construir el producto semidirecto

$$\left(\left(\frac{\mathbb{Z}}{(p)}\right)^4 \rtimes \frac{\mathbb{Z}}{(p)}, \odot\right)$$

considerando la operación

$$((a_1,a_2,a_3,a_4),b) \odot ((c_1,c_2,c_3,c_4),d) = \left((a_1,a_2,a_3,a_4) + (c_1,c_2,c_3,c_4)\begin{pmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\0&0&0&1\end{pmatrix}^b, b+d\right).$$

Remarcamos el interés de esta sección por la manera en la que permite fusionar dos herramientas distintas para la construcción de p-grupos.

5.7. p-grupos de matrices sobre $\frac{\mathbb{Z}}{(p^n)}$

Esta sección es algo más delicada porque hasta ahora hemos trabajado con cuerpos, pero $\frac{\mathbb{Z}}{(p^n)}$ solamente es un anillo, de modo que hay que ser cuidadosos con las limitaciones que impone.

Si consideramos el conjunto

$$T = \left\{ \begin{pmatrix} 1+ap & b \\ 0 & 1 \end{pmatrix} : a \in \{0,1,\dots,p-1\}, b \in \frac{\mathbb{Z}}{(p^2)} \right\}$$

con el producto usual de matrices obtenemos un p-grupo de orden p^3.

En T la operación de dos elementos resulta

$$\begin{pmatrix} 1+ap & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+\alpha p & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+(a+\alpha)p & (1+ap)\beta + b \\ 0 & 1 \end{pmatrix}.$$

Recordemos que en $\frac{\mathbb{Z}}{(p^2)}$ se tiene que $p^2 = 0$. Precisamente por ello para cada $a, \alpha \in \{0,1,\dots,p-1\}$, se tiene que $(1+ap)(1+\alpha p) = 1 + (a+\alpha)p + a\alpha p^2 = 1 + (a+\alpha)p$.

Remarcamos la importancia de tener cuidado con los inversos, una de esas limitaciones que impone no tener todas las ventajas de trabajar con cuerpos. En este caso, para cada $a \in \{0,1,\dots,p-1\}$, se obtiene que $(1+ap)(1-ap) = 1 - a^2p^2 = 1$. Esto es, para cada $a \in \{0,1,\dots,p-1\}$, $(1+ap)^{-1} = 1-ap$ en $\frac{\mathbb{Z}}{(p^2)}$, donde $-ap = (p-a)p$.

Además, es interesante reconocer que este grupo es isomorfo a nuestro conocido $\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p)}$.

Para demostrarlo basta con definir el isomorfismo adecuado.
Concretamente, si consideramos la apliación

$$\begin{array}{rcl} \varphi : T & \longrightarrow & \dfrac{\mathbb{Z}}{(p^2)} \rtimes \dfrac{\mathbb{Z}}{p} \\ \begin{pmatrix} 1+ap & b \\ 0 & 1 \end{pmatrix} & \longmapsto & (b,a) \end{array}$$

asegurar la isomorfía es casi inmediato.
La sobreyectividad es evidente, y por cardinalidad la biyectividad queda garantizada. Además, es simplemente cuestión de operar el deducir que

$$\varphi \begin{pmatrix} 1+ap & b \\ 0 & 1 \end{pmatrix} \varphi \begin{pmatrix} 1+\alpha p & \beta \\ 0 & 1 \end{pmatrix} = (b + (1+ap)\beta, a+\alpha)$$

y que

$$\varphi \begin{pmatrix} 1+(a+\alpha)p & (1+ap)\beta + b \\ 0 & 1 \end{pmatrix} = (b + (1+ap)\beta, a+\alpha),$$

asegurando que φ es homomorfismo.

De una manera similar, tomando en el conjunto

$$\tilde{T} = \left\{ \begin{pmatrix} 1+ap & d & e \\ 0 & 1+bp & f \\ 0 & 0 & 1+cp \end{pmatrix} : a,b,c \in \{0,1,\dots,p-1\}, d,e,f \in \frac{\mathbb{Z}}{(p^2)} \right\}$$

con el producto usual de matrices obtenemos un p-grupo de orden p^9.

En este caso podemos llegar a otra conclusión intersante, y es que hemos llegado a un grupo que tiene como subgrupo a $UT\left(3, \frac{\mathbb{Z}}{(p^2)}\right)$, una generalización del mismo concepto que el grupo de Heisenberg, pero ahora para algo más allá del cuerpo finito de p elementos.

Capítulo 6

Sobre la clasificación de p-grupos finitos

En este capítulo hablaremos a título informativo sobre la evolución en la clasificación de los p-grupos finitos. No cabe duda de que se han dado grandes pasos, pero también es evidente que queda mucho camino.

En los preliminares del capítulo 2 ya obtuvimos una información muy intersante sobre los grupos de orden p^2 gracias a la proposición 13, que nos garantizaba que todos eran abelianos. Una información que quedaba muy bien complementada en el capítulo 3, donde detallamos la existencia de una clasificación de los p-grupos finitos abelianos. Ese capítulo cerraba de manera precisa una parte muy interesante, nos permitía el control del caso conmutativo.

Con los ejemplos de los capítulos siguientes se aportaron nuevos casos que se salían de la confortable zona de los grupos abelianos, pero podemos notar que por muchos ejemplos que dimos, no hemos aportado una clasificación cerrada.

El motivo de ello es, precisamente, el gran camino que aún queda en la clasificación de los p-grupos finitos y que se sale de los objetivos de este texto. A lo largo de los años, ha habido ciertos avances en la clasificación de los grupos de orden p^n cuando n es pequeño, pero la tarea se ha ido volviendo progresivamente más difícil conforme aumenta el valor del exponente. El primer paso importante en este objetivo ocurrió en 1882, cuando el matemático alemán Eugen Netto logró clasificar los grupos de orden p^2. Fue el primer intento serio de avanzar en este campo. Apenas un año después, en 1883, un grupo de matemáticos, compuesto por Cole y Glover, Hölder y Young, consiguió avanzar en la clasificación de los grupos de orden p^3, y más tarde los dos últimos continuaron trabajando y obtuvieron resultados en la clasificación de los grupos de orden p^4. Sin embargo, después de estos primeros avances, pasaron cinco años hasta que, en 1898, el matemático Bagnera logró dar un gran paso al clasificar los grupos de orden p^5 [1]. A partir de este momento, el ritmo de los avances disminuyó considerablemente. Fue necesario esperar hasta el año 2004, cuando, después de varios intentos infructuosos, un equipo de matemáticos formado por Newman, O'Brien y Vaughan-Lee, finalmente logró la clasificación de los grupos de orden p^6 [9]. Este logro se consideró un avance significativo, y a estos dos últimos matemáticos también se les debe el mérito de haber logrado clasificar los grupos de orden p^7 [11], en 2005, solo un año más tarde. Desde entonces, han transcurrido ya 20 años, y aunque no se han producido avances tan rápidos ni tan significativos como en el pasado, la clasificación de los p-grupos finitos sigue siendo un área activa de investigación. En la actualidad, incluso los avances alcanzados en la clasificación de aquellos de orden pequeño se están incorporando a bases de datos computacionales especializadas.

Por todo el trabajo que ha llevado detrás y el interés que tiene, incluimos a continuación una tabla que muestra el número de grupos que hay, salvo isomorfismo, de orden p^n para $n \leq 5$:

p	2	3	$p \geq 5$
p^1	1	1	1
p^2	2	2	2
p^3	5	5	5
p^4	14	15	15
p^5	51	67	$2p + 61 + 2\gcd(p-1,3) + \gcd(p-1,4)$

Hemos adelantado que también se conocen los datos para $n = 6$ y $n = 7$, así que los incluimos también. Como era de esperar, las expresiones se complican en cuanto crece el exponente n del orden a estudiar p^n, y por ello los casos $n = 6$ y $n = 7$ los listamos:

- Caso p^6:
  - Existen 267 grupos de orden 2^6
  - Existen 504 grupos de orden 3^6.
  - Para $p \geq 5$, el número de grupos de orden p^6 viene dado por

$$3p^2 + 39p + 344 + 24\gcd(p-1,3) + 11\gcd(p-1,4) + 2\gcd(p-1,5).$$

- Caso p^7:
  - Existen 2328 grupos de orden 2^7
  - Existen 9310 grupos de orden 3^7.
  - Existen 34297 grupos de orden 5^7.
  - Para $p > 5$, el número de grupos de orden p^7 viene dado por

$$\begin{gathered} 3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455 \\ +(4p^2 + 44p + 291)\gcd(p-1,3) + (p^2 + 19p + 135)\gcd(p-1,4) \\ +(3p + 31)\gcd(p-1,5) + 4\gcd(p-1,7) + 5\gcd(p-1,8) \\ +\gcd(p-1,9). \end{gathered}$$

Dar expresiones cerradas y exactas de la cantidad de grupos de cada orden es, como se puede notar, terriblemente costoso. Sin embargo, ya en 1965 Charles C. Sims [4] halló una aproximación al número de grupos de orden p^n para cualquier primo p y natural n:

$$p^{\left(\frac{2}{27}n^3 + O\left(n^{\left(\frac{8}{3}\right)}\right)\right)}.$$

Destacamos que en este trabajo hemos aportado una cantidad ingente de p-grupos que avalan tal crecimiento.

6.1. Grupos de orden 2^n

Como hemos podido observar con los datos previos, la cantidad de grupos de orden p^n sigue una regla independiente cuando $p = 2$. En los últimos años no ha habido avances para p génerico, sin embargo en el caso de $p = 2$ sí se ha cerrado la clasificación para algunas potencias más. Gracias de nuevo a O'Brien se determinaron los 56092 grupos de orden 2^8 [10], y su colaboración con Besche y Eick demostró que de orden 2^9 hay 10494213 grupos [2]. Ellos mismos demostraron que de orden 2^{10} hay 49487367289 grupos no isomorfos.

Recogemos en la siguiente tabla todos los datos conocidos:

$\lvert G\rvert$	1	2	4	8	16	32	64	128	256	512	1024
Número de grupos	1	1	2	5	14	51	267	2328	56092	10494213	49487367289

Se deconoce el número de grupos que hay de orden $2^{11} = 2048$, pero gracias al resultado de Charles C. Sims [4] sí que se sabe que el número de grupos de orden 2^n se aproxima a

$$2^{\left(\frac{2}{27}n^3+O\left(n^{\left(\frac{8}{3}\right)}\right)\right)}.$$

6.2. Grupos de orden 3^n

También se observa que el caso para $p = 3$ sigue, como para $p = 2$, sus propias reglas. Como venimos remarcando, según se incrementa el orden el trabajo es más costoso. Sin embargo, como bien refleja [OEIS] es conocido el número de grupos no isomorfos cuyos ordenes son potencias de 3 hasta $3^9 = 19683$. La siguiente tabla recoge esos datos:

$\lvert G\rvert$	1	3	9	27	81	243	729	2187	6561	19683
Número de grupos	1	1	2	5	15	67	504	9310	1396077	5937876645

De hecho, esta sección está ampliamente motivada por ese último descubrimiento, del número de grupos no isomorfos de orden 3^9, ya que la clasificación de los grupos de orden 3^9 es uno de los más novedosos avances en el campo. De este logro es responsable David Burrel, que en 2023 mostró que hay 5937876645 grupos de tal orden [3].

6.3. Grupos de orden p^3 con $p \geq 3$

Ya se han presentado los 5 grupos que existen, salvo isomorfismo, de orden p^3 cuando $p \geq 3$. Recapitularemos ahora todos ellos, pues es una buena manera de reafirmar el interés de las herramientas que hemos ido describiendo.

En el capítulo 3 confirmamos que hay 3 posibles grupos abelianos no isomorfos de orden p^3, y son:

$$\frac{\mathbb{Z}}{(p^3)}, \qquad \frac{\mathbb{Z}}{(p^2)} \times \frac{\mathbb{Z}}{(p)}, \quad \text{y} \quad \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)}.$$

Después, en el capítulo 4, con la potente aportación que supone el producto semidirecto para la construcción de nuevos grupos mostramos la existencia del grupo no conmutativo

$$\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p)}.$$

Dimos todos los pasos necesarios para llegar a confirmar los requisitos que nos intersaban en la proposición 40, asegurando entonces que es no conmutativo de orden p^3.

Por último, el quinto grupo de orden p^3 protagonizó una sección completa, la sección 5.5 sobre el grupo de Heisemberg

$$\mathbb{H}_p = UT(3,p) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{3\times 3}(\mathbb{F}_p) \right\}.$$

Observación. Nótese que la exigencia de $p \geq 3$ para poder presentar los 5 grupos de la manera elegida radica en que la construcción matricial no aporta nada nuevo cuando $p = 2$, ya que $\mathbb{H}_2 = UT(3,2)$ es conmutativo.

6.4. Grupos de orden 8

Esta sección es importante para cerrar el estudio completo de los grupos de orden p^3. Como acabamos de mencionar, el caso $p = 2$ hay que abordarlo de manera algo distinta.

Sin embargo, para los grupos abelianos no cambia nada, es decir, tenemos:

$$\frac{\mathbb{Z}}{(8)}, \qquad \frac{\mathbb{Z}}{(4)} \times \frac{\mathbb{Z}}{(2)}, \quad \text{y} \quad \frac{\mathbb{Z}}{(4)} \times \frac{\mathbb{Z}}{(2)} \times \frac{\mathbb{Z}}{(2)}.$$

También la construcción del producto semidirecto

$$\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p)}$$

sigue siendo válida para $p = 2$.

Sin embargo, como bien adelantamos,

$$\mathbb{H}_2 = UT(3,2) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{3\times 3}(\mathbb{F}_2) \right\},$$

es abeliano. De hecho, es isomorfo a $\frac{\mathbb{Z}}{(4)} \times \frac{\mathbb{Z}}{(2)}$. Por tanto no lo consideramos.

Pero, sí disponemos de otro grupo no conmutativo de orden 8: el grupo cuaternio de Hamilton. Este grupo, debido al matemático dublinés que le dio el nombre en 1843, se descibe como el conjunto

$$Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$$

con la operación producto y las relaciones

- $ij = -ji = k$
- $-ik = ki = j$
- $jk = -kj = i$

Este grupo es bastante peculiar y bien conocido. Curiosamente, solo puede ser definido en el contexto de 2-grupos. Tiene propiedades intersantes, como que todos sus subgrupos son normales, algo que se dice, precisamente, ser hamiltoniano.

Con el grupo cuaternio cerramos la sección, así como el último hilo suelto de la clasificación de los grupos de orden p^3.

Capítulo 7

Grupos extraespeciales

Este capítulo entra en un tema bastante especializado de la teoría de grupos y supone un buen cierre del trabajo, recopilando algunos de los puntos que hemos ido exponiendo.

Definición 55. Un grupo **extraespecial** es un p-grupo G tal que:

- Su centro $Z(G)$ es un grupo cíclico de orden p.
- El cociente $G/Z(G)$ es un p-grupo abeliano elemental no trivial.

Nótese que no hay grupos extraespeciales de orden p porque incumplen la segunda condición de la definición previa. Tampoco hay grupos extraespeciales de orden p^2 por la proposición 13, ya que al ser abelianos su centro es todo el grupo y por tanto incumplen la primera condición de la definición de extraespecial.

Encontrar los grupos extraespeciales de orden p^3 es sencillo con todo el material visto, precisamente son los no abelianos. De hecho son los únicos por una argumentación similar a la de los grupos de orden p^2: en los grupos conmutativos su centro coincide con todo el grupo, de modo que la primera condición para ser extraespecial es imposible que la cumplan.

Con lo que hemos trabajado ya podemos verificar que los no abelianos de orden p^3 sí cumplen ambas condiciones. Recordemos que por la proposición 41 sabemos que el centro de cualquier grupo G no conmutativo de orden p^3 tiene orden p. Esto también garantiza que $|G/Z(G)| = \frac{|G|}{|Z(G)|} = p^2$. Por la proposición 13 cualquier grupo con p^2 elementos es abeliano. Además, $G/Z(G)$ ha de ser elemental, porque solo puede ser $\frac{\mathbb{Z}}{(p^2)}$ o $\frac{\mathbb{Z}}{(p)} \times \frac{\mathbb{Z}}{(p)}$, y si fuera cíclico entonces por la proposición 12 el grupo debería ser abeliano, en contra de nuestras condiciones.

De este modo y gracias a las secciones 6.3 y 6.4 aseguramos que:

- Si $p \geq 3$, los grupos extraespeciales de orden p^3 son $\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p)}$ y el grupo de Heisemberg $\mathbb{H}_p = UT(3, p)$.
- Si $p = 2$, los grupos extraespeciales de orden p^3 son $\frac{\mathbb{Z}}{(p^2)} \rtimes \frac{\mathbb{Z}}{(p)}$ y el grupo cuaternio de Hamilton.

La obtención de los grupos extraespeciales cuando la potencia de p es mayor que tres se logra definiendo otra construcción: el producto central. Entramos en detalles en la siguiente sección.

7.1. Producto central

El producto central es una construcción que guarda cierta relación con el producto directo, y considerando la importancia que ha tenido en esta memoria la vuelta de tuerca que le da el producto semidirecto, su definición ya no presentará grandes dificultades.

Hay dos posibilidades para el producto central, pero concretamente nos interesa la definición del producto central externo.

Definición 56. Dados dos grupos G y H con el mismo centro $Z = Z(G) = Z(H)$ definimos el conjunto

$$J = \{(a, b) : a, b \in Z, ab = 1\} = \{(a, a^{-1}) : a \in Z\}.$$

Entonces, decimos que el **producto central externo de G y H** es

$$G \otimes H = \frac{G \times H}{J}.$$

Observación. No hay convenio para la notación del producto externo, pero aquí consideraremos $\otimes$.

Nótese que siendo $Z = Z(G) = Z(H)$, el centro de $G \times H$ es $Z \times Z$. Además, al ser J un subgrupo de $Z \times Z$ tenemos que J es normal, lo que garantiza la correción de la definición 56.

Respecto a cardinalidad tenemos que si $|Z| = m$, entonces $|Z \times Z| = m^2$ y que $|J| = m$.
Es más,

$$\frac{Z \times Z}{J} \cong Z \quad \text{y} \quad Z(G \otimes H) \cong \frac{Z \times Z}{J} \cong Z = Z(G) = Z(H).$$

Volviendo al punto por el que nos interesaba el producto central, para la construcción de grupos extraespeciales de orden p^n con $n > 3$, demostramos la siguiente proposición:

Proposición 57. El producto central de dos p-grupos extraespeciales es extraespecial.

Demostración. Sean G y H dos grupos extraespeciales con el mismo centro $Z = Z(G) = Z(H)$, el cual es cíclico de orden p.

Veamos el cociente de $G \otimes H$ por su centro:

$$\frac{G \otimes H}{Z(G \otimes H)} = \frac{\frac{G \times H}{J}}{\frac{Z \times Z}{J}} \cong \frac{G \times H}{Z \times Z} \cong \frac{G}{Z} \times \frac{H}{Z},$$

donde la primera relación de isomorfía es consecuencia del segundo teorema de isomorfía.

Nótese que la expresión a la que hemos llegado es ya un producto de dos p-grupos abelianos elementales, luego

$$\frac{G \otimes H}{Z(G \otimes H)}$$

es también un p-grupo abeliano elemental.

■

Así pues, finalizaremos el trabajo detallando algunos ejemplos de construcción de grupos extraespeciales de orden p^n con $n > 3$. Sin embargo, antes cabe mencionar el siguiente resultado:

Proposición 58. Si G es un grupo extraespecial de orden p^n con $n > 3$, entonces puede escribirse como producto central de grupos extraespeciales de orden p^3.

En particular, el orden de tal G será p^{2m+1} para algún m natural.

La demostración no se detallará porque se sale de la línea de trabajo que sigue esta memoria, pero se puede consultar en la referencia bibiográfica [13]. Aún así, es curioso concretar que, dado un natural n, hay exactamente 2 grupos extraespeciales de orden $2n + 1$, de modo que a continuación resumimos cuales son. Nótese, que, como cabía esperar, se vuelve a distinguir entre el caso con $p = 2$ y $p \geq 3$:

- $p \geq 3$:
  - El producto central de n grupos extraespeciales de orden p^3 y exponente p.
    En este caso el grupo resultante tiene también exponente p.
  - El producto central de n grupos extraespeciales de orden p^3 con al menos un factor de exponente p^2.
    En este caso el grupo resultante tiene exponente p^2.
- $p = 2$:
  - El producto central de n grupos extraespeciales de orden 8, siendo un número impar de factores el grupo cuaternio de Hamilton.
  - El producto central de n grupos extraespeciales de orden 8, siendo un número par de factores el grupo cuaternio de Hamilton.

A continuación ya sí vamos a dar un ejemplo de como construir un grupo extraespecial de orden p^5 basándonos en el grupo de Heisenberg $\mathbb{H}_p = UT(3,p)$. Recordemos que su centro es

$$Z = Z(\mathbb{H}_p) = Z(UT(3,p)) = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{3\times 3}(\mathbb{F}_p) \right\}.$$

Ahora, siguiendo la misma notación que en la definición 56, el conjunto

$$J = \left\{ \left(\begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right) : c \in \mathbb{F}_p \right\}$$

nos permite construir el producto central

$$\mathbb{H}_p \otimes \mathbb{H}_p = \frac{\mathbb{H}_p \times \mathbb{H}_p}{J}.$$

Nótese que su orden es

$$|\mathbb{H}_p \otimes \mathbb{H}_p| = \left| \frac{\mathbb{H}_p \times \mathbb{H}_p}{J} \right| = \frac{p^3 \cdot p^3}{p} = p^5.$$

Se debe apreciar que este no es el único camino para construir grupos extraespeciales. Ya habíamos construido un grupo isomorfo a este $\mathbb{H}_p \otimes \mathbb{H}_p$ anteriormente, el ejemplo H_1 de la página 45. Recordamos su definición:

$$H_1 = \left\{ \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \in UT(4,p) \right\}.$$

Su exponente confirmamos que era p, y su centro es es sencillo de asegurar que es

$$Z(H_1) = \left\{ \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in UT(4,p) \right\},$$

que tiene orden p.

Podemos proseguir y conseguimos de esta forma grupos extraespeciales de orden p^{2n+1} y exponente p. Veamos el ejemplo de orden p^7, ya construido en el ejemplo B_2 de la página 35,

$$B_2 = \left\{ \begin{pmatrix} 1 & a & b & c & d \\ 0 & 1 & 0 & 0 & e \\ 0 & 0 & 1 & 0 & f \\ 0 & 0 & 0 & 1 & g \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in UT(5,p) \right\}.$$

En este caso también es fácil ver que

$$Z(B_2) = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 & d \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in UT(5,p) \right\},$$

lo que nos permite identificar un patrón que invita a declarar otro mecanismo para definir ciertos p-grupos extraespeciales con herramientas presentadas previamente.

Bibliografía

[1] G. Bagnera, La composizione dei gruppi finiti il cui grado è la quinta potenza di un numero primo, *Ann. Mat. Pura Appl.,* **3** no.1 (1898) 137–228.

[2] H. U. Besche, B. Eick, and E. A. O'Brien, The groups of order at most 2000, *Electron. Res. Announc. Amer. Math. Soc.,* **7** (2001) 1–4.

[3] D. Burrell, The number of p-groups of order 19683 and new lists of p-groups, *Communications in Algebra*, **51(6)** (2023) 2673–2679.

[4] Charles C. Sims, Enumerating p-groups, *Proceedings of the London Mathematical Society*, **15(3)** (1965) 151-166.

[5] Keith Conrad, Expository papers. `https://kconrad.math.uconn.edu/blurbs/`

[6] E. Z. Goren, *Group Theory. Notes for the course algebra 3*, McGill University (2003)

[7] John F. Humphreys, *A Course in Group Theory*, Oxford Science Publications (1996).

[8] R. James, M. F. Newman and E. A. O'Brien, The groups of order 128, *Journal of Algebra*, **129**(1990) 136–158.

[9] M. F. Newman, E. A. O'Brien and M. R. Vaughan-Lee, Groups and nilpotent Lie rings whose order is the sixth power of a prime, *J. Algebra*, **278** (2004) 383–401.

[10] E. A. O'Brien, The groups of order 256, *J. Algebra*, **143** (1991) 219–235.

[11] E. A. O'Brien and M. R. Vaughan-Lee, The groups with order p^7 for odd prime p, *J. Algebra*, **292** (2005) 243–258.

[12] Harvey E. Rose, *A Course on Finite Groups*, Springer (2009).

[13] M. A. Shabeeb and S. Srivastava, A study of extra special p-group, *Int. J. Sci. Engineering and Technology Research*, vol. 2, no. 19 (2013) 2223-2234.

[14] G. Sædén Ståhl, J. Laine, G. Behm, M. Boij, On p-groups of low power order, KTH Royal Institute of Technology, Sweden (2010).

[15] Michael Vaughan-Lee, Groups of order p^8 and exponent p, *Int. J. Group Theory*, **4** no. 4 (2015) 25-42.

[Wiki]

- Partition function (number theory). `https://en.wikipedia.org/wiki/Partition_function_(number_theory)`.
- Semidirect product. `https://en.wikipedia.org/wiki/Semidirect_product`.
- General linear group. `https://en.wikipedia.org/wiki/General_linear_group`

- Heisenberg group. https://en.wikipedia.org/wiki/Heisenberg_group
- Extra special group. https://en.wikipedia.org/wiki/Extra_special_group
- Central product. https://en.wikipedia.org/wiki/Central_product

[OEIS]

- OEIS A000041 Number of partitions of n. https://oeis.org/A000041
- OEIS A000679 Number of groups of order 2^n. https://oeis.org/A000679
- OEIS A090091 Number of groups of order 3^n. https://oeis.org/A090091
- OEIS A000001 Number of groups of order n. https://oeis.org/A000001