UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

Serie Anuladora Superior de un Anillo de Endomorfismos Finito

TESIS

que para obtener el título de:

Matemático

presenta:

Marcos Zyman Reinisch

Directora de Tesis:

Dra. María Alicia Aviñó Díaz

DIVISION DE ESTUDIOS PROFESIONALES

277473

FACULTAD DE CIENCIAS
SECCION ESCOLAR

MEXICO, D. F. 2000

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Serie Anuladora Superior de un Anillo de Endomorfismos Finito

Tesis que para obtener el título de Matemático presenta:

Marcos Zyman Reinisch

Facultad de Ciencias

Universidad Nacional Autónoma de México

Directora de Tesis:

Dra. María Alicia Aviñó Díaz

28 de mayo, 1999

UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MEXICO

MAT. MARGARITA ELVIRA CHÁVEZ CANO
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo de Tesis:

"Serie Anuladora Superior de un Anillo de Endomorfismos Finito"

realizado por Marcos Zyman Reinisch

con número de cuenta 9355096-1 , pasante de la carrera de Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis
Propietario Dra. María Alicia Aviñó Díaz

Propietario Dr. Raymundo Bautista Ramos

Propietario Dr. Ernesto Vallejo Ruiz

Suplente Dr. Rodolfo San Agustín Chi

Suplente M.en C. Mary Glazman Nowalski

Consejo Departamental de Matemáticas

A Adriana... por supuesto

Agradecimientos

Deseo expresar mis más afectuosos agradecimientos a:

María Alicia Aviñó, por ser una incomparable directora y maestra;

Raymundo Bautista y Ernesto Vallejo, por sus aportaciones y sugerencias;

Phill Schultz, por sus importantes contribuciones al capítulo II;

mis queridos padres: Sarita y Salomón, por su apoyo constante e incondicional;

mis fabulosos hermanos: Jayele, Sami y Jacobo. Sin la asistencia técnica de Jacobo, este trabajo no hubiera podido ser;

mis profesores y amigos, quienes indirecta o directamente participaron en la elaboración de esta tesis, así como en las angustias y alegrías.

¡Gracias a todos!

INTRODUCCIÓN

El estudio del anillo de endomorfismos y el grupo de automorfismos de un p-grupo abeliano finito G fue iniciado por K. Shoda en 1928 en su trabajo "Über die Automorphismen einer endlichen abelschen Gruppe" (ver referencia [8]). Posteriormente, R. S. Pierce en "Homomorphisms of Primary Abelian Groups" (ver [6]) estudia, entre otras cosas, las propiedades del radical del anillo $EndG$.

En el trabajo de M. A. Aviñó y R. Bautista "The Upper Annihilating Series of the Radical of the Endomorphism Ring of a Finite Abelian p-Group" [2] se desarrolla un método para determinar la serie central superior del máximo p-subgrupo normal de $AutG$.

En este trabajo calculamos la serie anuladora superior de un subanillo S asociado a un p-subgrupo de Sylow $P = S + I$ del grupo $AutG$, donde G se un grupo de tipo $(p^{n_1}, p^{n_1}, p^{n_2}, p^{n_2})$; con $n_1 > n_2$. Se extiende el concepto de serie anuladora para un subanillo, ya que en [2] aparece la definición para un ideal del anillo.

Esta tesis está dividida en tres capítulos.

En el primero estudiamos la teoría general de los p-grupos y de los grupos nilpotentes, así como el teorema fundamental de los grupos abelianos finitamente generados. En estos resultados se basa el desarrollo posterior del trabajo.

En el capítulo II presentamos conceptos y resultados acerca del anillo de endomorfismos $EndG$ y grupo de automorfismos $AutG$ de un p-grupo abeliano finito G de tipo $(p^{n_1}, p^{n_1}, p^{n_2}, p^{n_2})$ donde $n_1 > n_2$ y p es un número primo fijo. También definimos los conceptos de anulador y serie anuladora superior de un subanillo S de $EndG$.

El tercer capítulo constituye una caracterización de los ideales y anuladores de S, así como el cálculo de la longitud de la serie anuladora superior de S. Esta longitud es una cota superior para el grado de nilpotencia de un p-subgrupo de Sylow de $AutG$.

Destacamos por último que los resultados y cálculos del tercer capítulo son originales.

Índice General

Capítulo 1

Teoría General de los p-Grupos y de los Grupos Abelianos Finitamente Generados

En el curso del trabajo p denotará un número primo.

En este capítulo presentamos la teoría de los grupos abelianos y los p-grupos necesaria para el desarrollo del trabajo. Lo hemos dividido en dos secciones: la primera trata de los p-grupos y los grupos nilpotentes, y la segunda del teorema fundamental de los grupos abelianos finitamente generados.

p-Grupos y Grupos Nilpotentes

Definición Un grupo G es un **p-grupo** si todo elemento de G tiene orden una potencia del primo p. Un subgrupo de G es un **p-subgrupo** si el subgrupo es, él mismo, un p-grupo.

Definición Un **p-subgrupo de Sylow** de un grupo G es un p-subgrupo de orden máximo en G. Es decir, un p-subgrupo de G que no está contenido en ningún p-subgrupo mayor.

Definición Decimos que un grupo abeliano G es **suma directa** de algunos de sus subgrupos

$$G_1, G_2..., G_k$$

si todo elemento de G se expresa de manera única como

$$\sum_{i=1}^{k} g_i$$

donde cada $g_i \in G_i$. Escribimos entonces

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_k.$$

Definición Un grupo cíclico finito, cuyo orden es una potencia de un número primo p, es llamado **grupo cíclico primario** respecto a p.

Definición Un conjunto

$$\{x_1, ..., x_r\}$$

de elementos distintos de cero en un grupo abeliano es llamado **independiente** si siempre que existan $m_1, ..., m_r$ números enteros, tales que

$$\sum m_i x_i = 0$$

entonces

$$m_i x_i = 0$$

para toda i.

Lema 1.1 *Sea G un grupo abeliano. Entonces $\{x_1, ..., x_r\} \subset G$ es independiente si y sólo si*

$$\langle x_1, ..., x_r \rangle = \langle x_1 \rangle \oplus ... \oplus \langle x_r \rangle .$$

Demostración. La demostración de este lema es una consecuencia directa de las definiciones de independencia y suma directa. ■

Definición Sea G un p-grupo abeliano finito. Una **p-base** de G es un conjunto generador independiente. Es decir, $\{a_1, ..., a_n\}$ es una p-base de G si y sólo si

$$G = \oplus_{i=1}^{n} \langle a_i \rangle .$$

La demostración del siguiente teorema está en [7].

Teorema 1.1 (de la base de Burnside, 1912) *Si G es un p-grupo finito, entonces cualesquiera dos conjuntos generadores mínimales de G tienen la misma cardinalidad*

Como consecuencia del teorema 1.1, tenemos que todas las p-bases de un p-grupo abeliano finito tienen el mismo número de elementos.

Nuestro primer objetivo es caracterizar a los p-grupos finitos como aquéllos que tienen orden una potencia del primo p. Para esto necesitamos algunos resultados.

Lema 1.2 *Sean G un grupo y $g \in G$. Si $o(g) = m$ y $g^k = 1$, entonces m divide a k.*

Demostración. Por el algoritmo de la división,

$$k = mq + r$$

donde q, $r \in \mathbf{Z}$ y $0 \leq r < m$. Ahora:

$$g^k = g^{mq+r} = g^{mq} g^r = g^r = 1.$$

Si $r \neq 0$ tenemos que

$$o(g) \leq r$$

lo cual sería imposible pues

$$o(g) = m > r.$$

Entonces, $r = 0$ y por tanto m divide a k. ■

Lema 1.3 *Sean G y H dos grupos y sea $a \in G$ tal que $o(a)$ es finito. Supongamos también que*

$$f : G \to H$$

es un homomorfismo de grupos. Entonces $o(f(a))$ divide a $o(a)$.

Demostración.

$$(f(a))^{o(a)} = f(a)...f(a) = f(a...a) =$$

$$= f(1) = 1$$

Entonces $o(f(a))$ divide a $o(a)$ por el lema 1.2. ■

Lema 1.4 *Si G es un grupo abeliano finito y su orden es divisible por un primo p, entonces G contiene un elemento de orden p.*

Demostración. Sea $x \in G$, $x \neq 1$. Supongamos, como primer caso, que

$$o(x) = pm$$

para algún natural m. Entonces

$$o(x^m) = p$$

pues

$$(x^m)^p = x^{pm} = 1$$

y p es el menor entero positivo que satisface esta propiedad, ya que de lo contrario tendríamos

$$o(x) < pm.$$

Esto significa que x^m tiene orden p.

Supongamos ahora, como segundo caso, que

$$o(x) = t$$

con $(p, t) = 1$. Como G es abeliano,

$$\langle x \rangle \lhd G \text{ y } \left| \frac{G}{\langle x \rangle} \right| = \frac{|G|}{t}$$

por el teorema de Lagrange.

Mostraremos por inducción sobre $|G|$ que G tiene un elemento de orden p. Para la base de inducción, suponemos que G es de orden mínimo tal que p divide a $|G|$. Es decir,

$$|G| = p, \text{ y por tanto } G \simeq \mathbf{Z}_p.$$

Así, todo elmento de G distinto de la identidad genera a G. Esto significa que G es cíclico de orden p y por tanto tiene elementos de ese orden. Luego, la base de inducción es válida.

Fijamos el número $|G|$ y suponemos que el resultado vale para todos los grupos de orden menor que $|G|$ divisibles por p. Observamos que

$$\frac{|G|}{t}$$

es divisible por p pues

$$(t,p) = 1 \text{ y } p \text{ divide a } |G|.$$

Además,

$$\frac{|G|}{t} < |G|.$$

Por hipótesis de inducción, existe

$$\overline{y} \in \frac{G}{\langle x \rangle}$$

tal que

$$o(\overline{y}) = p.$$

Consideramos el homomorfismo canónico

$$\eta : G \to \frac{G}{\langle x \rangle}$$

y notamos que

$$\eta(y) = \overline{y}.$$

Por el lema 1.3, $o(\overline{y})$ divide a $o(y)$. Luego p divide a $o(y)$; es decir:

$$o(y) = pm',$$

y hemos vuelto al primer caso. Así, $y^{m'}$ es un elemento de G de orden p. ■

Lema 1.5 *Sea G un grupo. El número de conjugados de x en G es*

$$[G : C(x)]$$

donde $C(x)$ denota al subgrupo centralizador de x. Por tanto, este número es un divisor de $|G|$ si G es finito.

Demostración. Sean a y b elementos de G. Primero mostraremos que las siguientes condiciones son equivalentes:

(i) $axa^{-1} = bxb^{-1}$.

(ii) $a^{-1}b$ conmuta con x.

(iii) $a^{-1}b \in C(x)$.
(iv) a y b pertenecen a la misma clase lateral izquierda de $C(x)$.
(i)$\Rightarrow$(ii) $axa^{-1} = bxb^{-1} \Rightarrow axa^{-1}b = bx \Rightarrow x(a^{-1}b) = (a^{-1}b)x$.
Luego $a^{-1}b$ conmuta con x.
(ii)$\Rightarrow$(iii) Por definición de $C(x)$, si $a^{-1}b$ conmuta con x, entonces $a^{-1}b \in C(x)$.
(iii)$\Rightarrow$(iv) Sabemos que $aC(x) = bC(x) \Leftrightarrow a^{-1}b \in C(x)$.
(iv)$\Rightarrow$(i) $aC(x) = bC(x) \Rightarrow a^{-1}b \in C(x) \Rightarrow a^{-1}bx = xa^{-1}b \Rightarrow$
$bx = axa^{-1}b \Rightarrow bxb^{-1} = axa^{-1}$.
Por lo tanto las cuatro condiciones son equivalentes.

Definimos Ψ : {conjugados distintos de x} $\rightarrow$ {clases laterales izquierdas de $C(x)$} como

$$\Psi(axa^{-1}) = aC(x).$$

Ψ está bien definida: si $axa^{-1} = bxb^{-1}$, entonces a y b pertenecen a la misma clase lateral izquierda de $C(x)$, y tenemos que

$$aC(x) = bC(x).$$

Ψ es inyectiva: si $aC(x) = bC(x)$, entonces

$$axa^{-1} = bxb^{-1}.$$

Finalmente, Ψ es sobre pues para cualquier clase lateral izquierda $aC(x)$,

$$\Psi(axa^{-1}) = aC(x).$$

De aquí que Ψ es una biyección. Esto completa la demostración. ■

A continuación, demostramos un teorema de Cauchy:

Teorema 1.2 *Si G es un grupo finito cuyo orden es divisible por un primo p, entonces G tiene un elemento de orden p.*

Demostración. Podemos suponer que G no es abeliano, pues el caso abeliano está cubierto por el lema 1.4. Como G no es abeliano, existe $x \in G$ tal que

$$x \notin Z(G),$$

donde $Z(G)$ denota el centro de G. Luego, existe $y \in G$ tal que $xy \neq yx$. Entonces $y \notin C(x)$ y se tiene

$$|C(x)| < |G|.$$

Supongamos primero que p divide a $|C(x)|$. Procedemos por inducción sobre $|G|$, donde G es un grupo cuyo orden es divisible por p. El orden mínimo que puede tener G es p, de modo que verificar la base de inducción es suponer $|G| = p$. Si esto ocurre, G es cíclico de orden p, y tiene un elemento de ese orden.

Supongamos ahora el resultado para grupos de orden menor al número fijo $|G|$. Por hipótesis de inducción, $C(x)$ tiene un elemento de orden p, y por tanto G también. Esto completa la prueba en caso de que p divide a $|C(x)|$.

Consideremos ahora el caso en que p no divide a $|C(x)|$ para ningún x, elemento de $G \setminus Z(G)$. Como

$$|G| = [G : C(x)]\,|C(x)|$$

y p divide a $|G|$, entonces p divide a $[G : C(x)]$ para toda $x \in G \setminus Z(G)$ (aquí utilizamos el hecho de que p es primo). Consideramos ahora la partición de G en clases de conjugación. Sabemos que para todo $a \in Z(G)$, $\{a\}$ es una clase de conjugación. Al contar los elementos de G obtenemos la siguiente ecuación:

$$|G| = |Z(G)| + \sum_{x \in \Lambda} |Cl(x)|$$

donde Λ es un conjunto completo de elementos no conjugados que no pertenecen a $Z(G)$ y $Cl(x)$ denota la clase de conjugación de x.

Si $x \in G \setminus Z(G)$, por el lema 1.5,

$$|Cl(x)| = [G : C(x)]$$

($|Cl(x)|$es el número de conjugados distintos de x). Entonces

$$|G| = |Z(G)| + \sum_{\substack{x \in \Lambda \\ \text{ecuación de clase}}} [G : C(x)] \tag{1.1}$$

Como p divide a $[G : C(x)]$ para toda $x \in G \setminus Z(G)$, p también divide a

$$\sum_{x \in \Lambda} [G : C(x)]\,.$$

Además, p divide a $|G|$. Por lo tanto p divide a $|Z(G)|$.

Puesto que $Z(G)$ es un grupo abeliano finito cuyo orden es divisible por p, $Z(G)$ contiene un elemento de orden p por el lema 1.4. Además $Z(G) < G$ y por tanto G contiene un elemento de orden p. De este modo concluimos la demostración. ■

El siguiente corolario caracteriza a los p-grupos finitos como los que tienen orden una potencia de p.

Corolario 1.1 *Un grupo finito G es un p-grupo si y sólo si $|G|$ es una potencia de p.*

Demostración. Supongamos que $|G| = p^m$. Sea $x \in G$. Mostraremos que $o(x)$ es una potencia de p. En efecto, por el teorema de Lagrange: $|\langle x \rangle|$ divide a p^m. Esto significa que $|\langle x \rangle| = o(x)$ es una potencia de p. Luego, G es un p-grupo.

Inversamente, sea G un p-grupo finito. Para obtener una contradicción, supongamos que existe un primo q tal que $q \neq p$ y q divide a $|G|$. Por el teorema de Cauchy (1.2), G contiene un elemento de orden q. Esto contradice el hecho de que G es un p-grupo. Por lo tanto, $|G|$ es una potencia de p. De este modo concluimos la prueba del corolario. ■

Nuestro siguiente objetivo es definir a los grupos nilpotenetes y mostrar que todo p-grupo finito es nilpotente.

Definición Sea G un grupo. Una **serie normal** de G es una sucesión finita $G_0, G_1, ..., G_m$ de subgrupos normales de G tal que

$$1 = G_0 \leq G_1 \leq ... \leq G_m = G. \tag{1.2}$$

Definición Una serie normal de la forma 1.2 se llama **serie central** si todos sus factores son centrales. Es decir, si

$$\frac{G_{i+1}}{G_i} \leq Z\left(\frac{G}{G_i}\right)$$

para toda $i = 0, ..., m-1$. El número natural m es la **longitud** de la serie.

Definición Decimos que un grupo es **nilpotente** si tiene una serie central.

Definición Sea N un grupo nilpotente. Definimos el **grado de nilpotencia** de N como la longitud mínima de todas las series centrales en N.

Antes de probar que todo p-grupo finito es nilpotente, enunciamos y demostramos algunos resultados.

Teorema 1.3 *Si $G \neq 1$ es un p-grupo finito, entonces su centro $Z(G)$ es no trivial.*

Demostración. Supongamos que G es abeliano, entonces

$$Z(G) = G \neq 1$$

y el teorema es válido. Procedemos con la demostración para un grupo G no abeliano, es decir, suponemos que $G \neq Z(G)$. Consideremos de nuevo la ecuación 1.1:

$$|G| = |Z(G)| + \sum_{x \in \Lambda} [G : C(x)]$$

donde, igual que antes, Λ es un conjunto completo de elementos no conjugados de G que se encuentran fuera de $Z(G)$. Para cada $x \in \Lambda$, mostraremos que $C(x)$ es un subgrupo propio de G. En efecto, como $x \in \Lambda$ se cumple $x \notin Z(G)$. Luego, existe $y \in G$ tal que $xy \neq yx$ y por tanto $y \notin C(x)$. Así,

$$C(x) \subsetneq G.$$

Sea $x \in \Lambda$. Por el teorema de Lagrange, sabemos que

$$|G| = [G : C(x)]\,|C(x)|\,.$$

Como G es un p-grupo, por el corolario 1.1 tenemos que $|G| = p^m$. Puesto que $C(x) \lneq G$ se sigue que

$$|C(x)| = p^k$$

con $0 < k < m$. (Observamos que $x \notin Z(G)$ implica $x \neq 1$. Como

$$x \in C(x), \text{ se tiene } C(x) \neq 1.$$

Luego $0 < k$). Por lo anterior,

$$[G : C(x)] = p^l$$

donde $0 < l < m$. Notamos que $0 < l$ pues si $l = 0$, tendríamos

$$[G : C(x)] = 1$$

y $C(x) = G$; pero esto contradiría el hecho de que $C(x)$ es un subgrupo propio de G.

Luego p divide a

$$\sum_{x \in \Lambda} [G : C(x)]\,.$$

Por la ecuación 1.1, p divide a $|Z(G)|$. Por tanto

$$Z(G) \neq 1.$$

Esto concluye la demostración. ■

Lema 1.6 *Si G es un grupo y $H \lhd G$, entonces todo subgrupo de*

$$\frac{G}{H}$$

es de la forma

$$\frac{W}{H}$$

donde W es un subgrupo de G que contiene a H.

Demostración. Sea K un subgrupo de

$$\frac{G}{H}.$$

Sea

$$W = \{g \in G : gH \in K\}\,.$$

Veremos que W es un subgrupo de G que contiene a H:

(i) Si $w_1, w_2 \in W$ tenemos

$$w_1H, w_2H \in K,$$

luego

$$(w_1H)(w_2H) = w_1w_2H \in K$$

y por tanto

$$w_1w_2 \in W.$$

Así, W es cerrado bajo la operación binaria de G.

(ii) Como K es subgrupo de

$$\frac{G}{H},$$

entonces

$$1H \in K, \text{ de donde } 1 \in W.$$

Por lo tanto, la identidad de G está en W.

(iii) Sea $w \in W$. Mostraremos que $w^{-1} \in W$. En efecto, $w \in W$ implica que $wH \in K$. Como K es sugrupo de

$$\frac{G}{H},$$

$$(wH)^{-1} \in K$$

y

$$(wH)^{-1} = w^{-1}H \in K.$$

Por lo tanto,

$$w^{-1} \in W.$$

Así concluimos que W es un sugrupo de G.

Además, $H \subset W$ pues si $h \in H$, entonces $hH = 1H \in K$ y $h \in W$. Más aún, como $H \lhd G$ y $H \leq W$, entonces $H \lhd W$.

Lo único que falta ahora es mostrar que

$$\frac{W}{H} = K,$$

lo cual se cumple pues si

$$wH \in \frac{W}{H}$$

debe ocurrir que $w \in W$ y por definición de W se tiene que $wH \in K$. Inversamente, si $wH \in K$, entonces $w \in W$ y

$$wH \in \frac{W}{H}.$$

Luego

$$K = \frac{W}{H}.$$

Con esto concluimos la prueba del lema. ■

Lema 1.7 *Un grupo factor de un p-grupo es nuevamente un p-grupo.*

Demostración. Sean G un p-grupo y $H \lhd G$. Probaremos que

$$\frac{G}{H}$$

es un p-grupo. Sea

$$\overline{g} \in \frac{G}{H}.$$

Como G es p-grupo, se tiene que $o(g) = p^m$ y por tanto $(\overline{g})^{p^m} = \overline{g^{p^m}} = \overline{1}$. Por el lema 1.2, $o(\overline{g})$ divide a p^m. Esto significa que $o(\overline{g})$ es una potencia de p.

Por lo tanto

$$\frac{G}{H}$$

es un p-grupo. ■

Teorema 1.4 *Todo p-grupo finito es nilpotente.*

Demostración. Sea G un p-grupo finito. Nuestro objetivo es construir una serie central para G.

Si G es abeliano,

$$1 < G$$

es una serie normal y central pues claramente

$$\frac{G}{1} \leq Z\left(\frac{G}{1}\right) = \frac{G}{1} \simeq G.$$

Supongamos que G es no abeliano y por tanto no trivial. Sea H un subgrupo normal propio de G. Por el lema 1.7,

$$\frac{G}{H}$$

es p-grupo. Como H es propio,

$$\frac{G}{H} \neq 1.$$

Luego,

$$\frac{G}{H}$$

es un p-grupo finito no trivial. Por el teorema 1.3,

$$Z\left(\frac{G}{H}\right) \neq 1.$$

Utilizando el lema 1.6,

$$Z\left(\frac{G}{H}\right) = \frac{H_1}{H}$$

donde H_1 es un subgrupo de G que contiene a H. Puesto que

$$1 \neq Z\left(\frac{G}{H}\right) = \frac{H_1}{H},$$

H es un subgrupo propio de H_1.

Veremos ahora que H_1 es normal en G.

Sean $a \in G$, $x \in H_1$. Entonces

$$(a^{-1}xa)H = (a^{-1}H)(xH)(aH) \in \frac{H_1}{H}$$

pues

$$\frac{H_1}{H} = Z\left(\frac{G}{H}\right) \lhd \frac{G}{H}.$$

Así,

$$a^{-1}xa \in H_1.$$

Por lo tanto H_1 es normal en G. Hemos construido un subgrupo normal H_1 de G tal que

$$H \lneq H_1 \text{ y } Z\left(\frac{G}{H}\right) = \frac{H_1}{H}.$$

Consideramos al subgrupo normal H_1 y mediante el mismo procedimiento obtenemos un subgrupo normal H_2 tal que

$$H \lneq H_1 \lneq H_2 \text{ y } Z\left(\frac{G}{H_1}\right) = \frac{H_2}{H_1}.$$

Renombrando a estos subgrupos normales como G_i obtenemos una serie normal de la forma:

$$1 = G_0 \lneq G_1 \lneq G_2 \lneq \ldots \tag{1.3}$$

Como G es finito, la serie 1.3 debe terminar; de modo que existe un m tal que esta serie es en realidad

$$1 = G_0 \lneq G_1 \lneq G_2 \lneq \ldots \lneq G_m = G \tag{1.4}$$

En 1.4 se cumple además que

$$\frac{G_{i+1}}{G_i} = Z\left(\frac{G}{G_i}\right)$$

para toda $i = 0, \ldots, m-1$. Luego, 1.4 es una serie central de longitud m.

Por lo tanto, G es nilpotente. ■

Grupos Abelianos Finitamente Generados

Primero enunciamos y probamos resultados que conducen al teorema fundamental de los grupos abelianos finitamente generados.

Teorema 1.5 *Sea X un subconjunto de un grupo abeliano G no trivial. Las siguientes condiciones son equivalentes:*

(i) Cada elemento distinto de cero de G se expresa de manera única como

$$n_1x_1 + .. + n_rx_r$$

con $n_i \neq 0$, $n_i \in \mathbf{Z}$ para toda i y x_i distintos en X.

(ii) X genera a G y

$$n_1x_1 + ... + n_rx_r = 0$$

para $n_i \in \mathbf{Z}$ y $x_i \in X$ distintos, si y sólo si

$$n_i = 0$$

para toda i.

Demostración. Mostraremos primero la validez de la condición (ii) sabiendo que se cumple la condición (i). Como G es no trivial $X \neq 0$. Además $0 \notin X$ pues si $0 \in X$, entonces $x = x + 0$ para algún $x \in X$, $x \neq 0$ contradiciendo la unicidad de la expresión para x indicada en (i).

Por (i) X genera a G y

$$n_1x_1 + ... + n_rx_r = 0$$

si

$$n_1 = ... = n_r = 0.$$

Supongamos ahora que

$$n_1x_1 + ... + n_rx_r = 0$$

donde las x_i son distintas y alguna $n_j \neq 0$. Probaremos que esto no es posible. En efecto, omitiendo los términos con coeficiente cero y renumerando podemos asumir que todas las n_i son distintas de cero y

$$n_1x_1 + ...n_rx_r = 0.$$

De aquí tenemos que:

$$\begin{aligned} x_1 &= x_1 + n_1x_1 + ... + n_rx_r \\ &= (n_1 + 1)x_1 + ... + n_rx_r \end{aligned}$$

lo cual significa que existen dos maneras de expresar a $x_1 \neq 0$ contradiciendo así la unicidad indicada en (i). De este modo, (i) implica (ii)

Supongamos ahora (ii). Sea $a \in G$, $a \neq 0$. Como X genera a G podemos escribir

$$a = n_1 x_1 + ... n_r x_r.$$

Supongamos que a tiene otra expresión en términos de los elementos de X, a saber,

$$a = m_1 x_1 + ... + m_r x_r.$$

(Nótese que si algunos términos son cero es posible considerar el mismo número de sumandos en ambas expresiones). Restando:

$$0 = (n_1 - m_1)x_1 = ... = (n_r - m_r)x_r;$$

por (ii):

$$0 = n_1 - m_1 = ... = n_r - m_r$$

por lo tanto

$$n_i = m_i$$

para toda i. Así mostramos que la expresión para a es única y se cumple la condición (i). Este hecho concluye la prueba del teorema. ■

Definición Un grupo abeliano G con un conjunto generador X no vacío que satisface las condiciones del teorema 1.5 se llama **abeliano libre** y X se llama **base** de G.

Teorema 1.6 *Si G es un grupo abeliano libre no trivial con una base de r elementos, entonces*

$$G \simeq \mathbf{Z}^r.$$

Demostración. Sea

$$X = \{x_1, ..., x_r\}$$

una base de G. Sea $a \in G$, $a \neq 0$. Como X es base, a se expresa de manera única como

$$n_1 x_1 + ... + n_r x_r.$$

Sea

$$\Phi : G \to \mathbf{Z} \times \cdots \times \mathbf{Z}$$

dada por

$$a \longmapsto (n_1, ..., n_r).$$

Como la expresión para a es única, Φ está bien definida. Además, claramente Φ es inyectiva. Sea

$$(m_1, ..., m_r) \in \mathbf{Z} \times \cdots \times \mathbf{Z}.$$

Entonces

$$b = m_1 x_1 + \cdots + m_r x_r \in G$$

y

$$\Phi(b) = (m_1, ..., m_r).$$

Luego Φ es sobreyectiva. Por lo tanto Φ es una biyección. Mostraremos a continuación que Φ es morfismo de grupos. En efecto, sean

$$a = n_1x_1 + \cdots + n_rx_r$$

y

$$b = m_1x_1 + \cdots m_rx_r.$$

Entonces

$$\Phi(a+b) = \Phi\left[(n_1+m_1)x_1 + \cdots (n_r+m_r)x_r\right] =$$

$$= (n_1+m_1, ..., n_r+m_r) = (n_1, ..., n_r) + (m_1, ..., m_r) =$$

$$= \Phi(a) + \Phi(b).$$

Así, Φ es isomorfismo. ■

Teorema 1.7 *Sea G un grupo abeliano libre no trivial con una base finita. Entonces cada base de G es finita y todas ellas tienen el mismo número de elementos.*

Demostración. Sea

$$X = \{x_1, ..., x_r\}$$

una base de G. Por el teorema anterior

$$G \simeq \mathbf{Z}^r.$$

Consideremos

$$2G = \{2g : g \in G\},$$

el cual es un subgrupo de G. Por un razonamiento análogo al de la demostración del teorema 1.6

$$2G \simeq (2\mathbf{Z})^r.$$

Luego

$$\frac{G}{2G} \simeq \frac{\mathbf{Z}^r}{(2\mathbf{Z})^r}.$$

Mostraremos ahora que

$$\frac{\mathbf{Z}^r}{(2\mathbf{Z})^r} \simeq (\mathbf{Z}_2)^r.$$

Sea

$$\Psi : \mathbf{Z}^r \to (\mathbf{Z}_2)^r$$

definida como

$$(a_1, ..., a_r) \longmapsto (\overline{a_1}, ..., \overline{a_r}).$$

Ψ es una función sobeyectiva. Además, Ψ es morfismo pues:

$$\Psi\left[(a_1, ..., a_r) + (b_1, ..., b_r)\right] = \Psi(a_1 + b_1, ..., a_r + b_r) =$$

$$= \left(\overline{a_1 + b_1}, ..., \overline{a_r + b_r}\right) = \left(\overline{a_1} + \overline{b_1}, ..., \overline{a_r} + \overline{b_r}\right) =$$

$$= (\overline{a_1}, ..., \overline{a_r}) + \left(\overline{b_1}, ..., \overline{b_r}\right) = \Psi(a_1, ..., a_r) + \Psi(b_1, ..., b_r).$$

A continuación probaremos que el núcleo de Ψ es precisamente $2\mathbf{Z} \times \cdots \times 2\mathbf{Z}$. En efecto:

$$(a_1, ..., a_r) \in Ker\Psi \text{ si y sólo si } \Psi(a_1, ..., a_r) = (\overline{a_1}, ..., \overline{a_r}) = \left(\overline{0}, ..., \overline{0}\right)$$

si y sólo si

$$a_i \in 2\mathbf{Z}$$

para toda i, y lo anterior courre si y sólo si

$$(a_1, ..., a_r) \in 2\mathbf{Z} \times \cdots \times 2\mathbf{Z}.$$

Por lo tanto

$$Ker\Psi = 2\mathbf{Z} \times \cdots \times 2\mathbf{Z}.$$

Por el teorema del homomorfismo concluimos que

$$\frac{\mathbf{Z} \times \cdots \times \mathbf{Z}}{2\mathbf{Z} \times \cdots \times 2\mathbf{Z}} \simeq \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2.$$

Así,

$$\frac{G}{2G} \simeq \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2.$$

Esto significa que

$$\left|\frac{G}{2G}\right| = 2^r.$$

Si X_1 es cualquier otra base de G tal que $|X_1| = m$, llevando a cabo el mismo procedimiento tendríamos que

$$\frac{G}{2G} \simeq \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2 \ (m \text{ veces}).$$

Por tanto

$$\left|\frac{G}{2G}\right| = 2^m = 2^r$$

y

$$m = r.$$

Lo anterior significa que cualesquiera dos bases finitas de G tienen el mismo número de elementos.

Como último paso mostraremos que G no puede tener bases infinitas. Sea Y cualquier base de G y sean $y_1, ..., y_s$ elementos distintos de Y. Sea H el subgrupo de G generado por

$$Y_1 = \{y_1, ..., y_s\}$$

y K el subgrupo generado por

$$Y_2 = Y \setminus \{y_1, ..., y_s\}.$$

Probaremos que $G \simeq H \times K$. Sea $a \in G$, entonces

$$a = \sum_{y_{1_i} \in Y_1} n_i y_{1_i} + \sum_{y_{2_j} \in Y_2} m_j y_{2_j}$$

y esta expresión es única. Definimos $\Phi : G \to H \times K$ como

$$a \longmapsto \left(\sum_{y_{1_i} \in Y_1} n_i y_{1_i}, \sum_{y_{2_j} \in Y_2} m_j y_{2_j} \right)$$

Por la unicidad de la expresión para a, ésta es una función bien definida. Además Φ es inyectiva: supongamos que $\Phi(a) = \Phi(b)$ donde

$$a = \sum_{y_{1_i} \in Y_1} n_i y_{1_i} + \sum_{y_{2_j} \in Y_2} m_j y_{2_j}$$

y

$$b = \sum_{\widetilde{y_{1_i}} \in Y_1} \widetilde{n}_i y_{1_i} + \sum_{\widetilde{y_{2_j}} \in Y_2} \widetilde{m_j} y_{2_j}$$

entonces

$$\left(\sum_{y_{1_i} \in Y_1} n_i y_{1_i}, \sum_{y_{2_j} \in Y_2} m_j y_{2_j} \right) = \left(\sum_{y_{1_i} \in Y_1} \widetilde{n}_i y_{1_i}, \sum_{y_{2_j} \in Y_2} \widetilde{m_j} y_{2_j} \right).$$

Luego

$$\sum_{y_{1_i} \in Y_1} n_i y_{1_i} = \sum_{y_{1_i} \in Y_1} \widetilde{n}_i y_{1_i}$$

y

$$\sum_{y_{2_j} \in Y_2} m_j y_{2_j} = \sum_{y_{2_j} \in Y_2} \widetilde{m_j} y_{2_j}.$$

Como Y es base de G, debemos tener $n_i = \widetilde{n}_i$ y $m_j = \widetilde{m_j}$ para toda j e i. De aquí tenemos que $a = b$ y Φ es inyectiva. Claramente Φ es sobreyectiva. Realizando

cálculos directos, se verifica que Φ es morfismo. Luego Φ es un isomorfismo de grupos. Por lo tanto,

$$G \simeq H \times K.$$

De aquí tenemos los isomorfismos:

$$\frac{G}{2G} \simeq \frac{H \times K}{2H \times 2K} \simeq \frac{H}{2H} \times \frac{K}{2K}.$$

Por el análisis del inicio de la desmostración sabemos que

$$\left|\frac{H}{2H}\right| = 2^s$$

y por tanto

$$2^r = \left|\frac{G}{2G}\right| \geq 2^s$$

(estamos suponiendo, como al principio, que G tiene una base finita de r elementos). Así, $r \geq s$. Esto significa que Y no puede ser infinito, pues de lo contrario podríamos tomar $r < s$. De este modo concluimos la demostración. ■

Definición Sea G un grupo abeliano libre. Definimos el **rango** de G como el número de elementos en cualquier base de G.

Teorema 1.8 *Sea G un grupo abeliano finitamente generado, con conjunto generador $\{a_1, ...a_n\}$. Sea*

$$\Phi : \mathbf{Z} \times \cdots \times \mathbf{Z} \to G$$

definida por

$$(h_1, ..., h_n) \longmapsto h_1a_1 + \cdots + h_na_n.$$

Entonces Φ es epimorfismo.

Demostración. Es claro que Φ es una función bien definida. Si $a \in G$, entonces

$$a = h_1a_1 + \cdots h_na_n$$

pues G está generado por $\{a_1, ..., a_n\}$. Luego,

$$\Phi(h_1, ..., h_n) = a.$$

Esto muestra que Φ es sobreyectiva. Por último, veremos que es morfismo:

$$\Phi\left[(h_1, ..., h_n) + (k_1, ..., k_n)\right] = \Phi(h_1 + k_1, ..., h_n + k_n) =$$

$$= (h_1 + k_1)a_1 + \cdots + (h_n + k_n)a_n = (h_1a_1 + \cdots + h_na_n) + (k_1a_1 + \cdots k_na_n) =$$

$$= \Phi(h_1, ..., h_n) + \Phi(k_1, ..., k_n).$$

Por lo tanto, Φ es epimorfismo. ■

Teorema 1.9 *Si*

$$X = \{x_1, ..., x_r\}$$

es base de un grupo abeliano libre G y $t \in \mathbf{Z}$, entonces si $i \neq j$,

$$Y = \{x_1, ..., x_{j-1}, x_j + tx_i, x_{j+1}, ..., x_r\}$$

también es base de G.

Demostración. Notamos primero que

$$x_j = (-t)x_i + (x_j + tx_i).$$

Luego, podemos obtener al elemento x_j como combinación lineal de elementos del conjunto Y. Esto significa que Y también genera a G. Veremos finalmente que Y es base. Supóngase que

$$n_1x_1 + \cdots + n_{j-1}x_{j-1} + n_j(x_j + tx_i) + n_{j+1}x_{j+1} + \cdots + n_rx_r = 0.$$

Entonces,

$$n_1x_1 + \cdots + (n_i + n_jt)x_i + \cdots + n_jx_j + \cdots + n_rx_r = 0.$$

Como X es base, tenemos que

$$n_1 = \cdots = n_i + n_jt = \cdots = n_j = \cdots = n_r = 0.$$

Puesto que

$$n_j = n_i + n_jt = 0$$

entonces

$$n_i = -n_jt = 0.$$

Por lo tanto,

$$n_1 = \cdots = n_i = \cdots = n_j = \cdots = n_r = 0.$$

Como se cumple la propiedad (ii) del teorema 1.5, Y es base de G. Esto concluye la demostración. ■

Teorema 1.10 *Sea U_n un grupo abeliano libre de rango n y sea V un subgrupo no trivial de U_n. Entonces V es abeliano libre de rango k con $k \leq n$. Más aún, es posible elegir una base*

$$x_1, ..., x_n$$

de U_n; y una base

$$v_1, ..., v_k$$

de V, tales que $v_i = \varepsilon_i x_i$ para toda i, donde los ε_i son enteros positivos y ε_i divide a ε_{i+1} para $i = 1, 2, ..., k-1$.

Demostración. La demostración es por inducción sobre n. Si $n = 1$, entonces

$$U_1 = \langle a \rangle$$

es cíclico y, por la teoría de grupos cíclicos, cualquier subgrupo V es también cíclico generado por na.

Supongamos ahora que el teorema es válido para grupos de rango menor o igual que $n-1$.

Sean V un subgrupo de U_n, $V \neq 0$ y $\{u_1, ..., u_n\}$ base de U_n. Entonces, todo elemento de V tiene la forma

$$v = \sum n_i u_i \tag{1.5}$$

donde los n_i son enteros.

Sea m el menor entero positivo del conjunto de los *valores absolutos* de los coeficientes que se obtienen al escribir los elementos de V en la forma 1.5.

Observamos que al cambiar la base de U_n, el entero positivo m asociado a la nueva base puede ser distinto.

Escogemos una base de U_n tal que el entero positivo asociado a ella sea el menor posible, y lo designamos como ε_1. Sea u_1 el elemento de la base que tiene a ε_1 como coeficiente al escribir algún elemento v_1 de V como 1.5. Podemos poner entonces:

$$v_1 = \varepsilon_1 u_1 + a_2 u_2 + \cdots + a_n u_n.$$

Por el algoritmo de la división:

$$a_i = \varepsilon_1 q_i + r_i,\ 0 \leq r_i < \varepsilon_1 \text{ para toda } i \in \{2, ..., n\}.$$

Luego:

$$v_1 = \varepsilon_1 (u_1 + q_2 u_2 + \cdots + q_n u_n) + r_2 u_2 + \cdots + r_n u_n.$$

Por el teorema 1.9 podemos elegir

$$\{\overline{u}_1, ..., \overline{u}_n\}$$

como una nueva base de U_n donde

$$\begin{aligned} \overline{u}_1 &= u_1 + q_2 u_2 + \cdots + q_n u_n \\ \overline{u}_2 &= u_2 \\ &\vdots \\ \overline{u}_n &= u_n. \end{aligned}$$

De este modo,

$$v_1 = \varepsilon_1 \overline{u}_1 + r_2 \overline{u}_2 + \cdots + r_n \overline{u}_n.$$

Como ε_1 es el entero positivo más pequeño (en valor absoluto) que interviene como coeficiente en la representación de los elementos de V, debemos tener $r_i = 0$ para toda $i \in \{2, ..., n\}$. Por tanto,

$$v_1 = \varepsilon_1 \overline{u}_1.$$

Consideramos de nuevo el subgrupo V. Sea

$$V' = V \cap \langle \overline{u}_2, ..., \overline{u}_n \rangle .$$

Notamos que V' es subgrupo y que

$$\langle v_1 \rangle \cap V' = 0.$$

Supongamos primero que $V' = 0$. Mostramos que $V = \langle v_1 \rangle$. Sea

$$v = \alpha_1 \overline{u}_1 + \alpha_2 \overline{u}_2 + \cdots + \alpha_n \overline{u}_n \in V.$$

Por el algoritmo de la división,

$$\alpha_1 = \varepsilon_1 q + r,\ 0 \leq r < \varepsilon_1.$$

Luego,

$$\begin{aligned} v &= \varepsilon_1 q \overline{u}_1 + r \overline{u}_1 + \alpha_2 \overline{u}_2 + \cdots + \alpha_n \overline{u}_n - \\ &= q v_1 + r \overline{u}_1 + \alpha_2 \overline{u}_2 + \cdots + \alpha_n \overline{u}_n. \end{aligned}$$

Puesto que $q v_1 \in V$, debemos tener

$$r \overline{u}_1 + \alpha_2 \overline{u}_2 + \cdots + \alpha_n \overline{u}_n \in V.$$

Además, ε_1 es mínimo en el sentido conocido y por tanto $r = 0$. Así,

$$\alpha_2 \overline{u}_2 + \cdots + \alpha_n \overline{u}_n \in V$$

y dado que $V' = 0$, $\alpha_2 \overline{u}_2 + \cdots + \alpha_n \overline{u}_n = 0$. Por lo tanto,

$$v = \alpha_1 \overline{u}_1 = q \varepsilon_1 \overline{u}_1 = q v_1 \in \langle v_1 \rangle .$$

Supongamos ahora que $V' \neq 0$. Mostramos que $V = \langle v_1 \rangle \oplus V'$.
Basta mostrar que $V = \langle v_1 \rangle + V'$. Claramente $\langle v_1 \rangle + V' \subset V$. Sea

$$v = a_1 \overline{u}_1 + \cdots + a_n \overline{u}_n \in V, \text{ donde } |a_i| \geq \varepsilon_1 \text{ si } a_i \neq 0.$$

Si $a_1 = 0$ entonces

$$v \in \langle v_1 \rangle + V'.$$

Supongamos ahroa $a_1 \neq 0$. Escribimos:

$$a_1 = \varepsilon_1 q + r_1,\ 0 \leq r_1 < \varepsilon_1.$$

De este modo,

$$v - q\varepsilon_1\overline{u}_1 = r_1\overline{u}_1 + a_2\overline{u}_2 + \cdots + a_n\overline{u}_n \in V$$

pues $q\varepsilon_1\overline{u}_1 \in \langle v_1\rangle \subset V$; y puesto que $0 \leq r_1 < \varepsilon_1$, debemos tener que $r_1 = 0$. Luego.

$$a_2\overline{u}_2 + \cdots + a_n\overline{u}_n = v' \in V'.$$

Es así como obtenemos que

$$v = q\varepsilon_1\overline{u}_1 + v' \in \langle v_1\rangle + V'.$$

Por lo tanto, $V \subset \langle v_1\rangle + V'$ y como consecuencia de esto, $V = \langle v_1\rangle \oplus V'$.
Pero V' es un subgrupo de un grupo abeliano libre de rango $n-1$

$$U_{n-1} = \langle \overline{u}_2, ..., \overline{u}_n\rangle .$$

Por hipótesis de inducción, es posible elegir una base $\{\overline{\overline{u}}_2, ..., \overline{\overline{u}}_n\}$ de U_{n-1} de tal manera que V' tenga por base a $\{v_2, ..., v_k\}$ con

$$v_i = \varepsilon_i\overline{\overline{u}}_i,\ \varepsilon_i > 0 \text{ donde } \varepsilon_i \text{ divide a } \varepsilon_{i+1}.$$

Puesto que

$$U_n = \langle \overline{u}_1\rangle \oplus U_{n-1},$$

U_n tiene por base a $\{\overline{u}_1, \overline{\overline{u}}_2, ..., \overline{\overline{u}}_n\}$ y V tiene por base a $\{v_1, ..., v_k\}$ con

$$\begin{aligned} v_1 &= \varepsilon_1\overline{u}_1 \\ v_2 &= \varepsilon_2\overline{\overline{u}}_2 \\ &\vdots \\ v_k &= \varepsilon_k\overline{\overline{u}}_k \end{aligned}$$

y ε_i divide a ε_{i+1} para $i \in \{2, ..., k-1\}$. También por hipótesis de inducción tenemos que $k \leq n$, así que lo único que queda por demostrar es que ε_1 divide a ε_2.

Escribimos

$$\varepsilon_2 = q_1\varepsilon_1 + r_2,\ 0 \leq r_2 < \varepsilon_1.$$

El elemento $v_2 = \varepsilon_2\overline{\overline{u}}_2$ de V se escribe como

$$v_2 = q_1\varepsilon_1\overline{\overline{u}}_2 + r_2\overline{\overline{u}}_2$$

y

$$v_1 - v_2 = \varepsilon_1\left(\overline{u}_1 - q_1\overline{\overline{u}}_2\right) - r_2\overline{\overline{u}}_2.$$

Por el teorema 1.9 sabemos que $\{\overline{\overline{u}}_1, \overline{\overline{u}}_2, .., \overline{\overline{u}}_n\}$ es base de U_n donde

$$\overline{\overline{u}}_1 = \overline{u}_1 - q_1\overline{\overline{u}}_2.$$

De manera que en esta nueva base, el elemento $v = v_1 - v_2$ de V admite la representación

$$v = \varepsilon_1 \overline{\overline{u}}_1 - r_2 \overline{\overline{u}}_2$$

donde $0 \leq r_2 < \varepsilon_1$. Si $r_2 \neq 0$, ε_1 debe ser menor o igual que $|-r_2| = r_2$, lo cual es imposible. Luego, $r_2 = 0$ y ε_1 divide a ε_2.

La base de U_n formada por $\{x_1, ..., x_n\}$ donde

$$\begin{aligned} x_1 &= \overline{u}_1 \\ x_i &= \overline{\overline{u}}_i \text{ para } i \in \{2, ..., n\} \end{aligned}$$

y la base $\{v_1, ..., v_k\}$ de V satisfacen las propiedades deseadas. Así terminamos la demostración. ■

Teorema 1.11 *Todo grupo abeliano finitamente generado es isomorfo a un grupo de la forma*

$$\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \cdots \times \mathbf{Z}_{m_r} \times \mathbf{Z}^k;\ k \geq 0 \tag{1.6}$$

donde m_i divide a m_{i+1} para todo $i = 1, ..., r-1$.

Demostración. Sea G un grupo abeliano finitamente generado, con un conjunto generador de n elementos. Sea

$$F = \mathbf{Z} \times \cdots \times \mathbf{Z} \ (n \text{ factores}).$$

Consideramos a $\Phi : F \to G$ el epimorfismo del teorema 1.8. Denotamos al núcleo de Φ como K. Sabemos que F es libre de rango n pues

$$\{(1, 0, ..., 0), (0, 1, 0, ..., 0), ..., (0, 0, ..., 1)\}$$

es base de F. Por el teorema 1.10, existe una base de F, digamos $\{x_1, ..., x_n\}$ tal que $\{d_1 x_1, ..., d_s x_s\}$ es base de K para algunos enteros positivos $d_1, ..., d_s$ con la propiedad de que d_i divide a d_{i+1} para toda i. Por el teorema del homomorfismo tenemos que

$$G \simeq \frac{F}{K}.$$

Sea ahora

$$\Psi : F \to \mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_s} \times \mathbf{Z}^{n-s}$$

definida como

$$\Psi\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \left(\overline{\alpha}_1, ..., \overline{\alpha}_s, \alpha_{s+1}, ..., \alpha_n\right).$$

Se verifica directamente que Ψ es epimorfismo.

Por el teorema del homomorfismo, tenemos que:

$$\frac{F}{Ker\Psi} \simeq \mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_s} \times \mathbf{Z}^{n-s}.$$

Notamos a continuación que

$$Ker\Psi = K.$$

En efecto, si

$$a = a_1 d_1 x_1 + \cdots + a_s d_s x_s \in K,$$

entonces

$$\Psi(a) = (0, ..., 0)$$

y se tiene

$$K \subset Ker\Psi.$$

Inversamente, si

$$b = \sum_{i=1}^{n} b_i x_i \in Ker\Psi$$

entonces

$$(\overline{b}_1, ..., \overline{b}_s, b_{s+1}, ..., b_n) = (0, ..., 0),$$

de donde b_i es múltiplo de d_i para $1 \leq i \leq s$; y $b_i = 0$ para $s+1 \leq i \leq n$. Por lo tanto,

$$Ker\Psi \subset K.$$

Luego,

$$Ker\Psi = K.$$

De esta manera obtenemos el isomorfismo:

$$G \simeq \mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_s} \times \mathbf{Z}^{n-s}.$$

Observamos que puede ocurrir que $d_1 = 1$. De ser así, $\mathbf{Z}_{d_1}$ sería cero y se puede eliminar del producto directo, salvo isomorfismo. Si $d_2 = 1$ entonces eliminamos a $\mathbf{Z}_{d_2}$ del producto directo y así sucesivamente. Sea m_1 la primera d_i mayor que uno. Sea m_2 la segunda y m_r la r-ésima. De esta manera concluimos la demostración del teorema. Es decir, tenemos:

$$G \simeq \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \cdots \times \mathbf{Z}_{m_r} \times \mathbf{Z}^k;\ k \geq 0$$

donde m_i divide a m_{i+1} para toda $i = 1, ..., r-1$. ■

Definición Llamamos a

$$T = \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \cdots \times \mathbf{Z}_{m_r}$$

el **subgrupo de torsión** de G.

Notamos que el número m de factores de $\mathbf{Z}$ que aparecen en la expresión 1.6 es único. Para esto basta verificar que el grupo factor

$$\frac{G}{T}$$

es abeliano libre de rango m. En efecto, escribimos G como:

$$\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \cdots \times \mathbf{Z}_{m_r} \times \mathbf{Z} \times \cdots \times \mathbf{Z}.$$

Sea

$$\Phi : G \to \mathbf{Z} \times \cdots \times \mathbf{Z}$$

definida como

$$(\overline{a}_1, ..., \overline{a}_r, b_1, ..., b_m) \longmapsto (b_1, ..., b_m).$$

Claramente Φ es epimorfismo y

$$\ker \Phi = T.$$

Por el teorema fundamental del homomorfismo

$$\frac{G}{T} \simeq \mathbf{Z} \times \cdots \times \mathbf{Z}.$$

Por lo tanto,

$$\frac{G}{T}$$

es abeliano libre de rango m. Por el teorema 1.7, este número es invariante y por tanto también lo es el número de factores de $\mathbf{Z}$ en 1.6.

A continuación mostraremos en qué sentido se descomponen los grupos $\mathbf{Z}_{m_i}$ del teorema 1.11 en potencias de primos y más adelante probamos la unicidad de esta descomposición. Para tal fin, requerimos del siguiente resultado.

Teorema 1.12 *El grupo $\mathbf{Z}_m \times \mathbf{Z}_n$ es isomorfo a $\mathbf{Z}_{mn}$ si y sólo si m y n son primos relativos.*

Demostración. Supongamos que m y n son primos relativos. Consideremos el subgrupo de $\mathbf{Z}_m \times \mathbf{Z}_n$ generado por $(1,1)$. Investigamos el orden de este subgrupo. Notamos que

$$r(1,1) = (0,0)$$

si y sólo si r es múltiplo tanto de m como de n. Es decir, r es un múltiplo común de m y n. Luego, el orden de $(1,1)$ es el mínimo común múltiplo de m y n, que en este caso es mn. Así, el elemento $(1,1)$ genera un subgrupo de orden igual a

$$|\mathbf{Z}_m \times \mathbf{Z}_n|.$$

Por lo tanto

$$\langle (1,1) \rangle = \mathbf{Z}_m \times \mathbf{Z}_n.$$

Esto significa que $\mathbf{Z}_m \times \mathbf{Z}_n$ es cíclico de orden mn, y por tanto isomorfo a $\mathbf{Z}_{mn}$.

Supongamos ahora que el máximo común divisor de m y n es un número d mayor que 1. Entonces

$$\frac{mn}{d}$$

es divisible tanto por n como por m. Sea (r, s) cualquier elemento de $\mathbf{Z}_m \times \mathbf{Z}_n$. Entonces

$$\left(\frac{mn}{d}\right)(r, s) = (0, 0).$$

Esto significa que $\mathbf{Z}_m \times \mathbf{Z}_n$ no puede ser cíclico y por tanto no es isomorfo a $\mathbf{Z}_{mn}$. Así completamos la prueba. ■

Utilizando un argumento de inducción matemática obtenemos el siguiente:

Corolario 1.2 *El grupo*

$$\mathbf{Z}_{m_1} \times \cdots \times \mathbf{Z}_{m_n}$$

es isomorfo a $\mathbf{Z}_{m_1 \ldots m_n}$, *y por tanto cíclico, si y sólo si los números* $m_1, \ldots, m_n$ *son primos relativos dos a dos.*

Consideremos ahora al grupo cíclico finito $\mathbf{Z}_n$. Ponemos

$$n = (p_1)^{n_1} \cdots (p_r)^{n_r},$$

donde los p_i son primos distintos y los n_i números naturales. Utilizando el corolario anterior notamos que

$$\mathbf{Z}_n \simeq \mathbf{Z}_{p_1^{n_1}} \times \cdots \times \mathbf{Z}_{p_r^{n_r}}.$$

De este modo obtenemos la descomposición en potencias de primos del subgrupo de torsión de G.

Concluimos este capítulo con un teorema que indica la unicidad de esta descomposición.

Si G es un grupo cualquiera y n un natural, definimos:

$$G[n] := \{x \in G : nx = 0\}.$$

Claramente $G[n]$ es un subgrupo de G. Tenemos el siguiente lema:

Lema 1.8

$$\mathbf{Z}_{p^r}[p] \simeq \mathbf{Z}_p$$

para cualquier $r \geq 1$ *y cualquier* p *primo.*

Demostración. Mostramos que todo elemento distinto de cero de $\mathbf{Z}_{p^r}[p]$ tiene orden p. Si $x \in \mathbf{Z}_{p^r}[p]$, entonces

$$px = 0.$$

Por el lema 1.2 sabemos que $o(x)$ divide a p. De aquí que

$$o(x) = 1, \text{ o bien, } o(x) = p.$$

Luego, todo elemento distinto de cero de $\mathbf{Z}_{p^r}[p]$ tiene orden p.

Por el teorema de Lagrange,

$$|\mathbf{Z}_{p^r}[p]| \text{ divide a } |\mathbf{Z}_{p^r}|$$

y por tanto

$$|\mathbf{Z}_{p^r}[p]| = p^\gamma \text{ para } \gamma \geq 1.$$

Como $\mathbf{Z}_{p^r}[p]$ es cíclico,

$$\mathbf{Z}_{p^r}[p] = \langle y \rangle$$

donde $o(y) = p^\gamma$. Claramente γ no puede ser mayor que 1, pues todo elemento no nulo de $\mathbf{Z}_{p^r}[p]$ tiene orden p. Por lo tanto

$$|\mathbf{Z}_{p^r}[p]| = p$$

y

$$\mathbf{Z}_{p^r}[p] \simeq \mathbf{Z}_p.$$

Así terminamos la prueba del lema. ■

Corolario 1.3

$$(\mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}})[p] \simeq \mathbf{Z}_p \times \cdots \times \mathbf{Z}_p.$$

Demostración. Veamos que se cumple

$$(\mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}})[p] = \mathbf{Z}_{p^{\alpha_1}}[p] \times \cdots \times \mathbf{Z}_{p^{\alpha_k}}[p].$$

En efecto:

$$\begin{aligned} (a_1, ..., a_k) &\in (\mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}})[p] \text{ si y sólo si} \\ p(a_1, ..., a_k) &= (pa_1, ..., pa_k) = (0, ..., 0) \text{ si y sólo si} \\ (a_1, ..., a_k) &\in \mathbf{Z}_{p^{\alpha_1}}[p] \times \cdots \times \mathbf{Z}_{p^{\alpha_k}}[p]. \end{aligned}$$

Por el lema 1.8, el corolario es válido. ■

Teorema 1.13 *Sea*

$$T \simeq \mathbf{Z}_{p_1^{r_1}} \times \cdots \times \mathbf{Z}_{p_m^{r_m}} \tag{1.7}$$

el subgrupo de torsión de G. (Notamos que los números primos p_i no tienen por que ser todos distintos). Entonces esta descomposición es única, salvo permutación de los factores.

Demostración. Sea p un primo fijo.

Mostramos inicialmente que los elementos de T de orden una potencia de p, junto con el cero, forman un subgrupo T_p de T. Sean $x, y \in T_p$. Supongamos que

$$o(x) = p^\alpha \text{ y } o(y) = p^\beta.$$

Entonces

$$p^{\alpha+\beta}(x+y) = p^\alpha p^\beta (x+y) =$$

$$= p^\alpha p^\beta x + p^\alpha p^\beta y = 0.$$

Por el lema 1.2 debemos tener que $o(x+y)$ divide a $p^{\alpha+\beta}$. Luego, $o(x+y)$ es una potencia de p, y por tanto,

$$x + y \in T_p.$$

Por definición de T_p, $0 \in T_p$. Finalmente, si $x \in T_p$, $x \neq 0$ debemos tener $-x \in T_p$ pues

$$o(x) = o(-x).$$

De este modo probamos que T_p es un subgrupo de T.

Consideramos la descomposición de T en 1.7. Sean p un primo que aparece en esta descomposición y

$$\mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}}$$

la parte de tal descomposición que involucra a p. Mostraremos que

$$T_p \simeq \mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}}.$$

Para esto basta verificar que

$$\mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}} \times 0 \times \cdots \times 0$$

es el subgrupo de

$$\mathbf{Z}_{p_1^{r_1}} \times \cdots \times \mathbf{Z}_{p_m^{r_m}}$$

de los elementos de orden una potencia de p. Sea

$$(a_1, ..., a_k, 0, ..., 0) \in \mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}} \times 0 \times \cdots \times 0.$$

Como $\mathbf{Z}_{p^{\alpha_i}}$ es un p-grupo (ver el corolario 1.1), cada elemento de $\mathbf{Z}_{p^{\alpha_i}}$ tiene orden una potencia de p. Supongamos que $o(a_i) = p^{\beta_i}$ para toda i. Entonces

$$p^{(\sum_{i=1}^k \beta_i)}(a_1, ..., a_k, 0, ..., 0) = \Pi_{i=1}^k p^{\beta_i}(a_1, ..., a_k, 0, ..., 0) = (0, ..., 0).$$

Por el lema 1.2, $p^{(\sum_{i=1}^k \beta_i)}$ divide al orden de $(a_1, ..., a_k, 0, ..., 0)$. Por tanto, $(a_1, ..., a_k, 0, ..., 0)$ tiene orden una potencia de p.

A continuación mostramos que éstos son todos los elementos de

$$\mathbf{Z}_{p_1^{r_1}} \times \cdots \times \mathbf{Z}_{p_m^{r_m}}$$

que tienen orden una potencia de p. En efecto, sea

$$x \in \left(\mathbf{Z}_{p_1^{r_1}} \times \cdots \times \mathbf{Z}_{p_m^{r_m}}\right) \setminus \left(\mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}} \times 0 \times \cdots \times 0\right).$$

Vemos que x no puede tener orden una potencia de p. Como

$$(\mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}} \times 0 \times \cdots \times 0)$$

es grupo, debe ocurrir que $x \neq 0$ y por tanto x tiene alguna componente x_i distinta de cero tal que $x_i \in \mathbf{Z}_{p_i^{r_i}}$ donde $p_i \neq p$ (De lo contrario x sería cero). Escribimos

$$x = (x_1, ..., x_i, ..., x_n).$$

Demostramos que x no puede tener orden una potencia de p. Supongamos que

$$o(x) = m.$$

Entonces

$$mx = (mx_1, ..., mx_i, ..., mx_n) = (0, ..., 0)$$

y el orden de x_i divide a m por el lema 1.2. Puesto que $x_i \in \mathbf{Z}_{p_i^{r_i}}$ y éste es un p_i-grupo, el orden de x_i es una potencia de p_i. Esto significa que p_i aparece en la descomposición de m y por tanto m no es una potencia de p. De esta manera probamos que

$$T_p \simeq \mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}} \times 0 \times \cdots \times 0$$

y por tanto

$$T_p \simeq \mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}}.$$

Por último, supongamos que

$$T_p \simeq \mathbf{Z}_{p^{\alpha_1}} \times \cdots \times \mathbf{Z}_{p^{\alpha_k}} \simeq \mathbf{Z}_{p^{\beta_1}} \times \cdots \times \mathbf{Z}_{p^{\beta_s}} \tag{1.8}$$

con $\alpha_i \leq \alpha_{i+1}$; $\beta_i \leq \beta_{i+1}$. Debemos mostrar que

$$k = s \text{ y } \alpha_i = \beta_i \text{ para toda } i$$

para terminar la prueba de la unicidad de 1.7.

En efecto, por 1.8 y el corolario 1.3, tenemos

$$\mathbf{Z}_p \times \cdots \times \mathbf{Z}_p \ (k \text{ veces}) \simeq \mathbf{Z}_p \times \cdots \times \mathbf{Z}_p \ (s \text{ veces})$$

y por tanto

$$k = s \tag{1.9}$$

por un argumento de orden.

Finalmente, mostramos que $\alpha_i = \beta_i$ para toda i. Supongamos para tal fin que $\alpha_i = \beta_i$ para $i < j$. Procedemos a probar que $\alpha_j = \beta_j$. Consideramos al subgrupo de T_p:

$$p^{\alpha_j} T_p = \{p^{\alpha_j} x : x \in T_p\}.$$

Si $\alpha_j < \beta_j$ tendríamos:

$$p^{\alpha_j} T_p \simeq p^{\alpha_j}\mathbf{Z}_{p^{\alpha_1}} \times \cdots \times p^{\alpha_j}\mathbf{Z}_{p^{\alpha_k}} \simeq p^{\alpha_j}\mathbf{Z}_{p^{\beta_1}} \times \cdots \times p^{\alpha_j}\mathbf{Z}_{p^{\beta_k}}$$

donde

$$\begin{aligned} p^{\alpha_j}\mathbf{Z}_{p^{\alpha_i}} &= p^{\alpha_j}\mathbf{Z}_{p^{\beta_i}} \text{ si } i < j, \\ p^{\alpha_j}\mathbf{Z}_{p^{\alpha_j}} &= 0 \\ \text{y } p^{\alpha_j}\mathbf{Z}_{p^{\beta_i}} &\neq 0 \text{ si } i \geq j. \end{aligned}$$

Por tanto, el subgrupo $p^{\alpha_j} T_p$ tendría dos descomposiciones en potencias de primos con números diferentes de factores distintos de cero. Pero esto es imposible pues si

$$\overline{G} = p^{\alpha_j}\mathbf{Z}_{p^{\beta_1}} \times \cdots \times p^{\alpha_j}\mathbf{Z}_{p^{\beta_k}}$$

entonces $\overline{G}$ mismo es el subgrupo de los elementos de orden una potencia de p, y por la ecuación 1.9, no puede tener dos descomposiciones en potencias de primos con número distinto de factores. Luego, $\alpha_i = \beta_i$ para toda i. De esta manera completamos la demostración. ■

Capítulo 2

Anillo de Endomorfismos y Grupo de Automorfismos

Sea G un grupo abeliano finito. Como consecuencia del teorema fundamental de los grupos abelianos finitamente generados (ver teorema 1.11), podemos poner

$$G = C_{p_1^{m_1}} \oplus C_{p_2^{m_2}} \oplus \cdots \oplus C_{p_r^{m_r}} \tag{2.1}$$

donde los $C_{p_i^{m_i}}$ son subgrupos cíclicos primarios. Además, la expresión 2.1 es única, salvo el orden de los sumandos directos. Notamos también que los primos p_i no tienen por qué ser todos distintos.

Supongamos ahora que G es un p-grupo abeliano finito. Entonces los primos que aparecen en 2.1 son todos iguales pues cada subrupo cíclico primario tiene un generador de orden una potencia de p, y por tanto, cada subgrupo cíclico primario tiene orden p^{m_i} para algún entero positivo m_i. Luego, podemos escribir:

$$G = C_{p^{m_1}} \oplus C_{p^{m_2}} \oplus \cdots \oplus C_{p^{m_r}}. \tag{2.2}$$

La unicidad de 2.2 nos lleva a formular la siguiente definición.

Definición Sea G un p-grupo abeliano finito. Consideramos la descomposición 2.2 en subgrupos cíclicos primarios, y suponemos que

$$m_1 \geq \ldots \geq m_r.$$

Definimos el **tipo** [5] de G como el r-tuplo

$$(p^{m_1}, \ldots, p^{m_r})$$

o bien, simplemente,

$$(m_1, \ldots, m_r).$$

Sea G un p-grupo abeliano finito de tipo

$$(n_1, n_1, n_2, n_2)$$

donde p es un número primo cualquiera y tanto n_1 como n_2 son números naturales tales que $n_1 > n_2$. Escribimos

$$G = C_{p^{n_1}} \oplus C_{p^{n_1}} \oplus C_{p^{n_2}} \oplus C_{p^{n_2}}.$$

Supongamos que

$$C_{p^{n_1}} = \langle a_1 \rangle = \langle a_2 \rangle \text{ y } C_{p^{n_2}} = \langle a_3 \rangle = \langle a_4 \rangle$$

donde los a_i son elementos de G. Podemos poner entonces

$$G = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle \oplus \langle a_4 \rangle . \tag{2.3}$$

con

$$o(a_1) = o(a_2) = p^{n_1} \text{ y } o(a_3) = o(a_4) = p^{n_2}.$$

Además, por 2.3 y la definición de p-base, $\{a_1, a_2, a_3, a_4\}$ constituye una p-base de G.

Sea $EndG$ el anillo de los endomorfismos de G (los elementos de $EndG$ son todos los morfismos de grupo de G en sí mismo). "+" en $EndG$ denotará la suma habitual de funciones y "·" la composición.

Escribimos el grupo G en 2.3 como

$$G = G_1 \oplus G_2$$

donde

$$G_1 = \langle a_1 \rangle \oplus \langle a_2 \rangle$$

y

$$G_2 = \langle a_3 \rangle \oplus \langle a_4 \rangle .$$

Del trabajo de Fuchs [5] (quien a su vez cita a Shoda [8] para el caso en que G es finito) sabemos que:

$$EndG \simeq \begin{bmatrix} EndG_1 & Hom(G_2, G_1) \\ Hom(G_1, G_2) & EndG_2 \end{bmatrix}. \tag{2.4}$$

Veamos cómo se obtiene este isomorfismo. Sean

$$\eta \in EndG$$

y

$$g \in G,$$

entonces g se expresa de manera única como

$$g = g_1 + g_2, \text{ con } g_j \in G_j.$$

Ahora:

$$\eta(g_j) = g_{j1} + g_{j2}, \text{ con } g_{ji} \in G_i.$$

Definimos

$$\eta_{ij} : G_j \to G_i$$

como

$$\eta_{ij}(g_j) = g_{ji}.$$

Claramente,

$$\eta_{ij} \in Hom(G_j, G_i).$$

De este modo obtenemos la matriz (η_{ij}), correspondiente a η.

Inversamente, cualquier matriz

$$(\eta_{ij}) \in \begin{bmatrix} EndG_1 & Hom(G_2, G_1) \\ Hom(G_1, G_2) & EndG_2 \end{bmatrix}$$

define un endomorfismo η de la siguiente manera: si

$$g = g_1 + g_2,$$

consideramos

$$\eta : G \to G$$

dada por

$$\eta(g) = \sum_{i=1}^{2} \sum_{j=1}^{2} \eta_{ij}(g_j).$$

η es un endomorfismo de G. Es fácil verificar que la correspondencia

$$\eta \to (\eta_{ij})$$

es un isomorfismo.

Como una aplicación de 2.4, también en el libro de Fuchs, se obtiene el isomorfismo de anillos:

$$EndG \simeq \left\{ \begin{bmatrix} A_{11} & p^{n_1 - n_2} A_{12} \\ A_{21} & A_{22} \end{bmatrix} : A_{ij} \in \mathcal{M}_{2\times 2}(\mathbf{Z}_{p^{n_i}}) \right\}. \tag{2.5}$$

El producto en este anillo de matrices se define de la manera usual, pero las entradas de la matriz resultante se reducen módulo p^{n_1} o p^{n_2}, dependiendo del renglón. Además, los elementos de $Hom(G_j, G_i)$ corresponden a los bloques A_{ij}.

Un endomorfismo de G se conoce si sabemos cómo actúa sobre cada elemento de la p-base $\{a_1, a_2, a_3, a_4\}$. Desarrollamos aquí la descripción matricial de los elementos de $EndG$ dada por Shoda [8]. Veremos que esta descripción es la misma que la del isomorfismo 2.5.

Sea

$$A \in EndG$$

y supongamos que sabemos cómo actúa A sobre a_1, a_2, a_3 y a_4. Entonces:

$$A(a_1) = \alpha_{11}a_1 + \alpha_{21}a_2 + \alpha_{31}a_3 + \alpha_{41}a_4$$

para algunos α_{ij} únicos tales que α_{11} y α_{21} pertenecen a $\mathbf{Z}_{p^{n_1}}$ mientras que α_{31} y α_{41} pertenecen a $\mathbf{Z}_{p^{n_2}}$. Luego,

$$0 = A(0) = A(p^{n_1}a_1) = p^{n_1}A(a_1) = p^{n_1}\alpha_{31}a_3 + p^{n_1}\alpha_{41}a_4 \in C_{p^{n_2}} \oplus C_{p^{n_2}}.$$

Lo anterior occure siempre que $p^{n_1}\alpha_{31}$ y $p^{n_1}\alpha_{41}$ sean ambos múltiplos de p^{n_2}. Pero lo anterior es cierto para cualesquiera α_{31} y α_{41} en $\mathbf{Z}_{p^{n_2}}$ pues $n_1 > n_2$. Ahora,

$$A(a_2) = \alpha_{12}a_1 + \alpha_{22}a_2 + \alpha_{32}a_3 + \alpha_{42}a_4$$

donde $\alpha_{12}, \alpha_{22} \in \mathbf{Z}_{p^{n_1}}$ y $\alpha_{32}, \alpha_{42} \in \mathbf{Z}_{p^{n_2}}$. Entonces

$$0 = A(0) = A(p^{n_1}a_2) = p^{n_1}\alpha_{32}a_3 + p^{n_1}\alpha_{42}a_4 \in C_{p^{n_2}} \oplus C_{p^{n_2}}.$$

Esto también ocurre siempre que $p^{n_1}\alpha_{32}$ y $p^{n_1}\alpha_{42}$ sean ambos múltiplos de n_2, situación que se cumple para cualesquiera α_{32} y α_{42} en $\mathbf{Z}_{p^{n_2}}$.

De manera similar tenemos que

$$A(a_3) = \alpha_{13}a_1 + \alpha_{23}a_2 + \alpha_{33}a_3 + \alpha_{43}a_4$$

y

$$0 = A(p^{n_2}a_3) = p^{n_2}\alpha_{13}a_1 + p^{n_2}\alpha_{23}a_2 \in C_{p^{n_1}} \oplus C_{p^{n_1}}.$$

Pero esto tiene lugar cuando $p^{n_2}\alpha_{13}$ y $p^{n_2}\alpha_{23}$ son ambos múltiplos de p^{n_1}. Es decir, debemos tener

$$p^{n_2}\alpha_{13} = p^{n_1}\widetilde{\alpha_{13}} \text{ y } p^{n_2}\alpha_{23} = p^{n_1}\widetilde{\alpha_{23}}$$

para algunos $\widetilde{\alpha_{13}}$ y $\widetilde{\alpha_{23}}$ en $\mathbf{Z}_{p^{n_1}}$. Luego,

$$\alpha_{13} = p^{n_1-n_2}\widetilde{\alpha_{13}} \text{ y } \alpha_{23} = p^{n_1-n_2}\widetilde{\alpha_{23}}.$$

De este modo, tanto α_{13} como α_{23} deben ser múltiplos de $p^{n_1-n_2}$.

Finalmente,

$$A(a_4) = \alpha_{14}a_1 + \alpha_{24}a_2 + \alpha_{34}a_3 + \alpha_{44}a_4$$

y

$$0 = A(0) = A(p^{n_2}a_4) = p^{n_2}\alpha_{14}a_1 + p^{n_2}\alpha_{24}a_2 \in C_{p^{n_1}} \oplus C_{p^{n_1}}.$$

De modo similar, concluimos que esto ocurre siempre que α_{14} y α_{24} sean múltiplos de $p^{n_1-n_2}$.

Procediendo como lo hemos hecho, podemos representar al endomorfismo A como una matriz de la forma

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & p^{n_1-n_2}\alpha_{13} & p^{n_1-n_2}\alpha_{14} \\ \alpha_{21} & \alpha_{22} & p^{n_1-n_2}\alpha_{23} & p^{n_1-n_2}\alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{bmatrix} = \begin{bmatrix} A_{11} & p^{n_1-n_2}A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$

donde las entradas de los bloques bloque A_{11}; A_{12} pertenecen a $\mathbf{Z}_{p^{n_1}}$ y las de A_{21}, A_{22} a $\mathbf{Z}_{p^{n_2}}$. En el trabajo de Shoda se demuestra, para cualquier p-grupo abeliano finito, que el conjunto de estas matrices bajo la suma y producto de matrices definidos anteriormente constituye un anillo E isomorfo a $EndG$.

Definición Si R es un anillo, definimos el **radical de Jacobson** [1] de R, denotado

$$Jac(R),$$

como la intersección de los ideales izquierdos maximales en R.

Tenemos el siguiente resultado:

Teorema 2.1

$$Jac(E) \simeq \begin{bmatrix} pEndG_1 & Hom(G_2, G_1) \\ Hom(G_1, G_2) & pEndG_2 \end{bmatrix}.$$

Demostración. Por 2.5 y 2.4, basta probar:

$$Jac(E) = \left\{ \begin{bmatrix} pA_{11} & p^{n_1-n_2}A_{12} \\ A_{21} & pA_{22} \end{bmatrix} : A_{ij} \in \mathcal{M}_{2\times 2}(\mathbf{Z}_{p^{n_i}}) \right\}.$$

Definimos

$$\alpha : E \to \mathcal{M}(2,p) \times \mathcal{M}(2,p)$$

como

$$\begin{bmatrix} A_{11} & p^{n_1-n_2}A_{12} \\ A_{21} & A_{22} \end{bmatrix} \mapsto (A_{11}, A_{22}) \pmod{p}.$$

Se verifica directamente que α es un epimorfismo de anillos con

$$\ker \alpha = \begin{bmatrix} pA_{11} & p^{n_1-n_2}A_{12} \\ A_{21} & pA_{22} \end{bmatrix}.$$

Por el teorema del homomorfismo,

$$\frac{E}{\ker \alpha} \simeq \mathcal{M}(2,p) \times \mathcal{M}(2,p).$$

Si J es un ideal de $\mathcal{M}(2,p)$, entonces del conjunto de las posibles entradas de las matrices en J forman un ideal de $\mathbf{Z}_p$. Como $\mathbf{Z}_p$ es campo, tales entradas constituyen un ideal trivial de $\mathbf{Z}_p$, de manera que $\mathcal{M}(2,p)$ es un anillo simple.

Notamos que

$$Jac\mathcal{M}(2,p) = 0,$$

pues tanto

$$\left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a, b \in \mathbf{Z}_p \right\}$$

como

$$\left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in \mathbf{Z}_p \right\}$$

son ideales izquierdos maximales de $\mathcal{M}(2,p)$. Como la intersección de estos ideales es 0,

$$Jac\mathcal{M}(2,p) = 0.$$

Por el teorema 15.9 en [1],

$$Jac\left(\mathcal{M}(2,p) \times Jac\mathcal{M}(2,p)\right) = 0.$$

Luego,

$$Jac\left(\frac{E}{\ker \alpha}\right) = 0.$$

También se tiene que todos los elementos de $\ker \alpha$ son nilpotentes pues al multiplicar repetidas veces una matriz de la forma

$$A = \begin{bmatrix} pA_{11} & p^{n_1-n_2}A_{12} \\ A_{21} & pA_{22} \end{bmatrix},$$

se obtiene el siguiente patrón:

$$A^2 = \begin{bmatrix} pB_{11} & p^{n_1-n_2+1}B_{12} \\ pB_{21} & pB_{22} \end{bmatrix},$$

$$A^3 = \begin{bmatrix} p^2C_{11} & p^{n_1-n_2+1}C_{12} \\ pC_{21} & p^2C_{22} \end{bmatrix},$$

$$A^4 = \begin{bmatrix} p^2D_{11} & p^{n_1-n_2+2}D_{12} \\ p^2D_{21} & p^2D_{22} \end{bmatrix},$$

$$A^5 = \begin{bmatrix} p^3E_{11} & p^{n_1-n_2+2}E_{12} \\ p^2E_{21} & p^3E_{22} \end{bmatrix},$$

etc. Como E es finito, existe una s tal que $A^s = 0$. Esto muestra que $\ker \alpha$ es nil-ideal.

Por el corolario 15.12 en [1], tenemos:

$$\ker \alpha = Jac(E).$$

Es así como concluimos la prueba del teorema. ■

Sea $AutG$ el grupo de los automorfismos de G bajo la composición de funciones.

Teorema 2.2

$$AutG \simeq \begin{bmatrix} AutG_1 & Hom(G_2, G_1) \\ Hom(G_1, G_2) & AutG_2 \end{bmatrix}.$$

Demostración. Supongamos que

$$f = \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix}$$

es un elemento de $EndG$ tal que

$$f_{ii} \in AutG, \text{ para } i \in \{1, 2\}.$$

Mostraremos que

$$f \in AutG.$$

En efecto, escribimos

$$f = g + h, \text{ donde:}$$

$$g = \begin{bmatrix} f_{11} & 0 \\ 0 & f_{22} \end{bmatrix} \text{ y } h = \begin{bmatrix} 0 & f_{12} \\ f_{21} & 0 \end{bmatrix}.$$

Notamos que

$$g \in AutG.$$

Además, la matriz correspondiente a h tiene la forma

$$\begin{bmatrix} 0 & p^{n_1-n_2}A_{12} \\ A_{21} & 0 \end{bmatrix}$$

con

$$A_{12} \in \mathcal{M}_{2\times 2}(\mathbf{Z}_{p^{n_1}}) \text{ y } A_{21} \in \mathcal{M}_{2\times 2}(\mathbf{Z}_{p^{n_2}}).$$

En virtud del teorema 2.1, $h \in Jac(E)$.

Como g es inversible, existe

$$g^{-1} \in AutG$$

tal que

$$gg^{-1} = I.$$

Tenemos:

$$fg^{-1} = (g + h)g^{-1} = I + hg^{-1} = I - (-h)g^{-1} \in I - Jac(E),$$

pues $Jac(E)$ es un ideal de $EndG$. Veremos que

$$I - (-h)g^{-1}$$

es inversible en $EndG$. De la prueba del teorema 2.1 se sabe que todos los elementos de $Jac(E)$ son nilpotentes. Luego, existe una r tal que

$$I - \left[(-h)g^{-1}\right]^r = I.$$

Entonces

$$I - \left[(-h)g^{-1}\right]^r =$$

$$= \left[I - (-h)g^{-1}\right]\left[I + (-h)g^{-1} + \left((-h)g^{-1}\right)^2 + \cdots + \left((-h)g^{-1}\right)^{r-1}\right] = I.$$

Lo anterior significa que $I - (-h)g^{-1}$ es inversible. Así, existe

$$q \in AutG$$

tal que:

$$f\left(g^{-1}q\right) = I.$$

De este modo mostramos que

$$f \in AutG.$$

Inversamente, supongamos ahora que

$$f = \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix} \in AutG.$$

Entonces existe un elemento de $AutG$,

$$g = \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix}$$

tal que

$$\begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix}\begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix} = \begin{bmatrix} I_1 & 0 \\ 0 & I_2 \end{bmatrix},$$

con

$$I_1 \in AutG_1 \text{ y } I_2 \in AutG_2.$$

Luego,

$$f_{11}g_{11} + f_{12}g_{21} = I_1.$$

Notamos que a f_{12} le corresponde una matriz de la forma

$$p^{n_1-n_2}A_{12}, \text{ con } A_{12} \in \mathcal{M}_{2\times 2}(\mathbf{Z}_{p^{n_1}}).$$

Por otro lado, a g_{21} le asociamos una matriz

$$B_{21} \text{ en } \mathcal{M}_{2\times 2}(\mathbf{Z}_{p^{n_2}}).$$

Así, la matriz asociada a $f_{12}g_{21}$ es

$$p^{n_1-n_2}A_{12}B_{21}, \text{ con } A_{12}B_{21} \in \mathbf{Z}_{p^{n_1}}.$$

Como

$$Jac(EndG_1) = pEndG_1,$$

debemos tener

$$f_{12}g_{21} \in Jac(EndG_1).$$

Luego,

$$f_{11}g_{11} = I_1 - f_{12}g_{21} \in I_1 - Jac(EndG_1).$$

Por un razonamiento análogo al de la primera parte de la demostración,

$$f_{11}g_{11} \in AutG_1$$

y existe

$$(f_{11}g_{11})^{-1} \in AutG_1.$$

Así,

$$f_{11}\left[g_{11}\left(f_{11}g_{11}\right)^{-1}\right] = I_1,$$

y

$$f_{11} \in AutG_1.$$

Análogamente,

$$f_{22} \in AutG_1.$$

De este modo concluimos el prueba. ■

Si $A \in E$, se define $\det A$ de la manera usual, pero reducido módulo $\mathbf{Z}_{p^{n_2}}$. La teoría clásica de los determinantes es válida en este nuevo contexto. Tenemos los siguientes resultados:

Lema 2.1 *Sea* $A = \begin{bmatrix} A_{11} & p^{n_1-n_2}A_{12} \\ A_{21} & A_{22} \end{bmatrix} \in E$. *Entonces* $\det A$ *es no congruente con cero* $(\mathrm{mod}\, p)$, *si y sólo si* $\det A_{ii}$ *es no congruente con cero* $(\mathrm{mod}\, p)$; *para* $i \in \{1,2\}$. *Notamos que* $\det A_{ii}$ *denota al determinante usual.*

Demostración. Reduciendo módulo p y aplicando la teoría de determinantes, tenemos:

$$\det A = \det \begin{bmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{bmatrix} = \det A_{11} \det A_{22}.$$

Así establecemos el lema. ■

Lema 2.2 *Una matriz* A *de* E *representa un elemento de* $AutG$ *si y sólo si* $\det A$ *no es congruente con* 0 *módulo* p.

Demostración. Supongamos que

$$A \in AutG.$$

Como $AutG$ es un grupo finito, existe una r tal que

$$A^r = I,$$

donde I es la identidad en E. Luego,

$$\det A^r = \det A \cdots \det A = 1.$$

Así, $\det A$ es no congruente con cero $(\mathrm{mod}\, p)$.

Inversamente, supongamos que $\det A$ es no congruente con cero $(\mathrm{mod}\, p)$. Por el lema 2.1, $\det A_{ii}$ es no congruente con cero $(\mathrm{mod}\, p)$. De 2.5 y el teorema 2.2 tenemos los isomorfismos:

$$AutG \simeq \begin{bmatrix} AutG_1 & Hom(G_2, G_1) \\ Hom(G_1, G_2) & AutG_2 \end{bmatrix} \simeq$$

$$\simeq \begin{bmatrix} GL_2(\mathbf{Z}_{p^{n_1}}) & p^{n_1-n_2}\mathcal{M}_{2\times 2}(\mathbf{Z}_{p^{n_1}}) \\ \mathcal{M}_{2\times 2}(\mathbf{Z}_{p^{n_2}}) & GL_2(\mathbf{Z}_{p^{n_2}}) \end{bmatrix}.$$

Veremos que

$$A_{11} \in GL_2(\mathbf{Z}_{p^{n_1}}) \text{ y } A_{22} \in GL_2(\mathbf{Z}_{p^{n_2}}).$$

Como $\det A_{11}$ es no congruente con cero $(\mathrm{mod}\, p)$, $\det A_{11}$ es primo con p^{n_1}. Luego,

$$\det A_{11}$$

es un generador del grupo $\mathbf{Z}_{p^{n_1}}$. Esto significa que existe $m \in \mathbf{Z}_{p^{n_1}}$ tal que

$$m \det A_{11} = 1.$$

Escribimos

$$A_{11} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Notamos que la inversa de A_{11} es

$$(A_{11})^{-1} = m \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Por lo tanto,

$$A_{11} \in GL_2(\mathbf{Z}_{p^{n_1}}).$$

Análogamente se obtiene:

$$A_{22} \in GL_2(\mathbf{Z}_{p^{n_2}}).$$

Es así como concluimos que

$$A \in AutG.$$

De este modo terminamos la prueba. ■

Sea S el subconjunto de E de las matrices de la forma

$$\begin{bmatrix} pa_{11} & pa_{12} & p^{n_1-n_2}a_{13} & p^{n_1-n_2}a_{14} \\ a_{21} & pa_{22} & p^{n_1-n_2}a_{23} & p^{n_1-n_2}a_{24} \\ a_{31} & a_{32} & pa_{33} & pa_{34} \\ a_{41} & a_{42} & a_{43} & pa_{44} \end{bmatrix}$$

tales que las entradas de los renglones 1 y 2 están en $\mathbf{Z}_{p^{n_1}}$ y las de los renglones 3 y 4 pertenecen a $\mathbf{Z}_{p^{n_2}}$. Es inmediato que S es un subanillo de E.

Sea

$$P = S + I$$

donde I es la matriz identidad en E.

Nuestro objetivo en la siguiente sección es mostrar que P es un p-subgrupo de Sylow del grupo de matrices inversibles de E.

P es un p-Subgrupo de Sylow de $AutG$

Lema 2.3 *P es un subgrupo del grupo multiplicativo de E. (También denotamos este grupo multiplicativo como $AutG$).*

Demostración. Sea $GL(2,p)$ el grupo de las matrices inversibles de 2×2 con entradas en $\mathbf{Z}_p$, bajo el producto de matrices. Definimos

$$\Phi : AutG \to GL(2,p) \times GL(2,p)$$

como:

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & p^{n_1-n_2}\alpha_{13} & p^{n_1-n_2}\alpha_{14} \\ \alpha_{21} & \alpha_{22} & p^{n_1-n_2}\alpha_{23} & p^{n_1-n_2}\alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{bmatrix} \mapsto \left(\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}, \begin{bmatrix} \alpha_{33} & \alpha_{34} \\ \alpha_{43} & \alpha_{44} \end{bmatrix} \right) (\mathrm{mod}\, p).$$

Φ está bien definida pues

$$\det \begin{bmatrix} \alpha_{11} & \alpha_{12} & p^{n_1-n_2}\alpha_{13} & p^{n_1-n_2}\alpha_{14} \\ \alpha_{21} & \alpha_{22} & p^{n_1-n_2}\alpha_{23} & p^{n_1-n_2}\alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{bmatrix}$$

es no conguente con cero $(\mathrm{mod}\, p)$ si y sólo si tanto

$$\det \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$$

como

$$\det \begin{bmatrix} \alpha_{33} & \alpha_{34} \\ \alpha_{43} & \alpha_{44} \end{bmatrix}$$

es no congruente con cero (mod p). Cálculos directos muestran que Φ es morfismo de grupos. Además Φ es epimorfismo pues si

$$\left(\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}, \begin{bmatrix} \alpha_{33} & \alpha_{34} \\ \alpha_{43} & \alpha_{44} \end{bmatrix} \right) \in GL(2,p) \times GL(2,p)$$

entonces

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & 0 & 0 \\ \alpha_{21} & \alpha_{22} & 0 & 0 \\ 0 & 0 & \alpha_{33} & \alpha_{34} \\ 0 & 0 & \alpha_{43} & \alpha_{44} \end{bmatrix} \in AutG$$

ya que su determinante es igual a

$$\det \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \det \begin{bmatrix} \alpha_{33} & \alpha_{34} \\ \alpha_{43} & \alpha_{44} \end{bmatrix}.$$

Como ninguno de estos determinantes es congruente con cero módulo p, tampoco lo es su producto. Por lo tanto, Φ es epimorfismo.

Sea

$$K = \left\{ \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} : a \in \mathbf{Z}_p \right\}.$$

Claramente, $K \times K$ es un subgrupo de $GL(2,p) \times GL(2,p)$. Mostraremos que

$$S + I = \Phi^{-1}(K \times K).$$

Tomamos

$$A = \begin{bmatrix} pa_{11}+1 & pa_{12} & p^{n_1-n_2}a_{13} & p^{n_1-n_2}a_{14} \\ a_{21} & pa_{22}+1 & p^{n_1-n_2}a_{23} & p^{n_1-n_2}a_{24} \\ a_{31} & a_{32} & pa_{33}+1 & pa_{34} \\ a_{41} & a_{42} & a_{43} & pa_{44}+1 \end{bmatrix} \in S + I.$$

$A \in AutG$ pues su determinante no es congruente con cero (mod p), y

$$\Phi(A) \in K \times K.$$

Inversamente, sea

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & p^{n_1-n_2}\alpha_{13} & p^{n_1-n_2}\alpha_{14} \\ \alpha_{21} & \alpha_{22} & p^{n_1-n_2}\alpha_{23} & p^{n_1-n_2}\alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{bmatrix} \in \Phi^{-1}(K \times K).$$

Entonces

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \in K \text{ y } \begin{bmatrix} \alpha_{33} & \alpha_{34} \\ \alpha_{43} & \alpha_{44} \end{bmatrix} \in K,$$

y por tanto,

$$\alpha_{ii} \equiv 1 (\mathrm{mod}\, p)$$

y

$$\alpha_{12}, \alpha_{34} \equiv 0 (\mathrm{mod}\, p).$$

Así obtenemos que

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & p^{n_1-n_2}\alpha_{13} & p^{n_1-n_2}\alpha_{14} \\ \alpha_{21} & \alpha_{22} & p^{n_1-n_2}\alpha_{23} & p^{n_1-n_2}\alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{bmatrix} \in S + I$$

y tenemos

$$S + I = \Phi^{-1}(K \times K).$$

Concluimos que $P = S + I$ es un subgrupo de $AutG$ por ser la imagen inversa del grupo $K \times K$. ■

Ponemos

$$\Delta = Jac(E) + I$$

donde I es nuevamente la matriz identidad de E. Tenemos el siguiente lema.

Lema 2.4 *Δ es un p-subgrupo normal de AutG.*

Demostración. Consideramos de nuevo el epimorfismo

$$\Phi : AutG \to GL(2,p) \times GL(2,p)$$

definido en la demostración del lema 2.3. Probamos que

$$Ker\Phi = \Delta.$$

Sea

$$A = \begin{bmatrix} p\alpha_{11}+1 & p\alpha_{12} & p^{n_1-n_2}\alpha_{13} & p^{n_1-n_2}\alpha_{14} \\ p\alpha_{21} & p\alpha_{22}+1 & p^{n_1-n_2}\alpha_{23} & p^{n_1-n_2}\alpha_{24} \\ \alpha_{31} & \alpha_{32} & p\alpha_{33}+1 & p\alpha_{34} \\ \alpha_{41} & \alpha_{42} & p\alpha_{43} & p\alpha_{44}+1 \end{bmatrix} \in \Delta.$$

Claramente $\det A$ no es congruente con cero $(\mathrm{mod}\, p)$, de donde $A \in AutG$. Además, $\Phi(A) = 1$. Por tanto $A \in Ker\Phi$. Inversamente, si

$$B = \begin{bmatrix} \beta_{11} & \beta_{12} & p^{n_1-n_2}\beta_{13} & p^{n_1-n_2}\beta_{14} \\ \beta_{21} & \beta_{22} & p^{n_1-n_2}\beta_{23} & p^{n_1-n_2}\beta_{24} \\ \beta_{31} & \beta_{32} & \beta_{33} & \beta_{34} \\ \beta_{41} & \beta_{42} & \beta_{43} & \beta_{44} \end{bmatrix} \in Ker\Phi$$

entonces

$$\beta_{ii} \equiv 1(\mathrm{mod}\, p)$$

y

$$\beta_{12}, \beta_{21}, \beta_{34}, \beta_{43} \equiv 0(\mathrm{mod}\, p).$$

Por tanto $B \in \Delta$ y tenemos $Ker\Phi = \Delta$. Esto implica que Δ es un subgrupo normal de $AutG$. Además Δ es p-subgrupo pues $|\Delta| = |Jac(E)|$ es una potencia de p. ($|\Delta|$ se calcula con detalle después del teorema 2.3). ■

Lema 2.5 *Sea G un grupo finito tal que $|G| = p^n m$ donde p no divide a m. Sea H un p-subgrupo normal de G. Entonces H está contenido en la intersección de todos los p-subgrupos de Sylow de G. Además, esta intersección es un p-subgrupo normal de G y por tanto el máximo p-subgrupo normal.*

Demostración. Como H es un p-subgrupo, su orden es p^γ con $1 \leq \gamma \leq n$. Por el primer teorema de Sylow, existe un p-subgrupo de Sylow P_1 de G (de orden p^n) que contiene a H.

Sea P_2 cualquier otro p-subgrupo de Sylow de G. Por el segundo teorema de Sylow, existe $g \in G$ tal que

$$P_1 = g^{-1} P_2 g.$$

Luego,

$$H \leq g^{-1} P_2 g.$$

Si $h \in H$ entonces $g^{-1}hg$ también pertenece a H pues H es un subgrupo normal. Luego

$$g^{-1}hg \in g^{-1} P_2 g$$

y por tanto $h \in P_2$. Lo anterior implica que H está contenido en todo p-subgrupo de Sylow, y por tanto, en la intersección de todos ellos.

Finalmente notamos que si

$$P_1, ..., P_r$$

son todos los p-subgrupos de Sylow de G y $g \in G$, entonces

$$g^{-1} (\cap P_i)\, g = \cap \left(g^{-1} P_i g\right).$$

Por el segundo teorema de Sylow,

$$g^{-1} P_1 g, ..., g^{-1} P_r g$$

son todos los p-subgrupos de Sylow de G. Por tanto

$$g^{-1} (\cap P_i)\, g = \cap P_i$$

y $\cap P_i$ es un p-subgrupo normal de G.

Luego, $\cap P_i$ es el máximo p-subgrupo normal de G. ■

Denotamos por $O_p(AutG)$ al máximo p-subgrupo normal de $AutG$.

Lema 2.6 $\Delta = O_p(AutG)$.

Demostración. Por el teorema fundamental del homomorfismo:

$$\frac{AutG}{\Delta} \simeq GL(2,p) \times GL(2,p). \tag{2.6}$$

Vemos inicialmente que $GL(2,p) \times GL(2,p)$ no tiene p subgrupos normales. Para esto, consideramos a $\mathbf{Z}_p \times \mathbf{Z}_p$ como un $\mathbf{Z}_p$-espacio vectorial de dimensión 2. Sabemos que:

$$|GL(2,p)| = |Aut(\mathbf{Z}_p \times \mathbf{Z}_p)|.$$

Procedemos a contar los elementos de $Aut(\mathbf{Z}_p \times \mathbf{Z}_p)$; para tal fin basta contar las bases de $\mathbf{Z}_p \times \mathbf{Z}_p$. Existen $p^2 - 1$ elecciones posibles para el primer elemento básico (todos los elementos de $\mathbf{Z}_p \times \mathbf{Z}_p$ sin considerar al cero). Si (m,n) es uno de estos elementos básicos, entonces

$$(m,n), 2(m,n), ..., p(m,n)$$

son los elementos de $\mathbf{Z}_p \times \mathbf{Z}_p$ que están en el subespacio generado por (m,n). Por tanto existen $p^2 - p$ elecciones posibles para el segundo elemento básico. Así,

$$|Aut(\mathbf{Z}_p \times \mathbf{Z}_p)| = \left(p^2 - 1\right)\left(p^2 - p\right).$$

Luego,

$$\begin{aligned} |GL(2,p) \times GL(2,p)| &= \left(p^2-1\right)^2\left(p^2-p\right)^2 = \\ & p^2\left(p^2-1\right)^2(p-1)^2. \end{aligned}$$

Por el primer teorema de Sylow, los subgrupos de $GL(2,p) \times GL(2,p)$ de orden p^2 son precisamente los p-subgrupos de Sylow.

Consideramos a continuación los subgrupos de $GL(2,p)$:

$$H_1 = \left\{ \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} : a \in \mathbf{Z}_p \right\}$$

y

$$H_2 = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbf{Z}_p \right\}.$$

Entonces

$$H_1 \times H_1 \text{ y } H_2 \times H_2$$

son p-subgrupos de Sylow de $GL(2,p) \times GL(2,p)$ por tener ambos orden p^2. Además, la intersección de estos dos subgrupos es 1.

Por el lema 2.5, $GL(2,p) \times GL(2,p)$ no tiene p-subgrupos normales. Del isomorfismo 2.6, concluimos que

$$\frac{AutG}{\Delta}$$

no tiene p-subgrupos normales.

Por último, si existiera un p-subgrupo normal H de $AutG$ tal que $H \gneqq \Delta$, entonces

$$\frac{H}{\Delta}$$

sería un p-subgrupo normal de

$$\frac{AutG}{\Delta}$$

lo cual no es posible.

Por lo tanto,

$$\Delta = O_p(AutG).$$

Así terminamos la prueba del lema. ■

Por la demostración del lema 2.6, los p-subgrupos de Sylow de

$$\frac{AutG}{\Delta}$$

tienen orden p^2.

Lema 2.7 *Si*

$$\frac{H}{\Delta}$$

es un p-subgrupo de Sylow de

$$\frac{AutG}{\Delta}$$

entonces H es un p-subgrupo de Sylow de $AutG$.

Demostración. Basta mostrar que H es un p-subgrupo de orden máximo en $AutG$. Si existiera un p-subgrupo K con $K \gneqq H$,

$$H_1 = \frac{K}{\Delta}$$

sería un p-subgrupo de orden mayor que

$$H_2 = \frac{H}{\Delta}$$

y H_2 no sería de Sylow; de modo que el lema es válido. ■

Es así como obtenemos el siguiente teorema:

Teorema 2.3 *Los p-subgrupos de Sylow de $AutG$ tienen orden $|\Delta|p^2$.*

Al contar los elementos de $\Delta = Jac(E) + I$ y $P = S + I$ obtenemos:

$$|\Delta| = \left(p^{n_1-1}\right)^4 \left(p^{n_2-1}\right)^4 \left(p^{n_2}\right)^8 = p^{(4n_1+12n_2-8)}$$

y

$$|P| = p^{n_1} \left(p^{n_1-1}\right)^3 p^{n_2} \left(p^{n_2-1}\right)^3 \left(p^{n_2}\right)^8 = p^{(4n_1+12n_2-6)}.$$

Luego, el orden de los p-subgrupos de Sylow de $AutG$ es

$$|\Delta|\, p^2 = 4n_1 + 12n_2 - 6,$$

que es igual a $|P|$. Hemos demostrado el siguiente resultado:

Teorema 2.4 *Sea $P = S + I$ donde I es la matriz identidad de E. Entonces P es un p-subgrupo de Sylow de $AutG$.*

Serie Anuladora Superior y Serie Central

Lo que sigue conduce a la definición de serie anuladora superior de S.

Definición Sea

$$\{S_t\}_{t\in\{0,\ \cdots,n\}}$$

una sucesión de ideales de S tales que

$$S_0 = 0,$$

$$S_1 = AnnS,$$

($AnnS$ denota al anulador de S); y

$$\frac{S_t}{S_{t-1}} = Ann\left(\frac{S}{S_{t-1}}\right).$$

Llamamos a S_t el **t-ésimo anulador** de S.

Teorema 2.5

$$S_0 = 0$$

y

$$S_t = \{A \in S : AB \in S_{t-1},\ BA \in S_{t-1}\ \textit{para toda}\ B \in S\},$$

si $t > 0$.

Demostración. Sea

$$W_t = \{A \in S : AB \in S_{t-1},\ BA \in S_{t-1} \text{ para toda } B \in S\},\ t > 0.$$

Tenemos lo siguiente:

$$A \in S_t$$

si y sólo si

$$AB \equiv BA \equiv 0 \pmod{S_{t-1}}$$

para toda B en S. Esto ocurre si y sólo si AB y BA pertenecen a S_{t-1} para toda B en S; lo cual es verdad si y sólo si

$$A \in W_t.$$

De esta manera obtenemos el resutlado. ■

Definición Decimos que la sucesión de ideales de S

$$\{S_t\}_{t\in\{0,\ldots,n\}}$$

es una **serie anuladora superior** si cumple la propiedad:

$$0 = S_0 \subset S_1 \subset S_2 \subset \cdots \subset S_n = S.$$

Llamamos al número n **longitud** de la serie.

El siguiente teorema garantiza que si S tiene una serie anuladora superior de longitud n, este número es una cota superior para el grado de nilpotencia de $P = S + I$.

Teorema 2.6 *Sea*

$$P = S + I$$

como en el teorema 2.4. Una serie anuladora superior de S induce una serie central en P de igual longitud.

Demostración. Suponemos que S tiene la siguiente serie anuladora superior:

$$0 = S_0 \subset S_1 \subset S_2 \subset \cdots \subset S_n = S$$

de longitud n. A continuación inducimos una serie central en P. Sea

$$H = P \cap Z(E)$$

donde $Z(E)$ es el centro de E. Mostramos que H es un subgrupo normal de P. Sean $a + I$ y $b + I$ elementos de H. Entonces

$$(a + I)(b + I) = ab + a + b + I \in P.$$

Sea $c \in E$. Como $a+I$ y $b+I$ pertenecen a $Z(E)$, se tiene:

$$(a+I)(b+I)c = (a+I)c(b+I) = c(a+I)(b+I).$$

Por tanto,

$$(a+I)(b+I) \in Z(E)$$

y tenemos que

$$(a+I)(b+I) \in H.$$

Así, H es cerrado bajo la operación de P.

Sabemos que $(a+I)^{-1} \in P$. También se tiene: $(a+I)c = c(a+I)$ para todo $c \in E$. Luego, $c(a+I)^{-1} = (a+I)^{-1}c$ para todo $c \in E$. De aquí que

$$(a+I)^{-1} \in Z(E),$$

y por tanto, H es subgrupo de P.

Más aún, los elementos de H conmutan con todos los elementos de E, y en particular con los de P. Por lo tanto:

$$H \lhd P.$$

Para cada $t \in \{1, ..., n\}$ veremos que $S_t + I$ también un subgrupo normal de P. Sean $a+I$, $b+I \in S_t + I$. Entonces

$$(a+I)(b+I) = ab + a + b + I \in S_t + I.$$

Como $a + I \in P$, existe un entero positivo r tal que

$$(a+I)^r = I.$$

Pero

$$I = (a+I)^r = (a+I)(a+I)^{r-1} =$$

$$= (a+I)(a^{r-1} + (r-1)a^{r-2} + \cdots + (r-1)a + I).$$

Por lo tanto,

$$(a+I)^{-1} \in S_t + I.$$

De este modo probamos que $S_t + I$ es subgrupo de P.

A continuación verificamos que $S_t + I$ es normal en P. Sean $a + I \in S_t + I$, $b + I \in P$. Ponemos $(b+I)^{-1} = \overline{b} + I$, mismo que es un elemento de P. Tenemos lo siguiente:

$$\begin{aligned}(b+I)^{-1}(a+I)(b+I) &= (\overline{b}+I)(a+I)(b+I) = \\ &= (\overline{b}a + \overline{b} + a + I)(b+I) = \\ &= \overline{b}ab + \overline{b}a + \overline{b}b + \overline{b} + ab + a + b + I.\end{aligned}$$

Ahora,

$$I = (\overline{b} + I)(b + I) = \overline{b}b + \overline{b} + b + I$$

y

$$\overline{b}b + \overline{b} + b = 0.$$

Luego

$$(b + I)^{-1}(a + I)(b + I) = \overline{b}ab + \overline{b}a + ab + a + I \in S_t + I$$

pues S_t es ideal de S.

Por lo tanto, $S_t + I$ es un subgrupo normal de P.

Así, tanto H como $S_t + I$ son subgrupos normales de P. Luego, el producto $P_t = H(S_t + I)$ también es un subgrupo normal de P para toda $t \in \{1, ..., n\}$.

Notamos también que $P_n = P$ pues:

$$P = S + I = S_n + I \leq P_n.$$

Obtenemos así la serie normal

$$1 \leq P_1 \leq P_2 \leq \cdots \leq P_n = P. \tag{2.7}$$

Basta demostrar que 2.7 es una serie central en P. Sea

$$\overline{a + h} \in \frac{P_{t+1}}{P_t}.$$

Debemos verificar que

$$\overline{a + h} \in Z\left(\frac{P}{P_t}\right).$$

Consideramos un elemento $\overline{b + I}$ de

$$\left(\frac{P}{P_t}\right).$$

Tenemos:

$$\left(\overline{a + h}\right)\left(\overline{b + I}\right) = \left(\overline{b + I}\right)\left(\overline{a + h}\right)$$

si y sólo si

$$(a + h)(b + I)(a + h)^{-1}(b + I)^{-1} \in P_t.$$

Pero

$$(a + h)(b + I)(a + h)^{-1}(b + I)^{-1} =$$

$$= [(a + h)(b + I) - (b + I)(a + h)](a + h)^{-1}(b + I)^{-1} + I =$$

$$= (ab + a + hb + h - ba - bh - a - h)(a + h)^{-1}(b + I)^{-1} + I =$$

$$= (ab - ba)(a + h)^{-1}(b + I)^{-1} + I.$$

(Notamos que $hb = bh$ porque $h \subset Z(E)$). Ahora: $(ab - ba) \in S_t$ pues

$$a \in HS_{t+1} \text{ implica que } a = hs_{t+1} = (s+1)s_{t+1} = ss_{t+1} + s_{t+1}$$

donde $h \in H$, $s_{t+1} \in S_{t+1}$ y $s \in S$. Puesto que S_{t+1} es ideal de S, debemos tener que $a \in S_{t+1}$. Además, por definición de seric anuladora superior y dado que $b \in S$, también se tiene

$$(ab - ba) \in S_t.$$

Como $(a+h)^{-1}(b+I)^{-1} \in P$, tenemos

$$(a+h)^{-1}(b+I)^{-1} = c + I$$

para algún $c \in S$. Entonces:

$$(ab - ba)(a+h)^{-1}(b+I)^{-1} + I = (ab - ba)(c+I) + I =$$

$$= (ab - ba)c + ab - ba + I \in S_t + I \leq H(S_t + I) = P_t.$$

Por lo tanto,

$$(a+h)(b+I)(a+h)^{-1}(b+I)^{-1} \in P_t$$

y la serie 2.7 es central de longitud n. Esto completa la prueba del teorema. ■

Reiteramos: como el grado de nilpotencia de P es la longitud mínima de todas las series centrales de P, la longitud de una serie anuladora superior de S es una cota superior para el grado de nilpotencia de P, el cual es isomorfo a un p-subgrupo de Sylow de $AutG$.

El propósito del tercer capítulo es hallar la serie anuladora superior de S y su longitud para un p-grupo abeliano finito de tipo (n_1, n_1, n_2, n_2) con $n_1 > n_2$.

Capítulo 3

Serie Anuladora Superior de S

Sea G un p-grupo abeliano finito de tipo (n_1, n_1, n_2, n_2) con $n_1 > n_2$. Consideramos al anillo S como en el capítulo 2. Los objetivos de este capítulo, y del trabajo todo, son caracterizar los ideales y anuladores de S, así como obtener una cota superior para el grado de nilpotencia de $P = S + I$.

Caracterización de los Ideales de S

Comenzamos con un teorema que indica cómo son los ideales de S. Para esto, requerimos de una serie de lemas.

Lema 3.1 *Sea $\mathbf{Z}_n$ el anillo de los enteros módulo n. Si H es un subgrupo aditivo de $\mathbf{Z}_n$, entonces H es un ideal del anillo $\mathbf{Z}_n$.*

Demostración. Como todo subgrupo de $\mathbf{Z}_n$ es cíclico, $H = \langle a \rangle$ para algún $a \in \mathbf{Z}_n$. Sean $x \in \mathbf{Z}_n$ y $ma \in H$. Notamos que

$$x(ma) = (1 + \cdots + 1)ma = ma + \cdots + ma \in H.$$

Luego, H es ideal de $\mathbf{Z}_n$ y el lema es válido. ■

Definición Definimos

$$k = k(i) = \left\{ \begin{array}{l} 1 \text{ si } i = 1, 2 \\ 2 \text{ si } i = 3, 4 \end{array} \right\}.$$

Lema 3.2 *$p\mathbf{Z}_{p^{n_k}}$ y $p^{n_1 - n_2}\mathbf{Z}_{p^{n_k}}$ son, cada uno, subanillos de $\mathbf{Z}_{p^{n_k}}$.*

Demostración. $p\mathbf{Z}_{p^{n_k}}$ y $p^{n_1 - n_2}\mathbf{Z}_{p^{n_k}}$ son subgrupos de $\mathbf{Z}_{p^{n_k}}$. Por el lema 3.1, son ideales y por tanto subanillos de $\mathbf{Z}_{p^{n_k}}$. ■

Lema 3.3 *Sea H un ideal propio no trivial de $\mathbf{Z}_{p^{n_k}}$. Entonces todo elemento de H es múltiplo de p.*

Demostración. Por el lema 3.1 basta estudiar los subgrupos propios no triviales de $\mathbf{Z}_{p^{n_k}}$. Sabemos que cualquier subgrupo propio no trivial de $\mathbf{Z}_{p^{n_k}}$ está generado por un elemento de $\mathbf{Z}_{p^{n_k}}$ que no es primo con p^{n_k}. Por tanto, tal elemento debe ser múltiplo de p. Es decir, cualquier subgrupo propio no trivial está generado por un múltiplo de p. Esto concluye la prueba del lema. ■

Teorema 3.1 *Sea $\mathcal{I}$ un ideal de S. Entonces existe una función*

$$\beta : \mathrm{I}_4 \times \mathrm{I}_4 \to \mathbf{N}$$

tal que

$$\mathcal{I} = \left\{ \left(p^{n_k - \beta(i,j)}\alpha_{ij}\right)_{4\times 4} : \alpha_{ij} \in \mathbf{Z}_{p^{n_k}} \right\}.$$

Más aún, β satisface las siguientes propiedades:
(i)$\beta(i,j) \leq \beta(i-2,j)$, $i \geq 3$
$\beta(i,j) \leq \beta(i+2,j) + n_1 - n_2$, $i \leq 2$
(ii)$\beta(i,j) \leq \beta(i,j-1)$, $j \geq 2$
$\beta(i,j) \leq \beta(i,4) + n_1 - n_2$, $j \leq 2$
(iii)$\beta(i-1,j) \leq \beta(i,j) \leq \beta(i-1,j) + 1$, $i \in \{2,4\}$
$\beta(i,j+1) \leq \beta(i,j) \leq \beta(i,j+1) + 1$, $j \in \{1,3\}$.

Demostración. Fijamos la pareja (i,j). Sea $(\mathcal{I})_{ij}$ el conjunto de todas las entradas ij de las matrices en $\mathcal{I}$. Mostraremos inicialmente que $(\mathcal{I})_{ij}$ es un subgrupo aditivo del anillo correspondiente: $p\mathbf{Z}_{p^{n_k}}$, $p^{n_1-n_2}\mathbf{Z}_{p^{n_k}}$ ó $\mathbf{Z}_{p^{n_k}}$ (éstos son anillos por el lema 3.2). Sean a_{ij}, $b_{ij} \in (\mathcal{I})_{ij}$. Por definición de $(\mathcal{I})_{ij}$ existe una matriz A en $\mathcal{I}$ tal que el elemento a_{ij} aparece en la entrada ij de A; y existe una matriz B, también en $\mathcal{I}$, tal que b_{ij} aparece en la entrada ij de B. Como $\mathcal{I}$ es ideal de S, debemos tener que $A - B \in \mathcal{I}$. Ahora bien, la entrada ij de $A - B$ es precisamente $a_{ij} - b_{ij}$. Luego, también por definición de $(\mathcal{I})_{ij}$ debemos tener que $a_{ij} - b_{ij} \in (\mathcal{I})_{ij}$. Por lo tanto, $(\mathcal{I})_{ij}$ es un subgrupo aditivo del anillo correspondiente: $p\mathbf{Z}_{p^{n_k}}$, $p^{n_1-n_2}\mathbf{Z}_{p^{n_k}}$ ó $\mathbf{Z}_{p^{n_k}}$. Como éstos son subanillos (y por tanto subgrupos) de $\mathbf{Z}_{p^{n_k}}$, $(\mathcal{I})_{ij}$ también es subgrupo aditivo de $\mathbf{Z}_{p^{n_k}}$. Por el lema 3.1, $(\mathcal{I})_{ij}$ es un ideal de $\mathbf{Z}_{p^{n_k}}$.

A continuación consideramos distintos casos. Si $(\mathcal{I})_{ij} = 0$, tomamos $\beta(i,j) = 0$. De este modo, todo elemento de $(\mathcal{I})_{ij}$ es múltiplo de $p^{n_k-\beta(i,j)}$. Supongamos a continuación que $(\mathcal{I})_{ij}$ es propio no trivial. Por el lema 3.3 observamos que todo elemento de $(\mathcal{I})_{ij}$ es múltiplo de p. Sea γ_{ij} la menor potencia de p que aparece como factor de los elementos distintos de cero de $(\mathcal{I})_{ij}$. Observamos que debemos tener: $1 \leq \gamma_{ij} \leq n_k - 1$. Ponemos $\beta(i,j) = n_k - \gamma_{ij} > 0$. Por la elección de γ_{ij} todo elemento de $(\mathcal{I})_{ij}$ es múltiplo de $p^{n_k-\beta(i,j)}$. El último caso es tomar $(\mathcal{I})_{ij}$ como el anillo total. Aquí consideramos tres subcasos: si $(\mathcal{I})_{ij} = p\mathbf{Z}_{p^{n_k}}$ ponemos $\beta(i,j) = n_k - 1$ y notamos que todo elemento de $(\mathcal{I})_{ij}$ es múltiplo de $p^{n_k-\beta(i,j)} = p$. Si $(\mathcal{I})_{ij} = p^{n_1-n_2}\mathbf{Z}_{p^{n_1}}$ entonces elegimos $\beta(i,j) = n_2$ y todo elemento de $(\mathcal{I})_{ij}$ es múltiplo de $p^{n_1-\beta(i,j)}$. Finalmente, si $(\mathcal{I})_{ij} = \mathbf{Z}_{p^{n_k}}$ tomamos $\beta(i,j) = n_k$. De esta manera completamos todos los casos. Así construimos una función β de $\mathrm{I}_4 \times \mathrm{I}_4$ en $\mathbf{N}$ que concluye la primera parte de la demostración.

Procedemos ahora a verificar las propiedades de β. Como $\mathcal{I}$ es ideal de S, tenemos:

$$\mathcal{I}S \subset \mathcal{I} \text{ y } S\mathcal{I} \subset \mathcal{I}.$$

(i) Mostramos a continuación que

$$\beta(i,j) \leq \beta(i-2,j),\ i \geq 3.$$

Sea $A_{i-2,i}(p^{n_1-n_2})$ la matriz de S que tiene $p^{n_1-n_2}$ en la entrada $(i-2,i)$ y 0 en las demás. Sea $B = \left(p^{n_k-\beta(i,j)}\alpha_{ij}\right)$ una matriz cualquiera en $\mathcal{I}$. Entonces la fila $i-2$ de la matriz $A_{i-2,i}(p^{n_1-n_2})B$ es

$$p^{n_1-\beta(i,1)}\alpha_{i1} \quad p^{n_1-\beta(i,2)}\alpha_{i2} \quad p^{n_1-\beta(i,3)}\alpha_{i3} \quad p^{n_1-\beta(i,4)}\alpha_{i4}.$$

Sabemos que:

$$A_{i-2,i}(p^{n_1-n_2})B \in \mathcal{I}.$$

Luego,

$$n_1 - \beta(i,j) \geq n_1 - \beta(i-2,j).$$

Es decir,

$$\beta(i,j) \leq \beta(i-2,j)$$

para toda $i \geq 3$. Esto establece la primera parte de (i).

Ahora probamos que

$$\beta(i,j) \leq \beta(i+2,j) + n_1 - n_2,\ i \leq 2.$$

Sea $A_{i,i+2}(1)$ la matriz de S que tiene 1 en el lugar $(i,i+2)$ y 0 en los demás. Sea $B \in \mathcal{I}$. Entonces el renglón $i+2$ de la matriz $A_{i,i+2}(1)B$ es

$$p^{n_1-\beta(i,1)}\alpha_{i1} \quad p^{n_1-\beta(i,2)}\alpha_{i2} \quad p^{n_1-\beta(i,3)}\alpha_{i3} \quad p^{n_1-\beta(i,4)}\alpha_{i4}.$$

Como $A_{i,i+2}(1)B \in \mathcal{I}$, debemos tener

$$n_1 - \beta(i,j) \geq n_2 - \beta(i+2,j).$$

Luego

$$\beta(i,j) \leq n_1 - n_2 + \beta(i+2,j).$$

De este modo tenemos la segunda parte de (i).

(ii) Mostraremos que

$$\beta(i,j) \leq \beta(i,j-1),\ j \geq 2.$$

Sea $A_{j,j-1}(1)$, $j \in \{2,3,4\}$ la matriz que tiene 1 en el lugar $j,j-1$ y 0 en los demás. Sea $B \in \mathcal{I}$. Entonces la columna $j-1$ de la matriz $BA_{j,j-1}(1)$ es

$$\begin{matrix} p^{n_k-\beta(1,j)}\alpha_{1j} \\ p^{n_k-\beta(2,j)}\alpha_{2j} \\ p^{n_k-\beta(3,j)}\alpha_{3j} \\ p^{n_k-\beta(4,j)}\alpha_{4j} \end{matrix}.$$

Como $BA_{j,j-1}(1) \in \mathcal{I}$ entonces

$$n_k - \beta(i,j) \geq n_k - \beta(i,j-1)$$

y

$$\beta(i,j) \leq \beta(i,j-1).$$

De este modo concluimos la primera parte de (iv).

En seguida veremos que

$$\beta(i,j) \leq \beta(i,4) + n_1 - n_2,\ j \leq 2.$$

Consideramos la matriz $A_{j,4}(p^{n_1-n_2})$, misma que tiene $p^{n_1-n_2}$ en el lugar $j,4$ y 0 en el resto. Sea $B \in \mathcal{I}$. Entonces la cuarta columna de $BA_{j,4}(p^{n_1-n_2})$ es

$$\begin{matrix} p^{2n_1-n_2-\beta(1,j)}\alpha_{1j} \\ p^{2n_1-n_2-\beta(2,j)}\alpha_{2j} \\ p^{n_1-\beta(3,j)}\alpha_{3j} \\ p^{n_1-\beta(4,j)}\alpha_{4j} \end{matrix}.$$

Como $BA_{j,4}(p^{n_1-n_2}) \in \mathcal{I}$, entonces

$$2n_1 - n_2 - \beta(i,j) \geq n_1 - \beta(i,4)$$

si $i = 1,2$ y

$$n_1 - \beta(i,j) \geq n_2 - \beta(i,4)$$

si $i = 3,4$.

Luego, en todos los casos tenemos

$$\beta(i,j) \leq n_1 - n_2 + \beta(i,4),\ j \leq 2.$$

(iii) Sea $i \in \{2,4\}$. Veremos inicialmente que

$$\beta(i-1,j) \leq \beta(i,j).$$

Tomamos la matriz $A_{i,i-1}(1)$ que tiene 1 en el lugar $(i,i-1)$ y cero en los demás. Sea, como siempre, $B \in \mathcal{I}$. Entonces el i-ésimo renglón de $A_{i,i-1}(1)B$ es

$$p^{n_k-\beta(i-1,1)}\alpha_{i-1,1} \quad p^{n_k-\beta(i-1,2)}\alpha_{i-1,2} \quad p^{n_k-\beta(i-1,3)}\alpha_{i-1,3} \quad p^{n_k-\beta(i-1,4)}\alpha_{i-1,4}.$$

Puesto que $A_{i,i-1}(1)B \in \mathcal{I}$ debemos tener:

$$n_k - \beta(i-1,j) \geq n_k - \beta(i,j).$$

Luego,

$$\beta(i-1,j) \leq \beta(i,j).$$

A continuación mostramos que

$$\beta(i,j) \leq \beta(i-1,j)+1,\ i \in \{2,4\}\,.$$

En efecto, consideramos la matriz $A_{i-1,i}(p)$ de S que tiene p en el lugar $(i-1,i)$ y cero en los demás. Sea $B \in \mathcal{I}$.

Entonces el renglón $i-1$ del producto $A_{i-1,i}(p)B$ tiene la forma

$$p^{n_k-\beta(i,1)+1}\alpha_{i1} \quad p^{n_k-\beta(i,2)+1}\alpha_{i2} \quad p^{n_k-\beta(i,3)+1}\alpha_{i3} \quad p^{n_k-\beta(i,4)+1}\alpha_{i4}\ .$$

Como $A_{i-1,i}(p)B \in \mathcal{I}$, entonces

$$n_k-\beta(i,j)+1 \geq n_k-\beta(i-1,j).$$

De aquí que

$$\beta(i,j) \leq \beta(i-1,j)+1.$$

Por último, verificamos que

$$\beta(i,j) \leq \beta(i,j+1)+1,\ j \in \{1,3\}\,.$$

Sea $A_{j,j+1}(p)$ la matriz de S que tiene p en el lugar $(j,j+1)$. Sea $B \in \mathcal{I}$. Entonces la columna $j+1$ del producto $BA_{j,j+1}(p)$ tiene la forma

$$\begin{matrix} p^{n_1-\beta(1,j)+1}\alpha_{1j} \\ p^{n_1-\beta(2,j)+1}\alpha_{2j} \\ p^{n_2-\beta(3,j)+1}\alpha_{3j} \\ p^{n_2-\beta(4,j)+1}\alpha_{4j} \end{matrix}\ .$$

Como siempre, utilizamos que $BA_{j,j+1}(p) \in \mathcal{I}$ para obtener:

$$n_k-\beta(i,j)+1 \geq n_k-\beta(i,j+1).$$

Por tanto,

$$\beta(i,j) \leq \beta(i,j+1)+1$$

para $j \in \{1,3\}$.

Así concluimos la demostración del teorema. ■

Como S mismo es un ideal de S, existe una función

$$d : \mathrm{I}_4 \times \mathrm{I}_4 \to \mathrm{N}$$

tal que

$$S = \left\{ \left(p^{n_k-d(i,j)}\alpha_{ij}\right)_{4\times 4} : \alpha_{ij} \in \mathrm{Z}_{p^{n_k}} \right\}.$$

(ver el teorema 3.1). De hecho, la definición de d es la siguiente:

Definición Sea

$$d : \mathbf{I}_4 \times \mathbf{I}_4 \to \mathbf{N}$$

la función definida por la regla:

$$d(i,j) = \left\{ \begin{array}{c} n_k - 1 \text{ para } (i,j) \in \mathbf{I}_2 \times \mathbf{I}_2 \setminus \{(2,1)\} \cup \bar{\mathbf{I}}_4 \times \bar{\mathbf{I}}_4 \setminus \{(4,3)\} \\ n_1 \text{ si } (i,j) = (2,1) \\ n_2 \text{ en los demás casos} \end{array} \right\},$$

donde

$$\bar{\mathbf{I}}_4 = \{3,4\}\,.$$

A continuación, demostramos el recíproco del teorema 3.1.

Teorema 3.2 *Sea $\beta : \mathbf{I}_4 \times \mathbf{I}_4 \to \mathbf{N}$ una función que satisface las siguientes propiedades:*

(i)$\beta(i,j) \leq d(i,j)$
(ii)$\beta(i,j) \leq \beta(i-2,j)$, $i \geq 3$
$\beta(i,j) \leq \beta(i+2,j) + n_1 - n_2$, $i \leq 2$
(iii)$\beta(i,j) \leq \beta(i,j-1)$, $j \geq 2$
$\beta(i,j) \leq \beta(i,4) + n_1 - n_2$, $j \leq 2$
(iv)$\beta(i-1,j) \leq \beta(i,j) \leq \beta(i-1,j) + 1$, $i \in \{2,4\}$
$\beta(i,j+1) \leq \beta(i,j) \leq \beta(i,j+1) + 1$, $j \in \{1,3\}$.
Entonces

$$\mathcal{I}_\beta = \left\{ \left(p^{n_k - \beta(i,j)} \alpha_{ij}\right)_{4\times 4} : \alpha_{ij} \in \mathbf{Z}_{p^{n_k}} \right\}$$

es un ideal de S.

Demostración. Como $\mathcal{I}_d = S$, la propiedad (i) garantiza que $\mathcal{I}_\beta$ siempre está contenido en S.

Probaremos que $\mathcal{I}_\beta$ es un ideal de S. Si

$$A = \left(p^{n_k - \beta(i,j)} a_{ij}\right)$$

y

$$B = \left(p^{n_k - \beta(i,j)} b_{ij}\right)$$

pertenecen a $\mathcal{I}_\beta$, claramente

$$A - B = \left(p^{n_k - \beta(i,j)} a_{ij} - p^{n_k - \beta(i,j)} b_{ij}\right) = \left[p^{n_k - \beta(i,j)} \left(a_{ij} - b_{ij}\right)\right] \in \mathcal{I}_\beta.$$

Sea

$$E = \begin{bmatrix} pe_{11} & pe_{12} & p^{n_1-n_2}e_{13} & p^{n_1-n_2}e_{14} \\ e_{21} & pe_{22} & p^{n_1-n_2}e_{23} & p^{n_1-n_2}e_{24} \\ e_{31} & e_{32} & pe_{33} & pe_{34} \\ e_{41} & e_{42} & e_{43} & pe_{44} \end{bmatrix} \in S.$$

Calculamos AE para mostrar que está en $\mathcal{I}_\beta$. Escribimos a continuación la matriz producto AE indicando primero el lugar:

Para $i \in \{1,2\}$ tenemos:

$$(i,1)\ p^{n_1-\beta(i,1)+1}a_{i1}e_{11} + p^{n_1-\beta(i,2)}a_{i2}e_{21} + p^{n_1-\beta(i,3)}a_{i3}e_{31} + p^{n_1-\beta(i,4)}a_{i4}e_{41}$$

$$(i,2)\ p^{n_1-\beta(i,1)+1}a_{i1}e_{12} + p^{n_1-\beta(i,2)+1}a_{i2}e_{22} + p^{n_1-\beta(i,3)}a_{i3}e_{32} + p^{n_1-\beta(i,4)}a_{i4}e_{42}$$

$$(i,3)\ p^{2n_1-n_2-\beta(i,1)}a_{i1}e_{13} + p^{2n_1-n_2-\beta(i,2)}a_{i2}e_{23} + p^{n_1-\beta(i,3)+1}a_{i3}e_{33} + p^{n_1-\beta(i,4)}a_{i4}e_{43}$$

$$(i,4)\ p^{2n_1-n_2-\beta(i,1)}a_{i1}e_{14} + p^{2n_1-n_2-\beta(i,2)}a_{i2}e_{24} + p^{n_1-\beta(i,3)+1}a_{i3}e_{34} + p^{n_1-\beta(i,4)+1}a_{i4}e_{44}.$$

Para $i \in \{3,4\}$ tenemos:

$$(i,1)\ p^{n_2-\beta(i,1)+1}a_{i1}e_{11} + p^{n_2-\beta(i,2)}a_{i2}e_{21} + p^{n_2-\beta(i,3)}a_{i3}e_{31} + p^{n_2-\beta(i,4)}a_{i4}e_{41}$$

$$(i,2)\ p^{n_2-\beta(i,1)+1}a_{i1}e_{12} + p^{n_2-\beta(i,2)+1}a_{i2}e_{22} + p^{n_2-\beta(i,3)}a_{i3}e_{32} + p^{n_2-\beta(i,4)}a_{i4}e_{42}$$

$$(i,3)\ p^{n_1-\beta(i,1)}a_{i1}e_{13} + p^{n_1-\beta(i,2)}a_{i2}e_{23} + p^{n_2-\beta(i,3)+1}a_{i3}e_{33} + p^{n_2-\beta(i,4)}a_{i4}e_{43}$$

$$(i,4)\ p^{n_1-\beta(i,1)}a_{i1}e_{14} + p^{n_1-\beta(i,2)}a_{i2}e_{24} + p^{n_2-\beta(i,3)+1}a_{i3}e_{34} + p^{n_2-\beta(i,4)+1}a_{i4}e_{44}.$$

A continuación, utilizando las propiedades de β, escribimos las desigualdades que garantizan que cada entrada de la matriz AE tiene la forma $p^{n_k-\beta(i,j)}c_{ij}$.

Para $i \in \mathbf{I_4}$ obtenemos las desigualdades siguientes:

$$(1)\ \beta(i,1)-1, \beta(i,2), \beta(i,3), \beta(i,4) \leq \beta(i,1)$$

pues por la propiedad (iii),

$$\beta(i,4) \leq \beta(i,3) \leq \beta(i,2) \leq \beta(i,1).$$

$$(2)\ \beta(i,1)-1, \beta(i,2)-1, \beta(i,3), \beta(i,4) \leq \beta(i,2)$$

pues

$$\beta(i,4) \leq \beta(i,3) \leq \beta(i,2)$$

(propiedad (iii)) y

$$\beta(i,1)-1 \leq \beta(i,2)$$

(por la segunda parte de (iv)).

$$(3)\ \beta(i,1)-(n_1-n_2),\beta(i,2)-(n_1-n_2),\beta(i,3)-1,\beta(i,4)\leq\beta(i,3)$$

ya que

$$\beta(i,4)\leq\beta(i,3)$$

por (iii) y

$$\beta(i,2)-(n_1-n_2)\leq\beta(i,1)-(n_1-n_2)\leq\beta(i,4)\leq\beta(i,3)$$

(por (iii)).

$$(4)\ \beta(i,1)-(n_1-n_2),\beta(i,2)-(n_1-n_2),\beta(i,3)-1,\beta(i,4)-1\leq\beta(i,4)$$

puesto que

$$\beta(i,2)-(n_1-n_2)\leq\beta(i,1)-(n_1-n_2)\leq\beta(i,4)$$

(aplicando (iii)); y

$$\beta(i,3)-1\leq\beta(i,4)$$

(utilizando la propiedad (iv)).

De estas desigualdades obtenemos que $AE\in\mathcal{I}_\beta$. De manera análoga se demuestra que $EA\in\mathcal{I}_\beta$. Al probar que $EA\in\mathcal{I}_\beta$, se utiliza también la propiedad (ii).

Por lo tanto, $\mathcal{I}_\beta$ es un ideal de S. Esto concluye la demostración. ■

Definición Llamamos a la función β del teorema 3.2 **función ideal** de S.

La Serie Anuladora Superior

Corolario 3.1 *Supongamos que tenemos la serie anuladora superior de S:*

$$0=S_0\subset S_1\subset S_2\subset\cdots\subset S_n=S.$$

Entonces existe una función $f:\mathbf{I}_4\times\mathbf{I}_4\times(\mathbf{I}_n\cup\{0\})\to\mathbf{N}$ tal que

$$S_t=\left\{\left(p^{n_k-f(i,j,t)}\alpha_{ij}\right)_{4\times4}:\alpha_{ij}\in\mathbf{Z}_{p^{n_k}}\right\}$$

para todo anulador S_t de la serie.

Demostración. Esto es consecuencia directa del teorema 3.1 ya que la función β existe para cada ideal de S. En particular, existe una función ideal β^t para cada anulador S_t de la serie. Al considerar todos los anuladores de la serie podemos definir la función

$$f:\mathbf{I}_4\times\mathbf{I}_4\times(\mathbf{I}_n\cup\{0\})\to\mathbf{N}$$

mediante la regla

$$f(i,j,t) = \beta^t(i,j).$$

De este modo obtenemos el corolario. ■

El corolario 3.1 garantiza la existencia de una función que permite calcular las matrices de un anulador dado. En lo que sigue, establecemos las propiedades de la función f y llegamos a una definición recursiva de la misma.

Teorema 3.3 *Sea* $f : \mathrm{I}_4 \times \mathrm{I}_4 \times (\mathrm{I}_n \cup \{0\}) \to \mathrm{N}$ *la función del corolario 3.1. Consideramos también la función d, definida anteriormente. Entonces f satisface las siguientes propiedades:*

(i) $f(i,j,t) \leq d(i,j)$
(ii) $f(i,j,t-1) \leq f(i,j,t) \leq f(i,j,t-1)+1$
(iii) $f(i,j,t) \leq f(i-2,j,t-1)$, $i \geq 3$
$f(i,j,t) \leq f(i+2,j,t-1)+n_1-n_2$, $i \leq 2$
(iv) $f(i,j,t) \leq f(i,j-1,t-1)$, $j \geq 2$
$f(i,j,t) \leq f(i,4,t-1)+n_1-n_2$, $j \leq 2$
(v) $f(i-1,j,t) \leq f(i,j,t-1)$ y $f(i,j,t) \leq f(i-1,j,t-1)+1$, $i \in \{2,4\}$
(vi) $f(i,j,t) \leq f(i,j+1,t-1)+1$, $j \in \{1,3\}$.

Las propiedades (ii)-(vi) siguen siendo válidas si escribimos t en lugar de $t-1$.

Demostración. La demostración se basa en las propiedades de los anuladores S_t:

(1) $S_tS \subset S_{t-1}$, $SS_t \subset S_{t-1}$ (por definición de anulador)
(2) $S_tS \subset S_t$, $SS_t \subset S_t$ (los anuladores son ideales de S)
(3) $S_{t-1} \subset S_t$ (se trata de una serie).

(i) Para probar esta parte, notamos inicialmente que el último término de la serie anuladora superior es

$$S_n = S = \left\{\left(p^{n_k-d(i,j)}\alpha_{ij}\right)\right\}.$$

Consideramos ahora una terna arbitraria (i,j,t). Sabemos que los lugares (i,j) de las matrices en el anulador S_t tienen la forma $p^{n_k-f(i,j,t)}\alpha_{ij}$. Como S_t es un ideal de S, y por tanto está contenido en S, debe ocurrir que

$$n_k - f(i,j,t) \geq n_k - d(i,j).$$

Por tanto,

$$f(i,j,t) \leq d(i,j).$$

(ii) Puesto que $S_{t-1} \subset S_t$ debemos tener

$$n_k - f(i,j,t-1) \geq n_k - f(i,j,t).$$

Luego,

$$f(i,j,t-1) \leq f(i,j,t).$$

Ahora mostramos que

$$f(i,j,t) \leq f(i,j,t-1)+1.$$

Sea $A_{jj}(p)$ la matriz de S que tiene p en una entrada diagonal (j,j) cualquiera y 0 en las demás. Sea $B \in S_t$. Entonces la matriz $BA_{jj}(p)$ tiene por j-ésima columna a

$$\begin{matrix} p^{n_1-f(1,j,t)+1}\alpha_{12} \\ p^{n_1-f(2,j,t)+1}\alpha_{22} \\ p^{n_2-f(3,j,t)+1}\alpha_{32} \\ p^{n_2-f(4,j,t)+1}\alpha_{42} \end{matrix}$$

Como $BA_{jj}(p) \in S_{t-1}$ debemos tener:

$$n_k - f(i,j,t)+1 \geq n_k - f(i,j,t-1).$$

Luego,

$$f(i,j,t) \leq f(i,j,t-1)+1.$$

De este modo probamos (ii).

(iii) Mostramos a continuación que

$$f(i,j,t) \leq f(i-2,j,t-1),\ i \geq 3.$$

Sea $A_{i-2,i}(p^{n_1-n_2})$ la matriz de S que tiene $p^{n_1-n_2}$ en la entrada $(i-2,i)$ y 0 en las demás. Sea $B = \left(p^{n_k-f(i,j,t)}\alpha_{ij}\right)$ una matriz cualquiera en S_t. Entonces la fila $i-2$ de la matriz $A_{i-2,i}(p^{n_1-n_2})B$ es

$$p^{n_1-f(i,1,t)}\alpha_{i1} \quad p^{n_1-f(i,2,t)}\alpha_{i2} \quad p^{n_1-f(i,3,t)}\alpha_{i3} \quad p^{n_1-f(i,4,t)}\alpha_{i4}.$$

Por la propiedad (1)

$$A_{i-2,i}(p^{n_1-n_2})B \in S_{t-1}.$$

Luego,

$$n_1 - f(i,j,t) \geq n_1 - f(i-2,j,t-1).$$

Es decir,

$$f(i,j,t) \leq f(i-2,j,t-1)$$

para toda $i \geq 3$. Esto establece la primera parte de (iii).

Ahora probamos que

$$f(i,j,t) \leq f(i+2,j,t-1)+n_1-n_2,\ i \leq 2.$$

Sea $A_{i,i+2}(1)$ la matriz de S que tiene 1 en el lugar $(i,i+2)$ y 0 en los demás. Sea $B \in S_t$. Entonces el renglón $i+2$ de la matriz $A_{i,i+2}(1)B$ es

$$p^{n_1-f(i,1,t)}\alpha_{i1} \quad p^{n_1-f(i,2,t)}\alpha_{i2} \quad p^{n_1-f(i,3,t)}\alpha_{i3} \quad p^{n_1-f(i,4,t)}\alpha_{i4}.$$

Como $A_{i,i+2}(1)B \in S_{t-1}$, debemos tener

$$n_1 - f(i,j,t) \geq n_2 - f(i+2,j,t-1).$$

Luego

$$f(i,j,t) \leq n_1 - n_2 + f(i+2,j,t-1).$$

De este modo tenemos la segunda parte de (iii).

(iv) Mostraremos que

$$f(i,j,t) \leq f(i,j-1,t-1),\ j \geq 2.$$

Sea $A_{j,j-1}(1)$, $j \in \{2,3,4\}$ la matriz que tiene 1 en el lugar $j, j-1$ y 0 en los demás. Sea $B \in S_t$. Entonces la columna $j-1$ de la matriz $BA_{j,j-1}(1)$ es

$$\begin{matrix} p^{n_k - f(1,j,t)}\alpha_{1j} \\ p^{n_k - f(2,j,t)}\alpha_{2j} \\ p^{n_k - f(3,j,t)}\alpha_{3j} \\ p^{n_k - f(4,j,t)}\alpha_{4j} \end{matrix}.$$

Como $BA_{j,j-1}(1) \in S_{t-1}$ entonces

$$n_k - f(i,j,t) \geq n_k - f(i,j-1,t-1)$$

y

$$f(i,j,t) \leq f(i,j-1,t-1).$$

De este modo concluimos la primera parte de (iv).

En seguida veremos que

$$f(i,j,t) \leq f(i,4,t-1) + n_1 - n_2,\ j \leq 2.$$

Consideramos la matriz $A_{j,4}(p^{n_1-n_2})$, misma que tiene $p^{n_1-n_2}$ en el lugar $j, 4$ y 0 en el resto. Sea $B \in S_t$. Entonces la cuarta columna de $BA_{j,4}(p^{n_1-n_2})$ es

$$\begin{matrix} p^{2n_1-n_2-f(1,j,t)}\alpha_{1j} \\ p^{2n_1-n_2-f(2,j,t)}\alpha_{2j} \\ p^{n_1-f(3,j,t)}\alpha_{3j} \\ p^{n_1-f(4,j,t)}\alpha_{4j} \end{matrix}.$$

Como $BA_{j,4}(p^{n_1-n_2}) \in S_{t-1}$, entonces

$$2n_1 - n_2 - f(i,j,t) \geq n_1 - f(i,4,t-1)$$

si $i = 1,2$ y

$$n_1 - f(i,j,t) \geq n_2 - f(i,4,t-1)$$

si $i = 3, 4$.

Luego, en todos los casos tenemos

$$f(i,j,t) \leq n_1 - n_2 + f(i,4,t-1),\ j \leq 2.$$

(v) Sea $i \in \{2,4\}$. Veremos inicialmente que

$$f(i-1,j,t) \leq f(i,j,t-1).$$

Tomamos la matriz $A_{i,i-1}(1)$ que tiene 1 en el lugar $(i, i-1)$ y cero en los demás. Sea, como siempre, $B \in S_t$. Entonces el i-ésimo renglón de $A_{i,i-1}(1)B$ es

$$p^{n_k - f(i-1,1,t)}\alpha_{i-1,1} \quad p^{n_k - f(i-1,2,t)}\alpha_{i-1,2} \quad p^{n_k - f(i-1,3,t)}\alpha_{i-1,3} \quad p^{n_k - f(i-1,4,t)}\alpha_{i-1,4}\ .$$

Puesto que $A_{i,i-1}(1)B \in S_{t-1}$ debemos tener:

$$n_k - f(i-1,j,t) \geq n_k - f(i,j,t-1).$$

Luego,

$$f(i-1,j,t) \leq f(i,j,t-1).$$

A continuación mostramos que

$$f(i,j,t) \leq f(i-1,j,t-1) + 1,\ i \in \{2,4\}\,.$$

En efecto, consideramos la matriz $A_{i-1,i}(p)$ de S que tiene p en el lugar $(i-1,i)$ y cero en los demás. Sea $B \in S_t$.

Entonces el renglón $i-1$ del producto $A_{i-1,i}(p)B$ tiene la forma

$$p^{n_k - f(i,1,t)+1}\alpha_{i1} \quad p^{n_k - f(i,2,t)+1}\alpha_{i2} \quad p^{n_k - f(i,3,t)+1}\alpha_{i3} \quad p^{n_k - f(i,4,t)+1}\alpha_{i4}\ .$$

Como $A_{i-1,i}(p)B \in S_{t-1}$, entonces

$$n_k - f(i,j,t) + 1 \geq n_k - f(i-1,j,t-1).$$

De aquí que

$$f(i,j,t) \leq f(i-1,j,t-1) + 1.$$

De este modo terminamos la prueba de (v).

(vi) Por último, verificamos que

$$f(i,j,t) \leq f(i,j+1,t-1) + 1,\ j \in \{1,3\}\,.$$

Sea $A_{j,j+1}(p)$ la matriz de S que tiene p en el lugar $(j, j+1)$. Sea $B \in S_t$. Entonces la columna $j+1$ del producto $BA_{j,j+1}(p)$ tiene la forma

$$\begin{matrix} p^{n_1 - f(1,j,t)+1}\alpha_{1j} \\ p^{n_1 - f(2,j,t)+1}\alpha_{2j} \\ p^{n_2 - f(3,j,t)+1}\alpha_{3j} \\ p^{n_2 - f(4,j,t)+1}\alpha_{4j} \end{matrix}\ .$$

Como siempre, utilizamos que $BA_{j,j+1}(p) \in S_{t-1}$ para obtener:

$$n_k - f(i,j,t) + 1 \geq n_k - f(i,j+1,t-1).$$

Por tanto,

$$f(i,j,t) \leq f(i,j+1,t-1) + 1$$

para $j \in \{1,3\}$.

Finalmente, notamos que podemos escribir t en lugar de $t-1$ en las expresiones (ii)-(vi) por la propiedad (2) enunciada al inicio de esta demostración. Con esto terminamos la prueba del teorema. ■

Ahora probamos el recíproco del teorema 3.3.

Teorema 3.4 *Sea* $f : \mathbf{I}_4 \times \mathbf{I}_4 \times (\mathbf{I}_n \cup \{0\}) \to \mathbf{N}$ *una función que satisface las propiedades del teorema 3.3 y tal que*

$$f(i,j,0) = 0.$$

Entonces, para toda t, $0 \leq t \leq n$;

$$U_t = \left\{ \left(p^{n_k - f(i,j,t)} \alpha_{ij} \right)_{4\times 4} : \alpha_{ij} \in \mathbf{Z}_{p^{n_k}} \right\}$$

es un ideal de S *contenido en el el* t*-ésimo anulador* S_t.

Demostración. La prueba de que se cumplen las propiedades:

(1) $U_tS \subset U_{t-1}$, $SU_t \subset U_{t-1}$

(2) $U_tS \subset U_t$, $SU_t \subset U_t$

es análoga a la del teorema 3.2. Además, por la propiedad (ii) del teorema 3.3 también es válido:

(3) $U_{t-1} \subset U_t$.

Más aún, notamos que $U_0 = 0$ pues $f(i,j,0) = 0$.

La propiedad (2) muestra que U_t es un ideal de S para toda t.

Probamos ahora por inducción que U_t está contenido en S_t para toda t en $\{0,...,n\}$.

Para $t = 0$, tenemos:

$$U_0 = S_0 = 0.$$

Supongamos ahora que

$$U_{t-1} \subset S_{t-1}.$$

Mostramos que

$$U_t \subset S_t.$$

En efecto, como U_tS y SU_t están contenidos en U_{t-1}; por hipótesis de inducción debemos tener que U_tS y SU_t están contenidos en S_{t-1}. Por definición de anulador, obtenemos el resultado. Así concluimos la prueba del teorema. ■

Definición La función del teorema 3.4 se llama **función anuladora** del anillo S.

A continuación damos una definición recursiva de una función que permite caracterizar a los anuladores S_t. Primero definimos dos funciones: una "interna" a cada célula (g_1) y otra "externa" (g_0).

Definición Sea

$$g_1 : \mathbf{I}_5 \cup \{0\} \times \mathbf{I}_5 \cup \{0\} \times \mathbf{I}_n \cup \{0\} \to \mathbf{N} \cup \{\infty\}$$

definida por

$$g_1(i,j,t) = \infty \text{ si } (i,j) \notin \mathbf{I}_4 \times \mathbf{I}_4$$

y recursivamente para $(i,j) \in \mathbf{I}_4 \times \mathbf{I}_4$ como:

$$g_1(i,j,0) = 0.$$

Si $t \geq 1$:

$$g_1(i,j,t) = \min \left\{ \begin{array}{c} g_1(i,j,t-1)+1, g_1(i+1,j,t-1), g_1(i,j+1,t-1)+1 \\ g_1(i,j-1,t-1), g_1(i-1,j,t-1)+1 \end{array} \right\}$$

donde las expresiones en $t-1$ toman el valor ∞ si éstas *no actúan* en la célula de (i,j).

Definición Sea

$$g_0 : \mathbf{I}_5 \cup \{0\} \times \mathbf{I}_5 \cup \{0\} \times \mathbf{I}_n \cup \{0\} \to \mathbf{N} \cup \{\infty\}$$

definida como

$$g_0(i,j,t) = \infty \text{ si } (i,j) \notin \mathbf{I}_4 \times \mathbf{I}_4$$

y recursivamente para $(i,j) \in \mathbf{I}_4 \times \mathbf{I}_4$ como:

$$g_0(i,j,0) = 0.$$

Si $t \geq 1$:

$$g_0(i,j,t) = \min \left\{ \begin{array}{c} g_0(i,j^+,t-1)+n_1-n_2, g_0(i^+,j,t-1)+n_1-n_2, \\ g_0(i^-,j,t-1), g_0(i,j^-,t-1) \end{array} \right\}$$

donde

$$\begin{array}{rcl} i^+, j^+ & \in & \{3,4\} \text{ si } i,j \in \{1,2\}; \\ i^+, j^+ & \in & \{5\} \text{ en los otros casos.} \end{array}$$

e

$$\begin{array}{rcl} i^-, j^- & \in & \{1,2\} \text{ si } i,j \in \{3,4\}; \\ i^-, j^- & \in & \{5\} \text{ en los demás casos.} \end{array}$$

Definición Sea

$$g : \mathbf{I}_4 \times \mathbf{I}_4 \times \mathbf{I}_n \cup \{0\} \to \mathbf{N}$$

una función definida recursivamente como:

$$g(i,j,0) = 0.$$

Si $t \geq 1$:

$$g(i,j,t) = \min\{g_1(i,j,t), g_0(i,j,t), d(i,j)\}.$$

Teorema 3.5 *Consideramos la serie anuladora superior de* S

$$0 = S_0 \subset S_1 \subset S_2 \subset \cdots \subset S_n = S.$$

Entonces

$$S_t = \left\{ \left(p^{n_k - g(i,j,t)}\alpha_{ij}\right)_{4\times 4} : \alpha_{ij} \in \mathbf{Z}_{p^{n_k}} \right\}$$

para toda $t \in \{0, ..., n\}$, *donde* g *es la función recién definida.*

Demostración. Nuestro primer objetivo es demostrar que g es una función anuladora. La prueba es por inducción sobre t. Como $g(i,j,0) = 0$, la base de inducción es válida. Supongamos, como hipótesis de inducción, que g cumple:

(i)$g(i,j,t-1) \leq d(i,j)$

(ii)$g(i,j,t-2) \leq g(i,j,t-1) \leq g(i,j,t-2) + 1$

(iii)$g(i,j,t-1) \leq g(i-2,j,t-2)$, $i \geq 3$

$g(i,j,t-1) \leq g(i+2,j,t-2) + n_1 - n_2$, $i \leq 2$

(iv)$g(i,j,t-1) \leq g(i,j-1,t-2)$, $j \geq 2$

$g(i,j,t-1) \leq g(i,4,t-2) + n_1 - n_2$, $j \leq 2$

(v)$g(i-1,j,t-1) \leq g(i,j,t-2)$ y $g(i,j,t-1) \leq g(i-1,j,t-2)+1$, $i \in \{2,4\}$

(vi)$g(i,j,t-1) \leq g(i,j+1,t-2)+1$, $j \in \{1,3\}$.

Supongamos también que las propiedades (ii)-(vi) siguen siendo válidas si escribimos $t-1$ en lugar de $t-2$.

Utilizando la definición recursiva de g se verifica que se cumplen las propiedades (i)-(vi) para toda t. Lo único que requiere demostración es que:

$$g(i,j,t-1) \leq g(i,j,t)$$

y que las propiedades (ii)-(vi) siguen valiendo en la misma t.

Supongamos primero que $g = g_1$. Si

$$g(i,j,t) = g_1(i,j,t-1) + 1$$

entonces

$$g(i,j,t) \geq g_1(i,j,t-1) + 1 \geq g_1(i,j,t-1) \geq g(i,j,t-1).$$

Si

$$g(i,j,t) = g_1(i+1,j,t-1),\ i \in \{1,3\}$$

entonces

$$g(i,j,t) \geq g(i+1,j,t-1)$$

por definición de g. Por hipótesis de inducción,

$$g(i+1,j,t-1) \geq g(i,j,t-1).$$

Si

$$g(i,j,t) = g_1(i,j+1,t-1)+1,\ j \in \{1,3\}$$

entonces

$$g(i,j,t) \geq g(i,j+1,t-1)+1 \geq g(i,j,t-1).$$

Supongamos ahora que

$$g(i,j,t) = g_1(i,j-1,t-1),\ j \in \{2,4\}$$

entonces

$$g(i,j,t) \geq g(i,j-1,t-1) \geq g(i,j,t-1).$$

Si tenemos

$$g(i,j,t) = g_1(i-1,j,t-1)+1,\ i \in \{2,4\}$$

se cumple

$$g(i,j,t) \geq g(i-1,j,t-1)+1 \geq g(i,j,t-1).$$

Por tanto, $g = g_1$ es creciente en t.

Supongamos ahora que $g = g_0$. De manera análoga, consideramos los distintos subcasos, a saber:

(i) $g(i,j,t) = g_0(i,j^+,t-1)+n_1-n_2,\ j \in \{1,2\}$ implica:

$$g(i,j,t) \geq g(i,j^+,t-1)+n_1-n_2 \geq g(i,j,t-1).$$

(ii) Si $g(i,j,t) = g_0(i^+,j,t-1)+n_1-n_2,\ i \in \{1,2\}$ entonces

$$g(i,j,t) \geq g(i^+,j,t-1)+n_1-n_2 \geq g(i,j,t-1).$$

(iii) $g(i,j,t) = g_0(i^-,j,t-1),\ i \in \{3,4\}$ *implica que*

$$g(i,j,t) \geq g(i^-,j,t-1) \geq g(i,j,t-1).$$

(iv) Por último, $g(i,j,t) = g_0(i,j^-,t-1),\ j \in \{3,4\}$ da lugar a

$$g(i,j,t) \geq g(i,j^-,t-1) \geq g(i,j,t-1).$$

Finalmente, notamos que si $g(i,j,t) = d(i,j)$, claramente

$$g(i,j,t-1) \leq g(i,j,t).$$

Por lo tanto, g es creciente en t y se cumplen todas las propiedades (i)-(vi). También por ser g creciente, las propiedades (ii)-(vi) son válidas en la misma t. Así mostramos que g es una función anuladora.

Ponemos a continuación:

$$W_t = \left\{ \left(p^{n_k - g(i,j,t)}\alpha_{ij}\right)_{4\times 4} : \alpha_{ij} \in \mathbf{Z}_{p^{n_k}} \right\}.$$

Por el teorema 3.4, W_t es un ideal de S contenido en el t-ésimo anulador S_t para $t \in \{0,...,n\}$.

Mostramos ahora que $S_t \subset W_t$ para $t \in \{0,...,n\}$. De nuevo, la prueba es por inducción sobre t. Si $t = 0$, entonces $S_0 = 0 = W_0$. Supongamos, como hipótesis de inducción, que $S_{t-1} \subset W_{t-1}$. Tenemos en realidad

$$S_{t-1} = W_{t-1}.$$

Si f es la función anuladora asociada a los S_t, tenemos también

$$f(i,j,t-1) = g(i,j,t-1). \tag{3.1}$$

Basta probar que $f(i,j,t) \leq g(i,j,t)$. Utilizamos que f satisface las propiedades del teorema 3.3 y 3.1 para obtener las desigualdades siguientes:

(i)$f(i,j,t) \leq d(i,j)$

(ii)$f(i,j,t) \leq g(i,j,t-1) + 1$

(iii)$f(i,j,t) \leq g(i-2,j,t-1)$, $i \geq 3$

$f(i,j,t) \leq g(i+2,j,t-1) + n_1 - n_2$, $i \leq 2$

(iv)$f(i,j,t) \leq g(i,j-1,t-1)$, $j \geq 2$

$f(i,j,t) \leq g(i,4,t-1) + n_1 - n_2$, $j \leq 2$

(v)$f(i-1,j,t) \leq g(i,j,t-1)$ y $f(i,j,t) \leq g(i-1,j,t-1) + 1$, $i \in \{2,4\}$

(vi)$f(i,j,t) \leq g(i,j+1,t-1) + 1$, $j \in \{1,3\}$.

Puesto que g se define como el mínimo de estas expresiones en $t-1$, y f es menor ó igual que ese mínimo, debemos tener

$$f(i,j,t) \leq g(i,j,t).$$

Por lo tanto, $S_t = W_t$ para $t \in \{0,...,n\}$. Así concluimos la demostración. ■

El teorema 3.5 es el resultado central de este trabajo: la función anuladora g caracteriza a la serie anuladora superior de S.

A continuación obtenemos una expresión directa (no recursiva) para g cuando $n_1 - n_2 \geq 2$.

Definición Sea

$$h : \mathbf{I}_4 \times \mathbf{I}_4 \times \mathbf{I}_n \cup \{0\} \to \mathbf{N}$$

definida como:

$$h(i,j,t) = \left\{ \begin{array}{c} 0 \text{ si } t-j+i-4(k(i)-1) < 0 \\ \min\left\{ \left[\frac{t-j+i-4(k(i)-1)}{2} \right], d(i,j) \right\} \text{ si } t-j+i-4(k(i)-1) \geq 0 \end{array} \right\}$$

Teorema 3.6 *$h = g$ si $n_1 - n_2 \geq 2$.*

Demostración. La prueba es por inducción sobre t.

Si $t = 0$ se verifica fácilmente que $h(i,j,0) = 0$ para toda pareja $(i,j) \in \mathrm{I}_4 \times \mathrm{I}_4$. Esto muestra que $h(i,j,0) = g(i,j,0)$.

Si $t = 1$ también es fácil notar que $g(i,j,1) = 0 = h(i,j,1)$ para $(i,j) \neq (2,1)$. Ahora:

$$\begin{aligned} h(2,1,1) &= \min\left\{ \left[\frac{t-j+i-4(k(i)-1)}{2} \right], d(2,1) \right\} = \\ &= \min\{1, d(2,1)\} = \min\{1, n_1\} = 1 = g(2,1,1). \end{aligned}$$

Luego, para $t \in \{1,2\}$,

$$h(i,j,t) = g(i,j,t).$$

Supongamos ahora que $h(i,j,t-1) = g(i,j,t-1)$. Mostramos a continuación que $h(i,j,t) = g(i,j,t)$. Utilizando la definición de g y la hipótesis de inducción tenemos:

$$g(1,1,t) = \min\left\{ \begin{array}{c} n_1 - 1, h(1,1,t-1) + 1, h(3,1,t-1) + n_1 - n_2, \\ h(1,4,t-1) + n_1 - n_2, h(2,1,t-1), h(1,2,t-1) + 1 \end{array} \right\}. \tag{3.2}$$

Ahora:

$$h(1,1,t-1) = \min\left\{ n_1 - 1, \left[\frac{t-1}{2} \right] \right\}$$

$$h(3,1,t-1) = \min\left\{ \begin{array}{c} 0 \text{ si } t-3 < 0 \\ \min\left\{ n_2, \left[\frac{t-3}{2} \right] \right\} \text{ si } t-3 \geq 0 \end{array} \right\}$$

$$h(1,4,t-1) = \min\left\{ \begin{array}{c} 0 \text{ si } t-4 < 0 \\ \min\left\{ n_2, \left[\frac{t-4}{2} \right] \right\} \text{ si } t-4 \geq 0 \end{array} \right\}$$

$$h(2,1,t-1) = \min\left\{ n_1, \left[\frac{t}{2} \right] \right\}$$

$$h(1,2,t-1) = \left\{ \begin{array}{c} 0 \text{ si } t-2<0 \\ n_1 - 1, \left[\frac{t-2}{2}\right] \text{ si } t-2 \geq 0 \end{array} \right\}.$$

Vemos que $g(1,1,t) = h(2,1,t-1)$. Para esto, basta verificar que $h(2,1,t-1)$ es el mínimo de las expresiones que involucran a $t-1$ en 3.2.

Supongamos que

$$h(2,1,t-1) = n_1.$$

Si $h(1,1,t-1)+1 = n_1$ entonces

$$h(2,1,t-1) \leq h(1,1,t-1)+1.$$

Si $h(1,1,t-1)+1 = \left[\frac{t-1}{2}\right]+1$ entonces

$$n_1 \leq \left[\frac{t}{2}\right] \leq \left[\frac{t-1}{2}\right]+1.$$

Luego, en este caso también se cumple que

$$h(2,1,t-1) \leq h(1,1,t-1)+1.$$

Supongamos ahora que

$$h(2,1,t-1) = \left[\frac{t}{2}\right].$$

Si $h(1,1,t-1)+1 = n_1$ entonces

$$\left[\frac{t}{2}\right] \leq n_1$$

y

$$h(2,1,t-1) \leq h(1,1,t-1)+1.$$

Si

$$h(1,1,t-1)+1 = \left[\frac{t-1}{2}\right]+1$$

entonces

$$\left[\frac{t}{2}\right] \leq \left[\frac{t-1}{2}\right]+1$$

y por tanto se cumple de nuevo

$$h(2,1,t-1) \leq h(1,1,t-1)+1.$$

De manera análoga se demuestra que $h(2,1,t-1)$ es menor ó igual que el resto de las expresiones que involucran a $t-1$ en 3.2. Por lo tanto,

$$\begin{aligned} g(1,1,t) &= \min\{n_1-1, h(2,1,t-1)\} = \\ &= \min\left\{n_1-1, \left[\frac{t}{2}\right], n_1\right\} = \min\left\{n_1-1, \left[\frac{t}{2}\right]\right\} = \\ &= h(1,1,t). \end{aligned}$$

Del mismo modo se verifica que $g(i,j,t) = h(i,j,t)$ para los restantes (i,j). En el curso de algunos de estos cálculos es necesaria la hipótesis: $n_1 - n_2 \geq 2$.

Así concluimos la prueba del teorema. ■

Longitud de la Serie Anuladora Superior

Para finalizar este trabajo, obtenemos la longitud de la serie anuladora superior en el caso: $n_1 - n_2 \geq 2$.

Teorema 3.7 *La longitud de la serie anuladora superior de S es*

$$2n_1 - 1$$

si $n_1 - n_2 \geq 2$.

Demostración. Debemos probar los siguiente:
(i) $S_{2n_1-1} = S$ y
(ii) S_{2n_1-2} está propiamente contenido en S.
Sea $A \in S$. Entonces

$$A = \left(p^{n_k - d(i,j)}\alpha_{ij}\right).$$

Queremos verificar que

$$d(i,j) = h(i,j,2n_1-1).$$

En efecto,

$$h(1,1,2n_1-1) = \min\left\{\left[\frac{2n_1-1}{2}\right], n_1-1\right\}$$

pues $2n_1 - 1 > 0$.

Luego,

$$h(1,1,2n_1-1) = n_1 - 1 = d(1,1).$$

Del mismo modo,

$$h(1,2,2n_1-1) = \min\left\{\left[\frac{2n_1-2}{2}\right], n_1-1\right\}$$

ya que $2n_1 - 2 > 0$.

Entonces,

$$h(1,2,2n_1-1) = n_1 - 1 = d(1,2).$$

De manera análoga se verifica que

$$h(i,j,2n_1-1) = d(i,j)$$

para los (i,j) restantes. Por tanto,

$$S_{2n_1-1} = S.$$

Para demostrar (ii), basta exhibir una matriz en S que no pertenezca a S_{2n_1-2}. Ponemos

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \overline{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \in S.$$

Supongamos que $A \in S_{2n_1-2}$. Entonces

$$\overline{1} = \overline{p^{n_1-g(2,1,2n_1-2)}\alpha_{21}}$$

para algún $\alpha_{21} \in \mathbf{Z}$.

Ahora:

$$g(2,1,2n_1-2) = \min\left\{\left[\frac{2n_1-1}{2}\right], n_1\right\}$$

y por tanto

$$g(2,1,2n_1-2) = \min\{n_1-1, n_1\} = n_1 - 1.$$

Entonces

$$\overline{1} = \overline{p^{n_1-(n_1-1)}\alpha_{21}} = \overline{p\alpha_{21}}.$$

Por tanto, $1 - p\alpha_{21} = p^{n_1}\beta$ para algún $\beta \in \mathbf{Z}$, pero esto es imposible.

Así, S_{2n_1-2} está propiamente contenido en S. De esta manera terminamos la demostración. ■

El siguiente corolario (el último resultado de este trabajo) es una consecuencia directa del teorema anterior.

Corolario 3.2 *Si $n_1 - n_2 \geq 2$, entonces $2n_1 - 1$ es una cota superior para el grado de nilpotencia de P.*

Demostración. Este hecho es inmediato a partir del teorema precedente y del 2.6. ■

Bibliografía

[1] F. W. ANDERSON, K. R. FULLER, "Rings and Categories of Modules," Springer-Verlag, New York/Heidelberg/Berlin, 1974, 165-169.

[2] M. A. AVIÑÓ, R. BAUTISTA, The Upper Annihilating Series of the Radical of the Endomorphism Ring of a Finite Abelian p-Group, enviado a *Communications in Algebra.*

[3] P. DUBREIL, M. L. DUBREIL-JACOTIN, "Lecons d'Algebre Moderne," Collection Universitaire de Mathématiques, Dunod, Paris, 1961.

[4] J. B. FRALEIGH, "Algebra Abstracta," Addison-Wesley Iberoamericana, Wilmington, Delaware, 1987.

[5] L. FUCHS, "Abelian Groups," Third Edition, Second Reprint, Akadémiai Kiadó, Budapest, 1966, 43, 212-213.

[6] R. S. PIERCE, Homomorphisms of Primary Abelian Groups, *Topics in Abelian Groups*, J. M. Irwin and E. A. Walker, Scott, Foresman and Company, 1963, 215-310.

[7] J. J. ROTMAN, "An Introduction to the Theory of Groups," Third Edition, Allyn and Bacon, Inc., Boston/London/Sydney/Toronto, 1984, 73-81, 97.

[8] K. SHODA, Über die Automorphismen einer endlichen abelschen Gruppe, *Math. Ann.* 100 (1928), 674-686.