UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

ANILLO DE ENDOMORFISMOS Y GRUPO DE AUTOMORFISMOS DE UN p-GRUPO ABELIANO FINITO

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A :

M O I S E S   L U N A   B E N O S O

DIRECTOR DE TESIS: DRA. MARIA ALICIA AVIÑO DIAZ

2000

UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

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

"Anillo de endomorfismos y grupo de automorfismos de un p-grupo abeliano finito"

realizado por Luna Benoso Moisés

con número de cuenta 9455850-6 , pasante de la carrera de Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio

Atentamente

Director de Tesis Propietario	Dra. María Alicia Aviño Díaz	
Propietario	Dr. Raymundo Bautista Ramos	
Propietario	Dr. Juan Morales Rodríguez	
Suplente	Dra. Bertha María Tomé Arreola	
Suplente	Dr. Bernardo Llano Pérez	

Consejo Departamental de Matemáticas

DR. HÉCTOR MÉNDEZ LANGO

A mi sobrina Jéssica V

Deseo expresar mis agradecimientos a las personas siguientes:

A la Dra. María Alicia por la paciencia que me tuvo durante la realización de esta tesis, por la gran amistad, estimulo y confianza que siempre me ha brindado y por ser una excelente profesora que contribuyo en gran medida a mi formación Matemática.

A mis sinodales por sus observaciones, comentarios y correcciones que aportaron en este trabajo.

A Héctor, José Guadalupe, Gamaliel, Ana Lilia, Miguel, Raúl, Gabriel por su amistad y el apoyo que me han dado. A Rosalba por su afecto y comprensión.

A mis cuates Carlos, José Cruz y Alejandro por ayudarme en la elaboración de este trabajo.

A mis padres Cesáreo y Hermelinda por el cariño y apoyo que siempre me han brindado y por estar en los momentos que los necesite.

A mi hermano Benjamín por que ha sido importante para que yo terminara mis estudios y a mi hermana Esmeralda por su estimulo durante estos años y por haber tenido una hija maravillosa.

A mi prima Florencia por ser una persona muy disponible y haberme ayudado en momentos difíciles de mis estudios. A mi tío Juan y a mi prima Lilia ya que ellos contribuyeron de alguna forma en la realización de esta tesis.

Índice

Introducción

El estudio del grupo de automorfismos y del anillo de endomorfismos de un p-grupo abeliano finito G fué iniciado por K. Shoda en 1928, en su trabajo "*Ober die Automorphismen einer endlichen Abelshchen Gruppe*" [8]. En este trabajo se describen los endomorfismos de G mediante matrices cuyas entradas estan por filas en diferentes anillos $\mathbb{Z}_{p^n}$ y además, se da una caracterización para las matrices que representan automorfismos.

La estructura de los p-grupos abelianos finitos fué completamente descrita en 1878 por Frobenius y Stikelberger [5] mediante el "Teorema Fundamental de los Grupos Abelianos Finitamente Generados" y constituye en la teoría de grupos el primer teorema estructural.

En 1976 el profesor L. Kaloajnine de la Universidad Estatal de Kiev planteó estudiar el grupo de automorfismos de un p-gupo abeliano finito a partir de sus subgrupos y de la descripción de Shoda, en particular calcular el grado de nilpotencia de los p-subgrupos del grupo de automorfismos de G.

En el trabajo "*The maximal normal p-subgrupo of the automorphism group of a finite abelian p-group*", [9] M. A. Aviñó y R. Bautista describen completamente la serie central superior del p-grupo obteniendo su grado de nilpotencia en términos de los invariantes del grupo G. Para obtener este resultado describen una sucesión de ideales del radical de Jacobson del anillo de endomorfismos de G, que está asociada a la serie central superior (serie ascendente).

El objetivo de esta tesis es calcular el grado de nilpotencia de un p-subgrupo de Sylow P del grupo de automorfismos del grupo G, cuando G es de tipo $(p^m, p^m, p^m, p^n, p^n)$ con $m > n$, utilizando el metodo desarrollado en [9]. Este problema esta abierto y fué planteado a la directora de tesis por el matemático húngaro Lacsi Kovacks en 1996.

Los cinco capítulos de la tesis estan organizados como sigue. En el primer capítulo presentamos las definiciones y resultados de la teoría de grupos y anillos necesarios para el desarrollo del trabajo. Introducimos el concepto de serie anuladora y serie anuladora superior de un anillo.

En el capítulo 2, se describen matricialmente los endomorfirmos del grupo G y los resultados de K. Shoda en un lenguaje más moderno. Se calcula el orden del grupo de automorfismos de

G cuando G es de tipo $(p^m, p^m, p^m, p^n, p^n)$ con $m > n$ y se estudia el subanillo S del anillo $End\ G$ (Endomorfismos de G) el cual está asociado al p-subgrupo de Sylow $P = S + \{I\}$ de $aut\ G$ (Automorfismos de G)

En los capítulos 3 y 4 se describen los ideales de la serie anuladora superior de S mediante funciones y se obtiene la longitud de la serie

En el capítulo 5 se obtiene la serie central superior (ascendente) del grupo P y su grado de nilpotencia. Los resultados obtenidos en los capítulos 4 y 5 son resultados nuevos.

Capítulo 1

PRELIMINARES

En este capítulo presentamos las definiciones y resultados de la teoría de grupos y anillos, necesarios para el desarrollo de esta tesis.

1.1 Teoría de grupos abelianos.

Proposición 1.1 *Sean $H_1, \dots, H_n$, una familia de subgrupos de un grupo G y $H = H_1 \cdots H_n$. Entonces las siguientes condiciones son equivalentes:*

i) *$\overline{H} = H_1 \times \cdots \times H_n$ y H son isomorfos bajo la aplicación canónica que manda $(x_1, \dots, x_n) \to x_1 \cdots x_n$.*

ii) *$H_i \trianglelefteq H$ y cada elemento $x \in H$ puede expresarse de manera única como $x = x_1 \cdots x_n$ con $x_i \in H_i$.*

iii) *$H_i \trianglelefteq H$ para toda i, y si $x_1 \cdots x_n = e$, entonces cada $x_i = e$ con $x_i \in H_i$.*

iv) *$H_i \trianglelefteq H$ para toda i, y $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$.*

Demostración

i)⇒ii) Probemos que $H_i \trianglelefteq H$. El conjunto $M = \{(e, \dots, h_i, e, \dots, e) \in \overline{H} \mid h_i \in H_i\}$ es un subgrupo de $\overline{H}$. La función $h_i \to (e, \dots, h_i, e, \dots, e)$ es un isomorfismo entre H_i y M. La aplicación $\varphi : H \to H_1 \times \cdots \times H_{i-1} \times H_{i+1} \times \cdots \times H_n$, definida por $\varphi(g_1 \cdots g_n) = (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n)$ es un homomorfismo suprayectivo y $\ker \varphi = M \cong H_i$, esto prueba que $H_i \trianglelefteq H$. Sean $x = x_1 \cdots x_n = x'_1 \cdots x'_n$ con $x_i, x'_i \in H_i$, entonces por $i)$ dan la misma imagen bajo el isomorfismo, así $x_i = x'_i$.

ii)⇒iii) Sea $x_1 \cdots x_n = e$. También se tiene $e \cdots e = e$. Por unicidad de la representación $x_i = e$

para toda i

iii)$\Rightarrow$iv) Sea $x_i = x_1 \cdots x_{i-1}x_{i+1} \cdots x_n \in H_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_n)$. Entonces $e = x_1 \cdots x_{i-1}x_i^{-1}x_{i+1} \cdots x_n$. Por *iii)*, se tiene que $x_i^{-1} = e$ y $x_i = e$. Esto prueba *iv)*.

iv)$\Rightarrow$i) La función $\sigma : H_1 \times \cdots \times H_n \to H$ dada por $\sigma((x_1, \ldots, x_n)) = x_1 \cdots x_n$ es un homomorfismo, ya que para todo $x \in H_i$, $y \in H_j$ con $i \neq j$, $xy = yx$. La aplicación es inyectiva. En efecto, si $\varphi(x_1, \ldots, x_n) = x_1 \cdots x_n = e$, entonces $x_1^{-1} = x_2 \cdots x_n \in H_1 \cap (H_2 \cdots H_n)$, esto implica que $x_1^{-1} = e = x_1$. De donde $x_1 = x_2 = \cdots = x_n = e$. Por definición, la aplicación es suprayectiva. Entonces $H_1 \times \cdots \times H_n \cong H$. ■

Definición 1.2 *El producto directo de grupos abelianos se llama suma directa. Si $G = \bigoplus G_i$, cada G_i se dice sumando directo de G.*

Definición 1.3 *Un grupo G es un p-grupo, si todo elemento de G tiene orden alguna potencia de p, con p un número primo. Un subgrupo H de G es llamado un p-subgrupo de G si H es un p-grupo.*

Definición 1.4 *Un conjunto de elementos $\{a_1, a_2, \ldots, a_r\}$ de un p-grupo abeliano G es p-independiente si de la suma finita $\sum_{i=1}^{r} n_i a_i = 0$, se tiene que $n_i a_i = 0$ con $n_i \in \mathbb{Z}$ para todo $i \in \{1, \ldots, r\}$. Es decir, $n_i = 0$ si el $\mathbf{or}(a_i) = \infty$ y el $\mathbf{or}(a_i) \mid n_i$ si $\mathbf{or}(a_i) < \infty$.*

Definición 1.5 *Un conjunto $\{a_1, \ldots, a_r\}$ de elementos de un p-grupo abeliano G genera a G, si para todo $a \in G$, se tiene que $a = \sum_{i=1}^{r} n_i a_i$ con $n_i \in \mathbb{Z}$.*

Definición 1.6 *Un conjunto $\{a_1, \ldots, a_r\}$ de elementos de un p-grupo abeliano G es una p-base de G si es p-independiente y además genera al p-grupo G.*

La siguiente proposición se sigue partir de la definición anterior y de la Proposición 1.1.

Proposición 1.7 *El conjunto $\{a_1, \ldots, a_r\}$ es una p-base de un p-grupo abeliano G si, y sólo si, $G = \bigoplus_{i=1}^{r} \langle a_i \rangle$.*

El siguiente teorema está demostrado en [6] pag 97.

Teorema 1.8 (Teorema de la Base de Burnside)

Si G es un p-grupo finito, entonces dos conjuntos generadores mínimales tienen el mismo número de elementos.

La siguiente definición tiene sentido, como una consecuencia del teorema anterior, pues todo conjunto generador independiente es un conjunto generador mínimal.

Definición 1.9 *El p-rango de un p-grupo abeliano finito G, denotado $rank_pG$ es el número de elementos de una p-base de G.*

Teorema 1.10 (Grupos Abelianos Finitamente Generados)

Sea G un grupo abeliano finitamente generado. Entonces G se puede descomponer en suma directa de un número finito de grupos cíclicos C_i. Es decir,

$$G = C_1 \oplus \cdots \oplus C_k,$$

donde $C_1, \ldots, C_k$ son todos de orden infinito, o para algún $j < k$, $C_1, \ldots, C_j$ son de orden $m_1, \ldots, m_j$, respectivamente, con $m_1 \mid m_2 \mid \cdots \mid m_j$ y $C_{j+1}, \ldots, C_k$ son de orden infinito.

Demostración

Sea k el número más pequeño tal que G es generado por un conjunto de k elementos. El teorema se prueba por inducción sobre k.

Si $k = 1$, G es un grupo cíclico entonces la proposición es cierta. Sea $k > 1$, asumimos que la proposición es cierta para cada grupo generado por un conjunto de $k - 1$ elementos.

Primero se considera el caso cuando G tiene un conjunto generador $\{a_1, \ldots, a_k\}$ con la propiedad de que para todos los enteros $x_1, \ldots, x_k$ la igualdad $\sum_{i=1}^{k} x_i a_i = 0$ implica $x_i = 0$ para todo $i = 1, \ldots, k$. Por lo tanto, por la Proposición 1.1. *ii*), cada $g \in G$ tiene una única representación de la forma $g = \sum_{i=1}^{n} \alpha_i a_i$ con $\alpha_i \in \mathbb{Z}$.

Así $G = C_1 \oplus \cdots \oplus C_k$, donde $C_i = \langle a_i \rangle$ para $i = 1, \ldots, k$. Además $x_i a_i = 0$ implica $x_i = 0$, por tanto C_i es un grupo cíclico infinito. Entonces en este caso, G es suma directa de un número finito de subgrupos cíclicos infinitos.

Ahora supongamos que G no tiene un conjunto generador de k elementos con la propiedad anterior. Entonces dado algún conjunto generador $\{a_1, \ldots, a_k\}$ de G, existen enteros $x_1, \ldots, x_k$

(no todos cero) tal que

$$\sum_{i=1}^{k} x_i a_i = 0$$

entonces

$$\sum_{i=1}^{k} (-x_i)\, a_i = 0$$

así podemos asumir que $x_i > 0$ para algún i. Consideramos ahora todos los posibles conjuntos generadores de G con k elementos. Denotamos por X al conjunto de todas las $k-$tuplas $(x_1, \ldots, x_k)$ de enteros tal que

$$\sum_{i=1}^{t} x_i a_i = 0 \text{ con } x_i > 0 \text{ para algún } i,$$

para algún conjunto generador $\{a_1, \ldots, a_k\}$ de G.

Sea m_1 el menor entero positivo de alguna $k-$tupla en X. Sin pérdida de generalidad, tomamos a m_1 como la primera componente, para algún conjunto generador $\{a_1, \ldots, a_k\}$, entonces

$$m_1 a_1 + x_2 a_2 + \cdots + x_k a_k = 0 \tag{1}$$

por el algoritmo de la división podemos escribir $x_i = q_i m_1 + r_i$ donde $0 \leq r_i < m_1$ para cada $i = 2, \ldots, k$. Entonces en la igualdad (1) tenemos que

$$m_1 b_1 + r_2 a_2 + \cdots + r_k a_k = 0 \tag{2}$$

donde $b_1 = a_1 + q_2 a_2 + \cdots + q_k a_k$. Supongamos que $b_1 \neq 0$, ya que en caso contrario $a_1 = -q_2 a_2 - \cdots - q_k a_k$, y esto implica que G es generado por un conjunto de $k-1$ elementos, lo cual es una contradicción. Como $a_1 = b_1 - q_2 a_2 - \cdots - q_k a_k$, entonces $\{b_1, a_2, \ldots, a_k\}$ es un conjunto generador. Por la propiedad minimal de m_1, tenemos de (2) que $r_2 = \cdots = r_k = 0$, así $m_1 b_1 = 0$. Si $C_1 = \langle b_1 \rangle$, ya que m_1 es un entero positivo tal que $m_1 b_1 = m_1 b_1 + 0a_2 + 0a_3 + \cdots + 0a_k = 0$, entonces C_1 es cíclico de orden m_1.

Sea G_1 el subgrupo generado por $\{a_2, \ldots, a_k\}$. Veamos que $G = C_1 \oplus G_1$. Supongamos que $x_1 b_1 \in G$, para algún x_1, $0 \leq x_1 < m_1$. Entonces $x_1 b_1 = x_2 a_2 + \cdots + x_k a_k$ con $x_2, \ldots, x_k \in \mathbb{Z}$

Por tanto $x_1b_1 - x_2a_2 - \cdots - x_ka_k = 0$, de donde $x_1 = 0$ por la propiedad mínimal de m_1. Entonces $C_1 \cap G_1 = \{0\}$ y esto prueba que $G = C_1 \oplus G_1$.

Supongamos que G_1 es generado por $k-1$ elementos. G_1 no puede ser generado por un conjunto menor de $k-1$ elementos, porque entonces G sería generado por un conjunto menor de k elementos, lo cual es una contradicción. Por hipótesis de inducción

$$G_1 = C_2 \oplus \cdots \oplus C_k,$$

donde $C_1, \ldots, C_k$ son subgrupos cíclicos todos infinitos, o, para algún $j < k$, $C_2, \ldots, C_k$ son todos grupos cíclicos finitos de orden $m_2, \ldots, m_j$, respectivamente, con $m_2 \mid m_3 \mid \cdots \mid m_j$, y C_i son infinitos para $i > j$.

Sea $C_i = \langle b_i \rangle$ para $i = 2, \ldots, k$. Supongamos que C_2 es de orden m_2. Entonces $\{b_1, \ldots, b_k\}$ es un conjunto generador de G y $m_1b_1 + m_2b_2 + 0b_3 + \cdots + 0b = 0$

Repitiendo el mismo argumento, se concluye que $m_1 \mid m_2$. Esto completa la demostración del teorema. ■

Definición 1.11 *El entero $r = k - j$ del teorema anterior es llamado el rango libre o número de Betti de G y los enteros $m_1, \ldots, m_j$ son llamados los factores invariantes de G. La descomposición de G en el Teorema 1.10 es llamada la descomposición invariante de G.*

Proposición 1.12 *Sea G un grupo abeliano finito. Entonces existe una única lista de enteros $m_1, \ldots, m_k$ (todos mayores que uno), tal que $\operatorname{or}(G) = m_1 \cdots m_k$ con $m_1 \mid m_2 \mid \cdots \mid m_k$, y $G = C_1 \oplus \cdots \oplus C_k$, donde $C_1, \ldots, C_k$ son subgrupos cíclicos de G de orden $m_1, \ldots, m_k$ respectivamente. consecuentemente,*

$$G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}.$$

Demostración

Por el Teorema 1.10, $G = C_1 \oplus \cdots \oplus C_k$, donde $C_1, \ldots, C_k$ son subgrupos cíclicos de orden $m_1, \ldots, m_k$ respectivamente tal que $m_1 \mid m_2 \mid \cdots \mid m_k$. Además $|S \times T| = |S|\,|T|$, para S y T

conjuntos finitos, de donde

$$|G| = |C_1||C_2|\cdots|C_k| = m_1\cdots m_k.$$

Sabemos que un grupo cíclico de orden m es isomorfo a $\mathbb{Z}_m$, entonces

$$G \cong \mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_k}.$$

A continuación se demuestra que la lista de enteros $m_1,\ldots,m_k$ que cumple lo anterior es única. Supongamos que $G = C_1\oplus\cdots\oplus C_k = D_1\oplus\cdots\oplus D_l$ donde C_i, D_j son todos grupos cíclicos de G tales que

$$\begin{aligned} |C_i| &= m_i \text{ donde } m_1 \mid m_2 \mid \cdots \mid m_k, \\ |D_j| &= n_j \text{ donde } n_1 \mid n_2 \mid \cdots \mid n_l \end{aligned}$$

D_l tiene un elemento de orden n_l, pero cada elemento en G es de orden $\leq m_k$. Entonces $n_l \leq m_k$, por el mismo argumento $m_k \leq n_l$ entonces $m_k = n_l$.

Consideremos

$$\begin{aligned} m_{k-1}G &= (m_{k-1}C_1)\oplus\cdots\oplus(m_{k-1}C_{k-1})\oplus(m_{k-1}C_k) \\ &= (m_{k-1}D_1)\oplus\cdots\oplus(m_{k-1}D_{l-1})\oplus(m_{k-1}D_l) \end{aligned}$$

con $m_i \mid m_{k-1}$ para $i = 1,\ldots,k-1$. Tenemos que $m_{k-1}C_i = e$ para $i = 1,\ldots,k-1$. Entonces $m_{k-1}A = |m_{k-1}C_l| = |m_{k-1}D_l|$ y por tanto $|m_{k-1}D_j| = 1$ para $j = 1,\ldots,l-1$. De aquí que $n_{l-1} \mid m_{k-1}$ por simetría del argumento $m_{k-1} \mid n_{l-1}$. Por tanto $m_{k-1} = n_{l-1}$. Procediendo de esta manera se prueba que $m_{k-r} = n_{l-r}$ para $r = 0,1,2,\ldots$. Se tiene que $m_1\cdots m_k = |G| = n_1\cdots n_l$, y de aquí que $k = l$ y $m_i = n_i$, para $i = 1,\ldots,k$. ■

Definicion 1.13 *Si $G \cong \mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_k}$ con $m_1 \geq \cdots \geq m_k$, diremos que G es de tipo $(m_1,\ldots,m_k)$ y los enteros $m_1,\ldots,m_k$ son llamados los invariantes de G. Un p-grupo abeliano es homocíclico si es de tipo $(p^n, p^n, \cdots, p^n)$.*

Una partición de un entero positivo k es una r-upla $(k_1, k_2, \ldots, k_r)$ de enteros positivos tal que $k = \sum_{i=1}^{r} k_i$ con $k_i \leq k_{i+1}$ para todo $i = 1, \ldots, r-1$.

Lema 1.14 *Existe una correspondencia biyectiva de la familia F de grupos abelianos finitos no isomorfos de orden p^{α} y el conjunto $P(\alpha)$ de particiones de α*

Demostración

Sea $G \in F$ de tipo $(p^{\alpha_1}, \ldots, p^{\alpha_k})$ donde $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k$ y $\alpha_1 + \alpha_2 + \cdots + \alpha_k = \alpha$ Sea la aplicación $\sigma : F \to P(\alpha)$ definida por $\sigma(G) = (\alpha_1, \ldots, \alpha_k)$. σ es inyectiva por la Proposición 1.12. σ es sobreyectiva, ya que si $(\alpha_1, \ldots, \alpha_s) \in P(\alpha)$, entonces el grupo $\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_s}}$, es la preimagen de $(\alpha_1, \ldots, \alpha_s)$ ■

1.2 Grupos nilpotentes

Definición 1.15 *Sea G un grupo y A un subconjunto de G. El conjunto $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ para todo } a \in A\}$ es llamado el centralizador de A en G.*

$C_G(A)$ es un subgrupo de G. En efecto, $C_G(A) \neq \varnothing$ ya que $e \in C_G(A)$. Sean $x, y \in C_G(A)$, $(xy)a(xy)^{-1} = xyay^{-1}x^{-1} = xax^{-1} = a$ para todo $a \in A$. De aquí que $xy \in C_G(A)$ y analogamente $x^{-1} \in C_G(A)$.

Definición 1.16 *El subgrupo $Z(G) = C_G(G)$ es llamado el centro de G.*

Definición 1.17 *Sean G un grupo, x, y elementos de G y A, B subconjuntos no vacíos de G.*
1) *$[x, y] = x^{-1}y^{-1}xy$ es el conmutador de x e y.*
2) *$[A, B] = \langle [a, b] \mid a \in A,\ b \in B \rangle$ es el subgrupo generado por los conmutadores de elementos de A y de B.*
3) *$G' = \langle [x, y] \mid x, y \in G \rangle$ es el subgrupo de G generado por los conmutadores de todos los elementos de G, llamado el subgrupo conmutador de G o derivado de G*

Teorema 1.18 (Teorema de la Correspondencia de Grupos).
Sea $\Phi : G \longrightarrow G_1$ un homomorfismo de un grupo G sobre un grupo G_1. Entonces se tienen las siguientes proposiciones.
i) *Si $H \leq G$ entonces $\Phi(H) \leq G_1$.*

i') *Si* $H_1 \leq G_1$ *entonces* $\Phi^{-1}(H_1) \leq G$.

ii) *Si* $H \trianglelefteq G$ *entonces* $\Phi(H) \trianglelefteq G_1$

ii') *Si* $H_1 \trianglelefteq G_1$ *entonces* $\Phi^{-1}(H_1) \trianglelefteq G$

iii) *Si* $H \leq G$ *y* $H \supset \ker\Phi$ *entonces* $H = \Phi^{-1}(\Phi(H))$

iv) *La función* $H \longmapsto \Phi(H)$ *es una aplicación biyectiva entre la familia de subgrupos de* G *que contienen al* $\ker\Phi$ *y la familia de subgrupos de* G_1*, los subgrupos normales de* G *se corresponden con subgrupos normales de* G_1.

Demostración

i) Sean $a, b \in H$, $\Phi(a), \Phi(b) \in \Phi(H)$. Entonces

$$\Phi(a)(\Phi(b))^{-1} = \Phi(a)\Phi\left(b^{-1}\right) = \Phi\left(ab^{-1}\right) \subset \Phi(H)$$

ya que $ab^{-1} \in H$. De aqui que $\Phi(H) \leq G_1$.

i') Si $a, b \in \Phi^{-1}(H_1)$, entonces $\Phi(a), \Phi(b) \in H_1$. Como

$$\Phi\left(ab^{-1}\right) = \Phi(a)(\Phi(b))^{-1} \in H_1,$$

Se tiene que $ab^{-1} \in \Phi^{-1}(H_1)$ luego $\Phi^{-1}(H_1) \leq G$.

ii) Sea $\Phi(h) \in \Phi(H)$ y $g' \in G_1$. Entonces $g' = \Phi(g)$ para algún $g \in G$ por ser sobreyectiva. Como

$$g'^{-1}(\Phi(h))g' = (\Phi(g))^{-1}\Phi(h)\Phi(g) = \Phi\left(g^{-1}hg\right) \in \Phi(H),$$

ya que $H \trianglelefteq G$. Entonces $\Phi(H) \trianglelefteq G_1$.

ii') Sea $h \in \Phi^{-1}(H_1)$, $g \in G$. De donde $\Phi(h) \in H_1$, como

$$\Phi\left(g^{-1}hg\right) = (\Phi(g))^{-1}\Phi(h)\Phi(g) \in H_1$$

ya que $H_1 \trianglelefteq G_1$. Por consiguiente $g^{-1}hg \subset \Phi^{-1}(H_1)$, o sea $\Phi^{-1}(H_1) \trianglelefteq G$.

iii) Es claro que $H \subseteq \Phi^{-1}(\Phi(H))$. Si $x \in \Phi^{-1}(\Phi(H))$ entonces $\Phi(x) \in \Phi(H)$ y $\Phi(x) = \Phi(h)$ para algún $h \in H$. De aqui que $\Phi\left(xh^{-1}\right) = \Phi(e)$ y $xh^{-1} \in \ker\Phi \subseteq H$. Por lo tanto $x \subset H$ luego $H = \Phi^{-1}(\Phi(H))$.

iv) Sea $H_1 \leq G_1$. Por $i)'$ $\Phi^{-1}(H_1)$ es un subgrupo de G que contiene el $\ker\Phi$. Por $iii)$

$\Phi\left(\Phi^{-1}(H_1)\right) = H_1$, luego la función $H \mapsto \Phi(H)$ es suprayectiva. Sean $\Phi(H_1) = \Phi(H_2)$, donde H_1, H_2 son subgrupos de G que contienen el $\ker\Phi$, entonces $\Phi^{-1}(\Phi(H_1)) = \Phi^{-1}(\Phi(H_2))$. Por el inciso *iii)* se concluye que $H_1 = H_2$. La primera parte de *iv)* está probada por *ii)*. ■

Corolario 1.19 *Sea N un subgrupo normal de G. Dado algún subgrupo H_1 de G/N, existe un único subgrupo H de G tal que $H_1 = H/N$. Más aun $N \leq H \trianglelefteq G$ si, y sólo si, $H/N \trianglelefteq G/N$.*

Demostración

Tomando el homomorfismo natural $\Phi : G \longrightarrow G/N$ dado por $g \mapsto gN$, se tiene que, existe un único subgrupo H de G que contiene a N tal que $H_1 = \Phi(H) = H/N$. ■

Definición 1.20 *Sea $N \trianglelefteq G$. El homomorfismo $\Pi : G \to G/N$ definido por $\Pi(g) = gN$ es llamado la proyección natural de G en G/N. Si $\overline{H}$ es un subgrupo de G/N, la preimagen completa de $\overline{H}$ en G es la preimagen de $\overline{H}$ bajo la proyección natural.*

Por el teorema anterior la preimagen de $\overline{H}$ en G es un subgrupo de G.

A continuación definimos la Serie Central Superior (serie ascendente) de un grupo G. Para $n = 1$, $Z_1(G) = Z(G)$. Sea $Z(G/Z_1(G))$ el centro del grupo cociente $G/Z_1(G)$. Por el Corolario 1.19 existe un único subgrupo normal $Z_2(G)$ tal que

$$Z_2(G)/Z_1(G) = Z(G/Z_1(G)) \text{ con } Z_1(G) \subset Z_2(G).$$

Inductivamente se tiene un subgrupo normal $Z_n(G)$ de G tal que

$$Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$$

para todo entero positivo $n > 1$ $Z_n(G)$ es llamado el n-ésimo centro de G. Denotamos $Z_0(G) = \{e\}$. Por tanto:

$$Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$$

para todo entero positivo n.

Definición 1.21 *La sucesión ascendente de subgrupos normales de G,*

$$\{e\} = Z_0(G) \subset Z_1(G) \subset \cdots \subset Z_n(G) \subset \cdots,$$

es llamada la serie central superior de G si

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)) \text{ para todo } i$$

Lema 1.23 *Sea $\{e\} = Z_0(G) \subset Z_1(G) \subset \cdots \subset Z_n(G) \subset \cdots$ la serie central superior de un grupo G, entonces $Z_n(G) = \{x \in G \mid [x,y] \in Z_{n-1}(G) \text{ para todo } y \in G\}$.*

Demostración

$$\begin{aligned}
Z(G/Z_{n-1}(G)) &= \{xZ_{n-1}(G) \mid x \in G,\ yxZ_{n-1} = xyZ_{n-1}(G) \text{ para todo } y \in G\} \\
&= \{xZ_{n-1}(G) \mid x \in G,\ x^{-1}y^{-1}xy \in Z_{n-1}(G) \text{ para todo } y \in G\} \\
&= Z_n(G)/Z_{n-1}(G) = \{zZ_{n-1}(G) \mid z \in Z_n(G)\} \\
\text{así } Z_n(G) &= \{x \in G \mid x^{-1}y^{-1}xy \in Z_{n-1}(G) \text{ para todo } y \in G\} \\
\text{De aqui que } Z_n(G) &= \{x \in G \mid [x,y] \in Z_{n-1}(G) \text{ para todo } y \in G\}. \blacksquare
\end{aligned}$$

Definición 1.24 *Sea G un grupo. La sucesión de subgrupos de G.*

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G$$

se llama serie central si $G_i \trianglelefteq G$ y $G_i/G_{i-1} \leq Z(G/G_{i-1})$ para todo $i \in \{1, \ldots, r\}$. La longitud de la serie es el número r.

Definición 1.25 *Un grupo G es nilpotente si tiene una serie central, el grado de nilpotencia de G es la longitud mínima de todas las series centrales.*

Proposición 1.26 *Una sucesión de subgrupos de un grupo G, $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ es una serie central de G si, y sólo si, $[G_i, G] \leq G_{i-1}$ para todo i.*

Demostración

Supongamos que $\{G_i\}_{i \geq 0}$ es una serie central de G. Si $x \in G_i$, $y \in G$ se tiene que $xG_{i-1}yG_{i-1} = yG_{i-1}xG_{i-1}$. En efecto, como $G_i/G_{i-1} \leq Z(G/G_{i-1})$, se tiene que $xyG_{i-1} = yxG_{i-1}$. De aqui que $x^{-1}y^{-1}xy \in G_{i-1}$, es decir, $[x,y] \in G_{i-1}$. Esto prueba que $[G_i, G] \leq G_{i-1}$.

Ahora supongamos que para cada $i \in \{1, \ldots, n\}$, $[G_i, G] \leq G_{i-1}$. Si $x \in G_i$, $y \in G$ se tiene que $x^{-1}y^{-1}xy = [x,y] \in G_{i-1}$, ya que $G_{i-1} \leq G_i$. Entonces $y^{-1}xy \in G_i$ para todo

$y \in G$. así $G_i \leq G$ para todo $i \in \{1, \ldots, n\}$. Además para todo $x \in G_i$ y para todo $y \in G$, $x^{-1}y^{-1}xyG_{i-1} = G_{i-1}$. luego $xyG_{i-1} = yxG_{i-1}$ esto implica que $G_i/G_{i-1} \leq Z(G/G_{i-1})$. ■

Proposición 1.27 *G es nilpotente si, y sólo si, $Z_n(G) = G$ para algún entero positivo n.*

Demostración

Supongamos que $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G$ es una serie central de G, así $G_i/G_{i-1} \leq Z(G/G_{i-1})$ para todo i. Se tiene que $G_1 \subseteq Z(G) = Z_1(G)$. Supongamos que se cumple para $i-1$, por demostrar que $G_i \subseteq Z_i(G)$.

Para cada $x \in G_i$. y para todo $y \in G$, se tiene que

$$xG_{i-1}yG_{i-1} = yG_{i-1}xG_{i-1}, \text{ así } x^{-1}y^{-1}xy \in G_{i-1} \subseteq Z_{i-1}(G).$$

Además

$$Z_i(G) = \{x \in G \mid x^{-1}y^{-1}xy \in Z_1(G) \text{ para todo } y \in G\}$$

por lo tanto $G_i \subseteq Z_i(G)$.

Como $G = G_r \subseteq Z_r(G)$, y sabemos que $Z_r(G) \subseteq G = G_r$ se obtiene que $G = Z_r(G)$.
Si $Z_n(G) = G$ para algún entero positivo n, entonces esta serie es una serie central, por tanto G es nilpotente. ■

Lema 1.28 *Sea G un grupo nilpotente. El grado de nilpotencia de G es la longitud de la serie central superior.*

Demostración

Sean $\{G_i\}_{i\geq 0}$ una serie central de G de longitud mínima k y $\{Z_i\}_{i\geq 0}$ la serie central superior de G de longitud m.0 Por demostrar que $m = k$.

Por la proposición anterior se tiene que $G = G_k \leq Z_k$, como $Z_{n-1}(G)\, Z_m = G$ entonces $Z_m \leq Z_k$ por tanto $m \leq k$. Si $m < k$ entonces $\{Z_i\}_{i\geq 1}$ es una serie central de longitud menor que $\{G_i\}_{i\geq 1}$, lo cual es una contradicción. Por tanto $m = k$. ■

1.3 p-Grupos finitos.

Lema 1.29 *(Teorema de Cauchy para Grupos Abelianos)*
Sean G un grupo abeliano finito y p un número primo. Si p divide al orden de G, entonces G tiene un elemento de orden p.

Demostración

El teorema se demuestra por inducción sobre el orden de G, Sea $n = |G|$ y $p \mid n$.

Supongamos que el resultado es cierto para todos los grupos de orden m con $p \mid m$, y $m < n$. Si $\mathbf{or}(G) = p$ o si G es un grupo cíclico, existe un subgrupo cíclico de G de orden p, y por lo tanto existe un elemento de orden p. Supongamos ahora que existe $b \in G$ con $b \neq e$, tal que $G \neq \langle b \rangle$, el subgrupo cíclico generado por b. Si $p \mid \mathbf{or}(\langle b \rangle)$, hemos terminado. Si p no divide a $\mathbf{or}(\langle b \rangle)$, entonces p divide al orden de $\dfrac{G}{\langle b \rangle}$. Por hipótesis de inducción existe $\overline{a} \in \dfrac{G}{\langle b \rangle}$, $a \in G$, tal que $\mathbf{or}(\overline{a}) = p$. Sea $k = \mathbf{or}(a)$, entonces $a^k = e$ implica $\overline{a}^k = \overline{e}$, por lo tanto $p \mid k$, entonces existe un elemento de G de orden p. ■

Teorema 1.30 *(Teorema de Sylow)*
Sea G un grupo finito y p un número primo. Si p^m divide al orden de G, entonces G tiene un subgrupo de orden p^m.

Demostración

La prueba del teorema es por inducción sobre $n = \mathbf{or}(G)$. Si $n = 1$ el resultado es obvio. Asumimos que el resultado se cumple para todos los grupos de orden menor que n.

Si el orden del centro de G es divisible por p, entonces por el teorema anterior el centro de G contiene un elemento a de orden p. El grupo cíclico C generado por a es un subgrupo normal en G, y el grupo cociente G/C tiene orden $\dfrac{n}{p}$, el cual es divisible por p^{m-1}. Por hipótesis de inducción, G/C contiene un subgrupo H/C de orden p^{m-1}, queda probado el teorema en este caso.

Ahora consideremos el caso en el cual el orden del centro de G no es divisible por p. Consideramos la ecuación de clases de G:

$$n = \mathbf{or}(G) = \mathbf{or}(Z(G)) + \sum_a [G : N(a)],$$

donde la sumatoria se toma seleccionando un elemento para cada clase de elementos conjugados de G. Sabemos que $p \mid n$, pero p no divide al orden de $\mathbf{Z}(G)$. Entonces p no divide a $[G : N(a)]$ para algún $a \in G$, $a \notin \mathbf{Z}(G)$ esto implica que $p^m \mid \mathrm{or}(N(a))$ y $\mathrm{or}(N(a)) < \mathrm{or}(G)$.

Por hipótesis de inducción, $N(a)$ tiene un subgrupo de orden p^m, con lo cual terminamos la prueba. ■

Corolario 1.31 *(Teorema de Cauchy)*
Si el orden de un grupo finito G es divisible por un número primo p, entonces G tiene un elemento de orden p.

Demostración

Por el Teorema de Sylow existe un subgrupo de orden p. ■

Corolario 1.32 *Un grupo finito G es un p-grupo si, y sólo si, el orden de G es una potencia de p.*

Demostración

Si G tiene orden alguna potencia de p, se sigue que cada elemento tiene orden alguna potencia de p. Ahora asumimos que cada elemento en G tiene orden alguna potencia de p. Si existe un número primo $q \neq p$ que divide al orden de G, entonces por el Teorema de Cauchy, existe un elemento de orden q, lo cual es una contradicción. Así G tiene orden alguna potencia de p. ■

Definición 1.33 *Sea p un número primo. Un subgrupo H de G es un p-subgrupo de Sylow de G si es un p-subgrupo máximal de G. Si $\mathrm{or}(G) = p^\alpha t$ y $(p,t) = 1$, un p-subgrupo de Sylow de G es un p-subgrupo de orden p^α.*

El teorema de Sylow se enuncia de la siguiente manera:

Teorema 1.34 *Sea G un grupo finito con $\mathrm{or}(G) = p^\alpha t$ y $(p,t) = 1$. Entonces G contiene un p-subgrupo de Sylow.*

Proposición 1.35 *Si G es un p-grupo finito con más de un elemento, entonces $Z(G)$ tiene más de un elemento.*

Demostración

Sea H un subgrupo de G. Por el Teorema 1.30 tenemos que $p \mid [G : H]$, por la ecuación de clases de G y por hipótesis tenemos que $p \mid Z(G)$ Por tanto $|Z(G)| > 1$ ■

Proposición 1.36 *Todo p-grupo finito es nilpotente.*

Demostración.

Sea G un p-grupo finito. Probemos que G tiene una serie central

Si G es abeliano, claramente $1 \leq G$ es una serie central. Supongamos que G es no abeliano. Sea H un subgrupo normal propio de G, entonces $G/H \neq \bar{1}$. Sea $gH \in G/H$, como $g \in G$ entonces $|g| = p^m$, para algún $m \in \mathbb{N}$, por tanto $(gH)^{p^m} = g^{p^m}H = H$, entonces el orden de gH divide a p^m, es decir, el orden de gH es una potencia de p. De aquí que H es un p-subgrupo de G.

Por la Proposición 1.35, $Z(G/H)$ tiene más de un elemento, por el Corolario 1.19 existe un único subgrupo normal H_2 de G que contiene a H, tal que $Z(G/H) = H_2/H$, haciendo un procedimiento analogo con H_2 obtenemos H_3 que cumple $Z(G/H_2) = H_3/H_2$. Renombrando $H = H_1$, se tiene la siguiente serie: $1 \leq H_1 \leq H_2 \leq H_3 \cdots$

Como G es finito esta serie debe terminar, entonces existe una n tal que

$$1 \leq H_1 \leq H_2 \leq H_3 \cdots \leq H_n = G,$$

con $Z(G/H_i) = H_{i+1}/H_i$ para cada $i = 0, \ldots n-1$, por tanto G es nilpotente. ■

1.4 Serie anuladora superior de un anillo

La construcción de la serie anuladora superior de un anillo es de forma similar a la construcción de la serie central superior de un grupo. Un resultado análogo al Teorema 1.18 es el siguiente:

Teorema 1.37 (*Teorema de la Correspondencia de Anillos*)
Sea $f : R \to S$ un homomorfismo de un anillo R sobre un anillo S, y sea $N = \ker f$. Entonces la función $F : A \mapsto f(A)$ define una correspondencia inyectiva entre el conjunto de todos los ideales (ideales derechos, ideales izquierdos) en R que contienen a N y el conjunto de todos los

ideales (ideales derechos, ideales izquierdos) en S. Además se preserva el orden en el sentido que $A \subset B$ si, y sólo si, $f(A) \subset f(B)$.

Demostración

Sean K un ideal arbitrario en S y $A = f^{-1}(K)$ Probemos que A es un ideal en R . En efecto, si $a, b \in A$ y $r \in R$, entonces $f(a-b) = f(a) - f(b) \in K$, y $f(ar) = f(a) f(r) \in K$, ya que K es un ideal y $f(a) \in K$. Así $a - b \in f^{-1}(K)$ y $ar \in f^{-1}(K)$. Similarmente si $ra \in f^{-1}(K)$, entonces $A = f^{-1}(K)$ es un ideal en R. Análogamente se demuestra que si A es un ideal en R, entonces $f(A)$ es un ideal en S, consecuentemente la *función* F es sobreyectiva, puesto que un ideal K en S es de la forma $f(A)$ para algún ideal A en R. Se prueba que $K = f\left(f^{-1}(K)\right)$. Claramente $K \supseteq f\left(f^{-1}(K)\right)$. Sea $x \in K$, como f es sobreyectiva, existe un $a \in R$ tal que $f(a) = x$, entonces $a \in f^{-1}(K)$; así $x = f(a) \in f\left(f^{-1}(K)\right)$.

Ahora se demuestra que F es inyectiva Supongamos que A y B son ideales en R que contienen a N tal que $f(A) = f(B)$. Se afirma que $f^{-1}(f(A)) = A$. Sea $x \in f^{-1}(f(A))$, entonces $f(x) \in f(A)$. Esto implica $f(x) = f(a)$ para algún $a \in A$; así $x - a \in \ker f \subseteq A$, por lo tanto $x \in A$ y $f^{-1}(f(A)) \subseteq A$, la otra contención es clara Similarmente, $f^{-1}(f(B)) = B$, por lo tanto $f(A) = f(B)$ implica que $A = B$.

Finalmente, sean A y B ideales en R tal que $A \subset B$, entonces $f(A) \subseteq f(B)$. Si $f(A) = f(B)$ tenemos que $A = B$, por lo tanto $f(A) \subset f(B)$. Inversamente, si $f(A) \subset f(B)$. Entonces $A = f^{-1}(f(A)) \subseteq f^{-1}(f(B)) = B$. Como $f(A) \subset f(B)$ no puede suceder que $A = B$, así $A \subset B$

La correspondencia inyectiva entre el conjunto de ideales izquierdos o ideales derechos se establecen con los mismos argumentos. ■

Una importante consecuencia que nos permite construir a la serie anuladora superior es la siguiente.

Corolario 1.38 *Sea S un ideal de R. Dado un subanillo H_1 de R/S existe un único subanillo H de R tal que $H_1 = H/S$, más aún, H es un ideal de R si, y sólo si, H/S es un ideal de R/S.*

Demostración

Consideramos el homomorfismo natural $\Phi : R \to R/S$, por el Teorema 1.37, existe un único subanillo H de R que contiene a S tal que $H' = \Phi(H) = H/S$. ■

Definición 1.39 *Sea R un anillo, el conjunto $AnnR = \{a \in R \mid ab = ba = 0$ para todo $b \in R\}$ es llamado el anulador de R*

Lema 1.40 *$AnnR$ es un ideal de R*

Demostración

$R \neq \emptyset$ ya que $0 \in R$. Sean $a, b \in AnnR$ y $x \in \dot{R}$, entonces $(a-b)x = ax - bx = 0$, análogamente $x(a-b) = 0$, por lo tanto, $(a-b) \in R$. Sea $r \in R$ entonces $(ra)x = r(ax) = 0$ y $x(ra) = 0$, por lo tanto, $ra, ar \in AnnR$. ■

Construcción de la serie anuladora superior de un anillo R.

Para $n = 1$, sea $R_1 = AnnR$. Por el Lema 1.40 $Ann(R/R_1)$ es un ideal de R/R_1, por el Corolario 1.38, existe un único ideal R_2 de R tal que

$$R_2/R_1 = Ann(R/R_1) \text{ con } R_1 \subseteq R_2.$$

Inductivamente se obtiene un ideal R_n de R tal que

$$R_n/R_{n-1} = Ann(R/R_{n-1})$$

para algún entero positivo $n > 1$. R_n es llamado el n-ésimo anulador superior de R. A partir de esto se tiene la siguiente:

Definición 1.41 *La sucesión $0 = R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_n = R$ de ideales de un anillo R que cumplen $R_i/R_{i-1} = Ann(R/R_{i-1})$, la llamaremos la serie anuladora superior de R. El número n es la longitud de la serie anuladora superior de R*

Definición 1.42 *Una sucesión $0 = R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_n = R$ de ideales de R tales que $R_i/R_{i-1} \subseteq Ann(R/R_{i-1})$, la llamaremos serie anuladora de R.*

Proposición 1.43 *Sea R un anillo y $0 = R_0 \subsetneq R_1 \subsetneq \ldots \subsetneq R_n = R$ la serie anuladora superior de R. Entonces $R_i = \{A \subset R \mid AB \in R_{i-1}$ y $BA \in R_{i-1}$ para todo $B \in R\}$, $RR_i \subsetneq R_{i-1}$ y $R_iR \subsetneq R_{i-1}$*

Demostración

Sabemos que $R_t/R_{t-1} = \{MR_{t-1} \mid M \in R_t\}$ Además

$$\begin{aligned} Ann(R/R_{t-1}) &= \{AR_{t-1} \mid A \in R:\ ABR_{t-1} = BAR_{t-1} = R_{t-1} \text{ para todo } BR_{t-1} \in R/R_{t-1}\} \\ &= \{AR_{t-1} \mid A \in R:\ AB \in R_{t-1} \text{ y } BA \in R_{t-1} \text{ para todo } B \in R\} \\ &= R_t/R_{t-1}. \end{aligned}$$

así

$$R_t = \{A \in R \mid AB \in R_{t-1} \text{ y } BA \in R_{t-1} \text{ para todo } B \in R\}$$

Finalmente se tiene que $RR_t \subseteq R_{t-1}$ y $R_tR \subseteq R_{t-1}$. Si $A \in R_t$ entonces

$$AR_{t-1} \in R_t/R_{t-1} = Ann\left(\frac{R}{R_{t-1}}\right).$$

por lo tanto

$$ABR_{t-1} = BAR_{t-1} = R_{t-1} \text{ para todo } B \in R,$$

así $BA, AB \in R_{t-1}$. ■

Obsérve que la segunda parte de esta proposición se cumple si la sucesión de ideales es una serie anuladora de R.

Capítulo 2

ESTUDIO DEL ANILLO DE ENDOMORFISMOS DE UN p-GRUPO ABELIANO FINITO

Sean $EndG$ el anillo de endomorfismos de G (morfismos de G en G), y $AutG$ el grupo de automorfismos de G (bajo la composición de funciones). En este trabajo denotamos $J_n = \{1, \ldots, n\}$ para n un número natural fijo.

2.1 Representación matricial de endomorfismos y automorfismos de G.

Sea G un $p-$grupo abeliano finito de tipo $(p^{m_1}, p^{m_2}, \ldots, p^{m_n})$ con $m_1 \geq m_2 \geq \cdots \geq m_n$, es decir, $G = \bigoplus_{i=1}^{n} C_{p^{m_i}}$ donde cada $C_{p^{m_i}}$ es un subgrupo de G. Si $C_{p^{m_i}} = \langle x_i \rangle$ con or $\langle x_i \rangle = p^{m_i}$ para $i \in J_n$, entonces $\beta = \{x_1, x_2, \ldots, x_n\}$ es una $p-$base de G y $C_{p^{m_i}} \cong \mathbb{Z}_{p^{m_i}}$.

Definición 2.1 *Sea G un $p-$grupo abeliano finito de tipo $(p^{m_1}, p^{m_2}, \ldots, p^{m_n})$ y $F = \{a_{ij} \mid a_{ij} \in \mathbb{Z}_{p^{m_i}}$ para cada $i \in J_n\}$. Una matriz A sobre F con respecto a la p-base β es una función.*
$f : \beta \times \beta \to F$ tal que $f(x_i, x_j) \in \mathbb{Z}_{p^{m_i}}$ para todo $(i,j) \in J_n$. Diremos que A es una matriz $n \times n$ sobre F y $f(x_i, x_j)$ es llamada la (i,j) entrada de la matriz A y denotado por a_{ij} así se

escribe a $A = (a_{ij})_{n\times n}$ *con* $a_{ij} \in \mathbb{Z}_{p^{m_i}}$.

Denotamos al conjunto de matrices con respecto a la p-base β por $\mathcal{M}(\beta)$.

Definición 2.2 *En el conjunto* $\mathcal{M}(\beta)$ *se definen las siguientes operaciones:*
Sean $f \in \mathcal{M}(\beta)$, $g \in \mathcal{M}(\beta)$, $x_i, x_j \in \beta$.

1.1 $\quad (f+g)(x_i,x_j) = f(x_i,x_j) + g(x_i,x_j)$

1.2 $\quad (fg)(x_i,x_j) = \sum\limits_{k=1}^{n} f(x_i,x_k)\ \overline{g(x_k,x_j)}$ *con* $x_k \in \beta$

Para $k \leq i$, $\overline{g(x_k,x_j)}$ *es la reducción de* $g(x_k,x_j)$ *módulo* p^{m_i} *y si* $k > i$ *consideramos* $\overline{g(x_k,x_j)}$ *como* $g(x_k,x_j) \in \mathbb{Z}_{p^{m_i}}$

Se tiene que $(\mathcal{M}(\beta),+)$ es un grupo abeliano aditivo con $0 = (0_{ij}) \in \mathcal{M}(\beta)$ donde 0_{ij} es el neutro aditivo del anillo $\mathbb{Z}_{p^{m_i}}$.

Si $f,g,h \in \mathcal{M}(\beta)$ entonces

$$\begin{aligned}
f(x_i,x_j)\left(g(x_i,x_j)\,h(x_i,x_j)\right) &= \sum_{k=1}^{n} f(x_i,x_k)\left(\overline{\sum_{l=1}^{n} g(x_k,x_l)\,\overline{h(x_l,x_j)}}\right)\\
&= \sum_{l=1}^{n}\left(\sum_{k=1}^{n} f(x_i,x_k)\,\overline{g(x_k,x_l)}\right)\overline{h(x_l,x_j)},
\end{aligned}$$

por tanto $f(gh) = (fg)h$.

Además

$$\begin{aligned}
f(x_i,x_j)\left(g(x_i,x_j) + h(x_i,x_j)\right) &= f(x_i,x_j)\left((g+h)(x_i,x_j)\right)\\
&= \sum_{k=1}^{n} f(x_i,x_k)\,\overline{(g+h)(x_k,x_j)}\\
&= \sum_{k=1}^{n} f(x_i,x_k)\,\overline{(g(x_i,x_j) + h(x_i,x_j))}\\
&= \sum_{k=1}^{n} f(x_i,x_k)\,\overline{g(x_i,x_j)} + \sum_{k=1}^{n} f(x_i,x_k)\,\overline{h(x_i,x_j)},
\end{aligned}$$

así $f(g+h) = fg + fh$, analogamente $(f+g)h = fh + gh$. Por tanto $(\mathcal{M}(\beta),+,\cdot)$ es un anillo.

Sea $T \in EndG$, entonces $T(x_j) = \sum\limits_{i=1}^{n} \alpha_{ij} x_i$ con $f(x_i,x_j) = \alpha_{ij} \in \mathbb{Z}_{p^{m_i}}$. Se define la función

$$H \quad : \quad EndG \longrightarrow \mathcal{M}(\beta) \ \text{ como}$$

$$H(T) = f, \text{ donde } f(x_i, x_j) = \alpha_{ij} \in \mathbb{Z}_{p^{m_i}}.$$

Teorema 2.3 *H es un isomorfismo de anillos entre $EndG$ y $\mathcal{M}(\beta)$.*

Demostración

Sea T. $S \in EndG$, $x_j \in \beta$, $H(T) = f$ y $H(S) = g$

$$\begin{aligned}(T+S)(x_j) &= T(x_j) + S(x_j) = \sum_{i=1}^{n} f(x_i, x_j) x_i + \sum_{i=1}^{n} g(x_i, x_j) x_i \\ &= \left(\sum_{i=1}^{n} (f(x_i, x_j) + g(x_i, x_j)) x_i\right),\end{aligned}$$

así $H(T+S) = f + g = H(T) + H(S)$.

$$\begin{aligned}(T.S)(x_j) &= T(S(x_j)) = T\left(\sum_{k=1}^{n} g(x_k, x_j) x_k\right) = \sum_{k=1}^{n} g(x_k, x_j) T(x_k) \\ &= \sum_{k=1}^{n} \left(g(x_k, x_j) \sum_{i=1}^{n} f(x_i, x_k) x_i\right) \\ &= \sum_{i=1}^{n} \left(\sum_{k=1}^{n} f(x_i, x_k) g(x_k, x_j)\right) x_i \\ &= \sum_{i=1}^{n} (f.g)(x_i, x_j) x_i \qquad \textit{por } 2.2\end{aligned}$$

por lo tanto $H(T.S) = f.g = H(T).H(S)$. Entonces H es un homomorfismo.

Supongamos que $H(T_1) = H(T_2) = f$, entonces para $g \in G$, $g = \sum_{i=1}^{n} \alpha_i x_i$ con $x_i \in \beta$ $\alpha_i \in \mathbb{Z}_{p^{m_i}}$.

$$\begin{aligned}T_1(g) &= T_1\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{i=1}^{n} \alpha_i T(x_i) \\ &= \sum_{i=1}^{n} \left(\alpha_i \sum_{k=1}^{n} f(x_k, x_i) x_k\right) \qquad \textit{con } x_i, x_k \in \beta \\ &= \sum_{i=1}^{n} \alpha_i T_2(x_i) = T_2\left(\sum_{i=1}^{n} \alpha_i x_i\right) = T_2(g)\end{aligned}$$

así $T_1 = T_2$. Por lo tanto H es inyectiva

Finalmente, si $f \in \mathcal{M}(\beta)$, se define a T como :

$$T\left(\sum_{i=1}^{n} \alpha_i x_i\right) = \sum_{k=1}^{n} \alpha_i f(x_k, x_i)\, x_k, \text{ con } x_i, x_k \in \beta,$$

se afirma que $T \in EndG$, en efecto,

$$\begin{aligned}
T\left(\sum_{i=1}^{n} \alpha_i x_i + \sum_{i=1}^{n} \gamma_i x_i\right) &= T\left(\sum_{i=1}^{n} (\alpha_i + \gamma_i)\, x_i\right) \\
&= \sum_{k=1}^{n} (\alpha_i + \gamma_i)\, f(x_k, x_i)\, x_k, \text{ con } x_k \in \beta \\
&= \sum_{k=1}^{n} \alpha_i f(x_k, x_i)\, x_k + \sum_{k=1}^{n} \gamma_i f(x_k, x_i)\, x_k \\
&= T\left(\sum_{i=1}^{n} \alpha_i x_i\right) + T\left(\sum_{i=1}^{n} \alpha_i x_i\right)
\end{aligned}$$

además

$$\begin{aligned}
T\left(c\left(\sum_{i=1}^{n} \alpha_i x_i\right)\right) &= T\left(\sum_{i=1}^{n} c\alpha_i x_i\right) \\
&= \sum_{k=1}^{n} c\alpha_i f(x_k, x_i)\, x_k \\
&= c\sum_{k=1}^{n} \alpha_i f(x_k, x_i)\, x_k \\
&= cT\left(\sum_{k=1}^{n} \alpha_i x_i\right),
\end{aligned}$$

por último se concluye que si $x_j \in \beta$ entonces

$$T(x_j) = T\left(\sum_{i=1}^{n} \alpha_{ij} x_i\right) = \sum_{k=1}^{n} \alpha_{ij} f(x_k, x_i)\, x_k = \sum_{k=1}^{n} f(x_k, x_j)\, x_k,$$

así $H(T) = f$ Por lo tanto H es sobreyectiva. ∎

Observar que el isomorfismo H depende de la elección de la p-base β.

2.2 p-Grupo abeliano de tipo $(p^{m_1}, p^{m_2}, p^{m_3}, p^{m_4}, p^{m_5})$

A partir de aquí, y lo que sigue de la tesis se trabaja con un p-grupo abeliano finito G de rango 5 y de tipo $(p^{m_1}, p^{m_2}, p^{m_3}, p^{m_4}, p^{m_5})$ con $n_1 = m_1 = m_2 = m_3 > n_2 = m_4 = m_5$. Entonces $G = \bigoplus_{i=1}^{5} C_{p^{m_i}}$ con $C_{p^{m_i}}$ subgrupos cíclicos de orden p^{m_i}, así $C_{p^{m_i}} \cong \mathbb{Z}_{p^{m_i}}$. En todo el trabajo se usa indistintamente m_i ó n_i para escribir los invariantes del grupo, según cual nos convenga.

A continuación se describen los endomorfismos de G conociendo como actúan los elementos de una p-base de G. Sea $C_{p^{m_i}} = \langle x_i \rangle$ para todo $i \in J_5$, entonces $\{x_1, x_2, x_3, x_4, x_5\}$ es una p-base de G. Sea $A \in EndG$ entonces $A(x_j) = \sum_{i=1}^{5} a_{ij} x_i$ donde a_{ij} son enteros módulos p^{m_i}.

$$0 = A(0) = A(p^{n_1} x_1) = p^{n_1} A(x_1) = p^{n_1} \sum_{i=1}^{5} a_{i1} x_i = p^{n_1} a_{41} x_4 + p^{n_1} a_{51} x_5$$

la igualdad sucede si, y sólo si, $p^{n_1} a_{41} = p^{n_2} \overline{a_{41}}$ y $p^{n_1} a_{51} = p^{n_2} \overline{a_{51}}$, como $p^{n_1} > p^{n_2}$ entonces a_{41}, a_{51} toman cualquier valor en $\mathbb{Z}_{p^{n_2}}$.

Como $\operatorname{or}(x_1) = \operatorname{or}(x_2) = \operatorname{or}(x_3) = p^{n_1}$, analizando $A(p^{n_1} x_2)$ y $A(p^{n_1} x_3)$, se llega a que $a_{42}, a_{52}, a_{43}, a_{53}$ toman cualquier valor en $\mathbb{Z}_{p^{n_2}}$.

$$0 = A(0) = A(p^{n_2} x_4) = p^{n_2} A(x_4) = p^{n_2} \sum_{i=1}^{5} a_{i4} x_i = \sum_{i=1}^{3} p^{n_2} a_{i4} x_i$$

con $a_{i4} \in \mathbb{Z}_{p^{n_1}}$ para $i \in J_3$. Esto sucede si $p^{n_2} a_{i4} = p^{n_1} \overline{a_{i4}}$ asi $a_{i4} = p^{n_1 - n_2} \overline{a_{i4}}$ para todo $i \in J_3$. Análogamente $a_{i5} = p^{n_1 - n_2} \overline{a_{i5}}$ para todo $i \in J_3$.

Por el Teorema 2.4, el anillo $EndG$ es isomorfo al anillo de matrices cuadradas de la forma:

$$\left\{ \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & p^{n_1 - n_2}\alpha_{14} & p^{n_1 - n_2}\alpha_{15} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & p^{n_1 - n_2}\alpha_{24} & p^{n_1 - n_2}\alpha_{25} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & p^{n_1 - n_2}\alpha_{34} & p^{n_1 - n_2}\alpha_{35} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} & \alpha_{45} \\ \alpha_{51} & \alpha_{52} & \alpha_{53} & \alpha_{54} & \alpha_{55} \end{pmatrix} \mid \alpha_{ij} \in \mathbb{Z}_{p^{m_i}} \right\}.$$

Proposición 2.4 *El orden de EndG es* $p^{9n_1 + 16n_2}$

Demostración

El número de elementos de $EndG$ es el producto de los valores que puede tomar cada entrada módulo p^{m_i}. Por tanto $\mathbf{or}(EndG) = p^{9n_1+16n_2}$. ■

G puede ser considerado por suma de dos grupos homocíclicos $G = G_1 \oplus G_2$, donde G_1 y G_2 son grupos de tipo $(p^{m_1}, p^{m_2}, p^{m_3})$ y (p^{m_4}, p^{m_5}) respectivamente.

Sea $A \in EndG$, $\quad A : G = G_1 \oplus G_2 \longrightarrow G_1 \oplus G_2$. Y sea $g \in G$, $g = g_1 + g_2$ con $g_i \in G_i$, para $i \in J_2$. Entonces

$$A\,(g) = A\,(g_1) + A\,(g_2) = (g_{11} + g_{21}) + (g_{12} + g_{22}) \text{ con } g_{1i} \in G_1,\ g_{2i} \in G_2 \text{ para } i \in J_2$$

Se definen las siguientes funciones:

$$A_{ij} : G_j \longrightarrow G_i \text{ como } A_{ij}\,(g_j) = g_{ij}$$

puesto que $A_{ij} \in Hom\,(G_j, G_i)$. Por lo cual

$$EndG = \begin{pmatrix} EndG_1 & Hom\,(G_2, G_1) \\ Hom\,(G_1, G_2) & EndG_2 \end{pmatrix}$$

con $Hom\,(G_1, G_2) = p^{n_1 - n_2} M_{r_1 \times r_2}\,(\mathbb{Z}_{p^{n_1}})$, donde $M_{r_1 \times r_2}\,(\mathbb{Z}_{p^{n_1}})$ es el grupo aditivo $r_1 \times r_2$-matrices con entradas en los enteros módulo p^{n_1}, con $r_1 = 3$ y $r_2 = 2$.

Sea $A = (A_{ij})$ tal que $A_{ij} \in Hom\,(G_j, G_i)$, es decir, $A \in EndG$ con $A_{12} \equiv 0 \pmod{p^{n_1 - n_2}}$ y $A_{ij} \equiv 0 \pmod{p^{m_i}}$ para $i \neq 1$ y $j \neq 2$.

Lema 2.5 *Sea $A = (A_{ij})$ entonces* $\det A$ *no es congruente con cero* $\pmod{p}$ *si, y sólo si,* $\det A_{ii}$ *no es congruente con cero* $\pmod{p}$

Demostración

Desarrollando los determinantes tenemos que

$$\det A = \det A_{11} \cdot \det A_{22} \pmod{p} \ ■$$

A continuación se caracteriza matricialmente a $AutG$

Proposición 2.6 $AutG = \begin{pmatrix} AutG_1 & Hom(G_2, G_1) \\ Hom(G_1, G_2) & AutG_2 \end{pmatrix}$

Demostración

$\subseteq$) Sea $A = (A_{ij}) \in AutG$, demostraremos que $A \in \begin{pmatrix} AutG_1 & Hom(G_2, G_1) \\ Hom(G_1, G_2) & AutG_2 \end{pmatrix}$

Por hipótesis existe $B = (B_{ij}) \in AutG$ tal que $AB = I$, es decir,

$$\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} I_1 & 0 \\ 0 & I_2 \end{pmatrix}$$

donde $I_1 \in AutG_1$, $I_2 \in AutG_2$. Por tanto

$$A_{11}B_{11} + A_{12}B_{21} = I_1 \qquad (1)$$

$$A_{21}B_{12} + A_{22}B_{22} = I_2, \qquad (2)$$

entonces $A_{11}B_{11} = I_1 - A_{12}B_{21}$, puesto que $A_{12} \equiv 0 \pmod{p}$, entonces $A_{12}B_{21}$ es nilpotente mod p^{n_1}, es decir, existe una $k \in \mathbb{N}$ tal que: $(A_{12}B_{21})^k = 0 \pmod{p^{n_1}}$.

Así que:

$$(I_1 - A_{12}B_{21})\left(I_1 + A_{12}B_{21} + (A_{12}B_{21})^2 + \cdots + (A_{12}B_{21})^{k-1}\right) = I_1$$

por tanto $(A_{11}B_{11})^{-1} = I_1 + A_{12}B_{21} + (A_{12}B_{21})^2 + \cdots + (A_{12}B_{21})^{k-1}$ es el inverso de $A_{11}B_{11}$, de donde

$$I_1 = A_{11}B_{11}(A_{11}B_{11})^{-1} = A_{11}\left(B_{11}(A_{11}B_{11})^{-1}\right),$$

así $A_{11} \in AutG_1$, análogamente se demuestra que $B_{11} \in AutG_1$.

Similarmente se prueba que $A_{22}, B_{22} \in AutG_2$.

$\supseteq$) Sea $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \in \begin{pmatrix} AutG_1 & Hom(G_2, G_1) \\ Hom(G_1, G_2) & AutG_2 \end{pmatrix}$, probaremos que $A \in AutG$.

Sea $A = B + C$ con

$$B = \begin{pmatrix} A_{11} & 0 \\ 0 & A_{22} \end{pmatrix} \text{ y } C = \begin{pmatrix} 0 & A_{12} \\ A_{21} & 0 \end{pmatrix},$$

obsérvese que $B \in AutG$, así existe $B^{-1} \in AutG$ tal que $BB^{-1} = I$. Entonces

$$AB^{-1} = (B + C)\, B^{-1} = I + CB^{-1} \in EndG$$

realizando un argumento similar a la primera parte, se obtiene que AB^{-1} es inversible y se sigue que $A \in AutG$ ■

Proposición 2.7 *Sea* $A \in EndG$. *Entonces* $A \in AutG$ *si, y sólo si,* $\det A$ *no es congruente con cero* $(\operatorname{mod} p)$

Demostración

Sea $A \in AutG$, como **or** $(EndG)$ es finito, entonces **or** $(AutG)$ es finito, existe una k tal que $A^k = I$, así $\det(A^k) = \det A.\det A \;.\; \det A = 1$, por tanto $\det A$ no es congruente con cero $(\operatorname{mod}\ p)$

Ahora supongamos que $\det A$ no es congruente con cero $(\operatorname{mod}\ p)$, entonces $\det A_n$ no es congruente con cero $(\operatorname{mod}\ p)$, por tanto $(\det A_{22}, p^{n_1}) = 1$, así $\det A_{22} \in \mathbb{Z}_{p^{n_2}}$, existe una $k \leq p^{n_2}$ tal que $k \det A_{22} = 1$

Sea pues

$$A_{22} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix},$$

se observa que

$$k \begin{pmatrix} \alpha_{22} & -\alpha_{12} \\ -\alpha_{21} & \alpha_{11} \end{pmatrix} \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} = I_2$$

y

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} k \begin{pmatrix} \alpha_{22} & -\alpha_{12} \\ -\alpha_{21} & \alpha_{11} \end{pmatrix} = I_2,$$

de donde

$$k\begin{pmatrix} \alpha_{22} & -\alpha_{12} \\ -\alpha_{21} & \alpha_{11} \end{pmatrix}$$

es el inverso de A_{22}. Por tanto $A_{22} \in AutG_{22}$. Análogamente si

$$A_{11} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix}$$

el inverso es

$$\overline{k}\begin{pmatrix} \alpha_{22}\alpha_{33} - \alpha_{23}\alpha_{32} & \alpha_{13}\alpha_{32} - \alpha_{12}\alpha_{33} & \alpha_{12}\alpha_{23} - \alpha_{13}\alpha_{22} \\ \alpha_{23}\alpha_{31} - \alpha_{21}\alpha_{33} & \alpha_{11}\alpha_{33} - \alpha_{13}\alpha_{31} & \alpha_{13}\alpha_{21} - \alpha_{11}\alpha_{23} \\ \alpha_{21}\alpha_{32} - \alpha_{22}\alpha_{31} & \alpha_{12}\alpha_{31} - \alpha_{11}\alpha_{32} & \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \end{pmatrix},$$

donde $\overline{k}\det A_{11} = 1$, se concluye que $A_{11} \in AutG_{11}$.

Por la Proposición 2.6

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

entonces $A \in AutG$. ■

El siguiente resultado nos será de utilidad para obtener el orden del grupo $AutG$.

Lema 2.8 *Sean H y K subgrupos finitos de un grupo G,*

$$\mathrm{or}\,(HK) = \frac{\mathrm{or}\,(H)\,\mathrm{or}\,(K)}{\mathrm{or}\,(H \cap K)}$$

Demostración

Notamos que HK es la unión de clases izquierdas de K, es decir,

$$HK = \bigcup_{h \in H} hK,$$

cada conjunto cerrado de K tiene $\mathbf{or}\,(K)$ elementos, es suficiente encontrar el número de distintas clases izquierdas de la forma hK, con $h \in H$. Se tiene que $h_1K = h_2K$ para $h_1, h_2 \in H$ si y sólo si $h_2^{-1}h_1 \in K$. De esta manera $h_1K = h_2K$ si y sólo si $h_2^{-1}h_1 \in H \cap K$ si y sólo si $h_1(H \cap K) = h_2(H \cap K)$.

Así el número de clases distintas de la forma hK con $h \in H$, es el número de clases distintas $h(H \cap K)$, con $h \in H$. Por el Teorema de Lagrange

$$\mathbf{or}\,[H : H \cap K] = \frac{\mathbf{or}\,(H)}{\mathbf{or}\,(H \cap K)}$$

HK consiste de $\dfrac{\mathbf{or}\,(H)}{\mathbf{or}\,(H \cap K)}$ clases distintas de K (cada cual tiene $\mathbf{or}\,(K)$ elementos). De aquí, se sigue la igualdad. ■

Proposición 2.9 *El grupo $AutG$ tiene orden $p^{9n_1+16n_2-9}\Delta$ con $(p, \Delta) = 1$*

Demostración

El número de elementos de $AutG$ está dado por el producto del número de elementos posibles que pueden tomar $AutG_1$, $AutG_2$, $Hom\,(G_1, G_2)$, $Hom\,(G_2, G_1)$.

Calcularemos el número de elementos de $AutG_1$. Nótese que $G_1 \cong \mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_1}}$, para obtener el orden de $AutG_1$ basta contar el número de bases de G_1. Consideremos x_1 el primer elemento de una base, el orden de $\langle x_1 \rangle$ es p^{n_1}. Sean

$$\begin{aligned} H &= \{x \in G_1 \mid \mathbf{or}\,(x) = p^{n_1}\} \\ &\text{y} \\ H_1 &= \{x \in G_1 \mid \mathbf{or}\,(x) < p^{n_1}\} \end{aligned}$$

El número de primos relativos de p^{n_1} es $p^{n_1} - p^{n_1-1}$, así el número de elementos que no generan a $\mathbb{Z}_{p^{n_1}}$ es p^{n_1-1}; por tanto $\mathbf{or}(H_1) = p^{3n_1-3}$. Entonces el número posible de elecciones para x_1 es $\mathbf{or}(H) = \mathbf{or}(G_1) - \mathbf{or}(H_1) = p^{3n_1} - p^{3n_1-3}$

Eligamos x_2 el segundo miembro de la base. Sean

$$\begin{aligned} \overline{H} &= \{x \in G_1 \mid \mathbf{or}\,(x) = p^{n_1} \text{ y } x \notin \langle x_1 \rangle\} \\ &\text{y} \end{aligned}$$

$$\overline{H_1} = \{y \in G_1 \mid y = \alpha x_1 + z, \textit{ con } \alpha \in \mathbb{Z}_{p^{n_1}} \text{ y } z \in H_1\}$$

obsérve que $H_1, \langle x_1 \rangle, \overline{H_1}$ son subgrupos de G_1. Por el Lema 2.9

$$\text{or}\left(\overline{H_1}\right) = \frac{\text{or}\,(x_1)\,\text{or}\,(H_1)}{\text{or}\,(\langle x_1 \rangle \cap H_1)} = \frac{p^{n_1}p^{3n_1-3}}{p^{n_1-1}} = p^{3n_2-2}$$

como el orden de x_2 es p^{n_1} y además $x_2 \notin \langle x_1 \rangle$ entonces el número de elecciones para el segundo elemento de la base es $\text{or}\left(\overline{H}\right) = \text{or}\,(G_1) - \text{or}\left(\overline{H_1}\right) = p^{3n_1} - p^{3n_1-2}$.

Por último se contará el número de elecciones para x_3. Sean

$$\begin{aligned}
\widetilde{H} &= \{x \in G_1 \mid \text{ or}\,(x) = p^{n_1} \text{ y } x \in \langle x_1, x_2 \rangle\} \\
&\text{y} \\
\widetilde{H_1} &= \{y \in G_1 \mid \ y = \alpha_1 x_1 + \alpha_2 x_2 + z, \text{ con } \alpha_1, \alpha_2 \in \mathbb{Z}_{p^{n_1}} \text{ y } z \in H_1\},
\end{aligned}$$

entonces

$$\text{or}\left(\widetilde{H_1}\right) = \frac{\text{or}\,(\langle x_1, x_2 \rangle)\,\text{or}\,(H_1)}{\text{or}\,(\langle x_1, x_2 \rangle \cap H_1)} = \frac{p^{2n_1}p^{3n_1-3}}{p^{2n_2-2}} = p^{3n_1-1},$$

para elegir a x_3 hay tantas posibilidades como el orden de $\widetilde{H}$. Así $\text{or}\left(\widetilde{H}\right) = \text{or}\,(G_1) - \text{or}\left(\widetilde{H_1}\right) = p^{3n_1} - p^{3n_1-1}$.

Por tanto el número de posibles bases para G_1 es:

$$\begin{aligned}
\text{or}\,(H)\,\text{or}\left(\overline{H}\right)\text{or}\left(\widetilde{H}\right) &= \left(p^{3n_1} - p^{3n_1-3}\right)\left(p^{3n_1} - p^{3n_1-2}\right)\left(p^{3n_1-1}\right) \\
&= p^{9n_1-6}\left(p^3 - 1\right)\left(p^2 - 1\right)(p-1),
\end{aligned}$$

se concluye que:

$$\text{or}\,(AutG_1) = p^{9n_1-6}\left(p^3 - 1\right)\left(p^2 - 1\right)(p-1),$$

para calcular el orden de $AutG_2$, notemos que $G_2 \cong \mathbb{Z}_{p^{n_2}} \oplus \mathbb{Z}_{p^{n_2}}$, entonces con un argumento similar se demuestra que:

$$\text{or}\,(AutG_2) = \left(p^{2n_2} - p^{2n-2}\right)\left(p^{2n_2} - p^{2n_2-1}\right) = p^{4n_2-3}\left(p^2 - 1\right)(p-1),$$

consecuentemente

$$\begin{aligned}
\text{or}\,(AutG) &= \text{or}\,(AutG_1)\,\text{or}\,(AutG_2)\,\text{or}\,(Hom\,(G_1,G_2))\,\text{or}\,(Hom\,(G_2,G_1)) \\
&= p^{9n_1-6}\left(p^3-1\right)\left(p^2-\right)(p-1)\,p^{4n_2-3}\left(p^2-1\right)(p-1)\,p^{6n_2}p^{6n_2} \\
&= p^{9n_1+16n_2-9}\left(p^3-1\right)\left(p^2-1\right)^2(p-1)^2,
\end{aligned}$$

Si $\Delta = \left(p^3-1\right)\left(p^2-1\right)^2(p-1)^2$ Así se concluye que $(p,\Delta)=1$ ■

2.3 Estudio de S subconjunto de Endomorfismos de G

Es esta sección se define a un subconjunto S del anillo de endomorfismos de G que cumple que $S+I$ es un p-subgrupo de Sylow de $AutG$. Denotaremos $I_5=\{4,5\}$

Definición 2.10 *Sea*

$$e_{ij} = \begin{cases} p^{n_1-n_2} & \text{si } i \in J_3 \text{ y } j \in I_5 \\ 1 & \text{si } i > j \\ p & \text{si } i \leq j \quad \text{e} \quad (i \in I_5 \text{ o } j \in J_3) \end{cases}$$

definimos a $S=\{A=(a_{ij})\in EndG \mid a_{ij}=e_{ij}\alpha_{ij} \text{ con } \alpha_{ij}\in\mathbb{Z}_{p^{m_i}}\}$, *entonces*

$$S=\left\{\begin{pmatrix} p\alpha_{11} & p\alpha_{12} & p\alpha_{13} & p^{n_1-n_2}\alpha_{14} & p^{n_1-n_2}\alpha_{15} \\ \alpha_{21} & p\alpha_{22} & p\alpha_{23} & p^{n_1-n_2}\alpha_{24} & p^{n_1-n_2}\alpha_{25} \\ \alpha_{31} & \alpha_{32} & p\alpha_{33} & p^{n_1-n_2}\alpha_{25} & p^{n_1-n_2}\alpha_{35} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & p\alpha_{44} & p\alpha_{45} \\ \alpha_{51} & \alpha_{52} & \alpha_{53} & \alpha_{54} & p\alpha_{55} \end{pmatrix} \in EndG \mid \alpha_{ij}\in\mathbb{Z}_{p^{m_i}}\right\}$$

Lema 2.11 *S es un subanillo de $EndG$.*

Demostración

Es claro que $\overline{0}=(0_{ij})\in S$ (neutro aditivo de $EndG$). Sean $A=(a_{ij})\in S$, $B=(b_{ij})\in S$, con $a_{ij}=e_{ij}\alpha_{ij}$, $b_{ij}=e_{ij}\beta_{ij}$, $\alpha_{ij},\beta_{ij}\in\mathbb{Z}_{p^{m_i}}$, entonces $a_{ij}-b_{ij}=e_{ij}\left(\alpha_{ij}-\beta_{ij}\right)$, así $A-B\in S$

Si $A.B = C = (c_{ij})$, donde $c_{ij} = \sum_{k=1}^{5} e_{ik}\alpha_{ik}e_{kj}\beta_{kj}$. Por demostrar que $C \in S$.

1^{er} caso Si $i \in J_3$ y $j \in I_5$.

$$c_{ij} = \sum_{k=1}^{5} e_{ik}\alpha_{ik}e_{kj}\beta_{kj} = p^{n_1-n_2}\left(\sum_{k=1}^{3} e_{ik}\alpha_{ik}\beta_{kj} + \sum_{k=4}^{5} \alpha_{ik}e_{kj}\beta_{kj}\right) = p^{n_1-n_2}\gamma_{ij}.$$

2^{do} caso Si $i \leq j$ y $(i \in I_5$ o $j \in J_3)$.

$a)$ $i \in I_5$

$$c_{ij} = \sum_{k=1}^{5} e_{ik}\alpha_{ik}e_{kj}\beta_{kj} = p\left(\sum_{k=1}^{4} e_{ik}\alpha_{ik}\beta_{kj} + \alpha_{i5}e_{5j}\beta_{5j}\right) = p\gamma_{ij}$$

$b)$ $j \in J_3$

$$c_{ij} = \sum_{k=1}^{5} e_{ik}\alpha_{ik}e_{kj}\beta_{kj} = p\left(\sum_{k=1}^{5} \alpha_{ik}\beta_{kj}\right) = p\gamma_{ij}.$$

3^{er} caso Si $i > j$

$$\text{claramente } c_{ij} = \sum_{k=1}^{5} e_{ik}\alpha_{ik}e_{kj}\beta_{kj} = \gamma_{ij},$$

esto implica que $C \in S$. Por tanto S es un subanillo de $EndG$. ■

Proposición 2.12 *$S + I$ es un $p-$subgrupo de Sylow de $AutG$.*

Demostración

Primero probaremos que $S + I \subseteq AutG$. Sea $A = (A_{ij}) \in S$, con $A_{ij} \in Hom(G_j, G_i)$, entonces

$$A + I = \begin{pmatrix} A_{11} + I_1 & A_{12} \\ A_{21} & A_{22} + I_2 \end{pmatrix} \in S + I,$$

donde I_i es la identidad de $End(G_i)$ para $i \in J_2$.

Desarollando los determinantes y aplicando un argumento similar al lema 2.6 tenemos que

$$\det(A + I) = \det(A_{11} + I_1) . \det(A_{22} + I_2) \pmod{p}$$

$$\det(A_{11}+I_1) = \det\begin{pmatrix} pa_{11}+1 & pa_{12} & pa_{13} \\ a_{12} & pa_{22}+1 & pa_{23} \\ a_{31} & a_{32} & pa_{33}+1 \end{pmatrix}$$
$$= (pa_{11}+1)\left[(pa_{22}+1)(pa_{33}+1) - pa_{23}a_{32}\right] \pmod{p}$$

así $\det(A_{11}+I_1) \equiv 1 \pmod{p}$, análogamente $\det(A_{22}+I_2) \equiv 1 \pmod{p}$ Entonces $\det(A+I)$ no es congruente con cero módulo p Por tanto $A+I \in AutG$.

Ahora prueba que $S+I$ es un subgrupo de $AutG$. Claramente $S+I \neq \emptyset$ $(I \in S+I)$ Sean $A+I$, $B+I \in S+I$, entonces

$$(A+I)(B+I) = AB + A + B + I \in S+I\,,$$

por ser S un anillo. Por la Proposición 2.9, $AutG$ es un grupo finito entonces $A+I$ tiene orden finito, sea l el orden de $A+I$. Sea $k = l-1$, entonces

$$(A+I)^k = A^k + \binom{k}{1}A^{k-1} + \binom{k}{2}A^{k-2} + \ldots + \binom{k}{k-1}A + I \in S+I$$

por tanto $(A+I)^{l-1} \in S+1$, es el inverso de $A+I$. Se concluye que $S+I$ es subgrupo de $AutG$

Obsérve que el orden de $S+I$ es igual al orden de S.

$$\mathbf{or}\,(S+I) = \mathbf{or}\,(S) = p^{9n_1+16n_2-9}$$

por el Corolario 1.32, $S+I$ es un p-subgrupo, por la Proposición 2.9, $AutG = p^{9n_1+16n_2-9}\Delta$ con $(p,\Delta) = 1$, por la Teorema 1.34, $S+I$ es un p-subgrupo de Sylow ■

Capítulo 3

SERIE ANULADORA DE S Y SERIE CENTRAL DE S+I.

En lo que sigue p denotará un número primo.

3.1 Caracterización de los ideales de S.

Lema 3.1 *Cualquier subgrupo de $\mathbb{Z}_{p^n}$ es un ideal de $\mathbb{Z}_{p^n}$.*

Demostración

primero se demuestra que todo subgrupo de $\mathbb{Z}_{p^n}$ es de la forma $p^\alpha \mathbb{Z}_{p^n}$ con $0 \leq \alpha \leq p^n$. Sea H un subgrupo de $\mathbb{Z}_{p^n}$, como $\mathbb{Z}_{p^n}$ es cíclico, entonces H es un subgrupo cíclico, así $H = \langle a \rangle$ donde $a = p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ con p. p_i números primos y α, $\alpha_i \in \mathbb{N}$ para $i = 1 \ldots k$, así $(a, p^n) = p^\alpha$, con $0 \leq \alpha \leq n$ además $(p^\alpha, p^n) = p^\alpha$ por tanto $\text{or}\left(\langle p^\alpha \rangle\right) = \text{or}\left(\langle a \rangle\right) = \frac{p^n}{p^\alpha}$, entonces $\langle p^\alpha \rangle = \langle a \rangle = H$, pero $\langle p^\alpha \rangle = p^\alpha \mathbb{Z}_{p^n}$.

Afirmamos que un subgrupo de $\mathbb{Z}_{p^n}$ es un ideal de $\mathbb{Z}_{p^n}$. Sea $H = p^\alpha \mathbb{Z}_{p^n}$ para algún $0 \leq \alpha \leq n$ un subgrupo de $\mathbb{Z}_{p^n}$. Sea $x \in \mathbb{Z}_{p^n}$ entonces $xp^\alpha \mathbb{Z}_{p^n} \subseteq p^\alpha \mathbb{Z}_{p^n}$ ya que $xp^\alpha m = p^\alpha (xm)$ para todo $m \in \mathbb{Z}_{p^n}$. Análogamente $p^\alpha \mathbb{Z}_{p^n} x \subseteq p^\alpha \mathbb{Z}_{p^n}$. ■

Se caracteriza a los ideales de S, sea H un ideal del anillo S, y $A = (a_{ij}) \in H$ se denota por $(A)_{ij} = a_{ij}$. Consideramos al siguiente conjunto $N_{ij} = \left\{ (A)_{ij} \in \mathbb{Z}_{p^{m_i}} \mid A \in H \right\}$

Lema 3.2 *Sea $A = (a_{ij}) \subset H$, si H un ideal de S entonces N_{ij} es un ideal de $\mathbb{Z}_{p^{m_i}}$*

Demostración

El conjunto $N_{ij} \neq \emptyset$ ya que $(0)_{ij} \in N_{ij}$

Sean $(A)_{ij}, (B)_{ij} \in N_{ij}$ entonces existen $A = (a_{ij}), B = (b_{ij}) \in H$, así $A + B = (c_{ij})$

$$(A)_{ij} + (B)_{ij} = a_{ij} + b_{ij} = c_{ij} = (C)_{ij} \in \mathbb{Z}_{p^{m_i}},$$

además $-A = (-a_{ij})$, sea $(-A)_{ij} = -a_{ij}$, por tanto $(-A)_{ij} \in N_{ij}$, así N_{ij} es un subgrupo de $\mathbb{Z}_{p^{m_i}}$. Por el Lema anterior N_{ij} es un ideal de $\mathbb{Z}_{p^{m_i}}$. ■

Como todos los ideales de $\mathbb{Z}_{p^{m_i}}$ son de la forma $p^{\alpha}\mathbb{Z}_{p^{m_i}}$ para algún $0 \leq \alpha \leq m_i$. Por tanto $N_{ij} = p^{n_k - \beta_{ij}}\mathbb{Z}_{p^{m_i}}$ con $0 \leq n_k - \beta_{ij} \leq m_i$.

Definición 3.3 *Sean $f : J_5 \times J_5 \longrightarrow \mathbb{N}$ y $i^-, j^- \in J_3$, $i^+, j^+ \in I_5$; $i, j \in J_5$. Decimos que f es una función ideal si satisface las siguientes condiciones .*

1.1) $0 \leq f(i,j) \leq m_i$ *para todo* $i \in J_5$

1.2.) *a)* $f(i^+, j) \leq f(i^-, j)$

b) $f(i, j^+) \leq f(i, j^-)$

1.3) *a)* $f(i^-, j) \leq f(i^+, j) + n_1 - n_2$

b) $f(i, j^-) \leq f(i, j^+) + n_1 - n_2$

1.4) *a)* $f(i-1, j) \leq f(i,j)$ *si* $m_{i-1} = m_i$

b) $f(i+1, j) \leq f(i,j) + 1$ *si* $m_{i+1} = m_i$

$f(i+1, j) \leq f(1,j) + 1$ *si* $m_{i+1} = n_1$

1.5) *a)* $f(i, j+1) \leq f(i,j)$ *si* $m_j = m_{j+1}$

b) $f(i, j-1) \leq f(i,j) + 1$ *si* $m_{j-1} = m_j$

$f(i, j-1) \leq f(i,3) + 1$ *si* $m_{j-1} = n_1$.

Proposición 3.4 *$H = (H_{ij})$ es un ideal de S si, y sólo si, existe una función ideal $f : J_5 \times J_5 \longrightarrow \mathbb{N}$ tal que $H_{ij} = p^{m_i - f(i,j)} M_{ij}$.*

Demostración

Sea $H = (H_{ij})$ es un ideal de S. Por el Lema 3.2 $H_{ij} = p^{m_i - \beta_{ij}} M_{ij}$ con $0 \leq \beta_{ij} \leq m_i$. Sea $f : J_5 \times J_5 \longrightarrow \mathbb{N}$ tal que $f(i,j) = \beta_{ij}$, por demostrar que β_{ij} es una función ideal.

Sean $A = (a_{ij}) \in H$ y $B = (b_{ij}) \in S$ tal que $a_{ij} = p^{m_i - f(i,j)}\alpha_{ij}$ y $b_{ij} = e_{ij}\gamma_{ij}$ con $\alpha_{ij}, \beta_{ij} \in \mathbb{Z}_{p^{m_i}}$. $AB \in H$ si, y sólo si,

$$(a_{ij})(b_{ij}) = (ab)_{ij} = \sum_{k=1}^{5} a_{ik}b_{kj} = \sum_{k=1}^{5} p^{m_i - f(i,k)}\alpha_{ik}e_{kj}\gamma_{kj} \in H_{ij}$$

con $\alpha_{ik} \in \mathbb{Z}_{p^{m_i}}$ y $\gamma_{kj} \in \mathbb{Z}_{p^{m_k}}$. Esto sucede si, $a_{ik}b_{kj} \in H_{ij}$ para todo $k \in J_5$. Se prueba que f es una función ideal analizando los diferentes valores de e_{ij}

1ercaso. si $k > j$.

Entonces $a_{ik}b_{kj} = p^{m_i - f(i,k)}\alpha_{ik}\gamma_{kj} \in H_{ij}$. Si $p^{m_i - f(i,k)} \geq p^{m_i - f(i,j)}$, implica que $f(i,k) \leq f(i,j)$. Si $k \in I_5$ y $j \in J_3$ entonces $f(i,j^+) \leq f(i,j^-)$ (Propiedad 1.2.b). Si $k, j \in J_3$ o $k, j \in I_5$ entonces $m_k = m_j$, si $k = j+1$ se sigue que $f(i,j+1) \leq f(i,j)$(Propiedad 1.5.a).

2docaso. si $k \in j_3$ y $j \in I_5$.

Entonces $a_{ik}b_{kj} = p^{m_i - f(i,k) + n_1 - n_2}\alpha_{ik}\gamma_{kj} \in H_{ij}$. Si $p^{m_i - f(i,k)+n_1-n_2} \geq p^{m_i - f(i,j)}$, se sigue que $f(i,j^-) \leq f(i,j^+) + n_1 - n_2$ (Propiedad 1.3.b)

3ercaso. si $k \leq j$ y ($k \in I_5$ o $j \in J_3$)

Entonces $a_{ik}b_{kj} = p^{m_i - f(i,k)+1}\alpha_{ik}\gamma_{kj} \in H_{ij}$. Si $k \in I_5$ entonces $j \in J_3$ por tanto $m_i = m_k$. Si $j \in J_3$ entonces $k \in J_3$. Tomando $k = j - 1$ se obtiene que $f(i, j-1) \leq f(i,j) + 1$ si $m_{j-1} = m_j$ y $f(i, j-1) \leq f(i,3) + 1$ si $m_{j-1} = n_1$ (Propiedad 1.5.b)

Considerando la propiedad de ideal derecho de H, es decir, $BA \in H$ si, y sólo si,

$$(ba)_{ij} = \sum_{k=1}^{5} b_{ik}a_{kj} = \sum_{k=1}^{5} e_{ik}\gamma_{ik}p^{m_k - f(k,j)}\alpha_{kj} \in H_{ij}$$

sabemos $b_{ik}a_{kj} \in H_{ij}$. Analizando los casos de e_{ik} se tienen las demás propiedades de función ideal para f.

1ercaso. si $i > k$.

Entonces $b_{ik}a_{kj} = p^{m_k - f(k,j)}\gamma_{ik}\alpha_{kj} \subseteq H_{ij}$, implica que $p^{m_k - f(k,i)} \geq p^{m_i - f(i,j)}$, así $f(k,j) \leq f(k,j) + m_k - m_i$ con $m_k \geq m_i$ Si $k \in J_3$ y $i \in I_5$, se tiene que $m_k = n_1 > n_2 = m_i$, entonces $f(i^{-1}, j) \leq f(i^+, j) + n_1 - n_2$ (Propiedad 1.3.a). Si $i, k \in J_3$ o $i, k \in I_5$, $m_k = m_i$ tomando $k = i - 1$, tenemos que $f(i-1, j) \leq f(i,j)$ con $m_{i-1} = m_i$ (Propiedad 1.4.a).

2docaso. Si $i \in J_3$ y $k \in I_5$.

Tenemos que $b_{ik}a_{kj} = p^{m_k - f(k,j)+n_1-n_2}\gamma_{ik}\alpha_{kj} = p^{n_1 - f(k,j)} \subseteq H_{ij}$, y se sigue $p^{n_1 - f(k,j)} \geq p^{m_i - f(i,j)}$, como $i \in J_3$ entonces $m_i = n_1$. Por tanto $f(k,j) \leq f(i,j)$, es decir, $f(i^+ j) \leq f(i^-, j)$ (Propiedad 1.2.a).

3^{er}**caso** Si $i \leq k$ y $(i \in I_5$ o $k \in J_3)$.

Entonces $b_{ik}a_{kj} = p^{m_k - f(k,j)+1}\gamma_{ik}\alpha_{kj} \subseteq H_{ij}$, entonces, $p^{m_k - f(k,j)+1} \geq p^{m_i - f(i,j)}$con $m_i = m_k$, es decir, $f(k,j) \leq f(i,j) + 1$. Si $k = i+1$, se sigue que $f(i+1,j) \leq f(i,j+1)$ con $m_{i-1} = m_i$. (Propiedad 1.4.b).

En estos casos se acaba de demostrar que f cumple todas las condiciones de una función ideal.

Inversamente supongamos que f es una función ideal. Sea $A = (a_{ij}) \in H$, $B = (b_{ij}) \in S$ con $a_{ij} = p^{m_i - f(i,j)}\alpha_{ij}$, $b_{ij} = e_{ij}\beta_{ij}$, $\alpha_{ij}, \beta_{ij} \in \mathbf{Z}_{p^{m_i}}$. Entonces

$$(ab)_{ij} = \sum_{k=1}^{5} a_{ik}b_{kj} = \sum_{k=1}^{5} p^{m_i - f(i,k)}\alpha_{ik}e_{kj}\beta_{kj}\; AB \in H$$

esta igualdad sucede si, $(ab)_{ij} \in H_{ij}$ es decir si $a_{ik}b_{kj} \in H_{ij}$

Demostraremos que H es un ideal izquierdo probando que $a_{ik}b_{kj} \in H_{ij}$, analizando los casos de e_{ij}.

1^{er}**caso.** Si $k > j$

Se tiene que $a_{ik}b_{kj} = p^{m_i - f(i,k)}\alpha_{ik}\beta_{kj}$, por las propiedades 1 2.a y 1.5 se tiene que $f(i,k) \leq f(i,j)$ esto implica que $p^{m_i - f(i,k)} \geq p^{m_i - f(i,j)}$ así $a_{ik}b_{kj} \in H_{ij}$

2^{do}**caso.** Si $k \in J_3$, $j \in I_5$.

Entonces $a_{ik}b_{kj} = p^{m_i - f(i,k)+n_1-n_2}\alpha_{ik}\beta_{kj}$, por la propiedad 1 3.$b$ se sigue la desigualdad $f(i,k) \leq f(i,j) + n_1 - n_2$, entonces $p^{m_i - f(i,k)+n_1-n_2} \geq p^{m_i - f(i,j)}$, por tanto $a_{ik}b_{kj} \in H_{ij}$.

3^{er} **caso.** Si $k \leq j$ y $(k \in I_5$ o $j \in J_3)$.

Entonces $a_{ik}b_{kj} = p^{m_i - f(i,k)+1}\alpha_{ik}\beta_{kj}$, en cualquiera de los dos casos $f(i,k) \leq f(i,j) + 1$ por la propiedad 1.5.a y porque $m_k = m_j$, así $p^{m_i - f(i,k)+1} \geq p^{m_i - f(i,j)}$ por tanto $a_{ik}b_{kj} \in H_{ij}$.

Se concluye que $AB \in H$. Análogamente se demuestra que H es un ideal derecho ■

Sean $N = (n_{ij})$ y $M = (m_{ij})$ dos ideales de S, entonces existen funciones ideales f y q tal que, $a_{ij} = p^{m_i - f(i,j)}\alpha_{ij}$, $b_{ij} = p^{m_i - q(i,j)}\beta_{ij}$. Sea $(nm)_{ij}$ la entradad (i,j) del producto de NM.

Proposición 3.5 *Sean* $N = (n_{ij})$, $M = (m_{ij})$ *ideales de* S, *con* $(nm)_{ij} = p^{m_i - k(i,j)}\gamma_{ij}$, *entonces* $k(i,j) = \max_k \{f(i,k) + g(k,j) - m_k\}$

Demostración

$$\begin{aligned}(nm)_{ij} &= \sum_{k=1}^{5} n_{ik}m_{kj} = \sum_{k=1}^{5} p^{m_i - f(i,k)+m_k-g(k,j)}\alpha_{ik}\beta_{kj} \\ &= \sum_{k=1}^{5} p^{m_i-[f(i,k)+g(k,j)-m_k]}\alpha_{ik}\beta_{kj}. \blacksquare\end{aligned}$$

3.2 Serie anuladora de S.

Sea $0 = S_0 \subsetneq S_1 \subsetneq \ldots \subsetneq S_d = S$ una serie anuladora de S, donde cada S_t es un ideal de S, los cuales se han caracterizado en la sección anterior. Sea f_t la función ideal asociada a cada ideal S_t, entonces $S_t = \left(a_{ij}^t\right)$ esta determinado por $a_{ij}^t = p^{m_i - f_t(i,j)}\alpha_{ij}^t$. Estos ideales además cumple que $S_t/S_{t-1} \subset Ann\left(S/S_{t-1}\right)$. Esto da origen a que los ideales cumplan condiciones que relacionen a f_t con f_{t-1}.

Definición 3.6 *Sea* $f_t : J_5 \times J_5 \longrightarrow \mathbb{N}$ *una función para todo* $t \in \mathbb{N}$. *Decimos que* f_t *es una función anuladora de* S *si satisface las siguientes condiciones :*

2.1) $f_t(i,j) \leq f_{t-1}(i,j) + 1$

2.2) *a)* $f_t(i^+,j) \leq f_{t-1}(i^-,j)$

b) $f_t(i,j^+) \leq f_{t-1}(i,j^-)$

2.3) *a)* $f_t(i^-,j) \leq f_{t-1}(i^+,j) + n_1 - n_2$

b) $f_t(i,j^-) \leq f_{t-1}(i,j^+) + n_1 - n_2$

2.4) *a)* $f_t(i-1,j) \leq f_{t-1}(i,j)$ *si* $i \neq 4$

b) $f_t(i+1,j) \leq f_{t-1}(i,j) + 1$ *si* $i \neq 3$

$f_t(3,j) \leq f_{t-1}(1,j) + 1$

2.5) *a)* $f_t(i,j+1) \leq f_{t-1}(i,j)$ *si* $j \neq 3$

b) $f_t(i,j-1) \leq f_{t-1}(i,j) + 1$ *si* $j \neq 4$

$f_t(i,1) \leq f(i,3) + 1$

2.6) $f_{t-1}(i,j) \leq f_t(i,j) \leq f_d(i,j)$

Observese que las propiedades 2.1 a la 2.5 incluyendo $f_{t-1}(i,j) \leq f_t(i,j)$ implican las condiciones de función ideal que definimos en la sección 3.1.

Proposición 3.7 *Sea $\{S_l\}_{l\in J_d}$ una serie de ideales de S, con $S_d = S$, entonces $\left\{S_l = p^{m_i - f_l(i,j)}M_{ij}\right\}_{l\in J_d}$ es una serie anuladora de S si, y sólo si, f_l es una función anuladora.*

Demostración

Supongamos que $\{S_l\}_{l\in J_d}$ es una serie anuladora de S, entonces $S.S_l \subseteq S_{l-1}$ y $S_l.S \subseteq S_{l-1}$. Sea $S.S_l = (a_{ij})$ y $S_l.S = (b_{ij})$ que cumplen

$$a_{ij} \equiv 0 \left(\bmod\ p^{m_i - f_{l-1}(i,j)}\right),\ b_{ij} \equiv 0 \left(\bmod\ p^{m_i - f_{l-1}(i,j)}\right),$$

por ser S_l ideales tenemos $a_{ij} = p^{m_i - g(i,j)}\alpha_{ij}$, $b_{ij} = p^{m_i - h(i,j)}\beta_{ij}$, entonces

$$\begin{aligned} m_i - g(i,j) &\geq m_i - f_{l-1}(i,j) && (1)\\ m_i - h(i,j) &\geq m_i - f_{l-1}(i,j) && (2)\end{aligned}$$

por la Proposición 3.5

$$g(i,j) = \max_k \{f_d(i,k) + f_l(k,j) - m_k\}\ \ y\ h(i,j) = \max_k \{f_l(i,k) + f_d(k,j) - m_k\}$$

por tanto (1) y (2) se transforman en.

$$\begin{aligned} f_d(i,k) + f_l(k,j) - m_k &\leq f_{l-1}(i,j) && (3)\\ f_l(i,k) + f_d(k,j) - m_k &\leq f_{l-1}(i,j) && (4)\end{aligned}$$

por demostrar que f_l es una función anuladora. Si $k = i$ en (3)

$$\begin{aligned} m_i - 1 + f_l(i,j) - m_i &\leq f_{l-1}(i,j)\\ f_l(i,j) &\leq f_{l-1}(i,j) + 1 \qquad \text{(propiedad 2.1)}\end{aligned}$$

Si $k = i + 1$ en (3)

$$\begin{aligned} f_d(i,i+1) &= \begin{cases} m_{i+1} - 1 & si\ i \neq 3\\ n_2 & si\ i = 3\end{cases}\\ f_l(i+1,i) &\leq f_{l-1}(i,j) + 1 \quad \text{(propiedad 2.4 } b)\end{aligned}$$

$$f_t(4,j) \leq f_{t-1}(3,j),$$

estas dos desigualdades implican que

$$f_t(i^+,j) \leq f_{t-1}(i^-,j) \quad \text{(propiedad 2.2.}a\text{)}$$

Si $k = j+1$ en (4)

$$\begin{aligned} f_d(j+1,j) &= m_{j+1}, \text{ se obtiene que,} \\ f_t(i,j+1) &\leq f_{t-1}(i,j) \qquad \text{(propiedad 2.5.}a\text{)} \\ f_t(i,j^+) &\leq f_{t-1}(i,j^-) \quad \text{(propiedad 2.2.}b\text{)} \end{aligned}$$

Si $k = i-1$ en (3)

$$\begin{aligned} f_d(i,i-1) &= \begin{cases} m_{i-1} & si\ i \neq 4 \\ n_2 & si\ i = 4 \end{cases} \\ f_t(i-1,j) &\leq f_{t-1}(i,j) \quad \text{(propiedad 2.4.}a\text{)} \\ f_t(3,j) &\leq f_{t-1}(4,j) + n_1 - n_2 \end{aligned}$$

estas dos desigualdades implican que

$$f_t(i^-,j) \leq f_{t-1}(i^+,j) + n_1 - n_2 \qquad \text{(propiedad 2.3.}a\text{)}$$

si $k = j-1$ en (2)

$$\begin{aligned} f_d(j-1,j) &= \begin{cases} m_{j-1} & si\ j \neq 4 \\ n_2 & si\ j = 4 \end{cases} \\ f_t(i,j-1) &\leq f_{t-1}(i,j) + 1 \quad \text{(propiedad 2.5.}b\text{)} \\ f_t(i,3) &\leq f_{t-1}(i,4) + n_1 - n_2 \end{aligned}$$

se sigue que

$$f_t(i,j^-) \leq f_{t-1}(i,j^+) + n_1 - n_2 \quad \text{(propiedad 2.3.}b\text{)}$$

finalmente $S_{t-1} \subseteq S_t$ implica $p^{m_i - f_{t-1}(i,j)} \geq p^{m_i - f_t(i,j)}$, así, $f_{t-1}(i,j) \leq f_t(i,j)$ Análogamente de la condición $S_t \subseteq S_d$ para todo $t \in J_d$, se tiene $f_t(i,j) \leq f_d(i,j)$.

Inversamente supongamos f_t en una función anuladora, probaremos que $\{S_t = p^{m_i - f_t(i,j)} M_{ij}\}_{t \in J_d}$ es una serie anuladora de S.

Las propiedades 2.1 a la 2.5 incluyendo $f_{t-1}(i,j) \leq f_t(i,j)$ implican que f es una función ideal. Por la Proposición 3.4 S_t es un ideal de S,de la condición 2.6 tenemos que $S_{t-1} \subseteq S_t \subseteq S_d$. Falta por demostrar $S_t / S_{t-1} \subset Ann(S/S_{t-1})$, es decir, $S\,S_t \subseteq S_{t-1}$, $S_t\,S \subseteq S_{t-1}$. Recordemos que $S\,S_t = (a_{ij})$, $a_{ij} = p^{\,m_i - g(i,j)}\alpha_{ij}$ con $g(i,j) = \max_k \{f_d(i,k) + f_t(k,j) - m_k\}$ Se prueba que $f_d(i,k) + f_t(k,j) - m_k \leq f_{t-1}(i,j)$

1^er caso. Si $i \in J_3$, $k \in I_5$. Por la condición 2.2.a de función anuladora se tiene que

$$f_d(i,k) + f_t(k,j) - m_k = n_2 + f_t(k,j) - n_2 = f_t(i,j) \leq f_{t-1}(i,j)$$

2^do caso. Si $i > k$. De la propiedad 2.3 a, se sigue que

$$f_d(i,k) + f_t(k,j) - m_k = m_i + f_t(k,j) - m_k \leq f_t(k,j) + n_2 - n_1 \leq f_{t-1}(i,j)$$

ya que $i > k$ implica $m_k \leq m_i$.

3^er caso. Si $i \leq k$ y ($i \in I_5$ o $k \in J_3$) Por la condición 2.4.b obtenemos que

$$f_d(i,k) + f_t(k,j) - m_k = n_2 - 1 + f_t(k,j) - n_2 = f_t(k,j) - 1 \leq f_{t-1}(i,j)$$

Se ha demostrado que $g(i,j) \leq f_{t-1}(i,j)$, es decir, $p^{m_i - g(i,j)} \geq p^{m_i - f_{t-1}(i,j)}$, por tanto $S.S_t \subseteq S_{t-1}$ Análogamente se demuestra que $S_t\,S \subseteq S_{t-1}$, lo cual completa la prueba. ■

3.3 Serie central de S+I.

Sea $\mathcal{P} = S + I$ y $Z(EndG)$ el centro del anillo de endomorfismos de G Sea $H = \mathcal{P} \cap Z(EndG)$, aquí se demuestra que si $\{S_t\}_{t \in J_d}$ es una serie anuladora del subanillo S, entonces $\{S_t + H\}_{t \in J_d}$ es una serie central de $\mathcal{P}$

Lema 3.8 *$S_t + I$ es un subgrupo normal de $\mathcal{P} = S + I$.*

Demostración

Sean $a+I, b+I \in S+I$, entonces $(a+I)(b+I) = ab+a+b+I \in S_t+I$, ya que $ab+a+b \in S_t$, por ser S_t ideal de S. Sea $(a+I)^{-1} = a'+I \in S+I$, tal que, $(a+I)(a'+I) = I$ implica $aa'+a+a' = 0$, como $-aa'-a \in S_t$, por tanto $a' \in S_t$, así $a'+I \in S_t+I$.

Por demostrar que S_t es normal en $\mathcal{P}$. Sean $a+I \in S_t+I$, $c+I \in S+I$, con $a \in S_t$, $b \in S$, entonces

$$\begin{aligned}(c+I)(a+I)(c+I)^{-1} &= (c+I)(a+I)(c'+I)\\ &= cac'+cc'+ac'+c'+ca+c+a+I\\ &= cac'+ac'+ca+a+I \in S_t+I.\ (\text{ya que } cc'+c+c'=0),\end{aligned}$$

concluimos que $S_t+I \trianglelefteq \mathcal{P} = S+I$. ■

Lema 3.9 *H es un subgrupo normal de $\mathcal{P}$.*

Demostración

Sea $a+I, b+I \in H$, entonces $(a+I)(b+I) \in \mathcal{P}$, por ser $\mathcal{P}$ un subgrupo y además

$$(a+I)(b+I)z = (a+I)z(b+I) = z(a+I)(b+I)$$

para todo $z \in EndG$, ya que $(a+I), (b+I) \in Z(EndG)$, así $(a+I)(b+I) \in Z(EndG)$, implica que $(a+I)(b+I) \in H$.

Para $(a+I) \in H$, existe $(a+I)^{-1} \in \mathcal{P}$, tal que $(a+I)(a+I)^{-1} = I$, además:

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

para todo $z \in EndG$, entonces $(a+I)^{-1} \in Z(EndG)$, así $(a+I)^{-1} \in H$.

Por último, sean $(a+I) \in H$ y $(c+I) \in \mathcal{P}$, entonces:

$$(a+I)(c+I) = (c+I)(a+I),$$

porque $\mathcal{P} \subset EndG$ y $a+I \in Z(EndG)$. ■

Proposición 3.10 *$S_t + H$ es un subgrupo normal de $\mathcal{P}$.*

demostración

Por los resultados anteriores $S_t + I \trianglelefteq \mathcal{P}$ y $H \trianglelefteq \mathcal{P}$, entonces $(S_t + I)\,H \trianglelefteq \mathcal{P}$ Se prueba que $(S_t + I)\,H = S_t + H$, es decir, $S_tH \subseteq S_t$. Sean $a \in S_t$, $b + I \in H$, tenemos que:

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

En el capítulo anterior se demostró que $S + I$ es un $p-$subgrupo de Sylow de $AutG$ Por la Proposición 1.36 $S + I$ es nilpotente. Ahora se prueba que toda seria anuladora en S induce una serie central en $S + I$.

Definición 3.11 *Sea G un p-grupo abeliano finito, decimos que G es regular respecto a un subgrupo $H \subseteq AutG$ si la serie anuladora del anillo S induce a una serie central en H.*

Lema 3.12 *$S + I = S + H$ con $H = \mathcal{P} \cap Z\,(EndG)$.*

Demostración

Tenemos que $H \trianglelefteq \mathcal{P}$ y $S + H \trianglelefteq \mathcal{P}$. Así

$$\mathcal{P} = S + I \leq (S + I)\,H \subseteq S + H \leq \mathcal{P}, \text{ ya que } SH \subseteq S,$$

concluimos que $S + I = S + H$. $\blacksquare$

Proposición 3.13 *La serie anuladora $\{S_t\}_{t\in J_d}$ de S induce a una serie central en $\mathcal{P} = S + I$.*

Demostración

Consideramos las siguiente serie:

$$\mathcal{P} = S + I = S + H = S_d + H \supseteq \cdots \supseteq S_t + H \supseteq \cdots \supseteq S_1 + H \supseteq I.$$

demostraremos que es una serie central en $\mathcal{P}$.

Por la Proposición 3.10 $S_t + H \trianglelefteq S + H$ implica que $S_t + H \trianglelefteq S_{t+1} + H$. Por la Proposición 1.27 $\{S_t + H\}_{t\in J_d}$ es una serie central si, y sólo si, $[S_t + H, S + I] \leq S_{t-1} + H$ Sean $a + b \in$

$S_t + H$, $b + I \in S + I$ con $a \in S_t$, $h \in H$ y $b \in S$.

$$\begin{aligned}
[a+h, b+I] &= (a+h)(b+I)(a+h)^{-1}(b+I)^{-1} \\
&= [(a+h)(b+I) - (b+1)(a+h)](a+h)^{-1}(b+I) + I \\
&= (ab - ba)(a+h)^{-1}(b-I)^{-1} + I \in S_{t-1} + I \\
&\subseteq S_{t-1} + H,
\end{aligned}$$

ya que $ab \in S_t.S \subseteq S_{t-1}$, $ba \in S.S_t \subseteq S_{t-1}$. ■

Observar que la serie anuladora de S y la serie central de $\mathcal{P} = S + I$ tiene la misma longitud. Recordemos que el grado de nilpotencia de G, es la mínima longitud de todas las series centrales, por tanto el número d es una cota superior para el grado de nilpotencia de G.

Capítulo 4

SERIE ANULADORA SUPERIOR DE S.

A partir de este capítulo la serie $\{S_t\}_{t\in J_d}$ denotará a la serie anuladora superior de S. Hemos llegado a uno de los objetivos principales, encontrar una serie de funciones $\{F_t\}_{t\in J_d}$ que caracterize a los ideales $\{S_t\}_{t\in J_d}$.

4.1 Función anuladora superior.

En esta sección se determina la función F_t en termino de F_{t-1}, a partir de la definición de función anuladora. Así se obtiene una expresión de la función anuladora superior en terminos de los invariantes del grupo G.

(1) *Sea* $F_t : J_5 \times J_5 \longrightarrow \mathbb{N}$ *una función recursiva definida como:*

$F_0(i,j) = 0$ *para todo* $(i,j) \in J_5 \times J_5$

para $t \geq 1$

$$F_t(i,j) = \min \left\{ \begin{array}{c} F_{t-1}(i,j)+1, F_{t-1}(i^-,j), F_{t-1}(i,j^-), F_{t-1}(i^+,j)+n_1-n_2, \\ F_{t-1}(i,j^+)+n_1-n_2, F_{t-1}(i+1,j), F_{t-1}(i-1,j)+1, \\ F_{t-1}(i,j-1), F_{t-1}(i,j+1)+1, F_d(i,j) \end{array} \right\}$$

Siempre que tenga sentido la expresión dentro de la llave significa que si no existe $F_{t-1}(i,j)$ *no se toma esta expresión. Además* $F_{t-1}(i^-,j)$, $F_{t-1}(i,j^-)$, $F_{t-1}(i^+,j)$, $F_{t-1}(i,j^+)$, *estan* *definidas para $F_t(i^+,j)$, $F_t(i,j^+)$, $F_t(i^-,j)$, $F_t(i,j^-)$ respectivamente, las últimas cuatro expresiones cumplen $i,\ j \in J_3$ o bien $i,\ j \in I_5$.*

Esta función caracteriza la serie anuladora superior pero por conveniencia se usará la siguiente función recursiva.

(2) *Sea δ_{ij} la delta de Kronecker. Sea t un número natural fijo. Sea $f_t : J_5 \times J_5 \longrightarrow \mathbb{N}$ una función definida por:*

$f_o(i,j) = 0$ para todo $(i,j) \in J_5 \times J_5$

para $t \geq 1$

$$f_t(i,j) = \min \left\{ \begin{array}{c} f_{t-1}(i+1,j) + \delta_{i3}(n_1 - n_2),\, f_{t-1}(\bar{i},j) + 1,\, \overline{f_{t-1}}(i,j-1), \\ f_{t-1}(i,5) + k(j),\, f_d(i,j) \end{array} \right\}$$

donde

$$\begin{aligned} \bar{i} &= 1 + 3\delta_{i5} \quad y \\ v(j) &= \begin{cases} n_1 - n_2 & si\ j \in J_3 \\ 1 & si\ j \in I_5 \end{cases} \end{aligned}$$

y $\overline{f_t} : J_5 \times J_5 \longrightarrow \mathbb{N}$ es una función con regla de correspondencia:

$$\overline{f_t}(i,j-1) = \begin{cases} f_t(i,j-1) & si\ j \neq 1 \\ f_t(i,3) + 1 & \text{si } j = 1 \end{cases}.$$

Demostraremos por inducción que **1)** y **2)** son equivalentes. Por definición $F_0(i,j) = 0 = f_0(i,j)$ para todo $(i,j) \in J_5 \times J_5$. Para $t = 1$

$$\begin{aligned} F_1(i,j) &= 0 \text{ para todo } (i,j) \neq (3,1) \text{ y } F_1(3,1) = 1 \\ f_1(i,j) &= 0 \text{ para todo } (i,j) \neq (3,1) \text{ y } f_1(3,1) = 1 \end{aligned}$$

supongamos que se cumple para $t-1$. Por demostrar que $F_t(i,j) = f_t(i,j)$ para todo $(i,j) \in J_5 \times J_5$. Si $f_t(i,j) = f_{t-1}(i+1,j) + \delta_{i3}(n_1 - n_2)$, hay dos casos que analizar.

1) Si $i \neq 3$

$$f_t(i,j) = f_{t-1}(i+1,j) = F_{t-1}(i+1,j) \geq F_t(i,j)$$

2) Si $i = 3$

$$f_t(3,j) = f_{t-1}(4,j) + n_1 - n_2 = F_{t-1}\left(i^+,j\right) + n_1 - n_2 \geq F_t(3,j),$$

Si $f_t(i,j) = f_{t-1}\left(\bar{i},j\right) + 1$ con $\bar{i} = 1 + 3\delta_{i5}$, tambien hay dos casos.

1) Cuando $i \neq 5$ se tiene

$$f_t(i,j) = f_{t-1}(i,j) + 1 \geq f_t(i,j) + 1 \geq f_{t-1}(i,j) + 1 = F_t(i,j) + 1 \geq F_t(i,j)$$

2) Si $i = 5$

$$f_t(5,j) = f_{t-1}(4,j) + 1 = F_t(4,j) + 1 \geq F_t(i,j)$$

Si $f_t(i,j) = \overline{f_{t-1}}(i,j-1)$ con $\overline{f_t}(i,j-1) = \begin{cases} f_t(i,j-1) & si\ j \neq 1 \\ f_t(i,3)+1 & \text{si } j = 1 \end{cases}$ tenemos dos casos

1) Si $j \neq 1$

$$f_t(i,j) = f_{t-1}(i,j) = F_{t-1}(i,j) > F_{t-1}(i,j) + 1 \geq F_t(i,j)$$

2) Si $j = 1$

$$f_t(i,1) = f_{t-1}(i,3) + 1 = F_{t-1}(i,3) + 1 \geq F_t\left(i,j^-\right) \geq F_t(i,3)$$

Finalmente si $f_t(i,j) = f_{t-1}(i,5) + v(j)$ donde $v(j) = \begin{cases} n_1 - n_2 & si\ j \in J_3 \\ 1 & si\ j \in I_5 \end{cases}$ $f_{t-1}(i,5) + v(j) = F_{t-1}(i,5) + v(j) \geq F_{t-1}(i,5) + n_1 - n_2 \geq F_t(i,j)$. Con este análisis concluimos que $f_t(i,j) \geq F_t(i,j)$ para todo $(i,j) \in J_5 \times J_5$.

La demostración de $f_t(i,j) \leq F_t(i,j)$ se sigue de que f_t cumple las propiedades de la definición 3.6 de función anuladora. ■

Lo anterior da origen a la siguiente definición

Definición 4.1 *La función $F_t : J_5 \times J_5 \longrightarrow \mathbb{N}$ definida en (1) y (2) la llamaremos función anuladora superior.*

En los capítulos anteriores se caracterizaron los ideales de S, más aun, los ideales de una serie anuladora de S. Los ideales $\left\{S_t = \left(a_{ij}^t\right)\right\}_{t\in J_d}$ de la serie anuladora superior estan más restringidos, ya que deben satisfacer $(S_t/S_{t-1}) = Ann\,(S/S_{t-1})$. El siguiente resultado caracteriza los ideales S_t

Proposición 4.2 *Sea* $\left\{S_t = \left(a_{ij}^t\right)\right\}_{t\in J_d}$ *la serie anuladora superior de* S, *tal que* $a_{ij}^t = p^{m_i - g_t(i,j)}\alpha_{ij}$ *con* $\alpha_{ij} \in \mathbf{Z}_{p^{m_i}}$, *entonces* $g_t = F_t$, *donde* F_t *es la función anuladora superior*

Demostración

La prueba es por inducción sobre t. Para $t = 0$. Se tiene que $S_0 = (p^{m_i}\alpha_{ij})$ entonces $g_t(i,j) = 0$

Supongamos que se cumple la proposición para $t-1$ Por demostrar que $g_t = F_t$ Primero probemos que F_t satisface las propiedades de función anuladora definidas en el capítulo anterior De la siguientes desigualdades

$$F_t(i,j) \leq F_{t-1}(\bar{i},j) + 1 \text{ y } F_t(i,j) \leq F_{t-1}(i+1,j)$$

se obtienen las propiedades (2.1), $(2.2.a)$ y $(2.2.b)$

$$\begin{aligned}
F_t(i,j) &\leq F_{t-1}(i,j) + 1 \\
F_t(i^+,j) &\leq F_{t-1}(i^-,j) \\
F_t(i,j^+) &\leq F_{t-1}(i,j^-)
\end{aligned}$$

como F_t cumple:

$$F_t(3,j) \leq F_{t-1}(4,j) + n_1 - n_2 \text{ y } F_t(i,j) \leq F_{t-1}(i+1,j)$$

tenemos las condiciones $(2.3.a)$ y $(2.33\,b)$

$$\begin{aligned}
F_t(i^-,j) &\leq F_{t-1}(i^+,j) \\
F_t(i,j^-) &\leq F_{t-1}(i,j^+),
\end{aligned}$$

a partir de

$$F_t(i,j) \leq F_{t-1}(i+1,j) \text{ si } i \neq 3, F_t(i,j) \leq F_{t-1}(i,j),$$

se siguen las condiciones (2.4.a) y (2.4.b)

$$\begin{aligned} F_t(i-1,j) &\leq F_{t-1}(i,j) \text{ si } i \neq 4 \\ F_t(i+1,j) &\leq F_{t-1}(i,j)+1, \end{aligned}$$

las propiedades (2.5.a) y (2.5.b) son consecuencia de

$$F_t(i,j) \leq F_{t-1}(i,j-1) \ y \ F_t(4,j) \leq F_{t-1}(i,5)+1.$$

Por último se demuestra la propiedad (2.6)

$$F_{t-1}(i,j) \leq F_t(i,j) \leq F_d(i,j),$$

la segunda desigualdad se sigue directamente de la definición de S. Si $F_t(i,j) = F_{t-1}(i+1,j) + \delta_{i3}(n_1-n_2)$ entonces $F_t(i,j) \geq F_{t-1}(i,j)$ por (2.4). Si $F_t(i,j) = F_{t-1}(\bar{i},j)$ tenemos que $F_t(i,j) \geq F_{t-1}(i,j)$ por (2.3.a) y (2.2.a). Si $F_t(i,j) = F_{t-1}(i,j-1)$ entonces $F_t(i,j) \geq F_{t-1}(i,j)$. Finalmente si $F_t(i,j) = F_{t-1}(i,5)+v(j)$ se tiene que $F_t(i,j) \geq F_{t-1}(i,j)$. Por tanto $F_{t-1}(i,j) \leq F_t(i,j)$. Sea R^{F_t} el ideal asociado a la función F_t, Así

$$\frac{R^{F_t}}{S_{t-1}} \subseteq Ann\left(\frac{S}{S_{t-1}}\right) = \frac{S_t}{S_{t-1}},$$

entonces $R^{F_t} \subset S_t$, así $F_t \leq g_t$. Como g_t es una función asociada al t-ésimo anulador S_t entonces g_t cumple las condiciones de función anuladora, esto implica que $g_t \leq F_t$, con lo cual terminamos la prueba. ∎

A continuación se define la función $\lfloor\,\rfloor$ mayor entero con una pequeña variante, para los enteros *positivos*, y se obtiene una expresión de la función anuladora superior F_t, analizando los casos cuando $n_1 - n_2 = 1$ y $n_1 - n_2 > 1$.

Definición 4.3 *Sea* $x \in \mathbb{R}$, *tal que* $n \leq x < n+1$. *Sea* $\lfloor\,\rfloor : \mathbb{R} \longrightarrow \mathbb{Z}^+$ *una función definida como:*

$$\lfloor x \rfloor = \begin{cases} n & si\ x > 0 \\ 0 & si\ x \leq 0 \end{cases}$$

Recordemos que $m_1 = m_2 = m_3 = n_1$ y $m_4 = m_5 = n_2$

Definición 4.4 *Sea $d : J_5 \times J_5 \longrightarrow \mathbf{N}$ una función definida como:*

$$d(i,j) = \begin{cases} n_2 & si\ i \in J_3 \text{ y } j \in I_5 \\ m_i & si\ i > j \\ m_i - 1 & si\ i \leq j \text{ y } (i \in I_5 \text{ o } j \in J_3) \end{cases}$$

Como $d(i,j) = F_d(i,j)$ para todo $(i,j) \in J_5 \times J_5$ y recordando como definimos e_{ij}, se tiene que $p^{m_i - d(i,j)} = e_{ij}$, por tanto $A = (a_{ij}) \in S$ si, y sólo si, $a_{ij} = p^{m_i - d(i,j)}\alpha_{ij}$ con $\alpha_{ij} \in \mathbf{Z}_{p^{m_i}}$.

Definición 4.5 *Sean $g, h : J_5 \times J_5 \times J_d \longrightarrow \mathbf{N}$ las siguientes funciones:*

$$\begin{aligned} g(i,j,t) &= \min\left\{\left\lceil\frac{t + i - j + (-1)^{k+1}(k+1)}{5}\right\rceil, d(i,j)\right\} \\ h(i,j,t) &= \min\left\{\left\lceil\frac{t + i - j - 5(k-1)}{3}\right\rceil, d(i,j)\right\} \end{aligned}$$

donde $k : J_5 \longrightarrow \{1,2\}$ esta dada por

$$k = k(i) = \begin{cases} 1 & si\ i \in J_3 \\ 2 & si\ i \in I_5 \end{cases}$$

Teorema 4.6 *Sea $\left\{S_t = \left(p^{m_i - F(i,j,t)}\alpha_{ij}\right)\right\}_{t \in J_d}$ la serie anuladora superior de S.*

(i) *Si $n_1 - n_2 = 1$ entonces $F = g$.*

(ii) *Si $n_1 - n_2 > 1$ entonces $F = h$*

Demostración

(i) La prueba es por inducción sobre t. Para $t = 0$

$$g(i,j,0) = \left\lceil\frac{i - j + (-1)^{k+1}(k+1)}{5}\right\rceil,$$

si $i \in J_3$

$$g(i,j,0) = \left\lceil \frac{i-j+2}{5} \right\rceil = 0, \text{ ya que } i-j<3,$$

si $i \in I_5$

$$g(i,j,0) = \left\lceil \frac{i-j}{5} \right\rceil = 0, \text{ porque } i-j<5.$$

Así $g(i,j,0) = 0$, entonces $F(i,j,0) = g(i,j,0)$ para todo $(i,j) \in J_5 \times J_5$.

Supongamos que se cumple para $t-1$, es decir, $F(i,j,t-1) = g(i,j,t-1)$para *todo* $(i,j) \in J_5 \times J_5$. Probemos que $F(i,j,t) = g(i,j,t)$, analizando los casos $i \in J_3$ y $i \in I_5$.

1^{er}caso. Si $i \in J_3$.

Por *definición* la función anuladora superior y por la Proposición 4.2 se tienen que:

$$F(i,j,t) = \min\left\{ \left\lceil \frac{t+i-j+2}{5} \right\rceil + \delta_{i3}, \left\lceil \frac{t-j+2}{5} \right\rceil + 1, \overline{F}(i,j-1,t-1), \left\lceil \frac{t+i-4}{5} \right\rceil + 1, F(i,j,d) \right\}$$

$$\textit{con} \qquad \overline{F}(i,j-1,t-1) = \begin{cases} \left\lceil \dfrac{t+i-j+2}{5} \right\rceil & si\ j \neq 1 \\ \left\lceil \dfrac{t+i+3}{5} \right\rceil & si\ j = 1 \end{cases}.$$

Si $j \neq 1$, entonces $F(i,j,t) = F(i,j-1,t-1)$, ya que,

$$F(i,j-1,t-1) = \left\lceil \frac{t+i-j+2}{5} \right\rceil \leq \left\lceil \frac{t+i+1}{5} \right\rceil = \left\lceil \frac{t+i-4}{5} \right\rceil + 1.$$

Si $j=1$, entonces $F(i,1,t) = \left\lceil \frac{t+i+1}{5} \right\rceil$, porque:

$$\left\lceil \frac{t+i+1}{5} \right\rceil < \left\lceil \frac{t+6}{5} \right\rceil = \left\lceil \frac{t-j+2}{5} \right\rceil + 1,$$

como

$$\overline{F}(i,j-1,t-1) = \left\lceil \frac{t+i+3}{5} \right\rceil \geq \left\lceil \frac{t+i+1}{5} \right\rceil$$

además $g(i,j,t) = \left\lceil \frac{t+i-j+2}{5} \right\rceil$ para todo $(i,j) \in J_3 \times J_5$. Entonces $g(i,j,t) = F(i,j,t)$ para todo $i \in J_3$.

2^{do}caso. *si* $i \in I_5$.

Tenemos que:

$$F(i,j,t)=\min\left\{\left\lceil\frac{t+\overline{i+1}-j-4}{5}\right\rceil,\left\lceil\frac{t+\bar{i}-j+4}{5}\right\rceil+1,\overline{F}(i,j-1,t-1),\left\lceil\frac{t+i-1}{5}\right\rceil+1,F(i,j,d)\right\}$$

$$con \qquad \overline{F}(i,j-1,t-1)=\begin{cases}\left\lceil\frac{t+i-j-3}{5}\right\rceil & si\ j\neq 1\\ \left\lceil\frac{t+i-7}{5}\right\rceil+1 & si\ j=1\end{cases} \quad y\ \bar{i}=1+\delta_{i5}$$

Si $i=4$, entonces $F(4,j,t)=\left\lceil\frac{t-j+1}{5}\right\rceil$, ya que:

$$\begin{aligned}\left\lceil\frac{t+\overline{i+1}-j-4}{5}\right\rceil &= \left\lceil\frac{t-j+1}{5}\right\rceil\leq\left\lceil\frac{t-j+2}{5}\right\rceil=\left\lceil\frac{t-j-3}{5}\right\rceil+1=\left\lceil\frac{t+\bar{i}-j+4}{5}\right\rceil+1\\ \left\lceil\frac{t-j+1}{5}\right\rceil &\leq \left\lceil\frac{t-j+1}{5}\right\rceil\leq\overline{F}(4,j-1,t-1),\ \text{por último}\\ \left\lceil\frac{t-j+1}{5}\right\rceil &\leq \left\lceil\frac{t+2}{5}\right\rceil=\left\lceil\frac{t+i-1}{5}\right\rceil+1.\end{aligned}$$

Si $i=5$, de manera similar se concluye $F(5,j,t)=\left\lceil\frac{t-j+2}{5}\right\rceil$. Por consiguiente $F(i,j,t)=\left\lceil\frac{t+i-j-3}{5}\right\rceil$ para todo $(i,j)\in I_5\times J_5$. Por lo tanto $f=g$.

(ii) La prueba es por inducción sobre t.

$t=0$

$$h(i,j,0)=\left\lceil\frac{i-j-5(k-1)}{5}\right\rceil=0 \text{ para todo } (i,j)\in J_5\times J_5,$$

por tanto $F(i,j,0)=h(i,j,0)$, para todo $(i,j)\in J_5\times J_5$.

Supongamos que $F(i,j,t-1)=h(i,j,t-1)$ para todo $(i,j)\in J_5\times J_5$. Se prueba que $F(i,j,t)=h(i,j,t)$. De manera similar como se realizó la demostración de (i), se analizan los casos $i\in J_3$ y $i\in I_5$

1er caso Si $i\in J_3$.

Por definición de función anuladora superior

$$F(i,j,t)=\min\left\{\left\lceil\frac{t+i-j}{3}\right\rceil+\delta_{i3}(n_1-n_2),\left\lceil\frac{t-j}{3}\right\rceil+1,\overline{F}(i,j-1,t-1),\left\lceil\frac{t+i-6}{3}\right\rceil+h(j)\right\}$$

$$\text{con} \qquad \overline{F}(i,j-1,t-1) = \begin{cases} \left\lceil \dfrac{t+i-j}{3} \right\rceil & si\ j \neq 1 \\ \left\lceil \dfrac{t+i-4}{3} \right\rceil + 1 & si\ j = 1 \end{cases}$$

$$h(j) = \begin{cases} n_1 - n_2 & si\ j \in J_3 \\ 1 & si\ j \in I_5 \end{cases}$$

Si $j \neq 1$, entonces $F(i,j,t) = \left\lceil \dfrac{t+i-j}{3} \right\rceil$. Si $j = 1$, se demuestra de manera similar a la primera parte que $F(i,j,t) = \left\lceil \dfrac{t+i-1}{3} \right\rceil$.

2^{da}caso. Si $i \in I_5$.

Analizando cuando $i = 4$ y $i = 5$. Tenemos que $F(i,j,t) = \left\lceil \dfrac{t+i-j-5}{3} \right\rceil$, para todo $(i,j) \in I_5 \times J_5$. Concluimos que $F = g$. ■

4.2 Longitud de la serie anuladora superior.

En la sección anterior se obtienen dos expresiones de la función anuladora superior, es esta última parte del capítulo, se calcula las respectivas longitudes de las funciones, y se demuestra que estas son las longitudes de la serie anuladora superior, para los casos: $n_1 - n_2 = 1$ y $n_1 - n_2 > 1$.

Proposición 4.7 *Sea* $\left\{S_t = \left(p^{m_i - F(i,j,t)}\alpha_{ij}\right)\right\}_{t \in J_d}$ *la serie anuladora superior de* S

(i) *Si* $n_1 - n_2 = 1$, *entonces la longitud de la serie anuladora superior es* $d = 5n_1 - 3$.

(ii) *Si* $n_1 - n_2 > 1$, *entonces la longitud de la serie anuladora superior es* $d = 3n_1 - 1$.

Demostración

(i) Primero se prueba que $S_{5n_1-3} = S$.

Sea $A = (a_{ij}) \in S$, con $a_{ij} = p^{m_i - d(i,j)}\alpha_{ij}$, entonces $A = (a_{ij}) \in S_{5n_1-3}$ si, y sólo si, $a_{ij} = p^{m_i - F(i,j,5n_1-3)}\alpha_{ij}$. Ahora se demuestra que $d(i,j) = F(i,j,5n_1-3)$ para todo $(i,j) \in J_5 \times J_5$. Teniendo en cuenta que

$$F(i,j,5n_1-3) = \min\left\{ \left\lceil \frac{5n_1 - 3 + i - j + (-1)^{k+1}(k+1)}{5} \right\rceil, d(i,j) \right\},$$

por tanto demostrar la igualdad, es probar que.

$$d(i,j) \leq \left\lceil \frac{5n_1 - 3 + i - j + (-1)^{k+1}(k+1)}{5} \right\rceil$$

1er caso. Si $i > j$.

Si $i \in J_3$, entonces

$$d(i,j) = n_1 \leq \left\lceil \frac{5n_1 + i - j - 1}{5} \right\rceil = \left\lceil \frac{5n_1 - 3 + i - j + (-1)^{k+1}(k+1)}{5} \right\rceil.$$

Si $i \in I_5$, tenemos

$$d(i,j) = n_2 \leq \left\lceil \frac{5n_1 + i - j - 6}{5} \right\rceil = \left\lceil \frac{5n_2 + i - j - 1}{5} \right\rceil = \left\lceil \frac{5n_1 - 3 + i - j + (-1)^{k+1}(k+1)}{5} \right\rceil$$

2docaso. Si $i \in J_3$, $j \in I_5$.

Tenemos que $-4 \leq i - j \leq -1$ implica que $5n_2 - 5 \leq 5n_1 - 5 \leq 5n_1 + i - j - 1 \leq 5n_1 - 2$, así $n_2 = n_1 - 1 < \frac{5n_1+i-j-1}{5}$, por tanto

$$d(i,j) = n_2 \leq \left\lceil \frac{5n_1 + i - j - 1}{5} \right\rceil = \left\lceil \frac{t + i - j + (-1)^{k+1}(k+1)}{5} \right\rceil$$

3er caso. Si $i \leq j$ y $(i \in I_5$ o $j \in J_3)$.

Notar que si $i \in I_5$, entonces $j \in I_5$. Si $j \in J_3$, así $i \in J_3$. Por tanto si $i \leq j$ y $i, j \in J_3$, se tiene que: $2 \leq i - j \leq 0$, se sigue $5n_1 - 5 \leq 5n_1 - 3 \leq 5n_1 + i - j - 1$, así

$$d(i,j) = n_1 - 1 \leq \left\lceil \frac{5n_1 + i - j - 1}{5} \right\rceil$$

Si $i \leq j$ y $i, j \in I_5$, tenemos que $1 \leq i - j \leq 0$, implica que $5m_i - 5 \leq 5n_1 + i - j - 6$,

$$d(i,j) = n_2 - 1 \leq \left\lceil \frac{5n_1 + i - j - 6}{5} \right\rceil$$

se concluye que $F(i,j,5n_1 - 3) = d(i,j)$ para todo $(i,j) \in J_5 \times J_5$.

Finalmente veamos que $S_{5n_1-4} \subsetneq S$ Sea $A = (a_{ij}) \in S$ tal que $a_{ij} = \begin{cases} 1 & si \ (i,j) - (3,2) \\ 0 & en\ otro\ caso. \end{cases}$

Se afirma que $A \notin S_{5n_1-4}$, en efecto si $A \in S_{5n_1-4}$, entonces $1 = p^{n_1-F(3,2,5n_1-4)}\alpha_{32}$ con $\alpha_{32} \in \mathbb{Z}_{p^{n_1}}$. Como

$$F(3,2,5n_1-4) = \min\left\{\left\lceil\frac{5n_1-1}{5}\right\rceil, n_1\right\} = \{n_1-1, n_1\} = n_1-1,$$

por tanto $1 = p\alpha_{32}$, lo cual es imposible.

(ii) Demostraremos que $S_{3n_1-1} = S$.

Sea $A = (a_{ij}) \in S$, con $a_{ij} = p^{m_i-d(i,j)}\alpha_{ij}$, por demostrar $d(i,j) = F(i,j,3n_1-1)$ para todo $(i,j) \in J_5 \times J_5$.

1ercaso. Si $i > j$.

$$F(i,j,3n_1-1) = \min\left\{\left\lceil\frac{3n_1-1+i-j-5(k-1)}{3}\right\rceil, d(i,j)\right\}.$$

Si $i \in J_3$, entonces

$$d(i,j) = n_1 \leq \left\lceil\frac{3n_1-1+i-j}{3}\right\rceil.$$

Si $i \in I_5$, tenemos

$$d(i,j) = n_2 \leq \left\lceil\frac{3n_1+i-j-6}{3}\right\rceil,$$

ya que, $3n_2 < 3n_2+i-j \leq 3(n_2+2)+i-j-6 \leq 3n_1+i-j-6$. Concluimos que $F(i,j,3n_1-1) = m_i = d(i,j)$.

2docaso. Si $i \in J_3$, $j \in I_5$.

$$F(i,j,3n_1-1) = \min\left\{\left\lceil\frac{3n_1+i-j-6}{3}\right\rceil, d(i,j)\right\} = n_2 = d(i,j),\text{ se sigue del caso anterior.}$$

3ercaso. Si $i \leq j$ y $(i \in I_5$ o $j \in j_3)$.

Notemos que si $j \in J_3$, entonces $F(i,j,3n_1-1) = n_1-1$. Si $i \in I_5$, se sigue que $F(i,j,3n_1-1) = n_2-1$. Por tanto $F(i,j,3n_1.1) = m_i-1 = d(i.j)$. Así $F(i,j,3n_1.1) = d(i,j)$ para todo $(i,j) \in J_5 \times J_5$.

Por último vemos que $S_{3n_1-2} \subsetneq S$. Sea $A = (a_{ij}) \in S$ tal que $a_{ij} = \begin{cases} 1 & \text{si } (i,j) = (3,2) \\ 0 & \text{en otro caso.} \end{cases}$

Se afirma que $A \notin S_{3n_1-1}$, en caso contrario, $A \in S_{5n_1-4}$ entonces $1 \equiv 0 \bmod \left(p^{n_1-f(3,2,3n_1-2)}\right)$, es decir, $1 = p^{n_1 - f(3,2,3n_1-1)}\alpha_{32}$ con $\alpha_{32} \in \mathbf{Z}_{p^{n_1}}$. Como

$$f(3,2,3n_1-1) = \min\left\{\left[\frac{5n_1-1}{5}\right], n_1\right\} = \{n_1-1, n_1\} = n_1 - 1,$$

por tanto $1 = p\alpha_{32}$, lo cual es imposible. ■

Capítulo 5

SERIE CENTRAL SUPERIOR DE $S+I$.

5.1 Caracterización del centro de $S+H$.

En este subcapítulo se describe al conjunto $H = \mathcal{P} \cap Z\,(EndG)$, y consecuentemente son determinandos los elementos de $S+H$.

Lema 5.1 $Z(EndG) = \{\gamma I \ \mid \gamma \in \mathbb{Z}_{p^{n_1}},\ I$ es la identidad de $AutG.\}$.

Demostración

Recordar que $Z\,(EndG) = \{A \in EndG \mid AB = BA$ para todo $B \in EndG\}$. Se tiene que $\gamma I \in Z\,(EndG)$, ya que $(\gamma I)\,B = \gamma\,(IB) = \gamma B = B\gamma = B\,(\gamma I)$, para todo $B \in EndG$.

Sean $A = (a_{ij}) \in Z\,(EndG)$ y $B = (b_{ij}) \in EndG$. Entonces

$$(ab)_{ij} = \sum_{k=1}^{5} a_{ik} b_{kj} \equiv \sum_{i=1}^{5} b_{ik} a_{kj} = (ba)_{ij} \mod (p^{m_i}) \qquad (1)$$

como esta igualdad se cumple para todo $B \in EndG$, tomando a B como las matrices triangular superior y triangular inferior de $EndG$, siguientes

$$\begin{pmatrix} 1 & 1 & 1 & p^{n_1-n_2} & p^{n_1-n_2} \\ \overline{0} & 1 & 1 & p^{n_1-n_2} & p^{n_1-n_2} \\ \overline{0} & \overline{0} & 1 & p^{n_1-n_2} & p^{n_1-n_2} \\ \overline{0} & \overline{0} & \overline{0} & 1 & 1 \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & 1 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 1 & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ 1 & 1 & \overline{0} & \overline{0} & \overline{0} \\ 1 & 1 & 1 & \overline{0} & \overline{0} \\ 1 & 1 & 1 & 1 & \overline{0} \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

si B es la primera matriz se tiene las siguientes congruencias:

$$(ab)_{54} = a_{41} + a_{51} \equiv a_{41} \operatorname{mod}(p^{n_2}), \text{ entonces } a_{51} \equiv 0 \operatorname{mod}(p^{n_2}), \text{ así } a_{51} = \overline{0}$$

Analizando todas las congruencias, se caracteriza la parte inferior de la matriz A. Tomando a la segunda matriz como B, se determina la parte superior de A. De esta manera $A \in EndG$ si, y sólo si,

$$A = \begin{pmatrix} \overline{a_{11}} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{0} & \overline{a_{11}} & \overline{0} & \overline{0} & \overline{0} \\ \overline{0} & \overline{0} & \overline{a_{11}} & \overline{0} & \overline{0} \\ \overline{0} & \overline{0} & \overline{0} & \overline{a_{11}} & \overline{0} \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{a_{11}} \end{pmatrix} \in \{\gamma I \mid \gamma \in \mathbf{Z}_{p^{n_1}},\ I \text{ es la identidad de } AutG\} \blacksquare$$

Lema 5.2 $H = \{pM + I \mid M \in Z(EndG)\}$.

Demostración

Por el Lema anterior

$$H = \mathcal{P} \cap Z(EndG) = pZ(EndG) + I = \{pM + I \mid M \in Z(EndG)\} \blacksquare$$

Se tiene que

$$S + H = \{A + pM + I \mid A \in S \text{ y } M \in Z(EndG)\} = \{A + p\gamma I + I \mid A \in S \text{ y } \gamma \in \mathbb{Z}_{p^{n_1}}\}$$

A continuación se determinan los elementos del centro de $S+H$ en el siguiente resultado.

Proposición 5.3 $Z(S+H)=\{A'+pM+I \mid A'\in S_1=Ann(S),\ M\in EndG\}$

Demostración

Por definición $Z(S+H)=\{\overline{A}\in S+H \mid \overline{AB}=\overline{BA} \text{ para todo } \overline{B}\in S+H\}$

Sea $\overline{A}\in Z(S+H)$. entonces $\overline{A}$ es de la forma $\overline{A}=A+pM+I=A+p\gamma_1 I+I$ con $A\in S$ y $\gamma_1\in \mathbb{Z}_{p^{n_1}}$. Por tanto:

$$\overline{AB}=(A+p\gamma_1 I+I)(B+p\gamma_2 I+I)=(B+p\gamma_2 I+I)(A+p\gamma_1+I)=\overline{BA} \qquad (1)$$

se sigue:

$$(A+p\gamma_1 I)(B+p\gamma_2 I)=(B+p\gamma_2 I)(A+p\gamma_1 I) \qquad (2)$$

para todo $B\in S$, para todo $\gamma_2\in \mathbb{Z}_{p^{n_1}}$. Entonces $\overline{A}\in Z(S+H)$ si y sólo si $A+p\gamma_1 I\in Z(S+p\gamma_1 I)$. De esta manera se caracteriza los elementos de $Z(S+p\gamma_1 I)$, como

$$A+p\gamma_1 I=\begin{pmatrix} pa'_{11} & pa_{12} & pa_{13} & p^{n_1-n_2}a_{14} & p^{n_1-n_2}a_{15} \\ a_{21} & pa'_{22} & pa_{23} & p^{n_1-n_2}a_{24} & p^{n_1-n_2}a_{25} \\ a_{31} & a_{32} & pa'_{33} & p^{n_1-n_2}a_{34} & p^{n_1-n_2}a_{35} \\ a_{41} & a_{42} & a_{43} & pa'_{44} & pa_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & pa'_{55} \end{pmatrix} \text{ donde } a'_{ii}=a_{ii}+\gamma_1,$$

o bien, se puede escribir $A+p\gamma_1 I=(a_{ij})$ con $a_{ij}=e_{ij}\alpha_{ij}$ si $i\neq j$ y $a_{ii}=e_{ii}\alpha_{ii}+p\gamma_1$. Tomando

$$B+p\gamma_2 I=(b_{ij})=\begin{pmatrix} p & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ 1 & p & \overline{0} & \overline{0} & \overline{0} \\ 1 & 1 & p & \overline{0} & \overline{0} \\ 1 & 1 & 1 & p & \overline{0} \\ 1 & 1 & 1 & 1 & p \end{pmatrix},$$

realizando las operaciones de la igualdad (2).

$$(ab)_{ij} \cong (ba)_{ij} \operatorname{mod}(p^{m_i})$$

en la entrada (1,4) se tiene que $p^{n_1-n_2}a_{15} \cong 0 \operatorname{mod}(p^{n_1})$, así $a_{15} = p^{n_2}\beta_{15}$ Analizando todas las entradas, se tiene la parte superior de dicha matriz.

Si

$$B + p\gamma_2 I = (b_{ij}) = \begin{pmatrix} p & p & p & p^{n_1-n_2} & p^{n_1-n_2} \\ \bar{0} & p & p & p^{n_1-n_2} & p^{n_1-n_2} \\ \bar{0} & \bar{0} & p & p^{n_1-n_2} & p^{n_1-n_2} \\ \bar{0} & \bar{0} & \bar{0} & p & p \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} & p \end{pmatrix}$$

se obtiene la parte inferior de $A + p\gamma_2 I$. Así :

$$A + p\gamma_1 I = \begin{pmatrix} pa_{11} & \bar{0} & \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & pa_{22} & \bar{0} & \bar{0} & \bar{0} \\ p^{n_1-1}a_{31} & \bar{0} & pa_{33} & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & pa_{44} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} & pa_{55} \end{pmatrix} \text{ con } pa_{ii} \cong pa_{jj} \operatorname{mod}(p^{m_i}),$$

entonces:

$$\begin{aligned} \hat{A} &= (A + p\gamma_1) + (pa_{11}I - pa_{11}I) + I \\ &= \begin{pmatrix} 0 & \bar{0} & \bar{0} & \bar{0} & \bar{0} \\ 0 & pa_{22} - pa_{11} & \bar{0} & \bar{0} & \bar{0} \\ p^{n_1-1}a_{31} & \bar{0} & pa_{33} - pa_{11} & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & pa_{44} - pa_{11} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} & pa_{55} - pa_{11} \end{pmatrix} + pa_{11}I + I_5, \end{aligned}$$

como $pa_{ii} \equiv pa_{jj} \operatorname{mod}(p^{m_i})$, así esta matriz pertenece a $Ann(S) = S_1$, por tanto $Z(S+H) \subseteq \{A + p\gamma I + I \mid A \in S \text{ y } \gamma \in \mathbf{Z}_{p^{n_1}}\}$.

Veamos que cualquier elemento de $\{A' + pM + I \mid A' \in S_1 = Ann(S),\ M \in EndG\}$ pertenece a $Z(S+H)$, Sean $A'+p\alpha I+I$ un elemento de este conjunto y $B+p\gamma+I$ un elemento arbitrario de $S+H$ con $B\in S$. Así:

$$\begin{aligned}(A'+p\alpha I+I)(B+p\gamma I+I) &= A'B+A'p\gamma I+A'+p\alpha IB+p\alpha Ip\gamma I+p\alpha I+B+p\gamma I\\ &= BA'+Bp\gamma IA'+A'+Bp\alpha I+p\gamma Ip\alpha I+B+P\gamma I+I\\ &= (B+p\gamma I+I)(A'+p\alpha I+I).\end{aligned}$$

es lo que se queria demostrar. ■

5.2 Serie central superior de $S+I$.

Sea $\{Z_t\}_{t\geq 1}$ la serie central superior de $S+I=\mathcal{P}$. En la sección 3.3 se demostró que si $\{S_t\}$ es una serie anuladora de S, entonces $\{S_t+H\}_{t\in J_d}$ es una serie central de S en esta sección se concluye que si S_t es el t-ésimo anulador superior de S, entonces $Z_t=S_t+H$ es la t-ésima serie central superior de $S+I=\mathcal{P}$, probaremos el siguente resultado que se necesita para esta proposición.

Lema 5.4 *Sea $A\in S$. Entonces $A+I\in S_t+H$ si y sólo si. $A-a_{11}I\in S_t$.*

Demostración

Supongamos que $A+I\in S_t+H$. Como $H=\{p\gamma I+I \mid \gamma\in\mathbb{Z}_{p^{n_1}}\}$, se tiene que $A+I=B+p\gamma I$ con $B\in S_t$, así $A=B+p\gamma I$. Sea $A=(a_{ij})$ y $B=(a_{ij})$, entonces $a_{ij}=b_{ij}$ si $i\neq j$ y $a_{ii}=b_{ii}+p\gamma$. Sea $A-a_{11}I=(c_{ij})$, por tanto $c_{ij}=a_{ij}=b_{ij}$ si $i\neq j$ y $c_{ii}=a_{ii}-a_{11}=b_{ij}+p\gamma-a_{11}$, sabemos que $a_{11}\equiv o \bmod (p^{n_1-F(1,1,t)})$. Como $n_1-F(1,1,t)\geq n_i-F(i,i,t)$, por tanto $p^{n_1-F(1,1,t)}\geq p^{n_1-F(i,i,t)}$, así $c_{ij}=a_{ii}-a_{11}\equiv 0 \bmod (p^{n_i-F(i,i,t)})$, es decir, $A-a_{11}I\in S_t$.

Inversamente Supongamos que $A-a_{11}I\in S_t$, sea $A'=A-a_{11}I$, así $A=A'+a_{11}I$, entonces $A+I=A'+a_{11}I+I\in S_t+H$, ya que $a_{11}=pa'_{11}$. ■

Proposición 5.5 *Sea $\{Z_t\}_{t\geq 1}$ la serie central superior de $\mathcal{P}=S+I$, entonces $\{Z_t=S_t+H\}_{t\in J_d}$, donde $\{S_t\}$ es la serie anuladora superior de S.*

Demostración

Como $\{Z_t\}_{t\geq 1}$ es la serie central superior de $\mathcal{P}$, se tiene que $S_t + H \leq Z_t$. La prueba de esta desigualdad $Z_t \leq S_t + H$, es por inducción sobre t.

Para $t = 1$

$$Z_1 = Z(S+H) = \{A + H \mid A \in S_1\},$$

esta igualdad se sigue del Lema 5.2 y la Proposición 5.3. Por lo tanto $Z_1 \leq S_1 + H$.

Supongamos que para $t-1$, $Z_{t-1} \leq S_{t-1} + H$. Por demostrar que $Z_t \leq S_t + H$. Como $\{Z_t\}_{t\geq 1}$ es una serie central implica $[Z_t, \mathcal{P}] \leq Z_{t-1}$ (Proposición 1.26). Sea $A + I \in Z_t$, entonces para todo $B + I \in \mathcal{P}$.

$$[A + I, B + I] \in Z_{t-1} \leq S_{t-1} + H$$

$$\begin{aligned}
(A+I)(B+I)(A+I)^{-1}(B+I)^{-1} &= C + I \in S_{t-1} + H, \\
(A+I)(B+I) &= (C+I)(B+I)(A+I) \\
AB + A + B + I &= C(B+I)(A+I) + BA + B + A + I \\
AB - BA &= C(B+I)(A+I) \text{ para todo } B + I \subset \mathcal{P},
\end{aligned}$$

entonces $C + I \in S_{t-1} + H$ si, y sólo si, $C - c_{11}I \in S_{t-1}$ (Lema 5.4), es decir, $C \equiv c_{11}I \bmod (S_{t-1})$. Así

$$AB - BA \equiv c_{11}I(B+I)(A+I) \bmod (S_{t-1}) \text{ para todo } B \in S$$

Sea r un número fijo que pertenece a J_5. Sea $B = (b_{ij})$ tal que $b_{ij} = \begin{cases} e_{r2} & si\ (i,j) = (r,2) \\ \overline{0} & \text{en otro caso.} \end{cases}$,

donde e_{ij} cumple la Definición 2.10. Sean $A + I = \left(a'_{ij}\right)$ y $B + I = \left(b'_{ij}\right)$, con

$$\begin{aligned}
a'_{ij} &= \begin{cases} a_{ij} & si\ i \neq j \\ a_{ij} + 1 & si\ i = j \end{cases} \\
b'_{ij} &= \begin{cases} b_{ij} & si\ i \neq j \\ b_{ij} + 1 & si\ i = j \end{cases}
\end{aligned}$$

así hay cinco matrices diferentes para B, que cumplen :

$$(ab)_{ij} - (ba)_{ij} \equiv c_{11} I \left(a'b'\right)_{ij} \mod \left(p^{m_i - F(i,j,t-1)}\right) \qquad (1)$$

donde:

$$\begin{aligned}
(ab)_{ij} &= \begin{cases} \bar{0} & si \ (i,j) \neq (i,2) \\ e_{r2}a_{ir} & si \ (i,j) = (i,2) \end{cases} \\
(ba)_{ij} &= \begin{cases} \bar{0} & si \ (i,j) \neq (r,j) \\ e_{r2}a_{2j} & si \ (i,j) = (r,j) \end{cases} \\
\left(a'b'\right)_{ij} &= \begin{cases} a_{ij} & si \ (i,j) \neq (r,j) \\ a_{ij} + e_{r2}a_{2j} & si \ (i,j) = (r,j) \end{cases}
\end{aligned}$$

por lo tanto

$$\begin{aligned}
(ab)_{ij} &= \delta_{2j} e_{r2} a_{ir} \\
(ba)_{ij} &= \delta_{ri} e_{r2} a_{2j} \\
\left(a'b'\right)_{ij} &= a_{ij} + \delta_{ri} e_{r2} a_{2j}
\end{aligned}$$

Así la igualdad (1) se transforma en:

$$\delta_{2j} e_{r2} a_{ir} - \delta_{ri} e_{r2} a_{2j} \equiv c_{11} \left(a_{ij} + \delta_{ri} e_{r2} a_{2j}\right) \mod \left(p^{m_i - F(i,j,t-1)}\right)$$

si $i \neq r$ y $j = 2$

$$e_{r2} a_{ir} \equiv c_{11} a_{i2} \mod \left(p^{m_i - F(i,2,t-1)}\right) \qquad (2)$$

Por demostrar que $a_{ij} \equiv 0 \mod \left(p^{m_i - F(i,j,t)}\right)$. Como la función F depende de los invariantes de G, la demostración es por casos.

1ercaso. Si $n_1 = n_2 + 1$ entonces

$$F(i,j,t) = \min \left\{ \left\lceil \frac{t + i - j + (-1)^{k+1}(k+1)}{5} \right\rceil, d(i,j) \right\},$$

si $t < d$, entonces:

$$F(i,j,t) = \left[\frac{t+i-j+(-1)^{k+1}(k+1)}{5}\right]$$

así

$$e_{i2}a_{n} \equiv e_{11}a_{i2} \mod \left(p^{m_i - \left[\frac{t+i-3+(-1)^{k+1}(k+1)}{5}\right]}\right)$$

sabemos que

$$e_{11} \equiv 0 \mod \left(p^{n_1 - F(1,1,t-1)}\right)$$

Se afirma que $p^{m_i - F(i,2,t-1)} \leq p^{n_1 - F(1,1,t-1)}$, en efecto, si $k = 1$

$$m_i - F(i,2,t-1) \leq \left[\frac{5n_1 - (t+i-6)}{5}\right] \leq \left[\frac{5n_1 - (t+1)}{5}\right] = n_1 - F(1,1,t-1),$$

si $k = 2$

$$m_i - F(i,2,t-1) \leq \left[\frac{5n_1 - (t+i-1)}{5}\right] \leq \left[\frac{5n_1 - (t+1)}{5}\right] = n_1 - F(1,1,t-1)$$

por tanto

$$e_{11} \equiv 0 \mod \left(p^{m_i - F(i,2,t-1)}\right)$$

se sigue que

$$e_{r2}a_{n} \equiv 0 \mod \left(p^{m_i - F(i,2,t-1)}\right)$$

si $r = \{1,2\}$ tenemos que $e_{r2} = p$, luego,

$$a_{n} \equiv 0 \mod \left(p^{m_i - F(i,2,t-1)+1}\right)$$

como

$$F(i,1,t) = \left[\frac{t+i-1+(-1)^{k+1}(k+1)}{5}\right] \leq \left[\frac{t+i+2+(-1)^{k+1}(k+1)}{5}\right] = F(i,2,t-1)+1,$$

se llega a la siguiente congruencia

$$a_{ir} \equiv 0 \bmod \left(p^{m_i - F(i,1,t)}\right) \qquad (1)$$

si $k \geq 3$, entonces $e_{r2} = 1$, así

$$a_{ir} \equiv 0 \mod \left(p^{m_i - F(i,2,t-1)}\right)$$

además

$$F(i,j,k) = \left[\frac{t + i - k + (-1)^{k+1}(k+1)}{5}\right] \leq \left[\frac{t + i - 3 + (-1)^{k+1}(k+1)}{5}\right] = F(i,2,t-1)$$

por lo tanto

$$p^{m_i - F(i,k,t)} \geq p^{m_i - F(i,2,t-1)}$$

así

$$a_{ik} \equiv 0 \bmod \left(p^{m_i - F(i,k,t)}\right) \qquad (2),$$

de (1) y (2) se sigue que $a_{ij} \equiv 0 \mod \left(p^{m_i - F(i,j,t)}\right)$. Si $t = d$, entonces $F(i,j,t) = d(i,j)$

$$e_{r2} a_{ir} \equiv c_{11} a_{i2} \mod \left(p^{m_i - d(i,j)}\right)$$

claramente

$$p^{m_i - d(i,j)} \leq p^{n_1 - F(1,1,t-1)}$$

ya que $d(i,j) \geq F(1,1,t-1)$, así

$$a_{ik} \equiv 0 \bmod \left(p^{m_i - F(i,k,t)}\right) \qquad (3)$$

por tanto $A = (a_{ij}) \in S_t$.

2^{do}caso. Si $n_1 > n_2 + 1$. Entonces

$$F(i,j,t) = \min\left\{\left[\frac{t + i - j - 5(k-1)}{3}\right], d(i,j)\right\},$$

Si $t < d$, entonces

$$F(i,j,t) = \left[\frac{t + i - j - 5(k-1)}{3}\right]$$

Como C_{11} cumple que

$$c_{11} \equiv 0 \mod \left(p^{n_1 - F(1,1,t-1)}\right)$$

se tiene que

$$c_{11} \equiv 0 \mod \left(p^{m_1 - F(i,2,t-1)}\right)$$

así la congruencia (2) se transforma en

$$e_{i2}a_{ir} \equiv 0 \mod \left(p^{m_i - F(i,2,t-1)}\right)$$

Repitiendo un argumento similar al que se realizó en el primer caso se obtiene

$$a_{ij} \equiv 0 \mod \left(p^{m_i - F(i,j,t)}\right)$$

Si $t = d$, entonces $F(i,j,t) = d(i,j)$, de igual forma se tiene que

$$a_{ij} \equiv 0 \mod \left(p^{m_i - F(i,j,t)}\right)$$

De estos dos casos se concluye que $A \in S_t$, para $n_1 > n_2$, así $A + I \in S_t + I \leq (S_t + I)H = S_t + H$. Entonces $Z_t = S_t + H$ ■

Proposición 5.6 *Sea $\{Z_t\}_{t>1}$ la serie central superior de $S + I$, entonces*

(i) Si $n_1 - n_2 = 1$, la longitud de la serie central superior es $d = 5n_1 - 3$.

(ii) Si $n_1 - n_2 > 1$, la longitud de la serie central superior es $d = 3n_1 - 1$

Demostración

Como $\{Z_t = S_t + H\}_{t>1}$ La prueba se sigue directamente de la Proposición 4.7, ya que,

$$Z_d = S_d + H = S + H = S + I,$$

además

$$Z_{d-1} = S_{d-1} + H \subsetneq S + H = S + I,$$

este argumento es valido para (i), (ii), así queda demostrado ■

Finalmente tenemos el grado de nilpotencia de $S+I$ el cual depende de los invariantes de G.

Proposición 5.7 *El grado de nilpotencia de* $S+I$ *es*

$i)$ $d = 5n_1 - 3$ *si* $n_1 = n_2 + 1$.

$ii)$ $d = 3n_1 - 1$ *si* $n_1 > n_2 + 1$.

Demostración

Se sigue del lema 1.28. ■

Bibliografía

[1] A. G Kurosh. *The Theory of Groups*. volumen uno. Chelsea publishing company New York. N. Y. Segunda edición, pags 152-158.

[2] Baer. R *Primary Abelian Groups and their Automorphisms*. Amer. J. Math., Vol. 59 (1937). pags 99-117.

[3] David. S. Dummit. *Abstract Algebra*. university of Vermont. Concordia University, Montreal 1950. Prentice Hall pags 80-85, 170-174, 415-420.

[4] Derry. D. *On Finite Abelian p-Groups*. Bull. Amer. Math. soc., Vol 45 (1939), pag 874-888.

[5] Frobenius. G., Stikelberger. L. *Ober Gruppen von vertauschbaren Elementen*. T Reine Augew. Math., 86. 1878,. Pags 217-262.

[6] I. Kaplansky. *Infinite Abelian Groups*. University of Michigan Press 1954.

[7] J. Rotman. *An Introduction to the Theory of Groups*. University of Illinois. tercera edición. Allyn and Bacon. Inc.

[8] K. Shoda *Ober die Automorphismen einer endlichen Abelshchen Gruppe*. Math. Ann. 100 1928. pags 674-686..

[9] M. A. Aviñó and R. Bautista. *The maximal normal p-subgrupo of the automorphism group of a finite abelian p-group*. Preprints Instituto de matemáticas. UNAM, 1997.

[10] M. A. Aviñó. *On The Automorphism Group of Finite Abelian p-Group*. Preprints Instituto de Matemáticas. UNAM.

[11] P.B.Bhattacharya. *Basic Abstract Algebra*. Cambridge University Press 1986.