6
2 ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

BASES DE GRÖBNER ASOCIADAS A MODULOS FINITOS

T E S I S

QUE PARA OBTENER EL TITULO DE

MATEMATICO

PRESENTA

LUIS DAVID GARCIA PUENTE

DIRECTOR DE TESIS

DRA. MARIA ALICIA AVIÑO DIAZ

1999

277296

TESIS CON
FALLA DE ORIGEN

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

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO

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

Comunicamos a usted que hemos revisado el trabajo de Tesis:

Bases de Gröbner Asociadas a Módulos Finitos

realizado por *Luis David García Puente*

con número de cuenta *9561060-1* , pasante de la carrera de *Matemáticas*

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	*Dra. Maria Alicia Aviñó Diaz*	
Propietario	*Dr. Raymundo Bautista Ramos*	
Propietario	*Dr. Ernesto Vallejo Ruiz*	
Suplente	*Dr. Christof Geiss Hahn*	
Suplente	*Dr. Rodolfo San Agustin Chi*	

Consejo Departamental de *Matemáticas*
Matemático Julio César Guevara Bravo.

Bases de Gröbner Asociadas a Módulos Finitos

Luis David García Puente
Director de Tesis:
Dra. Maria Alicia Aviñó Diaz
C.U., México, D.F., 04510, México.

Dedicatorias

A mi abuelo *Francisco Puente Hernández*, por haber plantado la semilla de las Matemáticas en mi mente, por ese ejemplo de trabajo constante y de amor que es y será siempre mi modelo a seguir, y por todo su cariño que llevaré por siempre en mi corazón.

A mis padres, *Francisca Isabel Puente Morales* y *Luis David García León*, por el apoyo incondicional que siempre me han dado, especialmente durante el estudio de mi carrera, la realización de esta tesis y sobretodo para poder alcanzar la meta de estudiar un posgrado en el extranjero. Por todo su amor, sus exigencias, por impulsarme a ser mejor cada dia. Por haber formado esta hermosa familia de la cual estoy tan orgulloso de ser parte. Esta tesis, mi primer trabajo importante, es un tributo a ustedes padres mios, por todo lo que han hecho por mí, por ayudarme a ser quien quiero ser.

Agradecimientos

A *Dios* por todos mis fracasos y todos mis triunfos.

A la *Dra. Maria Alicia Aviñó Diaz* por su confianza, apoyo, amistad y cariño. Por ser una verdadera profesora, y por haber motivado en mí el estudio del Álgebra Computacional.

A mis sinodales por todas sus sugerencias y comentarios que ayudaron a mejorar esta tesis. Además por ser todos ellos un gran pilar en mi formación académica.

Al *Dr. Dieter Vossieck* por haberme iniciado en el estudio formal del Álgebra, y por ser un magnífico profesor.

A los doctores *Bernd Sturmfels*, *Michael Stillman*, y *Rekha Thomas*, por sus comentarios y sugerencias que mejoraron la parte de *bases de Gröbner*.

A *Ileana Borja*, *Diana Avella*, *Rita Vazquez*, *Teresa Velasco*, *Marcos Zyman*, y *Efrén Perez*, por su amistad y cariño sincero, y por toda su ayuda en estos cinco años.

A todos los profesores de la *Facultad de Ciencias*, y a todos mis amigos en esta.

A toda mi familia por su cariño y apoyo incondicional, especialmente a mis hermanos *Christian* y *Alain*.

A *Alejandro Silva Solis* por estar siempre presente, por ser la gran persona que es, gracias por todo, amigo mío.

Índice General

Introducción

Sea $\mathbb{Z}_{p^n}C_p$ el álgebra del grupo cíclico de orden p sobre los enteros módulo p^n. El estudio de los $\mathbb{Z}_{p^n}C_p$-módulos finitos fué iniciado por *G. Szekeres* en 1949, en su trabajo *"Determination of certain family of finite metabelian groups"*, ver [15]. Posteriormente *Aviño y Bautista* en *"The additive structure of indecomposable $\mathbb{Z}_{p^n}C_p$-modules"* calcularon la $\mathbb{Z}_{p^n}$-estructura de los $\mathbb{Z}_{p^n}C_p$-módulos inescindibles usando las *sucesiones de Ulm*, ver [5].

El propósito de esta tesis es calcular una p-base de los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de tipo $\mathscr{C} = (i, j)$, utilizando un tipo particular de bases de Gröbner introducidas por *Borges* en [7], llamadas bases de Gröbner asociadas a grupos abelianos finitos, lo cual facilitará el cálculo de estas p-bases, al evitar el difícil cálculo de los ordenes de todos los elementos de este tipo de módulos. Más aún, este nuevo método para encontrar una p-base de los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de tipo $\mathscr{C} = (i, j)$ se puede extender al caso general, para calcular una p-base de los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta y cadena cerrada de tipo arbitrario.

La mayor parte de la teoría tanto de módulos y grupos finitos, como de bases de Gröbner que es utilizada en esta tesis, ha sido desarrollada lo más autocontenidamente posible.

Los seis capítulos de esta tesis estan organizados como sigue. En el primer capítulo presentamos las definiciones y resultados de la teoría de p-grupos abelianos finitos y módulos sobre un álgebra, necesarios para el desarrollo de esta tesis, especialmente desarrollaremos la teoría de invariantes de Ulm, la cual será una herramienta fundamental en las demostraciones del capítulo 2.

En el capítulo 2 enunciamos algunos resultados que calculan la $\mathbb{Z}_{p^n}$-estructura de los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de tipo $\mathscr{C} = (i, j)$. Damos las definiciones de $\mathscr{C}$-cadena, Λ-módulo cadena abierta, y de tipo de un Λ-módulo, además presentamos las demostraciones completas de algunos resultados obtenidos en [5].

En el capítulo 3 profundizamos en la teoría desarrollada por Aviñó y Bautista en [5], demostrando un teorema que muestra explícitamente una p-base de los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de la forma $\mathscr{C} = (i, j)$, usando la teoría desarrollada en el capítulo 2 para demostrar este resultado.

En el capítulo 4 enunciamos los conceptos y resultados básicos de la teoría de Bases de Gröbner que utilizamos en esta tesis, dando primero una breve introducción a la teoría de anillos de polinomios, para después dar algunos fundamentos de las bases de Gröbner, especialmente enunciamos el *algoritmo de Buchberger*, debido a que lo usamos en algunas demostraciones del capítulo 5, aunque no damos su demostración por salirse de los propósitos de esta tesis.

Iniciamos el capítulo 5 dando una introducción a la teoría de bases de Gröbner de ideales tóricos. Definimos el concepto de bases de Gröbner asociadas a grupos abelianos finitos, y enunciamos sus propiedades utilizando el lenguaje introducido en la sección de bases de Gröbner de ideales tóricos. Es importante hacer notar que en este capítulo establecemos la relación entre las bases de Gröbner y los grupos abelianos finitos, a través de los teoremas enunciados en [7], para los cuales presentamos demostraciones completas en este capítulo.

Finalmente en el capítulo 6 definimos el concepto de p-base de Gröbner asociada a módulos finitos (grupos abelianos finitos). Modelamos el problema de calcular una p-base de estos $\mathbb{Z}_{p^n}C_p$-módulos utilizando la teoría de bases de Gröbner asociadas a grupos abelianos finitos, enunciando un resultado análogo al obtenido en el capítulo 3, encontrando lo que llamamos una p-base de Gröbner asociada a los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de la forma $\mathscr{C} = (i, j)$. Finalizamos este capítulo con algunos ejemplos de este resultado implementados en el sistema *Macaulay2*.
[1]

[1] Esta tesis fué escrita en LaTeX 2_ϵ, usando GNU Emacs bajo Linux 5.1.

Resultados

Los siguientes resultados se deben al autor de esta tesis:

- Teorema 2.8, pag. 27.
- Teorema 3.1, pag. 30.
- Teorema 5.4, pag. 59.
- Teorema 5.5, pag. 59.
- Proposición 5.6, pag. 62.
- Teorema 5.10, pag. 65.
- Teorema 6.1, pag. 70.

Capítulo 1

Teoría de p-Grupos Abelianos Finitos y Teoría de Módulos sobre un Álgebra

En este capítulo presentamos las definiciones y resultados de la teoría de p-grupos abelianos finitos y módulos sobre un álgebra, necesarios para el desarrollo de esta tesis.

1.1 p-Grupos abelianos finitos

Definición. Un grupo abeliano G tiene *generadores* X y *relaciones (de definición)* Δ si $G \cong F/R$, donde F es el grupo abeliano libre generado por X, Δ es un conjunto de combinaciones lineales sobre $\mathbb{Z}$ de elementos de X, y R es el subgrupo de F generado por Δ. Si X puede tomarse finito, entonces G es llamado *finitamente generado.*

Llamamos a (Δ, X) una *presentación* de G.

Definición. Un conjunto $\{x_1, \ldots, x_r\}$ de elementos no cero en un grupo abeliano es *independiente*[1] si, siempre que existan enteros $m_1, \ldots, m_r$ tales que $\sum_{i=1}^{r} m_i x_i = 0$, entonces se tiene que $m_i x_i = 0$.

[1] ver [13]

Lema 1.1. *Si G es un grupo abeliano, entonces $\{x_1, \ldots, x_r\} \subset G$ es independiente si, y sólo si, $\langle x_1, \ldots, x_r \rangle = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$.*

Demostración. Asumimos independencia; si $y \in \langle x_i \rangle \cap \langle \{x_j \mid j \neq i\} \rangle$, entonces existen enteros $m_1, \ldots, m_r$, tales que $y = -m_i x_i = \sum_{j \neq i} m_j x_j$, por lo tanto $\sum_{k=1}^{r} m_k x_k = 0$. Por la hipótesis de independencia tenemos que, $m_k x_k = 0 \, \forall \, k$, en particular $m_i x_i = 0$ de donde $y = 0$. Esto prueba que $\langle x_1, \ldots, x_r \rangle = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$. Para el regreso, asumimos que $\sum m_i x_i = 0$. Para cada j, tenemos que $-m_j x_j = \sum_{k \neq j} m_k x_k \in \langle x_j \rangle \cap \langle \{x_k \mid k \neq j\} \rangle = 0$. Por lo tanto, cada $m_j x_j = 0$ y $\{x_1, \ldots, x_r\}$ es independiente. □

Definición. Sea G un p-grupo abeliano finito, una *p-base* de G es un conjunto generador independiente, es decir $\{a_1, \ldots, a_n\}$ es una p-base de G si, y sólo si, $G = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle$.

El siguiente teorema está demostrado en [13], pag. 124.

Teorema 1.2 (Teorema de la base de Burnside, 1912). *Si G es un p-grupo finito, entonces cualquiera dos conjuntos generadores minimales tienen la misma cardinalidad, digamos,* $\dim G/\Phi(G)$, *donde $\Phi(G)$ es el subgrupo de Frattini*[2] *de G. Más aún, todo $x \notin \Phi(G)$ pertenece a algún conjunto generador minimal de G.*

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

Definición. El *p-rango* de un p-grupo abeliano finito G, denotado $\mathrm{r_p}(G)$ es el número de elementos de una p-base.

Definición. Sea G un grupo abeliano y m un número entero, definimos al subgrupo $G[m]$ como el subgrupo de G de todos los elementos cuyo orden divide a m, es decir $G[m] = \{x \in G \mid mx = 0\}$.

Definición. Si p es primo, entonces un p-grupo abeliano *elemental* es un grupo finito G isomorfo a $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$.

Proposición 1.3. *Todo grupo abeliano finito G de exponente primo p es un p-grupo abeliano elemental.*

[2]definido como la intersección de todos los subgrupos maximales de G

Demostración. Como espacio vectorial sobre $\mathbb{Z}_p$, G tiene base $\{x_1, \ldots, x_r\}$. Entonces $G = \langle x_1, \ldots, x_r \rangle$, porque toda base genera, y $G = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$, porque toda base es independente. □

Teorema 1.4 (Teorema de Bases). *Todo p-grupo abeliano finito G es suma directa de p-grupos abelianos cíclicos.*

Demostración. Probaremos este teorema usando inducción sobre n, donde $p^n G = 0$.

Si $n = 1$, entonces el teorema esta probado en la proposición 1.3.

Supongamos que $p^{n+1} G = 0$. Si $H = pG$, entonces $p^n H = 0$, por hipótesis de inducción tenemos que,

$$H = \sum_{i=1}^{r} \langle y_i \rangle .$$

Debido a que $y_i \in H = pG$, existen $z_i \in G$, tales que $pz_i = y_i$. Por el lema 1.1, tenemos que $\{y_1, \ldots, y_r\}$ es independiente, por lo tanto $\{z_1, \ldots, z_r\}$ es independiente, y de esta manera

$$L := \langle z_1, \ldots, z_r \rangle = \sum_{i=1}^{r} \langle z_i \rangle .$$

Para cada i, sea k_i el orden de y_i, de donde $k_i z_i$ tiene orden p. Entonces el subconjunto independiente $\{k_1 z_1, \ldots, k_r z_r\}$ del espacio vectorial $G[p]$ puede extenderse a una base de $G[p]$, digamos $\{k_1 z_1, \ldots, k_r z_r, x_1, \ldots, x_s\}$, por lo tanto

$$M := \langle x_1, \ldots, x_s \rangle = \sum_{j=1}^{s} \langle x_j \rangle$$

Demostraremos que $G = L \oplus M$, lo cuál completará la demostración del teorema.

(i) $L \cap M = 0$. Si $g \in L \cap M$, entonces $g = \sum b_i z_i = \sum a_j x_j$. Ahora $pg = 0$, pues $g \in M$, entonces $\sum p b_i z_i = 0$, por independencia tenemos que para toda i, $p b_i z_i = b_i y_i = 0$. Entonces como k_i es el orden de y_i, tenemos que existen c_i tales que $b_i = c_i k_i$, por lo tanto $\sum c_i k_i z_i - \sum a_j x_j = 0$, y por la independencia del conjunto $\{k_1 z_1, \ldots, k_r z_r, x_1, \ldots, x_s\}$, tenemos que cada término es igual a 0; por lo tanto $g = \sum a_j x_j = 0$.

(ii) $L + M = G$. Si $g \in G$, entonces $pg \in pG = H$, de donde $pg = \sum c_i y_i = \sum p c_i z_i$. Entonces $p(g - \sum c_i z_i) = 0$ y $g - \sum c_i z_i \in G[p]$, de donde $g - \sum c_i z_i = \sum b_i k_i z_i + \sum a_j x_j$, por lo tanto $g = \sum (c_i + b_i k_i) z_i + \sum a_j x_j \in L + M$. □

Como consecuencia de este teorema tenemos las siguientes definiciones.

Definición. Si G es un p-grupo abeliano finito, es decir G se descompone en la suma directa, $G = \sum C_i$, donde cada C_i es un p-grupo abeliano cíclico de orden p^{m_i} y $p^{m_1}|p^{m_2}|\cdots|p^{m_t}$, entonces decimos que G tiene *factores p-invariantes* $(p^{m_1}, \ldots, p^{m_t})$.

Definición. Si G es un p-grupo abeliano finito, $G = s_1\mathbb{Z}_p \oplus s_2\mathbb{Z}_{p^2} \oplus \cdots \oplus s_n\mathbb{Z}_{p^n}$. Decimos que G tiene *tipo* $(s_1, s_2, \ldots, s_n)$, denotado por $\underline{t}(G)$. Si $s_n \neq 0$, entonces p^n es el *exponente* de G.

Observación. Si $\underline{t}(G) = (s_1, s_2, \ldots, s_n)$, entonces $r_p(G) = \sum_{k=1}^{n} s_k$.

Definición. Sea G un p-grupo abeliano finito, si $a \in G$, $a \neq 0$, la *p-altura* de a, denotada $h_p(a)$ es el máximo número natural k, tal que la ecuación en x, $p^k x = a$, tiene solución en G.

En el siguiente teorema utilizamos la notación multiplicativa para poder tratar a los números encontrados por este teorema como exponentes, ya que precisamente los utilizaremos como exponentes de polinomios en el capítulo 4.

Teorema 1.5. *Sean G un grupo abeliano finito, $\{b_1, \ldots, b_l\} \subset G$, es posible determinar exponentes $m_k > 0$ y n_{k_i} tales que*

(i) m_1 es el orden de b_1,

(ii) Para cada $k \in [2, l]$ $b_k^{m_k} = \prod_{i=1}^{k-1} b_i^{n_{k_i}}$, donde $m_k = min\{m > 0 \mid b_k^m \in \langle b_1, \ldots, b_{k-1}\rangle\}$, y para toda $i \in [1, k-1]$, $n_{k_i} \in [0, m_i)$.

Demostración. La demostración se hará por inducción sobre l.

Si $l = 1$, como G es un grupo abeliano finito, entonces siempre podemos encontrar m_1 tal que $o(b_1) = m_1$.

Supongamos que el teorema se cumple para $k-1$, demostraremos que se cumple para k. Sabemos que existe m_k debido a que $b_k^{o(b_k)} \in \langle b_1, \ldots, b_{k-1}\rangle$, supongamos entonces que $j = max\{i \mid n_{k_i} \geqslant m_i\}$, de no existir j no habría más nada que probar, tomemos $n_{k_j} = r_1 m_j + r_2$, donde $r_2 \in [0, m_j)$, entonces

$$b_k^{m_k} = (\prod_{i=1}^{j-1} b_i^{n_{k_i}})(b_j^{m_j})^{r_1} b_j^{r_2} (\prod_{i=j+1}^{k-1} b_i^{n_{k_i}})$$

por inducción tenemos que

$$b_k^{m_k} = (\prod_{i=1}^{j-1} b_i^{(n_{k_i}+r_1 n_{j_i})}) b_j^{r_2} (\prod_{i=j+1}^{k-1} b_i^{n_{k_i}})$$

Observando que las condiciones para los exponentes se satisfacen para $i \in [j, k-1]$, continuamos en forma semejante con $\prod_{i=1}^{j-1} b_i^{(n_{k_i}+r_1 n_{j_i})}$, hasta que se cumplan las condiciones para todos los exponentes. □

1.2 Invariantes de Ulm

Sea G un p-grupo abeliano finito. Empezaremos construyendo algunos invariantes de G. Consideramos a los siguientes subgrupos

$$G, pG, p^2G, \ldots, p^nG = 0$$

esta es una *serie descendente* que empieza en G y termina en 0, denotamos por $G_s := p^sG$. Consideramos ahora al grupo cociente

$$G_s/G_{s+1} \; \forall \, s \in \{0, \ldots, n-1\}$$

Como $G_{s+1} = pG_s$, todos los elementos de este grupo cociente tienen orden p, es decir es un grupo elemental. Debido a esta observación este grupo cociente puede verse como un espacio vectorial sober $\mathbb{Z}_p$. Como cualquier espacio vectorial, su dimensión esta bien definida.

Teorema 1.6. *Sea G un p-grupo abeliano finito tal que G tiene una descomposición $G = \bigoplus_i C_i$, en suma directa de grupos cíclicos, entonces el número de C_i de orden $\geqslant p^{s+1}$ es* $\dim_{\mathbb{Z}_p}(G_s/G_{s+1})$.

Demostración. Sea B_k la suma directa de todos los C_i de orden p^k, supongamos que hay $b_k \geqslant 0$ sumandos en B_k. Entonces

$$G = B_1 \oplus \cdots \oplus B_t.$$

Ahora

$$p^sG = p^sB_{s+1} \oplus \cdots \oplus p^sB_t, \text{ pues } p^sB_1 = \cdots = p^sB_s = 0,$$

y

$$p^{s+1}G = p^{s+1}B_{s+2} \oplus \cdots \oplus p^{s+1}B_t.$$

Por lo tanto

$$p^sG/p^{s+1}G = p^sB_{s+1} \oplus (p^sB_{s+2}/p^{s+1}B_{s+2}) \oplus \cdots \oplus (p^sB_t/p^{s+1}B_t),$$

de donde se concluye que

$$\dim_{\mathbf{Z}_p}(G_s/G_{s+1}) = b_{s+1} + b_{s+2} + \cdots + b_t.$$

□

Definición. Si G es un p-grupo abeliano finito y $n \geqslant 0$, entonces $f_p(n, G) = \dim_{\mathbf{Z}_p}(G_n/G_{n+1}) - \dim_{\mathbf{Z}_p}(G_{n+1}/G_{n+2})$.

Teorema 1.7. *Si G es un p-grupo abeliano finito, entonces cualesquiera dos descomposiciones de G en suma directa de grupos cíclicos tiene el mismo número de sumandos de cada tipo. Más precisamente, para toda $n \geqslant 0$, el número de sumandos cíclicos de orden p^{n+1} es $f_p(n, G)$.*

Demostración. Para toda descomposición de G en suma directa de grupos cíclicos, el teorema 1.6 muestra que hay exactamente $f_p(n, G)$ sumandos cíclicos de orden p^{n+1}. El resultado se sigue debido a que $f_p(n, G)$ depende únicamente de G y no de la elección de la descomposición. □

Este teorema muestra que para un grupo finito, estas dimensiones son un conjunto completo de invariantes, pero todavía podemos hacerlo mejor.

Definición. Definimos $U_s := G_s \cap G[p]$.

Observación. El cociente U_s/U_{s+1} es también un espacio vectorial sobre $\mathbb{Z}_p$.

Definición. Definimos $\mathrm{f}(r, G)$ (aquí estoy utilizando la notación sugerida en [11]), el r-ésimo *invariante de Ulm*, como la dimensión sobre $\mathbb{Z}_p$ de U_r/U_{r+1}, es decir $\mathrm{f}(r, G) = \dim_{\mathbf{Z}_p}(U_r/U_{r+1})$.

Definición.

- Llamamos a U_r/U_{r+1} el r-ésimo *factor de Ulm*.
- Llamamos a $U_0/U_1, \ldots, U_{n-1}/U_n, \ldots$, la *sucesión de Ulm* de G.

Teorema 1.8. *Si G es un p-grupo abeliano finito, es decir G es suma directa de p-grupos abelianos cíclicos, entonces* $\mathrm{f}(n, G)$ *es el número de sumandos cíclicos de orden* p^{n+1}.

Demostración. Sea B_n la suma directa de todos los sumandos cíclicos de orden p^n, si es que hay alguno(en la descomposición dada de G), de tal forma que $G = B_1 \oplus \cdots \oplus B_k \oplus \cdots$, sea b_k el número de sumandos directos en B_k (por supuesto b_k puede ser 0). Tenemos entonces que

$$G[p] = B_1 \oplus pB_2 \oplus \cdots \oplus p^{k-1}B_k \oplus \cdots$$

y además que

$$p^n G = p^n B_{n+1} \oplus \cdots \oplus p^n B_k \oplus \cdots .$$

Por lo tanto, para toda $n \geqslant 0$,

$$U_n = p^n B_{n+1} \oplus p^{n+1} B_{n+2} \oplus \cdots ,$$

de donde

$$U_n / U_{n+1} \cong p^n B_{n+1}.$$

Por lo tanto, $\mathrm{f}(n, G) = \dim(p^n B_{n+1}) = b_{n+1}$. □

Observaciones.

- Sea G un p-grupo abeliano finito de exponente p^n y tipo $(s_1, s_2, \ldots, s_n)$, entonces $\mathrm{f}(k-1, G) = s_k$.
- Sea G un p-grupo abeliano finito de exponente p^n y tipo $(s_1, s_2, \ldots, s_n)$, entonces $\mathrm{r_p}(G) = \sum_{i=1}^{n} s_i = \sum_{i=1}^{n} \mathrm{f}(i-1, G)$.

1.3 Módulos finitos sobre un álgebra

Definición. Sea R un anillo conmutativo con 1. Un grupo abeliano M es un *R-módulo*, si existe una función $s : R \times V \to V$, (llamada multiplicación escalar y denotada por $(\alpha, v) \mapsto \alpha v$) tal que, para toda $\alpha, \beta, 1 \in R$ y $u, v \in M$:

(i) $(\alpha\beta)v = \alpha(\beta v)$;

(ii) $(\alpha+\beta)v = \alpha v + \beta v$;

(iii) $\alpha(u+v) = \alpha u + \alpha v$;

(iv) $1v = v$.

Definición. Sea M un R-módulo, diremos que M es *finito*, si M tiene un número finito de elementos.

Observación. Todo $\mathbb{Z}_{p^n}$-módulo finito M es un p-grupo abeliano finito.

Definición. [3] Un *álgebra* A sobre un anillo conmutativo (con unidad) R, es un anillo A (con unidad), junto con una multiplicación por escalares $R \times A \to A$, que induce en A una estructura de R-módulo, con la condición adicional

$$\alpha(ab) = (\alpha a)b = a(\alpha b)$$

para todo $\alpha \in R$, $a, b \in A$.

Definición. Un *A-módulo izquierdo* M, donde A es una R-álgebra, es un grupo abeliano M provisto de una multiplicación

$$\begin{array}{ccc} A \times M & \to & M \\ (a, v) & \mapsto & av \end{array}$$

que satisface

(i) $(ab)v = a(bv)$;

(ii) $(a+b)v = av + bv$;

(iii) $a(u+v) = au + av$;

(iv) $1v = v$.

para todo $a, b \in A$ y $u, v \in M$.

Como A es una R-álgebra, entonces todo A-módulo M es automáticamente un R-módulo con la multiplicación

$$\alpha v := (\alpha 1_A)v.$$

[3] ver [8].

De donde, se sigue que

$$\alpha(av) = (\alpha a)v = a(\alpha v)$$

para todo $\alpha \in R$, $a \in A$, $v \in M$.

En esta tesis A-módulo querrá decir A-módulo izquierdo.

Definición. Sea M un A-módulo, diremos que M es *finitamente generado*, si todo elemento de M puede ser escrito como una combinación A-lineal de elementos de algún subconjunto finito de M.

Observación. Si M es finito como grupo abeliano, entonces M es un módulo finitamente generado.

Definición. Se dice que un A-módulo M es *escindible*, si M puede expresarse como una suma directa de submódulos propios

$$M = M_1 \oplus M_2 \qquad (M_1, M_2 \neq 0)$$

En caso contrario, diremos que M es *inescindible.*

Definición. Sea M un A-módulo finitamente generado, donde A es un álgebra. El *soclo* de M, denotado $\operatorname{Soc} M$, es el único submódulo semisimple maximal de M.[4]

El soclo de un grupo G, es la suma de sus subgrupos simples. Debido a que un grupo abeliano es simple si, y sólo si, es un grupo cíclico de orden primo, se tiene que el $\operatorname{Soc} G$ de un p-grupo G es $G[p]$, ver [10], pag. 33.

Definición. El *álgebra de un grupo finito* G sobre un anillo conmutativo (con 1) R, denotada RG es la R-álgebra cuyos elementos son las aplicaciones

$$u : G \to R$$

con las operaciones

$$\begin{aligned}(u+v)(g) &= u(g) + v(g),\\ (uv)(g) &= \sum_{g_1 g_2 = g} u(g_1)v(g_2),\\ (\alpha u)(g) &= \alpha u(g)\end{aligned}$$

[4] ver [3], pag. 118.

con $\alpha \in R$, $u, v \in RG$, $g, g_1, g_2 \in G$.

Los elementos de RG usualmente se escriben como "sumas formales"

$$u = \alpha_1 g_1 + \cdots + \alpha_n g_n$$

con $G = \{g_1, \ldots, g_n\}$, $\alpha_i = u(g_i)$. Con esta notación las operaciones son

$$\sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i$$

$$\alpha \sum_{i=1}^{n} \alpha_i g_i = \sum_{i=1}^{n} \alpha \alpha_i g_i$$

$$\sum_{i=1}^{n} \alpha_i g_i \cdot \sum_{i=1}^{n} \beta_i g_i = \sum_{i,j} \alpha_i \beta_j g_i g_j.$$

Ejemplos. Sea $G = C_p$, donde C_p denota al grupo cíclico de orden p, y $R = \mathbb{Z}_{p^n}$, los enteros módulo p^n. Denotamos

$$\Lambda = \mathbb{Z}_{p^n} C_p,$$

al *álgebra de grupo* de C_p, sobre $\mathbb{Z}_{p^n}$.

Si C_p está generado por x, entonces los elementos de Λ son las combinaciones lineales formales

$$\sum_{i=0}^{p-1} a_i x^i,$$

con $a_i \in \mathbb{Z}_{p^n}$ y $x^0 = 1$ la unidad de C_p.

Los Λ-módulos izquierdos inescindibles han sido descritos por *Szekeres*[5] en 1949, por la acción de dos elementos en Λ, $\pi = x^{p-1} + x^{p-2} + \cdots + x + 1$ y $\phi = x - 1$, los cuales satisfacen las siguientes condiciones:

1. π y ϕ son nilpotentes,
2. $\pi\phi = \phi\pi = 0$,
3. $p = \pi + \phi^{p-1}\sigma(\phi)$

donde $\sigma(\phi)$ es un polinomio en ϕ.

Esto se probará en el capítulo 2.

[5] ver [15]

Capítulo 2

Estructura Aditiva de los $\mathbb{Z}_{p^n}C_p$-Módulos Cadena inescindibles

En este capítulo enunciaremos algunos resultados que calculan la $\mathbb{Z}_{p^n}$-estructura de los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de tipo $\mathscr{C} = (i, j)$.

2.1 Propiedades de π y ϕ

Lema 2.1. *Sean $\phi = x-1$ y $\pi = x^{p-1}+\cdots+x+1$ en Λ. Entonces se cumplen las siguientes condiciones:*

(i) $\pi\phi = \phi\pi = 0$,

(ii) $p = \pi + \phi^{p-1}\sigma(\phi)$,

(iii) *Si* $\sigma(\phi) = a_0 + a_1\phi + \cdots + a_r\phi^r$, *entonces* $a_0 \equiv -1 \pmod{p}$,

(iv) π *y* ϕ *son nilpotentes, con índice de nilpotencia* $n+1$ *y* $n(p-1)+1$ *respectivamente,*

(v) Los coeficientes de $\sigma(\phi)$ *son enteros no negativos menores que* p.

Demostración. Observamos que $\pi\phi = \phi\pi = x^p - 1 = 0$, lo cual demuestra (i), además

$$x^p - 1 = [(x-1)+1]^p - 1 = p(x-1) + pc_2(x-1)^2 + \cdots + pc_{p-1}(x-1)^{p-1} + (x-1)^p$$

con $(p, c_i) = 1$ para toda $i \in \{2, \ldots, p-1\}$.

Entonces

$$\pi = \frac{x^p - 1}{x - 1} = p + pc_2\phi + \cdots + pc_{p-1}\phi^{p-2} + \phi^{p-1},$$

despejando obtenemos

$$p = \pi - pc_2\phi - \cdots - pc_{p-1}\phi^{p-2} - \phi^{p-1} \tag{2.1}$$

Multiplicando esta ecuación (2.1) por ϕ y por ϕ^2 obtenemos

$$p\phi = -pc_2\phi^2 - \cdots - pc_{p-1}\phi^{p-1} - \phi^p \tag{2.2}$$

$$p\phi^2 = -pc_2\phi^3 - \cdots - pc_{p-1}\phi^p - \phi^{p+1} \tag{2.3}$$

subtituyendo (2.3) en (2.2) obtenemos

$$p\phi = pd_3\phi^3 + \cdots + pd_{p-1}\phi^{p-1} + d_p\phi^p + d_{p+1}\phi^{p+1}.$$

Multiplicando esta ecuación por ϕ^2, obtenemos

$$p\phi^3 = pd_3\phi^5 + \cdots + pd_{p-1}\phi^{p+1} + d_p\phi^{p+2} + d_{p+1}\phi^{p+3}.$$

Continuamos de la misma forma hasta obtener $p\phi = \sum_{p \leqslant s} e_s\phi^s$ y de manera similar $p\phi^{p-1} = \sum_{s \geqslant p} e_s^{(p-1)}\phi^s$. Sustituyendo estas ecuaciones en (2.1) obtenemos que

$$\begin{aligned} p &= \pi - \phi^{p-1} + \sum_{p \leqslant s} u_{s-p+1}\phi^s \\ &= \pi + \phi^{p-1}\sigma(\phi) \end{aligned}$$

donde $\sigma(\phi) = -1 + \sum_{p \leqslant s} u_{s-p+1}\phi^{s-p+1}$, lo cual demuestra los incisos (ii) y (iii).

Ahora utilizando la ecuación (2.2) podemos poner a cualquier ϕ^r, $r \geqslant p$ en términos de la forma $p\phi^u$ con $u \in \{1, \ldots, p-1\}$.

Entonces tenemos que

$$\begin{aligned} p &= \pi + \phi^{p-1}\sigma(\phi) \\ p &= \pi + \phi^{p-1}(-1 + a_1\phi + \cdots + a_{p-1}\phi^{p-1}) \end{aligned}$$

de donde

$$p^n = \pi^n + \phi^{n(p-1)}\sigma(\phi)^n = 0$$

multiplicando esta ecuación por π, obtenemos

$$\pi^{n+1} = 0$$

por lo tanto π es nilpotente.

Por (i) tenemos que ϕ es un divisor de cero, es decir ϕ no es inversible, entonces como Λ es un anillo local, ϕ es nilpotente, es decir existe i tal que $\phi^{i+1} = 0$, lo cual demuestra (iv). Más aún, ya demostramos que $\pi^n + \phi^{n(p-1)}\sigma(\phi)^n = 0$, es decir $-\pi^n = \phi^{n(p-1)}\sigma(\phi)^n$, con $\sigma(\phi)^n = -1 + b_1\phi + \cdots + b_i\phi^i$, entonces multiplicando esta ecuación por ϕ obtenemos

$$0 = -\phi^{n(p-1)+1} + b_1\phi^{n(p-1)+2} + \cdots + b_s\phi^i \quad \text{para algún } s.$$

De donde

$$\phi^{n(p-1)+1} = b_1\phi^{n(p-1)+2} + \cdots + b_s\phi^i \tag{2.4}$$

multiplicando por ϕ obtenemos

$$\phi^{n(p-1)+2} = b_1\phi^{n(p-1)+3} + \cdots + b_{s-1}\phi^i \tag{2.5}$$

$$\vdots$$

$$\phi^{i-1} = b_1\phi^i \tag{2.6}$$

$$\phi^i = b_1\phi^{i+1} = 0$$

Entonces $\phi^i = 0$, luego por (2.6) tenemos que $\phi^{i-1} = 0$, continuando de esta manera obtenemos que $\phi^{n(p-1)+2} = 0$ y utilizando la ecuación (2.4) llegamos a que $\phi^{n(p-1)+1} = 0$.

Ya tenemos que $p = \pi + \phi^{p-1}(-1 + a_1\phi + \cdots + a_{p-1}\phi^{p-1})$, si $a_1 \geqslant p$, entonces $a_1 = kp + r_1$ con $r_1 < p$, así que $a_1\phi = kp\phi + r_1\phi$, entonces si sustituimos p obtenemos

$$\begin{aligned} p =& \pi + \phi^{p-1}(-1 - k\phi^p + ka_1\phi^{p+1} + \cdots + ka_{p-1}\phi^{2p-1} + \\ & r_1\phi + a_2\phi^2 + \cdots + a_{p-1}\phi^{p-1}) \\ p =& \pi + \phi^{p-1}(-1 + r_1\phi + \cdots + a_{p-1}\phi^{p-1} + \\ & a_p\phi^p + \cdots + a_{2p-1}\phi^{2p-1}) \end{aligned}$$

si $a_2 \geqslant p$, entonces $a_2 = k_2 p + r_2$, con $r_2 < p$ entonces si sustituimos p obtenemos

$$\begin{aligned} p =& \pi + \phi^{p-1}(-1 + r_1\phi + r_2\phi^2 + a_3\phi^3 + \cdots + \\ & a_{p-1}\phi^{p-1} + a_p\phi^p + b_{p+1}\phi^{p+1} + \cdots + b_{2p}\phi^{2p}) \end{aligned}$$

Debido a que ϕ es nilpotente, es claro que repitiendo este proceso llegaremos al resultado deseado, para terminar la demostración de (v). □

A partir de esta demostración obtuvimos un algoritmo para calcular $\sigma(\phi)$, en el *Apéndice* damos una implementación de este algoritmo en el lenguaje $C{+}{+}$, a continuación presentamos algunos ejemplos de $\sigma(\phi)$, obtenidos con este algoritmo.

Ejemplos.

$p = 2$: $p = \pi + \phi(1)$

$p = 3$: $p = \pi + \phi^2(2 + \phi)$

$p = 5$: $p = \pi + \phi^4(4 + 2\phi + 3\phi^2 + \phi^3)$

2.2 Λ-módulos cadena

Definición. Una *cadena* $\mathscr{C}$ de dimensión m es una sucesión de m pares de números naturales $(i_1, j_1; \ldots ; i_m, j_m)$.

Definición. Sea $\mathscr{C} = (i_1, j_1; \ldots ; i_m, j_m)$ una cadena de dimensión m. Decimos que la sucesión de elementos $a_1, a_2, \ldots, a_m$ en un Λ-módulo M es una *cadena de la forma* $\mathscr{C} = (i_1, j_1; \ldots ; i_m, j_m)$ o una *$\mathscr{C}$-cadena* si:

1. $\phi^{i_1} a_1 \in \operatorname{Soc} M$ y $\pi^{j_m} a_m \in \operatorname{Soc} M$,
2. $\pi^{j_k} a_k = \phi^{i_{k+1}} a_{k+1} \; \forall \; k \in \{1, \ldots, m-1\}$.

Denotamos $d_k := \pi^{j_k} a_k = \phi^{i_{k+1}} a_{k+1} \; \forall \; k \in \{1, \ldots, m-1\}$.

A partir de este momento denotamos por $\mathscr{C}(a_1, \ldots, a_m)$ al Λ-submódulo M generado por los elementos de la $\mathscr{C}$-cadena $a_1, \ldots, a_m$.

Si $M = \mathscr{C}(a_1, \ldots, a_m)$, definimos $\mathscr{A}(M) = \pi(M) \cap \phi(M)$.

Si $a \in M$, denotamos por $i(a)$ al máximo número natural i tal que $\phi^i a \neq 0$, y por $j(a)$ al máximo número natural j tal que $\pi^j a \neq 0$.

Definición. Sea $\mathscr{C} = (i_1, j_1; \ldots ; i_m, j_m)$ una cadena de dimensión m. Decimos que $M = \mathscr{C}(a_1, \ldots, a_m)$ es un Λ-*módulo cadena abierta* si satisface:

(i) $i_1 = i(a_1) + 1$, $j_m = j(a_m) + 1$,

(ii) $\mathscr{A}(M) = \langle d_1 \rangle \oplus \langle d_2 \rangle \oplus \cdots \oplus \langle d_{m-1} \rangle$ si $m > 1$,
$\mathscr{A}(M) = 0$ si $m = 1$

(iii) $M/\mathscr{A}(M) = \langle \overline{a_1} \rangle \oplus \langle \overline{a_2} \rangle \oplus \cdots \oplus \langle \overline{a_m} \rangle$. Más aún $\langle \overline{a_s} \rangle$ es un módulo cadena abierta generado por $\overline{a_s}$ de la forma $\mathscr{C}_s = (i_s, j_s)$.

Si M es un Λ-módulo cadena abierta, decimos que la cadena $\mathscr{C} = (i_1, j_1; \ldots ; i_m, j_m)$ es el *invariante* de M.

Definición. Sea $\mathscr{C} = (i_1, j_1; \ldots ; i_m, j_m)$ una cadena de dimensión m, decimos que $\mathscr{C}$ tiene *periodo* $\underline{m}$ si $\underline{m} | m$ y además si $s \equiv t \pmod{\underline{m}}$ entonces $j_s = j_t$, $i_s = i_t$.

Definición. Sea $\mathscr{C} = (i_1, j_1; \ldots ; i_m, j_m)$ una cadena de dimensión m y periodo minimal $\underline{m}$. Decimos que $M = \mathscr{C}(a_1, \ldots, a_m)$ es un Λ-*módulo cadena cerrada* con polinomio característico $f(z)$, si las siguientes condiciones se satisfacen:

(i) $\phi^{i_1} a_1 = d_0 \neq 0$, $\pi^{j_m} a_m = d_m \neq 0$.

(ii) $d_m = \sum_{s=0}^{d-1} \lambda_s d_{s\underline{m}}$, con $\lambda_0 \neq 0$ y $(g(z))^t = f(z) = z^d - \sum_{s=0}^{d-1} \lambda_s z^s$ donde $g(z)$ es un polinomio irreducible sobre $\mathbb{Z}_p$ y d es un número natural distinto de cero tal que $m = d\underline{m}$.

(iii) $\mathscr{A} = \langle d_0 \rangle \oplus \langle d_1 \rangle \oplus \cdots \oplus \langle d_{m-1} \rangle$.

(iv) $M/\mathscr{A}(M) = \langle \overline{a_1} \rangle \oplus \cdots \oplus \langle \overline{a_m} \rangle$, donde $\overline{a_s}$ denota la clase de a_s módulo $\mathscr{A}(M)$. Más aún $\langle \overline{a_s} \rangle$ es un módulo cadena abierta generado por $\overline{a_s}$ de la forma $\mathscr{C}_s = (i_s, j_s)$.

Si M es un Λ-módulo cadena cerrada, decimos que la cadena $\underline{\mathscr{C}} = (i_1, j_1; \ldots ; i_{\underline{m}}, j_{\underline{m}})$ y el polinomio $f(z)$ son los *invariantes* de M.

Los siguientes teoremas están demostrados en el trabajo de Szekeres, para mayores referencias ver [5, 15].

Teorema 2.2. *Todo Λ-módulo finito M es la suma directa de cadenas abiertas y cadenas cerradas. Toda cadena abierta y toda cadena cerrada es inescindible, y dos cadenas son isomorfas sólo si poseen el mismo conjunto de invariantes.*

Teorema 2.3. *Si $M = \mathscr{C}(a_1, \ldots, a_m)$ es un Λ-módulo cadena abierta de la forma $\mathscr{C} = (i_1, j_1; \ldots ; i_m, j_m)$ entonces para todo $y \in M$, y se escribe de manera única como*

$$y = \sum_{s=1}^{m} \alpha_s a_s + \sum_{s=1}^{m} \sum_{t=1}^{i_s - 1} \beta_{s_t} \phi^t a_s + \sum_{s=1}^{m} \sum_{t=1}^{j_s - 1} \gamma_{s_t} \pi^t a_s + \sum_{s=1}^{m-1} \delta_s d_s \qquad (2.7)$$

donde $0 \leqslant \alpha_s < p$, $0 \leqslant \beta_{s_t} < p$, $0 \leqslant \gamma_{s_t} < p$, $0 \leqslant \delta_s < p$. Llamamos a la expresión anterior, la descomposición canónica de y.[1]

Nota 1: Para los propósitos de esta tesis, sólo estudiaremos los Λ-módulos cadena abierta, para el tratamiento de los Λ-módulos cadena cerrada ver [5].

Teorema 2.4. *Sea M un p-grupo abeliano finito de exponente p^n y de tipo $(s_1, s_2, \ldots, s_n)$. Consideramos los subconjuntos Y_k de M definidos por:*

$$Y_k = \{y_{k_1}, y_{k_2}, \ldots, y_{k_{s_k}}\} \quad \textit{donde } 1 \leqslant k \leqslant n,$$

tales que

(i) $Y_k \subset M[p^k]$,

(ii) $p^{k-1}\overline{Y_k} = \{p^{k-1}\overline{y_{k_1}}, \ldots, p^{k-1}\overline{y_{k_{s_k}}}\}$ *es una base del $\mathbb{Z}_p$-espacio vectorial U_{k-1}/U_k, donde $U_k = p^k M \cap M[p]$.*

Entonces $Y = \bigcup_{i=1}^{n} Y_i$ es una p-base de M.

Demostración. Primero demostraré que $\mathrm{o}(y_{k_l}) = p^k$ para todo $1 \leqslant k \leqslant n$, $1 \leqslant l \leqslant s_k$. Fijemos una k arbitraria, por (i) tenemos que $p^k y_{k_l} = 0$ para todo $1 \leqslant l \leqslant s_k$, por (ii) tenemos que $p^{k-1}\overline{y_{k_l}} \neq \bar{0}$, ahora bien $p^{k-1}\overline{y_{k_l}} = p^{k-1}y_{k_l} + U_k$, si $p^{k-1}y_{k_l} = 0$ entonces $\overline{y_{k_l}} = 0 + U_k = \bar{0}$, lo cual es una contradicción, por lo tanto $p^{k-1}y_{k_l} \neq 0$, de donde $\mathrm{o}(y_{k_l}) = p^k$.

Sabemos que todo grupo abeliano finito es suma directa de grupos cíclicos p-primarios, entonces por el teorema 1.8 tenemos que $\mathrm{f}(k-1, M)$ es el número de sumandos cíclicos de orden p^k. Para ver que Y genera a M basta observar que el número de elementos de Y es igual al p-rango de M y que los elementos de Y tienen órdenes iguales a los p-invariantes de M, ver pag. 4.

$$\sharp(Y) = \sum_{i=1}^{n} \sharp(Y_i) = \sum_{i=1}^{n} s_i = \sum_{i=1}^{n} \mathrm{f}(i-1, M) = \mathrm{r_p}(M).$$

[1] ver [5]

Por otro lado, ya demostramos que $o(y_{k_l}) = p^k$, es decir los elementos de Y tienen órdenes iguales a los p-invariantes de M.

Por último demostraré que Y es linealmente independiente.

Para todo $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant s_i$ sean $\alpha_{i_j} \in \mathbb{Z}_{p^n}$ tales que

$$\alpha_{1_1} y_{1_1} + \cdots + \alpha_{1_{s_1}} y_{1_{s_1}} + \cdots + \alpha_{n_1} y_{n_1} + \cdots + \alpha_{n_{s_n}} y_{n_{s_n}} = 0 \tag{2.8}$$

Por demostrar que para todo $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant s_i$, $\alpha_{i_j} y_{i_j} = 0$. Primero multiplico (2.8) por p^{n-1}, de donde:

$$p^{n-1}\alpha_{n_1} y_{n_1} + \cdots + p^{n-1}\alpha_{n_{s_n}} y_{n_{s_n}} = 0 \tag{2.9a}$$

que es igual a

$$\alpha_{n_1} p^{n-1} y_{n_1} + \cdots + \alpha_{n_{s_n}} p^{n-1} y_{n_{s_n}} = 0 \tag{2.9b}$$

Como $U_n = 0$, por el inciso (ii) tenemos que $\{p^{n-1}y_{n_1}, \ldots, p^{n-1}y_{n_{s_n}}\}$ es base del $\mathbb{Z}_p$-espacio vectorial U_{n-1}, por lo tanto para toda $1 \leqslant l \leqslant s_n$, $\alpha_{n_l} \equiv 0 \pmod{p}$, es decir $\alpha_{n_l} = \alpha'_{n_l} p$, de donde (2.9a) es igual a

$$p^{n-1}\alpha'_{n_1} p y_{n_1} + \cdots + p^{n-1}\alpha'_{n_{s_n}} p y_{n_{s_n}} = 0 \tag{2.9c}$$

Más aún (2.8) es igual a

$$\alpha_{1_1} y_{1_1} + \cdots + \alpha_{1_{s_1}} y_{1_{s_1}} + \cdots + \alpha'_{n_1} p y_{n_1} + \cdots + \alpha'_{n_{s_n}} p y_{n_{s_n}} = 0 \tag{2.10}$$

Multiplicamos (2.10) por p^{n-2}, obteniendo la siguiente ecuación:

$$\begin{aligned} &p^{(n-2)}\alpha_{(n-1)_1} y_{(n-1)_1} + \cdots + p^{(n-2)}\alpha_{(n-1)_{s_{(n-1)}}} y_{(n-1)_{s_{(n-1)}}} + \\ &p^{(n-2)}\alpha'_{n_1} p y_{n_1} + \cdots + p^{(n-2)}\alpha'_{n_{s_n}} p y_{n_{s_n}} = 0 \end{aligned} \tag{2.11a}$$

que es igual a

$$\begin{aligned} &\alpha_{(n-1)_1} p^{(n-2)} y_{(n-1)_1} + \cdots + \alpha_{(n-1)_{s_{(n-1)}}} p^{(n-2)} y_{(n-1)_{s_{(n-1)}}} + \\ &\alpha'_{n_1} p^{(n-1)} y_{n_1} + \cdots + \alpha'_{n_{s_n}} p^{(n-1)} y_{n_{s_n}} = 0 \end{aligned} \tag{2.11b}$$

Como ya observamos $\{p^{n-1}y_{n_1}, \ldots, p^{n-1}y_{n_{s_n}}\}$ es base del $\mathbb{Z}_p$-espacio vectorial U_{n-1}, y por (ii) tenemos que $\{p^{n-2}\overline{y_{(n-1)_1}}, \ldots, p^{n-2}\overline{y_{(n-1)_{s_{(n-1)}}}}\}$ es base del

$\mathbb{Z}_p$-espacio vectorial U_{n-2}/U_{n-1}, por el teorema del Rango para espacios vectoriales tenemos que $\{p^{n-2}y_{(n-1)_1}, \ldots, p^{n-2}y_{(n-1)_{s_{(n-1)}}}, p^{n-1}y_{n_1}, \ldots, p^{n-1}y_{n_{s_n}}\}$ es base del $\mathbb{Z}_p$-espacio vectorial U_{n-2}, por lo tanto para toda $1 \leqslant l \leqslant s_{n-1}$, y para toda $1 \leqslant l' \leqslant s_{n-1}$ tenemos que $\alpha_{(n-1)_l} \equiv 0 \pmod{p}$, es decir $\alpha_{(n-1)_l} = \alpha''_{(n-1)_l}p$, y que $\alpha'_{n_{l'}} \equiv 0 \pmod{p}$, es decir $\alpha'_{n_{l'}} = \alpha''_{n_{l'}}p$ de donde (2.8) es igual a

$$\begin{aligned}&\alpha_{1_1}y_{1_1} + \cdots + \alpha_{1_{s_1}}y_{1_{s_1}} + \cdots + \alpha''_{(n-1)_1}py_{(n-1)_1} + \cdots + \\ &\alpha''_{(n-1)_{s_{(n-1)}}}py_{(n-1)_{s_{(n-1)}}} + \alpha''_{n_1}p^2y_{n_1} + \cdots + \alpha''_{n_{s_n}}p^2y_{n_{s_n}} = 0\end{aligned} \tag{2.12}$$

Continuando de la misma manera, en un número finito de pasos obtenemos que la ecuación (2.8) es igual a

$$\begin{aligned}\alpha_{1_1}y_{1_1} + \cdots + \alpha_{1_{s_1}}y_{1_{s_1}} + \beta_{2_1}py_{2_1} + \cdots + \beta_{2_{s_2}}py_{2_{s_2}} + \cdots + \\ \beta_{n_1}p^{n-1}y_{n_1} + \cdots + \beta_{n_{s_n}}p^{n-1}y_{n_{s_n}} = 0\end{aligned} \tag{2.13}$$

Además obtenemos que

$$\{py_{2_1}, \ldots, py_{2_{s_2}}, \ldots, p^{n-1}y_{n_1}, \ldots, p^{n-1}y_{n_{s_n}}\}$$

es base del $\mathbb{Z}_p$-espacio vectorial U_1 y por hipótesis tenemos que $\{\overline{y_{1_1}}, \ldots, \overline{y_{1_{s_1}}}\}$ es base del $\mathbb{Z}_p$-espacio vectorial U_0/U_1. Por el teorema del Rango tenemos que

$$\{y_{1_1}, \ldots, y_{1_{s_1}}, py_{2_1}, \ldots, py_{2_{s_2}}, \ldots, p^{n-1}y_{n_1}, \ldots, p^{n-1}y_{n_{s_n}}\}$$

Es base del $\mathbb{Z}_p$-espacio vectorial U_0. Por lo tanto todos los coeficientes de la ecuación (2.13) son congruentes con 0 módulo p, lo que completa la demostración. □

Definición. Para cada $1 \leqslant l \leqslant n$, definimos $\vec{v}_l$ vector en $\mathbb{Z}^n$ de la siguiente manera:

$$\begin{aligned}(\vec{v}_l)_i = \ & 0 \quad \text{si } i \notin \{l, l-1\};\ (\vec{v}_l)_l = 1;\ (\vec{v}_l)_{l-1} = -1 \quad \text{si } l \neq 1, \\ \vec{v}_l = \ & (1, 0, 0, \ldots, 0) \qquad\qquad\qquad\qquad\qquad\qquad\quad \text{si } l = 1.\end{aligned}$$

Lema 2.5. *Sea M un p-grupo abeliano finito de tipo $(s_1, \ldots, s_n)$ y sean $\{y_1, y_2, \ldots, y_r\} \subset \operatorname{Soc} M$, tales que*

1. $\forall\, i \in \{1, \ldots, r\}\ \mathrm{h_p}(y_i) = l$

2. $\{y_1, y_2, \ldots, y_r\}$ *sea linealmente independiente módulo* U_{l+1},

entonces el tipo $\underline{\mathrm{t}}(M) = \underline{\mathrm{t}}\left(M/\langle y_1, \ldots, y_r\rangle\right) + r\vec{v}_{l+1}$.

Demostración. Como $\forall\ i \in \{1, \ldots, r\}$ $\mathrm{h_p}(y_i) = l$ entonces para todo $i \in \{1, \ldots, r\}$ $\exists\ x_i$ tal que $y_i = p^l x_i$, además como $y_i \in \operatorname{Soc} M$ entonces $x_i \in M[p^{l+1}]$.

Por otro lado como $\{y_1, y_2, \ldots, y_r\}$ es linealmente independiente módulo U_{l+1}, es posible extender este conjunto a una base de U_l/U_{l+1}, digamos $p^l\overline{X_{l+1}} = \{p^l\overline{x_1}, p^l\overline{x_2}, \ldots, p^l\overline{x_r}, p^l\overline{x_{(l+1)_{(r+1)}}}, \ldots, p^l\overline{x_{(l+1)_{s_{(l+1)}}}}\}$ como $\mathbb{Z}_p$-espacio vectorial.

Por el teorema 2.4 puedo construir una p-base $X = \bigcup_{i=1}^{n} X_i$ de M, de tal forma que X_{l+1} sea precisamente el conjunto que acabamos de construir. De aqui concluimos que

$$M \cong \mathbb{Z}_{p^{l+1}}x_1 \oplus \cdots \oplus \mathbb{Z}_{p^{l+1}}x_r \oplus M_0 \text{ para algún } M_0 \leq M.$$

entonces

$$M/\langle y_1, \ldots, y_r\rangle \cong \underbrace{\mathbb{Z}_{p^l} \oplus \cdots \oplus \mathbb{Z}_{p^l}}_{\text{r veces}} \oplus M_0.$$

Por lo tanto

$$\underline{\mathrm{t}}\left(M/\langle y_1, \ldots, y_r\rangle\right) = (0, \ldots, 0, \overset{l}{r}, 0, \ldots, 0) + \underline{\mathrm{t}}(M_0),$$

De donde concluimos que

$$\begin{aligned}
\underline{\mathrm{t}}\left(M/\langle y_1, \ldots, y_r\rangle\right) + r\vec{v}_{l+1} &= \underline{\mathrm{t}}(M_0) + (0, \ldots, 0, \overset{l}{r}, 0, \ldots, 0) \\
&\quad + (0, \ldots, 0, \overset{l}{-r}, r, 0, \ldots, 0) \\
&= \underline{\mathrm{t}}(M_0) + (0, \ldots, 0, \overset{l+1}{r}, 0, \ldots, 0) \\
&= \underline{\mathrm{t}}(M).
\end{aligned}$$

□

Corolario 2.6. *Dado* M *grupo finito p-primario y* $y \in \operatorname{Soc} M$ *tal que* $\mathrm{h_p}(y) = l$, *entonces* $\underline{\mathrm{t}}(M) = \underline{\mathrm{t}}\left(M/\langle y\rangle\right) + \vec{v}_{l+1}$.

2.3 Caracterización de Λ-módulos cadena abierta de tipo $\mathscr{C} = (i, j)$

Teorema 2.7. *Sea $M = \mathscr{C}(a)$ un Λ-módulo cadena abierta de la forma $\mathscr{C} = (i, j)$, generado por a. Si ponemos $i = t(p-1) + r$ tal que $0 < r \leqslant p-1$, entonces:*

$$\text{si } p > i \qquad M \cong (i-1)\mathbb{Z}_p \oplus \mathbb{Z}_{p^j} \tag{2.14a}$$

$$\text{si } p \leqslant i \ \ y \ \ t \geqslant j \qquad M \cong \mathbb{Z}_{p^{j-1}} \oplus r\mathbb{Z}_{p^{t+1}} \oplus (p-r-1)\mathbb{Z}_{p^t} \tag{2.14b}$$

$$\text{si } p \leqslant i \ \ y \ t < j \qquad M \cong \mathbb{Z}_{p^j} \oplus (r-1)\mathbb{Z}_{p^{t+1}} \oplus (p-r)\mathbb{Z}_{p^t} \tag{2.14c}$$

Más aún M tiene orden p^{i+j-1}.

Demostración. Suponemos $p > i$.

Sea $m \in M$ por la ecuación (2.7) $m = \alpha a + \sum_{t=1}^{i-1} \beta_t \phi^t a + \sum_{t=1}^{j-1} \gamma_t \pi^t a$.

Por otro lado, recordamos que $p = \pi + \phi^{p-1}\sigma(\phi)$, pero como por hipótesis $p > i$, entonces evaluado en M tenemos que $p = \pi$.

Entonces $pm = \pi m = \alpha\pi a + \sum_{t=2}^{j-1} \gamma_{t-1}\pi^t a$, por lo tanto si $pm = 0$, entonces $\alpha = 0$ y $\forall\ 1 \leqslant t \leqslant j-2 \quad \gamma_t = 0$, pues la descomposición (2.7) es única. Por lo tanto

$$M[p] = \left\langle \phi a, \ldots, \phi^{i-1}a, \pi^{j-1}a \right\rangle.$$

Además

$$\begin{aligned} pM &= \left\langle \pi a, \pi^2 a, \ldots, \pi^{j-1}a \right\rangle, \\ p^2 M &= \left\langle \pi^2 a, \ldots, \pi^{j-1}a \right\rangle, \\ &\vdots \\ p^{j-1}M &= \left\langle \pi^{j-1}a \right\rangle. \end{aligned}$$

Entonces para toda $j \geqslant 2$, tenemos que

$$M[p] \supset M[p] \cap pM = \cdots = M[p] \cap p^{j-1}M = \left\langle \pi^{j-1}a \right\rangle \supset M[p] \cap p^j M = 0.$$

Por lo tanto para todo $j \geqslant 2$ la sucesión de Ulm para M es

$$\begin{aligned} U_0/U_1 &= \langle \phi a, \ldots, \phi^{i-1} a \rangle \\ U_1/U_2 &= 0 \\ &\vdots \\ U_{j-2}/U_{j-1} &= 0 \\ U_{j-1}/U_j &= \langle \pi^{j-1} a \rangle \end{aligned}$$

De donde concluimos que

$$M \cong (i-1)\mathbb{Z}_p \oplus \mathbb{Z}_{p^j}.$$

Si $j = 1$ entonces $M = M[p] \cong i\mathbb{Z}_p = (i-1)\mathbb{Z}_p \oplus \mathbb{Z}_{p^j}$, lo cual termina la demostración para el caso (2.14a).

Suponemos $p \leqslant i$.

Probaré este resultado utilizando inducción sobre la *longitud*[2] de M.

En el caso $p = i$, $j = 1$, tenemos que

$$M = \langle \phi^{p-1} a, \ldots, \phi a, a \rangle,$$

Si $m = \alpha a + \sum_{t=1}^{i-1} \beta_t \phi^t a$, como $pm = \pi m + \phi^{p-1}\sigma(\phi)m = \phi^{p-1}(c_0 + c_1\phi + \cdots + c_{p-1}\phi^{p-1})m = c_0\phi^{p-1}m$, entonces $pm = c_0\alpha\phi^{p-1}a$.

Por lo tanto

$$pM = \langle \phi^{p-1} a \rangle,$$

Además si $pm = 0$ entonces $\alpha = 0$, por lo tanto

$$M[p] = \langle \phi^{p-1} a, \ldots, \phi a \rangle.$$

De donde

$$M[p] \supset pM \cap M[p] = \langle \phi^{p-1} a \rangle \supset p^2 M \cap M[p] = 0.$$

Por lo tanto la sucesión de Ulm de M es:

$$\begin{aligned} U_0/U_1 &= \langle \phi a, \ldots, \phi^{p-2} a \rangle \\ U_1/U_2 &= \langle \phi^{p-1} a \rangle \end{aligned}$$

[2]la *longitud* de M es la longitud de la *serie de composición* de M, ver capítulo 4 de [2].

Por lo anterior, como $i = p = (p-1)+1$ entonces $t = r = j = 1$ y

$$M \cong \mathbb{Z}_{p^2} \oplus (p-2)\mathbb{Z}_p \quad \text{que corresponde al caso (2.14b).}$$

Tomemos M arbitraria y asumamos que la proposición es válida para toda M' tal que $l(M') < l(M)$, donde $l(M)$ es la longitud de M. Demostraremos el resultado para M.

Recordamos que $p \leqslant i$.

(a) Suponemos $t < j-1$.

Sea $\bar{M} = M/\langle \pi^{j-1}a \rangle$. Afirmamos que $\mathrm{h_p}(\pi^{j-1}a) = j-1$, para ello basta observar las siguientes igualdades:

$$\begin{aligned} pa &= \pi a + \phi^{p-1}\sigma(\phi)a \\ &\vdots \\ p^{j-1}a &= \pi^{j-1}a + \phi^{(p-1)(j-1)}\sigma(\phi)^{j-1}a \end{aligned}$$

Como $i = t(p-1)+r$ con $0 < r \leqslant p-1$ entonces $(j-1)(p-1) \geqslant i$, por lo tanto $p^{j-1}a = \pi^{j-1}a$, es decir $\mathrm{h_p}(\pi^{j-1}a) = j-1$.

Por el corolario 2.6 $\underline{\mathrm{t}}\,(M/\langle \pi^{j-1}a \rangle) = \underline{\mathrm{t}}(M) - \vec{v}_j$. Por otro lado $\bar{M}$ tiene la forma $\mathscr{C}' = (i, j-1)$ con $j-1 > t$.

Por inducción utilizando (2.14c) tenemos que

$$\bar{M} \cong \mathbb{Z}_{p^{j-1}} \oplus (r-1)\mathbb{Z}_{p^{t+1}} \oplus (p-r)\mathbb{Z}_{p^t}.$$

Entonces

$$M \cong \mathbb{Z}_{p^j} \oplus (r-1)\mathbb{Z}_{p^{t+1}} \oplus (p-r)\mathbb{Z}_{p^t}.$$

Por lo tanto para $p \leqslant i$, $t < j-1$ se cumple el teorema.

(b) Supongamos ahora que $t > j-1$

Sea $\bar{M} = M/\langle \phi^{i-1}a \rangle$. Afirmamos que $\mathrm{h_p}(\phi^{i-1}a) = t$, para ello basta observar las siguientes igualdades:

$$\begin{aligned} pa &= \pi a + \phi^{p-1}\sigma(\phi)a \\ &\vdots \\ p^t a &= \pi^t a + \phi^{t(p-1)}\sigma(\phi)^t a \end{aligned}$$

Como $t \geqslant j$ entonces $\pi^t a = 0$, por lo tanto $p^t a = \phi^{t(p-1)}\sigma(\phi)^t a$, de donde $p^t\phi^{r-1}a = \phi^{i-r}\sigma(\phi)^t\phi^{r-1}a = \phi^{i-1}c_0 a$, donde c_0 es el coeficiente constante de $\sigma(\phi)^t$ y como es invertible entonces $p^t c_0^{-1}\phi^{r-1}a = \phi^{i-1}a$ es decir $\mathrm{h}_{\mathrm{p}}(\phi^{i-1}a) = t$.

Por el corolario 2.6 $\underline{\mathrm{t}}\,(M/\langle\phi^{i-1}a\rangle) = \underline{\mathrm{t}}(M) - \vec{v}_{t+1}$. Por otro lado $\bar{M}$ tiene la forma $\mathscr{C}' = (i-1, j)$, con $t \geqslant j$.

Si $r > 1$, entonces $i - 1 = t(p-1) + (r-1)$.

Por inducción utilizando (2.14b) tenemos que

$$\bar{M} \cong \mathbb{Z}_{p^{j-1}} \oplus (r-1)\mathbb{Z}_{p^{t+1}} \oplus (p-r)\mathbb{Z}_{p^t}.$$

Entonces

$$M \cong \mathbb{Z}_{p^{j-1}} \oplus r\mathbb{Z}_{p^{t+1}} \oplus (p-r-1)\mathbb{Z}_{p^t}.$$

Si $r = 1$ entonces $i - 1 = (t-1)(p-1) + (p-1)$.

Suponemos $t > j$. Si $p > i - 1$ es decir $p = i$ entonces $i - 1 = p - 1 = 0(p-1) + p - 1$, de donde $j < t = 0$ lo cual es imposible. Por lo tanto estamos en el caso $p \leqslant i - 1$, $t > j$.

Por inducción utilizando (2.14b) tenemos que

$$\bar{M} \cong \mathbb{Z}_{p^{j-1}} \oplus (p-1)\mathbb{Z}_{p^t}$$

Entonces

$$M \cong \mathbb{Z}_{p^{j-1}} \oplus (p-2)\mathbb{Z}_{p^t} \oplus \mathbb{Z}_{p^{t+1}}.$$

Si $j = t$ entonces $t - 1 < j$, además como ya observamos $p \leqslant i - 1$, entonces por inducción utilizando (2.14c) tenemos que

$$\bar{M} \cong \mathbb{Z}_{p^j} \oplus (p-2)\mathbb{Z}_{p^t} \oplus \mathbb{Z}_{p^{t-1}}$$

Entonces

$$M \cong (p-2)\mathbb{Z}_{p^t} \oplus \mathbb{Z}_{p^{t-1}} \oplus \mathbb{Z}_{p^{t+1}}.$$

que es el caso (2.14b) con $j = t$ y $r = 1$.

Por lo tanto el teorema se cumple para el caso (2.14b).

(c) Supongamos que $j-1=t$ es decir $t<j$

Suponemos $r=1$.

Sea $\bar{M}=M/\langle\phi^{i-1}a\rangle$. Afirmamos que $\mathrm{h_p}(\phi^{i-1}a)=t-1$, para ello basta observar las siguientes igualdades:

$$\begin{aligned}
pa &= \pi a+\phi^{p-1}\sigma(\phi)a\\
&\vdots\\
p^{t-1}a &= \pi^{t-1}a+\phi^{(t-1)(p-1)}\sigma(\phi)^{t-1}a\\
p^{t-1}\phi^{p-1}a &= \phi^{(t-1)(p-1)+(p-1)}\sigma(\phi)^{t-1}a\\
p^{t-1}\phi^{p-1}a &= \phi^{(t)(p-1)}\sigma(\phi)^{t-1}a\\
p^{t-1}\phi^{p-1}a &= \phi^{i-1}\sigma(\phi)^{t-1}a\\
p^{t-1}\phi^{p-1}a &= \phi^{i-1}c_0a
\end{aligned}$$

Donde c_0 es el coeficiente constante de $\sigma(\phi)^{t-1}$ y como es invertible entonces $p^{t-1}c_0^{-1}\phi^{r-1}a=\phi^{i-1}a$ es decir $\mathrm{h_p}(\phi^{i-1}a)=t-1$.

Por el corolario 2.6 $\underline{\mathrm{t}}\,(M/\langle\phi^{i-1}a\rangle)=\underline{\mathrm{t}}(M)-\vec{v}_t$. Por otro lado $\bar{M}$ tiene la forma $\mathscr{C}'=(i-1,j)$, con $i-1=(t-1)(p-1)+p-1$, $t-1<j$.

Si $p=i$ es decir $p>i-1$ entonces $i-1=p-1=0(p-1)+p-1$, de donde $t-1=0$ es decir $t=1$.

Entonces por inducción utilizando (2.14a) tenemos que

$$\bar{M}\cong\mathbb{Z}_{p^j}\oplus(i-2)\mathbb{Z}_p$$

Por lo tanto, recordando que $\vec{v}_1=(1,0,\ldots,0)$

$$M\cong\mathbb{Z}_{p^j}\oplus(i-1)\mathbb{Z}_p.$$

que es el caso (2.14c) con $p=i$, $j>t=1$, $r=1$.

Si $p<i$ es decir $p\leqslant i-1$, entonces por inducción utilizando (2.14c) tenemos que

$$\bar{M}\cong\mathbb{Z}_{p^j}\oplus(p-2)\mathbb{Z}_{p^t}\oplus\mathbb{Z}_{p^{t-1}}$$

Entonces

$$M\cong\mathbb{Z}_{p^j}\oplus(p-1)\mathbb{Z}_{p^t}$$

que es el caso (2.14c) con $r = 1$.

Suponemos $r > 1$.

Sea $\bar{M} = M/\langle \phi^{i-1}a \rangle$. Afirmamos que $\mathrm{h_p}(\phi^{i-1}a) = t$, para ello basta observar las siguientes igualdades:

$$\begin{aligned} pa &= \pi a + \phi^{p-1}\sigma(\phi)a \\ &\vdots \\ p^t a &= \pi^t a + \phi^{t(p-1)}\sigma(\phi)^t a \\ p^t\phi^{r-1}a &= \phi^{t(p-1)}\sigma(\phi)^t\phi^{r-1}a \\ p^t\phi^{r-1}a &= \phi^{i-1}\sigma(\phi)^t\phi^{r-1}a \\ p^t\phi^{r-1}a &= \phi^{i-1}c_0 a \end{aligned}$$

Donde c_0 es el coeficiente constante de $\sigma(\phi)^t$ y como es invertible entonces $p^t c_0^{-1}\phi^{r-1}a = \phi^{i-1}a$ es decir $\mathrm{h_p}(\phi^{i-1}a) = t$.

Por el corolario 2.6 $\underline{\mathrm{t}}\,(M/\langle \phi^{i-1}a \rangle) = \underline{\mathrm{t}}(M) - \vec{v}_{t+1}$. Por otro lado $\bar{M}$ tiene la forma $\mathscr{C}' = (i-1, j)$, con $t < j$. Como $r > 1$, entonces $i - 1 = t(p-1) + (r-1)$.

Si $p = i$ entonces $i = 1(i-1) + 1$, de donde $r = 1$ lo cual es imposible pues por hipótesis $r > 1$.

Si $p < i$, es decir $p \leqslant i - 1$ entonces por inducción utilizando (2.14c) tenemos que

$$\bar{M} \cong \mathbb{Z}_{p^j} \oplus (r-2)\mathbb{Z}_{p^{t+1}} \oplus (p-r+1)\mathbb{Z}_{p^t}.$$

Entonces

$$M \cong \mathbb{Z}_{p^j} \oplus (r-1)\mathbb{Z}_{p^{t+1}} \oplus (p-r)\mathbb{Z}_{p^t}.$$

por lo que el teorema se cumple para $j - 1 = t$. Con lo cual terminamos la demostración del caso (2.14c).

□

A continuación presentamos algunos ejemplos de Λ-módulos cadena abierta de tipo $\mathscr{C} = (i, j)$ y su $\mathbb{Z}_{p^n}$-estructura obtenida a partir de este teorema, estos ejemplos son importantes pues a través de ellos ejemplificaremos todos los resultados de esta tesis conforme vayamos enunciándolos.

Ejemplos.

1. $p = 7$, $n = 3$, $\mathscr{C} = (\overset{i}{6}, \overset{j}{3})$, $i = \overset{t}{0}(p-1) + \overset{r}{6}$. Como $p > i$ entonces $p = \pi$; y además por la ecuación (2.14a) tenemos que

$$M \cong \mathbb{Z}_{p^3} \oplus 5\mathbb{Z}_p$$

2. $p = 5$, $n = 4$, $\mathscr{C} = (\overset{i}{4}, \overset{j}{4})$, $i = \overset{t}{0}(p-1) + \overset{r}{4}$. Como $p > i$ entonces $p = \pi$; y además por la ecuación (2.14a) tenemos que

$$M \cong \mathbb{Z}_{p^4} \oplus 3\mathbb{Z}_p$$

3. $p = 3$, $n = 4$, $\mathscr{C} = (\overset{i}{7}, \overset{j}{3})$, $i = \overset{t}{3}(p-1) + \overset{r}{1}$, utilizando el lema 2.1 tenemos que $p = \pi + 2\phi^2 + \phi^3$. Como $p \leqslant i$ y $t \geqslant j$ entonces por la ecuación (2.14b) tenemos que

$$M \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^4} \oplus \mathbb{Z}_{p^3}$$

4. $p = 3$, $n = 4$, $\mathscr{C} = (\overset{i}{9}, \overset{j}{4})$, $i = \overset{t}{4}(p-1) + \overset{r}{1}$, utilizando el lema 2.1 tenemos que $p = \pi + 2\phi^2 + \phi^3$. Como $p \leqslant i$ y $t \geqslant j$ entonces por la ecuación (2.14b) tenemos que

$$M \cong \mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^5} \oplus \mathbb{Z}_{p^4}$$

5. $p = 5$, $n = 2$, $\mathscr{C} = (\overset{i}{7}, \overset{j}{2})$, $i = \overset{t}{1}(p-1) + \overset{r}{3}$, utilizando el lema 2.1 tenemos que $p = \pi + 4\phi^4 + 2\phi^5 + 3\phi^6$. Como $p \leqslant i$ y $t < j$ entonces por la ecuación (2.14c) tenemos que

$$M \cong 3\mathbb{Z}_{p^2} \oplus 2\mathbb{Z}_p$$

6. $p = 3$, $n = 5$, $\mathscr{C} = (\overset{i}{7}, \overset{j}{5})$, $i = \overset{t}{3}(p-1) + \overset{r}{1}$, utilizando el lema 2.1 tenemos que $p = \pi + 2\phi^2 + \phi^3$. Como $p \leqslant i$ y $t < j$ entonces por la ecuación (2.14c) tenemos que

$$M \cong \mathbb{Z}_{p^5} \oplus 2\mathbb{Z}_{p^3}$$

Teorema 2.8. *Sea $M = \mathscr{C}(a)$ un Λ-módulo cadena abierta de la forma $\mathscr{C} = (i, j)$, generado por a. Entonces M es un p-grupo abeliano finito generado por $X = \{a, \phi a, \ldots, \phi^{i-1}a, \pi a, \ldots, \pi^{j-1}a\}$ y con relaciones de definición*

$$\Delta = \{pa = \pi a - \phi^{p-1}\sigma(\phi)a,\ p\phi a = \phi^{p-1}\sigma(\phi)\phi a, \ldots, p\phi^{i-1}a = 0,$$
$$p\pi a = \pi^2 a, \ldots, p\pi^{j-2}a = \pi^{j-1}a,\ p\pi^{j-1}a = 0\}.$$

Demostración. La primera parte es una consecuencia inmediata del teorema 2.3, por lo que sólo resta demostrar que Δ es conjunto de relaciones de definición.

Sean $x, y \in M$, por la ecuación (2.7) tenemos que

$$x = \alpha a + \sum_{k=1}^{i-1} \alpha_k \phi^k a + \sum_{l=1}^{j-1} \beta_l \pi^l a$$
$$y = \gamma a + \sum_{k=1}^{i-1} \gamma_k \phi^k a + \sum_{l=1}^{j-1} \delta_l \pi^l a$$

con $0 \leqslant \alpha,\ \alpha_k,\ \beta_l,\ \gamma_k,\ \delta_l < p$, para toda $k \in [1, i-1]$, $l \in [1, j-1]$. Primero demostraremos que

$$x + y = \lambda_0 a + \sum_{k=1}^{i-1} \lambda_k \phi^k a + \sum_{l=1}^{j-1} \mu_l \pi^l a$$

con $0 \leqslant \lambda_k,\ \mu_l < p$, para toda $k \in [0, i-1]$, $l \in [1, j-1]$, utilizando las relaciones en Δ. Esto es un resultado inmediato del lema 2.1 inciso (v), ya que este demuestra que $\sigma(\phi)$ tiene coeficientes menores que p, por lo tanto si en la suma $x + y$, aparece algún término con coeficiente mayor o igual a p, digamos ν_s entonces $\nu_s = p + r_s$ con $r_s < p$, y utilizando la ecuación correspondiente en Δ, sustituimos este término por una expresión en π y ϕ, con coeficientes menores que p.

Sea $\Gamma(\boldsymbol{X})$ el grupo abeliano libre sobre $\mathbb{Z}_{p^n}$, es decir el $\mathbb{Z}_{p^n}$-módulo libre, generado por $\boldsymbol{X} = \{x_1, \ldots, x_i, y_1, \ldots, y_{j-1}\}$. Observamos que existe una biyección $\eta : \boldsymbol{X} \to X$, dada por $\eta(x_1) = a$; $\eta(x_k) = \phi^{k-1}a$, con $2 \leqslant k \leqslant i$; $\eta(x_l) = \pi^l a$, con $1 \leqslant l \leqslant j-1$.

Extendemos esta biyección a $\Gamma(\boldsymbol{X})$ de tal forma que sea un morfismo de grupos abelianos.

$$\begin{array}{rccc} \hat{\eta}: & \Gamma(\boldsymbol{X}) & \to & M \\ & \sum_{k=1}^{i} \alpha_k x_k + \sum_{k=1}^{j-1} \beta_k y_k & \mapsto & \sum_{k=0}^{i-1} \alpha_{k+1} \phi^k a + \sum_{k=1}^{j-1} \beta_k \pi^k a \end{array}$$

Suponemos que $\sigma(\phi) = -1 + c_1\phi + \cdots + c_{n(p-1)}\phi^{n(p-1)}$. Probaremos que $\ker(\hat{\eta})$ está generado por los siguientes elementos de $\Gamma(\boldsymbol{X})$:

$$\begin{aligned}
r_1 &= px_1 - y_1 + x_p - c_1x_{p+1} - \cdots - c_{i-p}x_i \\
r_2 &= px_2 + x_{p+1} - c_1x_{p+2} - \cdots - c_{i-p-1}x_i \\
&\vdots \\
r_i &= px_i \\
r_{i+1} &= py_1 - y_2 \\
r_{i+2} &= py_2 - y_3 \\
&\vdots \\
r_{i+j-1} &= py_{j-1}
\end{aligned}$$

Sea $\Delta_1 = \{r_1, \ldots, r_{i+j-1}\}$. Observamos que $\Delta_1 \subset \ker(\hat{\eta})$, luego $\langle\Delta_1\rangle \subset \ker(\hat{\eta})$. Por otra parte, supongamos que $\hat{\eta}(m) = \hat{\eta}(\sum_{k=1}^{i}\alpha_k x_k + \sum_{k=1}^{j-1}\beta_k y_k) = 0$, entonces si llamamos $\phi^0 a = a$ tenemos que

$$\sum_{k=0}^{i-1}\alpha_{k+1}\phi^k a + \sum_{k=1}^{j-1}\beta_k\pi^k a = 0$$

Si $0 \leqslant \alpha_k < p$ y $0 \leqslant \beta_k < p$, entonces por el teorema 2.3 $\alpha_1 = \cdots = \alpha_i = \beta_1 = \cdots = \beta_{j-1} = 0$, por lo que $m = 0$.

Por otro lado, si suponemos que existen coeficientes mayores o iguales que p entonces ponemos $\alpha_k = \bar{\alpha}_k p + \alpha_k'$ para toda $k \in [1, i]$ y $\beta_k = \bar{\beta}_k p + \beta_k'$ para toda $k \in [1, j-1]$, con $0 \leqslant \alpha_k' < p$ y $0 \leqslant \beta_k' < p$, entonces

$$\hat{\eta}(m) = p(\sum_{k=0}^{i-1}\bar{\alpha}_{k+1}\phi^k a + \sum_{k=1}^{j-1}\bar{\beta}_k\pi^k a) + \sum_{k=0}^{i-1}\alpha_{k+1}'\phi^k a + \sum_{k=1}^{j-1}\beta_k'\pi^k a$$

Sea ahora

$$\hat{\eta}(m - \sum_{k=1}^{i}\bar{\alpha}_k r_k - \sum_{k=i+1}^{i+j-1}\bar{\beta}_{k-i}r_k) = \sum_{k=0}^{i-1}\alpha_{k+1}''\phi^k a + \sum_{k=1}^{j-1}\beta_k''\pi^k a$$

Si de nuevo tenemos que en esta expresión hay coeficientes mayores o iguales a p, entonces realizamos el mismo procedimiento hasta obtener

$$\hat{\eta}(m - \sum_{k=1}^{i}\bar{\alpha}_k^{(l)} r_k - \sum_{k=i+1}^{i+j-1}\bar{\beta}_{k-i}^{(l)}r_k) = \sum_{k=0}^{i-1}\alpha_{k+1}^{(l)}\phi^k a + \sum_{k=1}^{j-1}\beta_k^{(l)}\pi^k a$$

Con $0 \leqslant \alpha_k^{(l)} < p$, $0 \leqslant \beta_k^{(l)} < p$, y como

$$\hat{\eta}(m - \sum_{k=1}^{i} \bar{\alpha}_k^{(l)} r_k - \sum_{k=i+1}^{i+j-1} \bar{\beta}_{k-i}^{(l)} r_k) = 0$$

entonces $\alpha_s^{(l)} = \beta_s^{(l)} = 0$, para toda s. Luego

$$m - \sum_{k=1}^{i} \bar{\alpha}_k^{(l)} r_k - \sum_{k=i+1}^{i+j-1} \bar{\beta}_{k-i}^{(l)} r_k = 0$$

Por lo tanto

$$m = \sum_{k=1}^{i} \bar{\alpha}_k^{(l)} r_k - \sum_{k=i+1}^{i+j-1} \bar{\beta}_{k-i}^{(l)} r_k$$

Es decir $m \in \langle \Delta_1 \rangle$, de donde $\ker(\hat{\eta}) \subset \langle \Delta_1 \rangle$ lo cual demuestra el teorema. $\square$

Capítulo 3

p-base de un $\mathbb{Z}_{p^n}C_p$-módulo cadena abierta de la forma $\mathscr{C} = (i, j)$

Aquí profundizamos en la teoría desarrollada por Aviñó y Bautista en [5], demostrando un teorema que muestra explícitamente una p-base de un $\mathbb{Z}_{p^n}C_p$-módulo cadena abierta la forma $\mathscr{C} = (i, j)$.

Teorema 3.1. *Sea $M = \mathscr{C}(a)$ un Λ-módulo cadena abierta de la forma $\mathscr{C} = (i, j)$, generado por a. Si ponemos $i = t(p-1) + r$ tal que $0 < r \leqslant p-1$, entonces:*

$$si\ p > i \qquad Y = \{a, \phi a, \ldots, \phi^{i-1}a\} \tag{3.1a}$$

$$si\ p \leqslant i\ \ y\ si\ \ t \geqslant j \qquad Y = \{a, \phi a, \ldots, \phi^{p-2}a, \pi a\} \tag{3.1b}$$

$$si\ p \leqslant i\ \ y\ si\ t < j \qquad Y = \{a, \phi a, \ldots, \phi^{p-1}a\} \tag{3.1c}$$

es una p-base de M.

Demostración. Caso (3.1a): suponemos $p > i$.

Por el teorema 2.7 tenemos que

$$exp(M) = p^j \ \text{ y } \ \underline{t}(M) = (i-1, 0, \ldots, 0, \overset{j}{1})$$

Sean

$$Y_1 = \{\phi a, \ldots, \phi^{i-1}a\}$$
$$\vdots$$
$$Y_j = \{a\}$$

Sea $m \in M$ por la ecuación (2.7) $m = \alpha a + \sum_{t=1}^{i-1} \beta_t \phi^t a + \sum_{t=1}^{j-1} \gamma_t \pi^t a$.

Por otro lado, recordamos que $p = \pi + \phi^{p-1}\sigma(\phi)$, pero como por hipótesis $p > i$, entonces $p = \pi$.

Entonces $pm = \pi m = \alpha\pi a + \sum_{t=2}^{j-1} \gamma_{t-1}\pi^t a$, por lo tanto si $pm = 0$, entonces $\alpha = 0$ y $\gamma_t = 0$, para todo $1 \leqslant t \leqslant j-2$, pues la descomposición (2.7) es única. Por lo tanto

$$M[p] = \langle \phi a, \ldots, \phi^{i-1}a, \pi^{j-1}a \rangle .$$

Además

$$\begin{aligned} pM &= \langle \pi a, \pi^2 a, \ldots, \pi^{j-1}a \rangle , \\ p^2M &= \langle \pi^2 a, \ldots, \pi^{j-1}a \rangle , \\ &\vdots \\ p^{j-1}M &= \langle \pi^{j-1}a \rangle . \end{aligned}$$

Entonces para toda $j \geqslant 2$, tenemos que

$$M[p] \supset M[p] \cap pM = \cdots = M[p] \cap p^{j-1}M = \langle \pi^{j-1}a \rangle \supset M[p] \cap p^jM = 0.$$

Sabemos que tanto U_0, como U_0/U_1 son $\mathbb{Z}_p$-espacios vectoriales, por lo que utilizando el *teorema del Rango* para espacios vectoriales llegamos a que $\overline{Y_1}$ es base de $U_0/U_1 = M[p]/\langle \pi^{j-1}a \rangle$.

Para demostrar que $p^{j-1}\overline{Y_j} = \{p^{j-1}\bar{a}\}$ es base de $U_{j-1}/U_j \cong U_{j-1} = \langle \pi^{j-1}a \rangle$, es suficiente observar que:

$$p^{j-1}\bar{a} \cong p^{j-1}a = \pi^{j-1}a$$

Por el teorema 2.4 tenemos que

$$Y = Y_1 \cup Y_j \text{ es una } p\text{-base de } M.$$

Caso (3.1b): suponemos $p \leqslant i$, $t \geqslant j$.

Por el teorema 2.7 tenemos que

$$M \cong \mathbb{Z}_{p^{j-1}} \oplus r\mathbb{Z}_{p^{t+1}} \oplus (p-r-1)\mathbb{Z}_{p^t}$$

Por lo tanto

$$exp(M) = p^{t+1}$$

y además

$$\underline{t}(M) = (0, \ldots, 0, \overset{j-1}{1}, 0, \ldots, 0, p - \overset{t}{r} - 1, r).$$

Definimos

$$\begin{aligned} Y_{j-1} &= \{\pi a\} \\ Y_t &= \{\phi^r a, \phi^{r+1} a, \ldots, \phi^{p-2} a\} \\ Y_{t+1} &= \{a, \phi a, \ldots, \phi^{r-1} a\} \end{aligned}$$

$p^{j-1}\pi a = \pi^j a = 0$, entonces

$$Y_{j-1} \subset M[p^{j-1}]$$

$p^t \phi^r a = \phi^{t(p-1)} \sigma(\phi)^t \phi^r a = \phi^{t(p-1)+r} \sigma(\phi)^t a = \phi^i \sigma(\phi)^t a = 0$, además para toda $r \leqslant k \leqslant p-2$, tenemos que $k = r + \eta_k$, con $\eta_k \geqslant 0$, entonces $p^t \phi^k a = p^t \phi^{r+\eta_k} a = \phi^i \sigma(\phi)^t \phi^{\eta_k} a = 0$, por lo tanto

$$Y_t \subset M[p^t]$$

$p^{t+1} a = \phi^{(t+1)(p-1)} \sigma(\phi)^{t+1} a = \phi^{i+(p-1-r)} \sigma(\phi)^{t+1} a = 0$, además para toda $0 \leqslant k \leqslant r-1$, tenemos que $p^{t+1} \phi^k a = \phi^{i+(p-1-r)} \sigma(\phi)^{t+1} \phi^k a = 0$, por lo tanto

$$Y_{t+1} \subset M[p^{t+1}]$$

Demostraré que $p^t \overline{Y_{t+1}}$ es base de $U_t / U_{t+1} \cong U_t$.

Sabemos que $\mathrm{f}(t, M) = r$, y es claro que $\sharp(p^t \overline{Y_{t+1}}) = r$, por lo tanto basta demostrar que $p^t \overline{Y_{t+1}}$ es linealmente independiente. Como $U_{t+1} = 0$ entonces basta demostrar que $p^t Y_{t+1}$ es linealmente independiente.

$$\begin{aligned} p^t \phi^{r-1} a &= \phi^{t(p-1)+r-1} \sigma(\phi)^t a = \phi^{i-1}(c_0 + c_1 \phi + \cdots) a = c_0 \phi^{i-1} a \\ p^t \phi^{r-2} a &= \phi^{i-2}(c_0 + c_1 \phi + \cdots) a = c_0 \phi^{i-2} a + c_1 \phi^{i-1} a \\ &\vdots \\ p^t \phi a &= \phi^{i-(r-1)}(c_0 + c_1 \phi + \cdots) a \\ &= c_0 \phi^{i-r+1} a + c_1 \phi^{i-r+2} a + \cdots + c_{r-2} \phi^{i-1} a \\ p^t a &= \phi^{i-r}(c_0 + c_1 \phi + \cdots) a \\ &= c_0 \phi^{i-r} a + c_1 \phi^{i-r+1} a + \cdots + c_{r-1} \phi^{i-1} a \end{aligned}$$

Por la unicidad de la ecuación (2.7) se deduce que

$$L_1 = \{\phi^{i-r}a, \phi^{i-r+1}a, \ldots, \phi^{i-1}a\}$$

es linealmente independiente.

Sea $T : U_t/U_{t+1} \to U_t/U_{t+1}$, la transformación lineal definida por

$$\begin{aligned} T(\phi^{i-r}a) &= p^t a \\ T(\phi^{i-r+1}a) &= p^t \phi a \\ &\vdots \\ T(\phi^{i-1}a) &= p^t \phi^{r-1} a \end{aligned} \tag{3.2}$$

Sea C la matriz asociada a T en la base L_1 es decir

$$C := \begin{pmatrix} c_0 & 0 & 0 & \ldots & 0 \\ c_1 & c_0 & 0 & \ldots & 0 \\ c_2 & c_1 & c_0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{r-1} & c_{r-2} & c_{r-3} & \ldots & c_0 \end{pmatrix}$$

Por la definición de C es claro que

$$\begin{aligned} C\phi^{i-r}a &= p^t a \\ C\phi^{i-r+1}a &= p^t \phi a \\ &\vdots \\ C\phi^{i-1}a &= p^t \phi^{r-1} a \end{aligned} \tag{3.3}$$

Por el lema 2.1 sabemos que si $\sigma(\phi) = a_0 + a_1\phi + \cdots + a_{p-1}\phi^{p-1}$, entonces $a_0 \equiv -1 \pmod{p}$. Por lo tanto $c_0 \equiv (-1)^t \pmod{p}$, y como C es una matriz con r renglones entonces, $\det(C) \equiv (-1)^{tr} \pmod{p}$, es decir C es invertible.

Por lo tanto C es una matriz de cambio de base, lo cual demuestra que

$$\{p^t a, p^t \phi a, \ldots, p^t \phi^{r-1} a\}$$

es linealmente independiente.

Por lo tanto $p^t \overline{Y_{t+1}}$ es base de U_t/U_{t+1}.

Demostraré que $p^{t-1}\overline{Y_t}$ es base de U_{t-1}/U_t.

Sabemos que $\mathrm{f}(t-1, M) = p-r-1$, por lo tanto basta demostrar que $p^{t-1}\overline{Y_t}$ es linealmente independiente, pues además demostraríamos que $\sharp(p^{t-1}\overline{Y_t}) = p-r-1$.

$$\begin{aligned} p^{t-1}\overline{\phi^r a} &= \overline{\phi^{(t-1)(p-1)+r}\sigma(\phi)^{t-1}a} = \overline{\phi^{i-(p-1)}(b_0 + b_1\phi + \cdots)a} \\ &= b_0\overline{\phi^{i-(p-1)}a} + b_1\overline{\phi^{i-p+2}a} + \cdots + b_{p-2}\overline{\phi^{i-1}a} \end{aligned}$$

De las ecuaciones (3.3) se deduce que $\{\phi^{i-r}a, \ldots, \phi^{i-1}a\} \subset U_t$, por lo que

$$\begin{aligned} p^{t-1}\overline{\phi^r a} &= b_0\overline{\phi^{i-(p-1)}a} + b_1\overline{\phi^{i-p+2}a} + \cdots + b_{p-r-2}\overline{\phi^{i-r-1}a} \\ p^{t-1}\overline{\phi^{r+1}a} &= \overline{\phi^{i-p+2}(b_0 + b_1\phi + \cdots)a} \\ &= b_0\overline{\phi^{i-p+2}a} + b_1\overline{\phi^{i-p+3}a} + \cdots + b_{p-3}\overline{\phi^{i-1}a} \\ &= b_0\overline{\phi^{i-p+2}a} + b_1\overline{\phi^{i-p+3}a} + \cdots + b_{p-r-3}\overline{\phi^{i-r-1}a} \\ &\vdots \\ p^{t-1}\overline{\phi^{p-2}a} &= \overline{\phi^{i-r-1}(b_0 + b_1\phi + \cdots)a} \\ &= b_0\overline{\phi^{i-r-1}a} + b_1\overline{\phi^{i-r}a} + \cdots + \overline{b_r\phi^{i-1}a} \\ &= b_0\overline{\phi^{i-r-1}a} \end{aligned}$$

Por la unicidad de la ecuación (2.7) se deduce que

$$L_2 = \{\phi^{i-p+1}a, \phi^{i-p+2}a, \ldots, \phi^{i-r-1}a\}$$

es linealmente independiente. Además como

$$\begin{aligned} \alpha_1\overline{\phi^{i-p+1}a} + \alpha_2\overline{\phi^{i-p+2}a} + \cdots + \alpha_{p-r-1}\overline{\phi^{i-r-1}a} &= \bar{0} \\ \overline{\alpha_1\phi^{i-p+1}a + \cdots + \alpha_{p-r-1}\phi^{i-r-1}a} &= \bar{0} \end{aligned}$$

entonces existen $\beta_1, \ldots, \beta_r$ tales que

$$\begin{aligned} \alpha_1\phi^{i-p+1}a + \cdots + \alpha_{p-r-1}\phi^{i-r-1}a &= \beta_1\phi^{i-r}a + \cdots + \beta_r\phi^{i-1}a \\ \alpha_1\phi^{i-p+1}a + \cdots + \alpha_{p-r-1}\phi^{i-r-1}a - \beta_1\phi^{i-r}a - \cdots - \beta_r\phi^{i-1}a &= 0 \end{aligned}$$

pero por la unicidad de la ecuación (2.7) se deduce que
$\{\phi^{i-p+1}a, \phi^{i-p+2}a, \ldots, \phi^{i-r-1}a, \phi^{i-r}a, \ldots, \phi^{i-1}a\}$ es linealmente independiente, por lo tanto $\alpha_1 = \cdots \alpha_{p-r-1} = 0$, de donde concluimos que

$$\{\overline{\phi^{i-p+1}a}, \overline{\phi^{i-p+2}a}, \ldots, \overline{\phi^{i-r-1}a}\}$$

es linealmente independiente.

Sea $T : U_{t-1}/U_t \to U_{t-1}/U_t$, la transformación lineal definida por

$$\begin{aligned} T(\overline{\phi^{i-p+1}a}) &= p^{t-1}\overline{\phi^r a} \\ T(\overline{\phi^{i-p+2}a}) &= p^{t-1}\overline{\phi^{r+1}a} \\ &\vdots \\ T(\overline{\phi^{i-r-1}a}) &= p^{t-1}\overline{\phi^{p-2}a} \end{aligned} \tag{3.4}$$

Sea B la matriz asociada a T en la base L_2 es decir

$$B := \begin{pmatrix} b_0 & 0 & 0 & \ldots & 0 \\ b_1 & b_0 & 0 & \ldots & 0 \\ b_2 & b_1 & b_0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{p-r-2} & b_{p-r-3} & b_{p-r-4} & \ldots & b_0 \end{pmatrix}$$

Por la definición de B es claro que

$$\begin{aligned} B\overline{\phi^{i-p+1}a} &= p^{t-1}\overline{\phi^r a} \\ B\overline{\phi^{i-p+2}a} &= p^{t-1}\overline{\phi^{r+1}a} \\ &\vdots \\ B\overline{\phi^{i-r-1}a} &= p^{t-1}\overline{\phi^{p-2}a} \end{aligned} \tag{3.5}$$

Por el lema 2.1 sabemos que si $\sigma(\phi) = a_0 + a_1\phi + \cdots + a_{p-1}\phi^{p-1}$, entonces $a_0 \equiv -1 \pmod{p}$. Por lo tanto $b_0 \equiv (-1)^{t-1} \pmod{p}$, y como B es una matriz con $p - r - 1$ renglones entonces, $\det(B) \equiv (-1)^{(t-1)(p-r-1)} \pmod{p}$, es decir B es invertible.

Por lo tanto B es una matriz de cambio de base, lo cual demuestra que

$$\{p^{t-1}\overline{\phi^r a}, p^{t-1}\overline{\phi^{r+1}a}, \ldots, p^{t-1}\overline{\phi^{p-2}a}\}$$

es linealmente independiente.

Por lo tanto $p^{t-1}\overline{Y_t}$ es base de U_{t-1}/U_t.

Demostraré que $p^{j-2}\overline{Y_{j-1}}$ es base de U_{j-2}/U_{j-1}.

$$p^{j-2}\overline{Y_{j-1}} = \left\{p^{j-2}\overline{\pi a}\right\} = \left\{\overline{\pi^{j-1}a}\right\}$$

Entonces $\pi^{j-1}a \in U_{j-2}$, y como $\mathrm{f}(j-2, M) = 1$, y es claro que $\sharp(p^{j-2}\overline{Y_{j-1}}) = 1$, por lo tanto

$$p^{j-2}\overline{Y_{j-1}} \text{ es base de } U_{j-2}/U_{j-1}$$

Por el teorema 2.4 tenemos que

$$Y = Y_{j-1} \cup Y_t \cup Y_{t+1} \text{ es una } p\text{-base de } M.$$

Caso (3.1c): suponemos $p \leqslant i$, $t < j$.

Por el teorema 2.7 tenemos que

$$M \cong \mathbb{Z}_{p^j} \oplus (r-1)\mathbb{Z}_{p^{t+1}} \oplus (p-r)\mathbb{Z}_{p^t}$$

Por lo tanto

$$exp(M) = p^j$$

y además

$$\underline{\mathrm{t}}(M) = (0, \ldots, 0, \overset{t}{p-r}, \overset{t+1}{r-1}, 0, \ldots, 0, \overset{j}{1}).$$

Definimos

$$\begin{aligned} Y_t &= \{\phi^r a, \phi^{r+1}a, \ldots, \phi^{p-1}a\} \\ Y_{t+1} &= \{\phi a, \phi^2 a, \ldots, \phi^{r-1}a\} \\ Y_j &= \{a\} \end{aligned}$$

Como p^j es el exponente de M, entonces

$$Y_j \subset M[p^j]$$

$p^t\phi^r a = \phi^{t(p-1)}\sigma(\phi)^t\phi^r a = \phi^{t(p-1)+r}\sigma(\phi)^t a = \phi^i\sigma(\phi)^t a = 0$, además para toda $r \leqslant k \leqslant p-1$, tenemos que $k = r + \eta_k$, con $\eta_k \geqslant 0$, entonces $p^t\phi^k a = p^t\phi^{r+\eta_k} a = \phi^i\sigma(\phi)^t\phi^{\eta_k} a = 0$, por lo tanto

$$Y_t \subset M[p^t]$$

$p^{t+1}\phi a = \phi^{(t+1)(p-1)}\sigma(\phi)^{t+1}\phi a = \phi^{i+(p-r)}\sigma(\phi)^{t+1} a = 0$, además para toda $0 \leqslant k \leqslant r-1$, tenemos que $p^{t+1}\phi^k a = \phi^{i+(p-1-r)}\sigma(\phi)^{t+1}\phi^k a = 0$, por lo tanto

$$Y_{t+1} \subset M[p^{t+1}]$$

Demostraré que $p^{j-1}\overline{Y_j}$ es base de $U_{j-1}/U_j \cong U_{j-1}$.

$$p^{j-1}\overline{Y_j} = \{p^{j-1}\overline{a}\} \cong \{p^{j-1}a\}$$

Entonces $p^{j-1}a \in U_{j-1}$, y como $\mathrm{f}(j-1, M) = 1$, y es claro que $\sharp(p^{j-1}\overline{Y_j}) = 1$, por lo tanto

$$p^{j-1}\overline{Y_j} \text{ es base de } U_{j-1}/U_j$$

Demostraré que $p^t\overline{Y_{t+1}}$ es base de U_t/U_{t+1}.

Sabemos que $\mathrm{f}(t, M) = r-1$, por lo tanto basta demostrar que $p^t\overline{Y_{t+1}}$ es linealmente independiente, ya que así demostraríamos tambien que $\sharp(p^t\overline{Y_{t+1}}) = r-1$.

Sea $y \in M$, entonces por la ecuación (2.7) $y = \alpha a + \sum_{k=1}^{i-1}\alpha_k\phi^k a + \sum_{l=1}^{j-1}\beta_l\pi^l a$ entonces

$$\begin{aligned} p^{t+1}y &= \alpha p^{t+1}a + \sum_{k=1}^{i-1}\alpha_k p^{t+1}\phi^k a + \sum_{l=1}^{j-1}\beta_l p^{t+1}\pi^l a \\ &= \alpha\pi^{t+1}a + \beta_1\pi^{t+2}a + \cdots + \beta_{j-t-2}\pi^{j-1}a \end{aligned}$$

Sea $w \in U_{t+1}$, entonces $pw = 0$, y además $w = p^{t+1}y$, para alguna $y \in M$, es decir $w = \alpha\pi^{t+1}a + \beta_1\pi^{t+2}a + \cdots + \beta_{j-t-2}\pi^{j-1}a$, por lo tanto $pw = \alpha\pi^{t+2}a + \beta_1\pi^{t+3}a + \cdots \beta_{j-t-3}\pi^{j-1}a$. Por la unicidad de la ecuación (2.7) tenemos que $\alpha = 0$ y que $\beta_1 = \cdots = \beta_{j-t-3} = 0$, entonces $w = \beta_{j-t-2}\pi^{j-1}a$, es decir $U_{t+1} = \langle\pi^{j-1}a\rangle$.

$$
\begin{aligned}
p^t\overline{\phi a} &= \overline{\phi^{t(p-1)+1}\sigma(\phi)^t a} = \overline{\phi^{i-r+1}(c_0 + c_1\phi + \cdots)a} \\
&= c_0\overline{\phi^{i-r+1}a} + c_1\overline{\phi^{i-r+2}a} + \cdots + c_{r-2}\overline{\phi^{i-1}a} \\
p^t\overline{\phi^2 a} &= \overline{\phi^{i-r+2}(c_0 + c_1\phi + \cdots)a} \\
&= c_0\overline{\phi^{i-r+2}a} + c_1\overline{\phi^{i-r+3}a} + \cdots + c_{r-3}\overline{\phi^{i-1}a} \\
&\vdots \\
p^t\overline{\phi^{r-1}a} &= \overline{\phi^{i-1}(c_0 + c_1\phi + \cdots)a} = c_0\overline{\phi^{i-1}a}
\end{aligned}
$$

Por la unicidad de la ecuación (2.7) se deduce que

$$L_3 = \{\phi^{i-r+1}a, \phi^{i-r+2}a, \ldots, \phi^{i-1}a\}$$

es linealmente independiente. Además como

$$
\begin{aligned}
\alpha_1\overline{\phi^{i-r+1}a} + \alpha_2\overline{\phi^{i-r+2}a} + \cdots + \alpha_{r-1}\overline{\phi^{i-1}a} &= \bar{0} \\
\overline{\alpha_1\phi^{i-r+1}a + \cdots + \alpha_{r-1}\phi^{i-1}a} &= \bar{0}
\end{aligned}
$$

entonces existe β tal que

$$
\begin{aligned}
\alpha_1\phi^{i-r+1}a + \cdots + \alpha_{r-1}\phi^{i-1}a &= \beta\pi^{j-1}a \\
\alpha_1\phi^{i-r+1}a + \cdots + \alpha_{r-1}\phi^{i-1}a - \beta\pi^{j-1}a &= 0
\end{aligned}
$$

pero por la unicidad de la ecuación (2.7) se deduce que
$\{\phi^{i-r+1}a, \phi^{i-r+2}a, \ldots, \phi^{i-1}a, \pi^{j-1}a\}$ es linealmente independiente, por lo tanto $\alpha_1 = \cdots \alpha_{r-1} = 0$, de donde concluimos que

$$\{\overline{\phi^{i-r+1}a}, \overline{\phi^{i-r+2}a}, \ldots, \overline{\phi^{i-1}a}\}$$

es linealmente independiente.

Sea $T : U_t/U_{t+1} \to U_t/U_{t+1}$, la transformación lineal definida por

$$
\begin{aligned}
T(\overline{\phi^{i-r+1}a}) &= p^t\overline{\phi a} \\
T(\overline{\phi^{i-r+2}a}) &= p^t\overline{\phi^2 a} \\
&\vdots \\
T(\overline{\phi^{i-1}a}) &= p^t\overline{\phi^{r-1}a}
\end{aligned}
\tag{3.6}
$$

Sea C la matriz asociada a T en la base L_3 es decir

$$C := \begin{pmatrix} c_0 & 0 & 0 & \dots & 0 \\ c_1 & c_0 & 0 & \dots & 0 \\ c_2 & c_1 & c_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{r-2} & c_{r-3} & c_{r-4} & \dots & c_0 \end{pmatrix}$$

Por la definición de C es claro que

$$\begin{aligned} C\overline{\phi^{i-r+1}a} &= p^t\overline{\phi a} \\ C\overline{\phi^{i-r+2}a} &= p^t\overline{\phi^2 a} \\ &\vdots \\ C\overline{\phi^{i-1}a} &= p^t\overline{\phi^{r-1}a} \end{aligned} \tag{3.7}$$

Por el lema 2.1 sabemos que si $\sigma(\phi) = a_0 + a_1\phi + \cdots + a_{p-1}\phi^{p-1}$, entonces $a_0 \equiv -1 \pmod{p}$. Por lo tanto $c_0 \equiv (-1)^t \pmod{p}$, y como C es una matriz con $r-1$ renglones entonces, $\det(C) \equiv (-1)^{t(r-1)} \pmod{p}$, es decir C es invertible.

Por lo tanto C es una matriz de cambio de base, lo cual demuestra que

$$\{p^t\overline{\phi a}, p^t\overline{\phi^2 a}, \dots, p^t\overline{\phi^{r-1}a}\}$$

es linealmente independiente.

Por lo tanto $p^t\overline{Y_{t+1}}$ es base de U_t/U_{t+1}.

Demostraré que $p^{t-1}\overline{Y_t}$ es base de U_{t-1}/U_t.

Sabemos que $\mathrm{f}(t-1, M) = p - r$, por lo tanto basta demostrar que $p^{t-1}\overline{Y_t}$ es linealmente independiente, pues así demostraríamos que $\sharp(p^{t-1}\overline{Y_t}) = p - r$.

$$\begin{aligned} p^{t-1}\overline{\phi^r a} &= \overline{\phi^{(t-1)(p-1)+r}\sigma(\phi)^{t-1}a} = \overline{\phi^{i-(p-1)}(b_0 + b_1\phi + \cdots)a} \\ &= b_0\overline{\phi^{i-(p-1)}a} + b_1\overline{\phi^{i-p+2}a} + \cdots + b_{p-2}\overline{\phi^{i-1}a} \end{aligned}$$

De las ecuaciones (3.7) se deduce que $\{\phi^{i-r+1}a, \ldots, \phi^{i-1}a\} \subset U_t$, por lo que

$$\begin{aligned}
p^{t-1}\overline{\phi^r a} &= b_0\overline{\phi^{i-(p-1)}a} + b_1\overline{\phi^{i-p+2}a} + \cdots + b_{p-r-1}\overline{\phi^{i-r}a} \\
p^{t-1}\overline{\phi^{r+1}a} &= \overline{\phi^{i-p+2}(b_0 + b_1\phi + \cdots)a} \\
&= b_0\overline{\phi^{i-p+2}a} + b_1\overline{\phi^{i-p+3}a} + \cdots + b_{p-3}\overline{\phi^{i-1}a} \\
&= b_0\overline{\phi^{i-p+2}a} + b_1\overline{\phi^{i-p+3}a} + \cdots + b_{p-r-2}\overline{\phi^{i-r}a} \\
&\vdots \\
p^{t-1}\overline{\phi^{p-1}a} &= \overline{\phi^{i-r}(b_0 + b_1\phi + \cdots)a} \\
&= b_0\overline{\phi^{i-r}a} + b_1\overline{\phi^{i-r+1}a} + \cdots + b_{r-1}\overline{\phi^{i-1}a} \\
&= b_0\overline{\phi^{i-r}a}
\end{aligned}$$

Por la unicidad de la ecuación (2.7) se deduce que

$$L_4 = \{\phi^{i-p+1}a, \phi^{i-p+2}a, \ldots, \phi^{i-r}a\}$$

es linealmente independiente. Además como

$$\begin{gathered}
\alpha_1\overline{\phi^{i-p+1}a} + \alpha_2\overline{\phi^{i-p+2}a} + \cdots + \alpha_{p-r}\overline{\phi^{i-r}a} = \bar{0} \\
\overline{\alpha_1\phi^{i-p+1}a + \cdots + \alpha_{p-r}\phi^{i-r}a} = \bar{0}
\end{gathered}$$

entonces existen $\beta_1, \ldots, \beta_{r-1}, \gamma$ tales que

$$\begin{gathered}
\alpha_1\phi^{i-p+1}a + \cdots + \alpha_{p-r}\phi^{i-r}a = \beta_1\phi^{i-r+1}a + \cdots + \beta_{r-1}\phi^{i-1}a + \gamma\pi^{j-1}a \\
\alpha_1\phi^{i-p+1}a + \cdots + \alpha_{p-r}\phi^{i-r}a - \beta_1\phi^{i-r+1}a - \cdots - \beta_{r-1}\phi^{i-1}a - \gamma\pi^{j-1}a = 0
\end{gathered}$$

pero por la unicidad de la ecuación (2.7) se deduce que

$$\{\phi^{i-p+1}a, \phi^{i-p+2}a, \ldots, \phi^{i-r}a, \phi^{i-r+1}a, \ldots, \phi^{i-1}a, \pi^{j-1}a\}$$

es linealmente independiente, entonces $\alpha_1 = \cdots \alpha_{p-r} = 0$, por lo tanto

$$\{\overline{\phi^{i-p+1}a}, \overline{\phi^{i-p+2}a}, \ldots, \overline{\phi^{i-r}a}\}$$

es linealmente independiente.

Sea $T : U_{t-1}/U_t \to U_{t-1}/U_t$ la transformación lineal dada por

$$\begin{aligned} T(\overline{\phi^{i-p+1}a}) &= p^{t-1}\overline{\phi^r a} \\ T(\overline{\phi^{i-p+2}a}) &= p^{t-1}\overline{\phi^{r+1}a} \\ &\vdots \\ T(\overline{\phi^{i-r}a}) &= p^{t-1}\overline{\phi^{p-1}a} \end{aligned} \tag{3.8}$$

Sea B la matriz asociada a T en la base L_4, es decir

$$B := \begin{pmatrix} b_0 & 0 & 0 & \dots & 0 \\ b_1 & b_0 & 0 & \dots & 0 \\ b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{p-r-1} & b_{p-r-2} & b_{p-r-3} & \dots & b_0 \end{pmatrix}$$

Por la definición de B es claro que

$$\begin{aligned} B\overline{\phi^{i-p+1}a} &= p^{t-1}\overline{\phi^r a} \\ B\overline{\phi^{i-p+2}a} &= p^{t-1}\overline{\phi^{r+1}a} \\ &\vdots \\ B\overline{\phi^{i-r}a} &= p^{t-1}\overline{\phi^{p-1}a} \end{aligned} \tag{3.9}$$

Por el lema 2.1 sabemos que si $\sigma(\phi) = a_0 + a_1\phi + \cdots + a_{p-1}\phi^{p-1}$, entonces $a_0 \equiv -1 \pmod{p}$. Por lo tanto $b_0 \equiv (-1)^{t-1} \pmod{p}$, y como B es una matriz con $p - r$ renglones entonces, $\det(B) \equiv (-1)^{(t-1)(p-r)} \pmod{p}$, es decir B es invertible.

Por lo tanto B es una matriz de cambio de base, lo cual demuestra que

$$\{p^{t-1}\overline{\phi^r a}, p^{t-1}\overline{\phi^{r+1}a}, \dots, p^{t-1}\overline{\phi^{p-1}a}\}$$

es linealmente independiente.

Por lo tanto $p^{t-1}\overline{Y_t}$ es base de U_{t-1}/U_t.

Por el teorema 2.4 tenemos que

$$Y = Y_{j-1} \cup Y_t \cup Y_{t+1} \text{es una } p\text{-base de } M.$$

□

A continuación mostramos las p-bases de nuestros ejemplos de $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta.

1. $p=7$, $n=3$, $\mathscr{C}=(\overset{i}{6},\overset{j}{3})$, $i=\overset{t}{0}(p-1)+\overset{r}{6}$, $p=\pi$

$$M\cong\mathbb{Z}_{p^3}\oplus 5\mathbb{Z}_p$$

Por la ecuación (3.1a) tenemos que la p-base de M es

$$Y=\{a,\phi a,\phi^2 a,\phi^3 a,\phi^4 a,\phi^5 a\}$$

2. $p=5$, $n=4$, $\mathscr{C}=(\overset{i}{4},\overset{j}{4})$, $i=\overset{t}{0}(p-1)+\overset{r}{4}$, $p=\pi$

$$M\cong\mathbb{Z}_{p^4}\oplus 3\mathbb{Z}_p$$

Por la ecuación (3.1a) tenemos que la p-base de M es

$$Y=\{a,\phi a,\phi^2 a,\phi^3 a\}$$

3. $p=3$, $n=4$, $\mathscr{C}=(\overset{i}{7},\overset{j}{3})$, $i=\overset{t}{3}(p-1)+\overset{r}{1}$, $p=\pi+2\phi^2+\phi^3$.

$$M\cong\mathbb{Z}_{p^2}\oplus\mathbb{Z}_{p^4}\oplus\mathbb{Z}_{p^3}$$

Como $p\leqslant i$ y $t\geqslant j$ entonces por la ecuación (3.1b) tenemos que

$$Y=\{a,\phi a,\pi a\}$$

4. $p=3$, $n=4$, $\mathscr{C}=(\overset{i}{9},\overset{j}{4})$, $i=\overset{t}{4}(p-1)+\overset{r}{1}$, $p=\pi+2\phi^2+\phi^3$.

$$M\cong\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^5}\oplus\mathbb{Z}_{p^4}$$

Como $p\leqslant i$ y $t\geqslant j$ entonces por la ecuación (3.1b) tenemos que

$$Y=\{a,\phi a,\pi a\}$$

5. $p=5$, $n=2$, $\mathscr{C}=(\overset{i}{7},\overset{j}{2})$, $i=\overset{t}{1}(p-1)+\overset{r}{3}$, $p=\pi+4\phi^4+2\phi^5+3\phi^6$.

$$M\cong 3\mathbb{Z}_{p^2}\oplus 2\mathbb{Z}_p$$

Como $p\leqslant i$ y $t<j$ entonces por la ecuación (3.1c) tenemos que

$$Y=\{a,\phi a,\phi^2 a,\phi^3 a,\phi^4 a\}$$

6. $p = 3$, $n = 5$, $\mathscr{C} = (\overset{i}{7}, \overset{j}{5})$, $i = \overset{t}{3}(p-1) + \overset{r}{1}$, $p = \pi + 2\phi^2 + \phi^3$.

$$M \cong \mathbb{Z}_{p^5} \oplus 2\mathbb{Z}_{p^3}$$

Como $p \leqslant i$ y $t < j$ entonces por la ecuación (3.1c) tenemos que

$$Y = \{a, \phi a, \phi^2 a\}$$

Capítulo 4

Bases de Gröbner

En este capítulo enunciamos los conceptos y resultados básicos de la teoría de bases de Gröbner. Para ello primero enunciaremos las propiedades de los anillos de polinomios; y después las propiedades básicas de las bases de Gröbner de ideales de polinomios.

4.1 Polinomios

Definición. Un *Monoide* es un conjunto M con una operación binaria "$\cdot$" definida en él, y un elemento distinguido $1 \in M$ tal que:

(i) "$\cdot$" es asociativa.

(ii) $1 \cdot a = a \cdot 1 = a \quad \forall\, a \in M$

M se llama *abeliano* si "$\cdot$" es conmutativa.

Ejemplos. Sea $n \in \mathbb{N}$. El conjunto $\mathbb{N}^n$ de todas las n-tuples de números naturales con la operación de suma componente a componente, es un monoide abeliano llamado *monoide aditivo* $\mathbb{N}^n$.

Definición. Un *homomorfismo* de un monoide M a un monoide N es una función $\varphi\colon M \to N$ con las siguientes dos propiedades:

(i) $\varphi(a)\varphi(b) = \varphi(ab) \quad \forall\, a, b \in M$

(ii) $\varphi(1_M) = 1_N$.

El lema siguiente está demostrado en [7].

Lema 4.1. *Sea S un anillo conmutativo y $\{c_1, \ldots, c_n\} \subset S$. La función*

$$\begin{array}{rccc} \sigma: & \mathbb{N}^n & \longrightarrow & S \\ & (v_1, \ldots, v_n) & \longmapsto & c_1^{v_1} \cdot \cdots \cdot c_n^{v_n} \end{array}$$

es un homomorfismo de $(\mathbb{N}^n, (0), +)$ en $(S, 1, \cdot)$.

En todo el capítulo K denotará un campo y M un monoide abeliano.

Definición. Si f es una función de M en K, entonces el *soporte* de f se define como

$$sop(f) = \{\, u \in M \mid f(u) \neq 0 \,\}.$$

Notación. Denotamos por $K[M]$ (también denotado por KM), al conjunto de todas las funciones $f\colon M \to K$ con soporte finito.

Definimos las funciones de suma y producto en $K[M]$ de la siguiente manera:

Definición. Dados $f, g \in M$ y $\forall\, u \in M$,

$$\begin{aligned} (f+g)(u) &= f(u) + g(u) \\ (fg)(u) &= \sum_{\substack{v,w \in M \\ vw = u}} f(v)g(w). \end{aligned}$$

obteniendo el siguiente resultado:
La proposición siguiente está demostrada en [6].

Proposición 4.2. *$K[M]$ es un anillo cuyo cero es la función f, que satisface $f(u) = 0 \quad \forall\, u \in M$, y cuyo 1 es la función definida por*

$$1_{K[M]}(u) = \begin{cases} 1 & si\ u = 1_M \\ 0 & \text{cualquier otro caso} \end{cases}$$

Observación. $K[M]$ con las operaciones anteriores es una K-álgebra, llamada álgebra de monoide.

Definición.

- El anillo $K[M]$ es llamado *anillo monomial.* Si M es el monoide aditivo $\mathbb{N}^n$, entonces es llamado *anillo de polinomios* en n variables sobre K. Los elementos del anillo polinomial son llamados *polinomios.*

- Una función $f \in K[M]$ es llamada *monomio* si solo tiene un único valor diferente de cero.

Ahora introduciremos brevemente la notación y terminología usual de los polinomios[1]. Denotaremos por $(v) = (v_1, \ldots, v_n)$ a los elementos de $\mathbb{N}^n = M$. Identificaré cada $a \in K$ con su imagen $i(a) \in K[M]$, donde i es el homomorfismo inclusión de K en $K[M]$, asi que $a \in K$ denota un elemento de K y una función que llamaré *polinomio constante.*

Ahora para $1 \leqslant j \leqslant n$, definimos

$$(\epsilon_j) = (0, \ldots, 0, \underset{\substack{\uparrow \\ j}}{1}, 0, \ldots, 0) \in M,$$

Sea η el homomorfismo inclusión, $\eta : M \to K[M]$. Denotamos por $X_i \in K[M]$ al monomio $\eta((\epsilon_i))$, es decir

$$X_i((v)) = \begin{cases} 1 & \text{si } (v) = (\epsilon_i) \\ 0 & \text{cualquier otro caso} \end{cases}$$

X_i es llamada la i-ésima *indeterminada.* Es claro que toda $(v) \in M$ tiene una única representación de la forma

$$(v_1, \ldots, v_n) = \sum_{v_1 \text{ sumandos}} (\epsilon_1) + \cdots + \sum_{v_n \text{ sumandos}} (\epsilon_n).$$

Aplicando η a esta ecuación vemos que cualquier monomio en $K[M]$ de la forma $\eta((v))$ con $(v) \in M$, puede ser escrito como

$$\eta((v)) = X_1^{v_1} \cdot \cdots \cdot X_n^{v_n},$$

El conjunto de todos los monomios de la forma $X_1^{v_1} \cdot \cdots \cdot X_n^{v_n}$ es denotado por $T(X_1, \ldots, X_n)$, o simplemente T cuando es claro el número de variables.

[1]Para un desarrollo más detallado ver [6].

Siendo T un monoide abeliano bajo la multiplicación en $K[M]$, y como además $\eta(M) = T$, entonces η es un isomorfismo entre los monoides

$$\begin{array}{rccc} \eta\colon & (\mathbb{N}^n, (0), +) & \longrightarrow & (T, 1_{K[M]}, \cdot) \\ & (v_1, \ldots, v_n) & \longmapsto & X_1^{v_1} \cdot \cdots \cdot X_n^{v_n} \end{array}$$

Además la estructura de $(T, 1_{K[M]}, \cdot)$ es independiente de K, lo que permite referirnos al *monoide* (abeliano libre) T generado por las variables $X_1, \ldots, X_n$, sin especificar al campo K.

No es difícil demostrar que todo polinomio $f \in K[M]$ tiene una única representación como una suma de monomios distintos por pares, dada por

$$f = \sum_{(v) \in sop(f)} f((v)) \cdot X_1^{v_1} \cdot \cdots \cdot X_n^{v_n}.$$

En otras palabras, para cada $f \in K[M]$, existe un único subconjunto finito $N \subset M$ y un único conjunto $\{ a_{(v)} \mid (v) \in N \}$ de elementos distintos de cero de K tales que

$$f = \sum_{(v) \in N} a_{(v)} X_1^{v_1} \cdot \cdots \cdot X_n^{v_n}.$$

Notación. $K[X_1, \ldots, X_n]$, denotará el anillo de polinomios $K[M]$. En realidad $K[X_1, \ldots, X_n]$ es el resultado de adjuntar las variables $X_1, \ldots, X_n$ a K, pero para nuestros propósitos es suficiente considerarlo como una notación adicional.

En lo subsiguiente utilizaremos indistintamente ambas notaciones, en la sección donde desarrollo la teoría básica de las bases de Gröbner utilizaré más a menudo $K[X_1, \ldots, X_n]$, sin embargo cuando hable acerca de bases de Gröbner asociadas a grupos abelianos finitos utilizaré la notación $K[M]$.

Definición. El *grado total* del monomio $X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdots X_n^{\alpha_n}$ es la suma de los exponentes $\alpha_1 + \cdots + \alpha_n$. A veces el grado total es llamado *longitud* y denotado por $l(X_1^{\alpha_1} \cdots X_n^{\alpha_n})$.

Para simplificar la notación denotaremos $\alpha = (\alpha_1, \ldots, \alpha_n)$ y

$$X^{\alpha} = X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdots X_n^{\alpha_n}$$

Definición. Sea $f = \sum_\alpha a_\alpha X^\alpha, \quad a_\alpha \in K$ un polinomio en $K[X_1, \ldots, X_n]$.

- Llamamos a_α el *coeficiente* del monomio X^α.
- Si $a_\alpha \neq 0, \quad$ entonces llamamos a $a_\alpha X^\alpha$ un *término* de f.
- El *grado* de f, denotado por $\deg(f)$, es el máximo *grado total* de los monomios en f con coeficiente distinto de cero.

4.2 Bases de Gröbner

En esta sección definimos los órdenes monomiales en $K[X_1, \ldots, X_n]$. Daremos los ejemplos más importantes de estos para nuestro trabajo; enunciaremos algunos conceptos básicos de la teoría de Bases de Gröbner y algunas de las propiedades de estas bases.

Definición. Un *orden monomial* en $K[X_1, \ldots, X_n]$ es cualquier relación $>$ en $\mathbb{N}^n$, o equivalentemente, cualquier relación en el conjunto de monomios X^α, $\alpha \in \mathbb{N}^n$, que cumpla las siguientes condiciones:

(i) $>$ es un *orden total* (o lineal) en $\mathbb{N}^n$.

(ii) Si $\alpha > \beta$ y $\gamma \in \mathbb{N}^n$ entonces $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ es un *buen orden* en $\mathbb{N}^n$.

Algunos ejemplos importantes de órdenes monomiales[2] son los siguientes:

Orden Lexicográfico Sea $\alpha = (\alpha_1, \ldots, \alpha_n)$ y $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. Decimos que $\alpha >_{lex} \beta$ si en el vector diferencia $\alpha - \beta \in \mathbb{Z}^n$ la primer entrada (de derecha a izquierda) distinta de cero es positiva. Escribiremos $X^\alpha >_{lex} X^\beta$ si $\alpha >_{lex} \beta$

Orden Graduado Lexicográfico Sea $\alpha, \beta \in \mathbb{N}^n$ Decimos que $\alpha >_{grlex} \beta$ si $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, o $|\alpha| = |\beta|$ y $\alpha >_{lex} \beta$.

Observación. Es importante observar que cualquier orden depende de como estén ordenadas las variables. En general para n variables existen $n!$ ordenes distintos del mismo tipo (lexicográfico, graduado lexicográfico, etc.).

[2]En [9, 1, 6] se definen más órdenes

Definición. Sea $f = \sum_\alpha a_\alpha X^\alpha$ un polinomio ($\neq 0$) en $K[X_1, \ldots, X_n]$ y sea $>$ un orden monomial.

(i) El *multigrado* (o *grado*) de f es

$$\deg(f) = \max_{>}(\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0)$$

(ii) El *coeficiente principal* de f es

$$\mathrm{lc}_>(f) = a_{\deg(f)} \in K$$

(iii) El *monomio principal* (o *monomio inicial*) de f es

$$\mathrm{in}_>(f) = X^{\deg(f)}$$

(iv) El *término principal* de f es

$$\mathrm{lt}_>(f) = \mathrm{lc}_>(f) \cdot \mathrm{in}_>(f).$$

El siguiente teorema está demostrado en [9], pag. 61.

Teorema 4.3 (Algoritmo de la División). *Fijemos un orden monomial $>$ y sea $F = (f_1, \ldots, f_s)$ una s-tupla ordenada de polinomios en $K[X_1, \ldots, X_n]$. Entonces todo $f \in K[X_1, \ldots, X_n]$ puede ser escrito como*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

donde $a_i, r \in K[X_1, \ldots, X_n]$, y $r = 0$ o r es una combinación lineal, con coeficientes en K, de monomios, ninguno de los cuales es divisible por algún $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$. Llamaremos a r, residuo *de f dividido entre F. Más aún, si $a_i f_i \neq 0$, entonces tenemos que*

$$\deg(f) \geqslant \deg(a_i f_i).$$

Observación. El residuo r depende del ordenamiento de la s-tupla.

Definición. Un ideal $I \subset K[X_1, \ldots, X_n]$ es un *ideal monomial* si existe un subconjunto $A \subset \mathbb{N}^n$ tal que $I = \langle X^\alpha \mid \alpha \in A \rangle$.

Definición. Sea $I \neq \emptyset$ un ideal en $K[X_1, \ldots, X_n]$

(i) Denotamos por $\mathrm{lt}(I)$ al ideal generado por los terminos principales de I, es decir

$$\mathrm{lt}(I) = \langle \mathrm{lt}(f) \mid f \in I \rangle$$

(ii) Llamamos *ideal inicial*, al ideal monomial generado por los monomios iniciales de I, y lo denotamos $\mathrm{in}(I)$ es decir

$$\mathrm{in}(I) = \langle \mathrm{in}(f) \mid f \in I \rangle$$

Observación. Estos dos ideales son iguales, sin embargo hemos enunciado ambas definiciones pués en la literatura es más común trabajar con $\mathrm{lt}(I)$, ver por ejemplo [1] pag. 32, a diferencia de esta tesis en la que trabajamos más con $\mathrm{in}(I)$, para evitarnos operar con coeficientes.

Definición. Los monomios que no son elementos del ideal inicial $\mathrm{in}(I)$, son llamados *monomios estándar.*

Definición. Fijemos un orden monomial. Un subconjunto finito $G = \{ g_1, \ldots, g_s \}$ de un ideal I es una *base de Gröbner* si

$$\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle = \mathrm{lt}(I)$$

Equivalentemente G es una *base de Gröbner* si

$$\langle \mathrm{in}(g_1), \ldots, \mathrm{in}(g_s) \rangle = \mathrm{in}(I)$$

En el siguiente ejemplo mostraremos una base[3] de un ideal que no es base de Gröbner.

Ejemplos. Sea $I \subset \mathbb{Q}[x, y]$ el ideal generado por $G = \{f_1, f_2\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$, entonces G no es una base de Gröbner de I con respecto a $>_{grlex}$, con $x > y$.

Sea $f_3 = yf_1 - xf_2$ entonces $f_3 \in I$, ahora $f_3 = x^3y - 2xy^2 - x^3y + 2xy^2 - x^2 = -x^2$, por lo tanto $x^2 \in \mathrm{in}(I)$, pero por otro lado es claro que $x^2 \notin \langle \mathrm{in}(f_1), \mathrm{in}(f_2) \rangle = \langle x^3, x^2y \rangle$.

A continuación enunciaremos algunas propiedades básicas de estas bases de Gröbner.

[3]Recordando que por base de un ideal entendemos un conjunto generador de este.

Proposición 4.4. *Sea* $G = \{g_1, \ldots, g_s\}$ *una base de Gröbner de un ideal* $I \subset K[X_1, \ldots, X_n]$ *y sea* $f \in K[X_1, \ldots, X_n]$. *Entonces existe un único* $r \in K[X_1, \ldots, X_n]$ *con las siguientes propiedades*

(i) Ningún término de r *es divisible por algún* $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)$.

(ii) Existe $g \in I$ *tal que* $f = g + r$.

En particular, r *es el residuo de la división de* f *entre* G *sin importar el orden de los elementos de* G *usado en el algoritmo de la división.*

Demostración. El algoritmo de la división nos da $f = a_1g_1 + \cdots + a_sg_s + r$, donde r satisface (i). De aquí también obtenemos (ii), al poner $g = a_1g_1 + \cdots + a_sg_s \in I$, además de estar probando la existencia de r.

Para probar la unicidad, supongamos que $f = g_1 + r_1 = g_2 + r_2$ tales que satisfacen (i) y (ii). Entonces $r_2 - r_1 = g_1 - g_2 \in I$, si $r_2 \neq r_1$, entonces $\mathrm{lt}(r_2 - r_1) \in \mathrm{lt}(I) = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$. Por lo tanto $\mathrm{lt}(r_2 - r_1)$ es divisible por algún $\mathrm{lt}(g_i)$. Pero esto es imposible pues ningún término de r_1 o r_2 es divisible por algún $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)$. Entonces $r_2 - r_1 = 0$ lo cual prueba la unicidad.

La parte final de la proposición se sigue de la unicidad de r. □

Observación. Esta proposición nos dice que todo polinomio f puede ser escrito módulo I, como una combinación K-lineal de monomios estándar.

Corolario 4.5. *Sea* $G = \{g_1, \ldots, g_s\}$ *una base de Gröbner del ideal* $I \subset K[X_1, \ldots, X_n]$ *y sea* $f \in K[X_1, \ldots, X_n]$. *Entonces* $f \in I$ *si, y sólo si, el residuo de la división de* f *entre* G *es cero.*

Demostración. Si el residuo es cero entonces ya observamos en la proposición anterior que $f \in I$. Ahora dado $f \in I$, entonces $f = f + 0$ satisface las condiciones de la proposición anterior, por la unicidad del residuo tenemos que 0 es el residuo de f bajo la división por G. □

Esta propiedad es tomada algunas veces como definición de *base de Gröbner*, pues esta propiedad se cumple si, y sólo si, $\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle = \mathrm{lt}(I)$.

Definición. Sea G una base de Gröbner, denotamos por $\overline{f}^G$ al residuo de la división de f entre G. Llamamos a $\overline{f}^G$ la *forma normal* (o *forma estándar*) de f *módulo* G.

Observación. Si G no es base de Gröbner, entonces $\overline{f}^G$, es el conjunto de residuos de f módulo G, tomando todos los ordenes distintos de polinomios en G.

Definición. Sea G una base de Gröbner de I ideal de $K[X_1, \ldots, X_n]$. Definimos $\mathrm{std}(G)$ como el conjunto de monoides estándar módulo G, es decir

$$\mathrm{std}(G) = \{t \in T \mid t \notin \langle \mathrm{in}(G) \rangle\}.$$

Los siguientes resultados están demostrados en [1], sección 1.6.

Teorema 4.6. *Sea I un ideal de $K[X_1, \ldots, X_n]$. Los siguientes enunciados son equivalentes para $G = \{g_1, \ldots, g_s\} \subset I$.*

(i) G es una base de Gröbner de I.

(ii) $f \in I \iff \overline{f}^G = \{0\}$.

(iii) $f \in I \iff f = \sum_{i=1}^{s} h_i g_i$ *con* $\mathrm{in}(f) = \max_{1 \leqslant i \leqslant s}(\mathrm{in}(h_i)\,\mathrm{in}(g_i))$.

(iv) $\forall\, f \in I \quad \exists\, i \in \{1, \ldots, s\}$ *tal que* $\mathrm{in}(g_i) \mid \mathrm{in}(f)$.

Corolario 4.7. *Si G es una base de Gröbner de I, entonces $I = \langle G \rangle$.*

Demostración. Claramente $\langle g_1, \ldots, g_s \rangle \subset I$, dado que cada $g_i \in I$. Para la inclusión inversa sea $f \in I$, entonces $\overline{f}^G = 0$, de donde $f \in \langle g_1, \ldots, g_s \rangle$. □

Observación. Toda base de Gröbner G de un ideal I es una base de I, es decir $I = \langle G \rangle$.

Proposición 4.8. *Todo ideal $I \subset K[X_1, \ldots, X_n]$ distinto de cero tiene una base de Gröbner.*

Los siguientes teoremas están probados en [9] en el capítulo 2, secciones 6 y 7, aquí sólo los enunciaremos con el fin de mostrar el algoritmo de Buchberger, el cual calcula una base de Gröbner dado un conjunto finito generador de un ideal de polinomios.

Definición. Sean $f, g \in K[x_1, \ldots, x_n]$ polinomios distintos de cero.

(i) Si $\deg(f) = \alpha$ y $\deg(g) = \beta$, entonces sea $\gamma = (\gamma_1, \ldots, \gamma_n)$, donde $\gamma_i = max(\alpha_i, \beta_i)$ para cada i. Llamamos x^γ el *mínimo común múltiplo* de $\mathrm{in}(f)$ e $\mathrm{in}(g)$, denotado $x^\gamma = \mathrm{mcm}(\mathrm{in}(f), \mathrm{in}(g))$.

(ii) El *S-polinomio* de f y g es la combinación

$$S(f,g) = \frac{x^\gamma}{\mathrm{lt}(f)} \cdot f - \frac{x^\gamma}{\mathrm{lt}(g)} \cdot g$$

Teorema 4.9. *Sea I un ideal de polinomios y $G = \{g_1, \ldots, g_t\}$ una base de I. Entonces G es una base de Gröbner de I si, y sólo si, para todas las parejas $i \neq j$, el residuo de la división de $S(g_i, g_j)$ por G (listado en algún orden) es cero.*

Teorema 4.10 (Algoritmo de Buchberger). *Sea $I = \langle f_1, \ldots, f_s \rangle \neq 0$ un ideal de polinomios. Entonces una base de Gröbner de I puede ser construida por el siguiente algoritmo, en un número finito de pasos:*

```
Input: F = (f_1, ..., f_s)
Output: una base de Gröbner G = (g_1, ..., g_t) de I, con F ⊂ G
G := F
REPEAT
    G' := G
    FOR cada pareja {p, q}, p ≠ q en G' DO
        S := S(p,q)^{G'}
        IF S ≠ 0 THEN G := G ∪ {S}
UNTIL G = G'
```

Como ejemplo de este algoritmo, daremos una base de Gröbner del ejemplo de la página 50.

Ejemplos. Sea $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$.

Empezamos el algoritmo, entonces $G := \{f_1, f_2\}$ y $G' := G$,

$$f_3 = S(f_1, f_2) = y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2$$

Como ya vimos $\overline{f_3}^G = f_3$, entonces $G := G \cup \{f_3\}$. Por lo tanto $G \neq G'$ y continuamos con el algoritmo, ahora tomando $G' := G$. Es claro que ahora si $\overline{f_3}^G = 0$.

$$f_4 = S(f_1, f_3) = (-1)(x^3 - 2xy) - x(-x^2) = 2xy$$

También tenemos que $\overline{f_4}^G = f_4$, entonces $G := G \cup \{f_4\}$.

$$f_5 = S(f_2, f_3) = (-1)(x^2y - 2y^2 + x) - y(-x^2) = 2y^2 - x$$

También tenemos que $\overline{f_5}^G = f_5$, entonces $G := G \cup \{f_5\}$. Por lo tanto $G \neq G'$ y continuamos con el algoritmo, ahora tomando $G' := G$. Es claro que ahora si $\overline{f_4}^G = \overline{f_5}^G = 0$.

Es fácil comprobar que todos los S-polinomios generados por estos cinco polinomios se reducen a cero módulo G, por lo que solo mostraremos el procedimiento para un solo S-polinomio, $S(f_2, f_5)$:

$$S(f_2, f_5) = 2y(x^2y - 2y^2 + x) - x^2(2y^2 - x) = x^3 - 4y^3 + 2xy$$

Es claro que $f_3 | x^3$ y que $f_5 | -4y^3 + 2xy$, por lo tanto $\overline{S(f_2, f_5)}^G = 0$.

Por lo tanto $G = \{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, 2xy, 2y^2 - x\}$ es una base de Gröbner para I.

Definición. Una *base de Gröbner minimal* de un ideal I es una *base de Gröbner* G de I tal que:

(i) $\mathrm{lc}(p) = 1 \qquad \forall\, p \in G.$

(ii) $\mathrm{lt}(p) \notin \langle \mathrm{lt}(G - \{p\}) \rangle \qquad \forall\, p \in G.$

Ahora obtendremos una base de Gröbner minimal, de la base de Gröbner obtenida en el ejemplo anterior.

Lo primero que tenemos que hacer, es multiplicar a los generadores de I, por constantes de tal forma que los coeficientes principales de todos los polinomios sean iguales a 1, obteniendo la siguiente base de Gröbner:

$$\{x^3 - 2xy, x^2y - 2y^2 + x, x^2, xy, y^2 - \frac{1}{2}x\}$$

Luego eliminamos todos los polinomios f_j, tales que existe $i \neq j$ con $\mathrm{in}(f_i) | \mathrm{in}(f_j)$. Es fácil observar que $\mathrm{in}(f_3) | \mathrm{in}(f_1)$ y que $\mathrm{in}(f_3) | \mathrm{in}(f_2)$, por lo

tanto podemos eliminar a f_1 y f_2 de la base de Gröbner, es claro que estos son los únicos polinomios que podemos eliminar de esta manera, por lo tanto una base de Gröbner minimal de I es:

$$\{x^2, xy, y^2 - \frac{1}{2}x\}$$

Por otro lado, tenemos que para toda $a \in \mathbb{Q}$, $\{x^2 + axy, xy, y^2 - \frac{1}{2}x\}$, es también una base de Gröbner minimal de I, con lo cual observamos que estas bases de Gröbner minimales no son únicas, de hecho para este ejemplo en particular tenemos una infinidad de bases de Gröbner minimales, sin embargo podemos eliminar este problema, al fijarnos en la "mejor" de estas bases de Gröbner minimales.

Definición. Una *base de Gröbner reducida* de un ideal I es una *base de Gröbner* G de I tal que:

(i) $\mathrm{lc}(p) = 1 \; \forall \, p \in G$.

(ii) $\forall \, p \in G$, ningún monomio de p pertenece a $\langle \mathrm{in}(G - \{p\}) \rangle$.

Es claro que la única base de Gröbner reducida de I es obtenida cuando $a = 0$, es decir

$$\{x^2, xy, y^2 - \frac{1}{2}x\}$$

En general, tenemos el siguiente resultado, el cual esta demostrado en [9] pag. 90.

Teorema 4.11. *Dado un orden monomial $>$, la base de Gröbner reducida de un ideal I es única.*

Capítulo 5

Bases de Gröbner Asociadas a Grupos Abelianos Finitos

En este capítulo damos una breve introducción a las bases de Gröbner de ideales tóricos. Definimos el concepto de base de Gröbner asociada a un p-grupo abeliano finito, y damos sus propiedades utilizando el lenguaje introducido en la sección de ideales tóricos.

5.1 Bases de Gröbner de ideales tóricos

En esta sección estudiamos una clase especial de ideales en $K[X] = K[x_1, \ldots, x_n]$.

Sea p un número primo, fijemos primero un subconjunto $\bar{C} = \{\bar{c_1}, \ldots, \bar{c_n}\} \subset \bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}}$, con $k_i \geqslant 1$. Identificamos cada vector $\bar{c_i}$ con un monomio $\mathbf{t}^{\bar{c_i}}$ en el anillo de grupo $K[\bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}}] \cong K[t_1, \ldots, t_d]/\langle t_1^{p^{k_1}} - 1, \ldots, t_d^{p^{k_d}} - 1\rangle$, donde $\{t_1, \ldots, t_d\}$ es un conjunto de indeterminadas. Ahora consideramos el homomorfismo de semigrupos

$$\begin{array}{rccc} \gamma: & \mathbb{N}^n & \to & \bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}} \\ & \mathbf{u} = (u_1, \ldots, u_n) & \mapsto & u_1\bar{c_1} + \cdots + u_n\bar{c_n} \end{array}$$

La imagen de γ es el subgrupo de $\bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}}$

$$\mathbb{N}\bar{C} = \{\lambda_1\bar{c_1} + \cdots + \lambda_n\bar{c_n} \mid \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}.$$

La función γ se extiende a un homomorfismo de álgebras de semigrupo

$$\begin{array}{rccl} \hat{\gamma}: & K[X] & \to & K[t_1,\ldots,t_d]/\langle t_1^{p^{k_1}}-1,\ldots,t_d^{p^{k_d}}-1\rangle \\ & x_i & \mapsto & t^{\bar{c}_i} \end{array}$$

Denotamos al núcleo de $\hat{\gamma}$ por $I_{\bar{C}}$ y lo llamamos *ideal tórico* de $\bar{C}$. El lema siguiente especifica un sistema de generadores del ideal tórico $I_{\bar{C}}$.

Lema 5.1. *El ideal tórico $I_{\bar{C}}$ está generado como K-espacio vectorial por el conjunto de binomios*

$$\{\boldsymbol{x}^{\boldsymbol{u}} - \boldsymbol{x}^{\boldsymbol{v}} \mid \boldsymbol{u},\boldsymbol{v} \in \mathbb{N}^n \text{ con } \gamma(\boldsymbol{u}) = \gamma(\boldsymbol{v})\}.$$

Demostración. Un binomio $\boldsymbol{x}^{\boldsymbol{u}} - \boldsymbol{x}^{\boldsymbol{v}}$ pertenece a $I_{\bar{C}}$ si, y sólo si, $\gamma(\boldsymbol{u}) = \gamma(\boldsymbol{v})$. Por lo que es suficiente demostrar que cada polinomio en $I_{\bar{C}}$ es una combinación K-lineal de estos binomios. Fijemos un orden monomial $<$ en $K[X]$. Supongamos que $f \in I_{\bar{C}}$ no puede ser escrito como combinación lineal de binomios. Escogemos un polinomio f con esta propiedad tal que el término inicial $\text{in}(f) = \boldsymbol{x}^{\boldsymbol{u}}$ sea minimal con respecto al orden de términos $<$. Al expandir $f(t^{\bar{c}_1},\ldots,t^{\bar{c}_n})$ nos da cero. Particularmente el término $t^{\gamma(\boldsymbol{u})} = \hat{\gamma}(\boldsymbol{x}^{\boldsymbol{u}})$ debe cancelarse durante esta expansión. Entonces existe otro monomio $\boldsymbol{x}^{\boldsymbol{v}} < \boldsymbol{x}^{\boldsymbol{u}}$ en f tal que $\gamma(\boldsymbol{v}) = \gamma(\boldsymbol{u})$. Por hipótesis el polinomio $f' = f - \boldsymbol{x}^{\boldsymbol{u}} + \boldsymbol{x}^{\boldsymbol{v}}$ no puede ser escrito como una combinación K-lineal de binomios en $I_{\bar{C}}$. Pero por otro lado tenemos que $\text{in}(f') < \text{in}(f)$, lo cual es una contradicción. □

Todo vector $\boldsymbol{u} \in \mathbb{Z}^n$ puede ser escrito de manera única como $\boldsymbol{u} = \boldsymbol{u}^+ - \boldsymbol{u}^-$, donde $\boldsymbol{u}^+$ y $\boldsymbol{u}^-$ son no negativos y tienen soporte disjunto. Más precisamente, la i-ésima coordenada de $\boldsymbol{u}^+$ es igual a u_i si $u_i > 0$ o es igual a 0 en caso contrario. Si denotamos por $\ker(\gamma)$ al subgrupo (subretícula) de $\mathbb{Z}^n$ que consiste de todos los vectores u tales que $\gamma(\boldsymbol{u}^+) = \gamma(\boldsymbol{u}^-)$, entonces el lema 5.1 puede ser enunciado de la siguiente manera

Lema 5.2. $I_{\bar{C}} = \langle \boldsymbol{x}^{\boldsymbol{u}^+} - \boldsymbol{x}^{\boldsymbol{u}^-} \mid \boldsymbol{u} \in \ker(\gamma)\rangle$.

Proposición 5.3. *Para todo orden monomial $<$ existe un conjunto finito de vectores $\bar{\mathcal{G}}_\Delta \subset \ker(\gamma)$ tal que la base de Gröbner reducida de $I_{\bar{C}}$ con respecto a $<$ es igual a*

$$\mathcal{G}_{\bar{C}} := \{\boldsymbol{x}^{\boldsymbol{u}^+} - \boldsymbol{x}^{\boldsymbol{u}^-} \mid \boldsymbol{u} \in \bar{\mathcal{G}}_\Delta\}.$$

Demostración. Por el teorema de la base de Hilbert podemos seleccionar un subconjunto finito de $\ker(\gamma)$ tal que los binomios correspondientes generan a $I_{\bar{C}}$. Aplicamos el algoritmo de Buchberger a estos binomios. Las operaciones de reducción y formación de S-polinomios preservan la estructura binomial (es decir toda base de Gröbner de un ideal binomial es binomial). Además cualquier polinomio nuevo que se genere mediante este algoritmo también pertenece a $\{\boldsymbol{x}^{\boldsymbol{u}^+} - \boldsymbol{x}^{\boldsymbol{u}^-} \mid \boldsymbol{u} \in \ker(\gamma)\}$, lo cual demuestra la proposición. □

5.2 Ideales tóricos relacionados con grupos abelianos finitos

En esta sección estudiamos los ideales tóricos introducidos en la sección anterior, que aparecen relacionados con los grupos abelianos finitos. Lo cual nos permitirá desarrollar la teoría de bases de Gröbner asociadas a grupos abelianos finitos, con un lenguaje más actual al utilizado en [7].

Sea G un p-grupo abeliano finito, y sea $\mathcal{B} = \{b_1, \ldots, b_d\}$ una p-base de G. Ahora sea $C = \{c_1, \ldots, c_n\}$ con $n \geqslant d$, un conjunto generador de G. Cada elemento c_i de C, puede descomponerse en forma única como $c_i = c_{i_1} b_1 + \cdots + c_{i_d} b_d$, con $0 \leqslant c_{i_j} < o(b_j)$, para toda $j \in [1, d]$, por lo tanto podemos identificar a cada c_i con $\bar{c}_i = (c_{i_1}, \ldots, c_{i_d}) \in \bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}}$, con $p^{k_j} = o(b_j)$, para toda $j \in [1, d]$.

Entonces tenemos un conjunto $\bar{C} = \{\bar{c_1}, \ldots, \bar{c_n}\} \subset \bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}}$ y el homomorfismo de semigrupos

$$\begin{array}{rccc} \gamma: & \mathbb{N}^n & \to & \bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}} \\ & \boldsymbol{u} = (u_1, \ldots, u_n) & \mapsto & u_1\bar{c_1} + \cdots + u_n\bar{c_n} \end{array}$$

Como ya vimos en la sección anterior esta función puede extenderse a un homomorfismo entre álgebras de semigrupo

$$\begin{array}{rccc} \hat{\gamma}: & K[X] & \to & K[t_1, \ldots, t_d]/\langle t_1^{p^{k_1}} - 1, \ldots, t_d^{p^{k_d}} - 1\rangle \\ & x_i & \mapsto & t^{\bar{c}_i} \end{array}$$

El núcleo de $\hat{\gamma}$ es un ideal tórico, el cual denotamos por $I_{\bar{C}}$. Por lo tanto se cumplen los resultados obtenidos en la sección anterior para este tipo de ideales.

Ahora supongamos que Δ es un conjunto de relaciones de G, de tal forma que (Δ, C) es una presentación de G. Supongamos que las relaciones en Δ se

escriben de la siguiente manera

$$u_1c_1 + \cdots + u_nc_n = 0 \quad \text{con } \boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n$$

Usando la notación $\boldsymbol{u}^+$ y $\boldsymbol{u}^-$, podemos escribir las relaciones en Δ de la siguiente manera

$$u_1^+c_1 + \cdots + u_n^+c_n = u_1^-c_1 + \cdots + u_n^-c_n$$

donde $\boldsymbol{u}^+ = (u_1^+, \ldots, u_n^+) \in \mathbb{N}^n$ y $\boldsymbol{u}^- = (u_1^-, \ldots, u_n^-) \in \mathbb{N}^n$. Luego, se tiene que $\gamma(\boldsymbol{u}^+) = \gamma(\boldsymbol{u}^-)$.

Denotemos por

$$\bar{\Delta} = \{\boldsymbol{u} \in \mathbb{Z}^n \mid u_1c_1 + \cdots + u_nc_n = 0 \in \Delta\}.$$

Entonces tenemos el siguiente teorema

Teorema 5.4. *Sea (C, Δ) una presentación de G. Entonces $\bar{\Delta}$ genera a* $\ker(\gamma)$.

Demostración. Tenemos que $\ker(\gamma) = \{\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n \mid \gamma(\boldsymbol{u}^+) = \gamma(\boldsymbol{u}^-)\}$. Por lo tanto si $\boldsymbol{u} \in \ker(\gamma)$ entonces $u_1c_1 + u_2c_2 + \cdots + u_nc_n = 0$.

Como (C, Δ) es una presentación de G entonces tenemos que $G \cong \mathbb{Z}^n/\langle\bar{\Delta}\rangle$, donde $\langle\bar{\Delta}\rangle$ es el subgrupo generado por $\bar{\Delta}$. Esto quiere decir que si $u \in \ker(\gamma)$ entonces $u \in \langle\bar{\Delta}\rangle$.

Finalmente por la definición de $\bar{\Delta}$ es claro que $\langle\bar{\Delta}\rangle \subset \ker(\gamma)$. □

Si definimos $\mathcal{G}_\Delta := \{u_1c_1 + u_2c_2 + \cdots + u_nc_n = 0 \mid \boldsymbol{u} = (u_1, \ldots, u_n) \in \bar{\mathcal{G}}_\Delta\}$ entonces tenemos el siguiente teorema.

Teorema 5.5. *$\mathcal{G}_\Delta$ es un sistema de relaciones asociadas a C de G, es decir $(\mathcal{G}_\Delta, C)$ es otra presentación de G.*

Demostración. Sea Δ un sistema de relaciones asociadas a C de G, por lo que tenemos que $G \cong \mathbb{Z}^n/\langle\bar{\Delta}\rangle$. Es suficiente demostrar que $\langle\bar{\Delta}\rangle = \langle\bar{\mathcal{G}}_\Delta\rangle$.

Por el teorema 5.4 tenemos que $\langle\bar{\Delta}\rangle = \ker(\gamma)$, entonces tenemos que $\{\boldsymbol{x}^{\boldsymbol{u}^+} - \boldsymbol{x}^{\boldsymbol{u}^-} \mid \boldsymbol{u} \in \bar{\Delta}\}$ genera a $I_{\bar{C}}$ como ideal. En efecto, si $\boldsymbol{u_1} = \boldsymbol{u_1^+} - \boldsymbol{u_1^-} \in \bar{\Delta}$ y $\boldsymbol{u_2} = \boldsymbol{u_2^+} - \boldsymbol{u_2^-} \in \bar{\Delta}$ y sea $\boldsymbol{v} = \boldsymbol{u_1} + \boldsymbol{u_2} \in \ker(\gamma)$, entonces

$$\boldsymbol{x}^{\boldsymbol{v}^+} - \boldsymbol{x}^{\boldsymbol{v}^-} = \boldsymbol{x}^{\boldsymbol{u_2^+}}(\boldsymbol{x}^{\boldsymbol{u_1^+}} - \boldsymbol{x}^{\boldsymbol{u_1^-}}) + \boldsymbol{x}^{\boldsymbol{u_1^-}}(\boldsymbol{x}^{\boldsymbol{u_2^+}} - \boldsymbol{x}^{\boldsymbol{u_2^-}})$$

Similarmente si v tiene más sumandos, por lo que

$$I_{\bar{C}} = \left\langle x^{u^+} - x^{u^-} \mid u \in \bar{\Delta} \right\rangle$$

Aplicando el algoritmo de Buchberger a este conjunto de polinomios obtenemos una base de Gröbner $\mathcal{G}$ de $I_{\bar{C}}$. Ahora nos fijaremos en un paso de este proceso.

Llamamos $P(v)$ al binomio $x^{v^+} - x^{v^-}$, con $v \in \Delta$. Sean $u_1, u_2 \in \bar{\Delta}$, sin perdida de generalidad suponemos que $\text{in}(P(u_1)) = x^{u_1^+}$ e $\text{in}(P(u_2)) = x^{u_2^+}$. Entonces existen $w_1, w_2 \in \mathbb{N}^n$ tales que el S-polinomio de $P(u_1)$ y $P(u_2)$ es igual a

$$\begin{aligned} S(P(u_1), P(u_2)) &= x^{w_1}(x^{u_1^+} - x^{u_1^-}) - x^{w_2}(x^{u_2^+} - x^{u_2^-}) \\ &= x^{w_2+u_2^-} - x^{w_1+u_1^-} \end{aligned}$$

Como $w_1 + u_1^+ = w_2 + u_2^+$, entonces $\gamma(w_2 + u_2^-) = \gamma(w_2 + u_2^+) = \gamma(w_1 + u_1^+) = \gamma(w_1 + u_1^-)$, por lo que si $v = (w_2 + u_2^-) - (w_1 + u_1^-)$, entonces $P(v) = S(P(u_1), P(u_2))$ y $v \in \ker(\gamma)$. Más aún, $v = (w_2+u_2^-)-(w_1+u_1^-) = (w_2+u_2^-)-(w_1+u_1^-)+(w_1+u_1^+)-(w_2+u_2^+) = (u_1^+-u_1^-)-(u_2^+-u_2^-) = u_1 - u_2$. Por lo tanto tenemos que

$$\langle \bar{\Delta} \rangle = \langle \bar{\Delta} \cup \{v\} \rangle$$

Sea Ω el conjunto de todos los S-polinomios generados por el algoritmo de Buchberger. Entonces por el razonamiento anterior tenemos que, si $\bar{\Omega} = \{v \in \mathbb{Z}^n \mid P(v) \in \Omega\} \subset \ker(\gamma)$ entonces

$$\langle \bar{\Delta} \rangle = \langle \bar{\Delta} \cup \bar{\Omega} \rangle$$

Llamamos $\bar{\Theta} = \bar{\Delta} \cup \bar{\Omega}$, entonces tenemos que

$$\mathcal{G} = \{P(v) \mid v \in \bar{\Theta}\}$$

Ahora reducimos esta base de Gröbner. Fijemonos en un paso de la reducción. Sea $v \in \bar{\Theta}$, si existe $u \in \bar{\Theta} \backslash \{v\}$ tal que $\text{in}(x^{u^+} - x^{u^-})$ divide a algún término de $x^{v^+} - x^{v^-}$ (sin perdida de generalidad suponemos que $\text{in}(x^{u^+} - x^{u^-}) = x^{u^+}$ divide a x^{v^+}), entonces al reducir obtenemos

$$x^{v^+} - x^{v^-} - x^w(x^{u^+} - x^{u^-}) = x^{w+u^-} - x^{v^-}$$

Para algún $w \in \mathbb{N}^n$. Si definimos

$$u_1 = u_1^+ - u_1^- = (w + u^-) - v^-$$

Entonces tenemos que $\gamma(u_1^+) = \gamma(w) + \gamma(u^-) = \gamma(w) + \gamma(u^+) = \gamma(v^+) = \gamma(v^-) = \gamma(u_1^-)$. Por lo tanto $u_1 \in \ker(\gamma)$. Por otro lado tenemos que

$$\begin{aligned} v &= w + u^+ - v^- \\ &= w + u^+ - v^- + (w + u^-) - (w + u^-) \\ &= (u^+ - u^-) + (u_1^+ - u_1^-) \end{aligned}$$

Por lo tanto tenemos que

$$\langle \bar{\Delta} \rangle = \langle \bar{\Theta} \rangle = \langle (\bar{\Theta} \cup \{u_1\}) - \{v\} \rangle$$

y además

$$\mathcal{G}' = \{P(w) \mid w \in (\bar{\Theta} \cup \{u_1\}) - \{v\}\}$$

es tambien una base de Gröbner de I_C.

Por la unicidad de las bases de Gröbner reducidas tenemos que

$$\langle \bar{\Delta} \rangle = \langle \bar{\mathcal{G}}_\Delta \rangle$$

Es decir $\mathcal{G}_\Delta$ es un sistema de relaciones asociado a C de G. □

5.3 Bases de Gröbner asociadas a GAF

En esta sección desarrollamos la teoría de bases de Gröbner asociadas a grupos abelianos finitos, utilizando la notación y los resultados de bases de Gröbner de ideales tóricos.

Sea $K[X] = K[x_1, \ldots, x_n]$ el anillo de polinomios en n indeterminadas y T el monoide libre abeliano generado por el conjunto de indeterminadas X, y sea $<$ un orden monomial en T.

Además sea G un p-grupo abeliano finito generado por el conjunto $C = \{c_1, \ldots, c_n\}$. Sea $\mathcal{B} = \{b_1, \ldots, b_d\}$ una p-base de G.[1] Entonces cada elemento c_i de C se descompone en forma única de la siguiente manera $c_i = b_1^{c_{i_1}} b_2^{c_{i_2}} \cdots b_d^{c_{i_d}}$,

[1] Cuando veamos a G como el grupo generado por $\mathcal{B}$ usaremos la notación multiplicativa.

con $0 \leqslant c_{i_j} < o(b_j)$ para toda $j \in [1,d]$, por lo tanto podemos identificar a cada c_i con $\bar{c_i} = (c_{i_1}, \ldots, c_{i_d}) \in \bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}}$, con $p^{k_j} = o(b_j)$, para toda $j \in [1,d]$.

Definimos al homomorfismo γ' de la siguiente manera

$$\begin{array}{rccc} \gamma' : & T & \to & G \\ & x_i & \mapsto & c_i \end{array}$$

Como $T \cong \mathbb{N}^n$, dado por el isomorfismo $x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n} \mapsto (u_1, \ldots, u_n)$ entonces γ' induce al homomorfismo γ definido al principio del capítulo.

$$\begin{array}{rccc} \gamma : & \mathbb{N}^n & \to & \bigoplus_{i=1}^{d} \mathbb{Z}_{p^{k_i}} \\ & \boldsymbol{u} = (u_1, \ldots, u_n) & \mapsto & u_1\bar{c_1} + \cdots + u_n\bar{c_n} \end{array}$$

Sea $\tilde{\gamma}$ la extensión natural de γ' a un homomorfismo entre las K-álgebras $K[T]$ y $K[G]$.

Sea $\hat{\gamma}$ el homomorfismo

$$\begin{array}{rccc} \hat{\gamma} : & K[X] & \to & K[\boldsymbol{b}^{\pm 1}] \\ & x_i & \mapsto & \boldsymbol{b}^{\bar{c_i}} \end{array}$$

Donde $\boldsymbol{b} = b_1 b_2 \cdots b_d$, y $K[\boldsymbol{b}^{\pm 1}]$ es el anillo de grupo de G. Entonces $\ker(\hat{\gamma})$ es el ideal tórico denotado por I_C.

Por la definición de γ' tenemos que $x_i \mapsto c_i$ y por la definición de $\mathcal{B}$ tenemos que para toda i, hay una correspondencia biyectiva entre c_i y $b_1^{c_{i_1}} b_2^{c_{i_2}} \cdots b_d^{c_{i_d}}$, tomando $0 \leqslant c_{i_k} < o(b_k)$ para toda $k \in [1,d]$. Por lo que identificando a cada c_i con $\boldsymbol{b}^{\bar{c_i}}$ tenemos que se cumple la siguiente proposición

Proposición 5.6.

$$\ker(\tilde{\gamma}) = \ker(\hat{\gamma}).$$

Definición. La base de Gröbner asociada a G con respecto a $(<, C)$ es la base de Gröbner reducida con respecto a $<$ del $\ker(\tilde{\gamma}) = I_C$, y la denotamos por $\mathcal{G}_C$.

Lema 5.7.

(i) Para cada $c \in G$, existe $w \in T$ (que denotaremos w_c), mínimo con respecto a $<$, tal que $\tilde{\gamma}(w) = c$.

(ii) $w \in \text{std}(\mathcal{G}_C)$ *si, y sólo si,* $w = w_{\tilde{\gamma}(w)}$.

Demostración. (i) : w_c existe porque $<$ es un buen orden.
(ii) : $w \neq w_{\tilde{\gamma}(w)}$ si, y sólo si, existe $v < w$ tal que $\tilde{\gamma}(v) = \tilde{\gamma}(w)$, esto es, si, y sólo si, $w \in \langle \text{in}(\mathcal{G}_C) \rangle$, pues si $\tilde{\gamma}(v) = \tilde{\gamma}(w)$ entonces $\tilde{\gamma}(v) - \tilde{\gamma}(w) = 0$, es decir $\tilde{\gamma}(w - v) = 0$ por lo tanto $w - v \in \ker(\tilde{\gamma})$ entonces $w \in \text{in}(I_C)$. □

Definición. w_c se denomina la menor representación del elemento c con respecto a $<$.

El siguiente teorema pertenece a la teoría general de bases de Gröbner, pero por ser un teorema técnico que utilizamos en las demostraciones de los teoremas siguientes, lo enunciamos en este capítulo.

Notación. Sea $t = \prod_{i=1}^{r} x_i \in T$, con $m \geqslant 2$ entonces denotamos

- $\text{si}(t) = \prod_{i=1}^{r-1} x_i$,
- $\text{sf}(t) = \prod_{i=2}^{r} x_i$.

Teorema 5.8. *Sea* $\mathcal{G}$ *una base de Gröbner reducida de un ideal* I *con respecto a* $>$, *entonces*

(i) Para cada $t \in \text{in}(I)$ *se cumple una y sólo una de las siguientes condiciones*

(1) $t \in X = \{x_1, \ldots, x_n\}$

(2) $l(t) \geqslant 2$ *y existe* $x_i \in X \cap \text{in}(I)$ *tal que* $t = \text{si}(t)x_i$

(3) Existen $t_1 \in T$ *(posiblemente* 1*),* $x_i \in X$, $w \in \text{std}(\mathcal{G})$, *tales que* $x_i w \in \text{in}(I)$ *y* $t = t_1 x_i w$

(ii) Si $x_i \in X$, $w \in \text{std}(\mathcal{G})$, $(w \neq 1)$, *y* $\text{si}(x_i w) \in \text{std}(\mathcal{G})$, *entonces no existe* $t \in \text{in}(I)$ *tal que* $t \neq x_i w$ *y* $t | x_i w$

(iii) $\text{in}(\mathcal{G})$ *esta formado por los términos* $t \in T$ *que pertenecen a uno de los siguientes tipos*

Tipo I: $t \in X \cap \text{in}(I)$

Tipo II: $t = x_i w$, *donde* $x_i \in X$, $w \in \text{std}(\mathcal{G})$ *y* $\text{si}(x_i w) \in \text{std}(\mathcal{G})$

Demostración. (i) : Si $t \in X$ entonces (i_1) se cumple, si $t \notin X$ entonces $l(t) \geqslant 2$ por lo tanto existe $v \in T$ y $x_i \in X$ tal que $t = vx_i$ si $x_i \in \text{in}(I)$ entonces (i_2) se cumple, si $x_i \notin \text{in}(I)$ entonces $t = \text{si}(v)x_jx_i = v_2w_2$ si $w_2 \in \text{in}(I)$ entonces $w = x_i$, $t_1 = v_2$ y $t = t_1x_jw$ cumple con (i_3) si $w_2 \notin \text{in}(I)$ entonces $t = \text{si}(v_2)x_kw_2 = v_3w_3$ si $w_3 \in \text{in}(I)$ entonces $t = v_3x_kw_2$ cumple con (i_3) en caso contrario, continuamos con el mismo proceso un número finito de pasos hasta obtener $t = t_1x_iw$ que cumple con (i_3) lo cual demuestra (i).

(ii) : Sea $v = x_iw \in T$ tal que $w \in \text{std}(\mathcal{G})$ y $\text{si}(v) \in \text{std}(G)$, suponemos que existe $t \in \text{in}(I)$ tal que $t|v$ entonces $v \in \text{in}(I)$, como $w \in \text{std}(\mathcal{G})$ entonces $t \nmid w$, es decir $t = x_iu$ para alguna $u \in T$ distinta de 1 (de lo contrario $\text{si}(x_iw) \notin \text{std}(\mathcal{G})$), por otro lado como $\text{si}(v) \in \text{std}(\mathcal{G})$ entonces $t \nmid \text{si}(v)$, lo cual implica que $u \nmid \text{si}(w)$ y como $u|w$ entonces $u = w$ y $t = x_iw$.

(iii) : Es claro que el coeficiente principal de los términos de tipo I y tipo II es igual a 1, además para toda i tenemos que x_i no puede ser dividido por algún término en $\langle \text{in}(\mathcal{G}) - \{x_i\}\rangle$, y por el inciso (ii) tenemos que ningún término t de tipo II, puede ser dividido por algún término en $\langle \text{in}(\mathcal{G}) - \{t\}\rangle$. Por lo tanto basta demostrar que los términos de tipo I y tipo II, genera a $\text{in}(I)$, es decir basta demostrar que si $t \in \text{in}(I)$, entonces t es múltiplo de algún término tipo I o tipo II.

Sea $t \in \text{in}(I)$, por el inciso (i) tenemos lo siguiente, si t cumple (i_1) entonces $t \in X$ y por lo tanto t es de tipo I, si t cumple (i_2) entonces $t = \text{si}(t)x_i$ con $x_i \in X \cap \text{in}(I)$ es decir $x_i|t$ y x_i es de tipo I. Supongamos t cumple con (i_3) es decir $t = t_ix_iw$ con $x_i \in X$, $w \in \text{std}(\mathcal{G})$ y $x_iw \in \text{in}(I)$ si $\text{si}(x_iw) \in \text{std}(\mathcal{G})$ entonces habremos concluido, en caso contrario repetimos el procedimiento un número finito de veces, empezando ahora con $\text{si}(x_iw)$, hasta obtener el resultado deseado. Luego, el conjunto de los términos tipo I y tipo II es generador de $\text{in}(I)$. □

Teorema 5.9. *$\mathcal{G}_C$ esta formada por los siguientes tipos de binomios:*

Tipo I: $x_i - w_{c_i}$ *donde* $x_i > w_{c_i}$,

Tipo II: $x_iw_c - w_{c_ic}$ *donde* $x_i \in X$, $c \in G$, $x_iw_c > w_{c_ic}$ *y* $\text{si}(x_iw_c) \in \text{std}(\mathcal{G}_C)$.

Demostración.

$$\tilde{\gamma}(x_i - w_{c_i}) = \tilde{\gamma}(x_i) - \tilde{\gamma}(w_{c_i}) = c_i - c_i = 0$$
$$\tilde{\gamma}(x_iw_c - w_{c_ic}) = \tilde{\gamma}(x_iw_c) - \tilde{\gamma}(w_{c_ic}) = c_ic - c_ic = 0$$

Entonces $x_i - w_{c_i} \in I_C$ de donde $x_i \in X \cap \text{in}(I_C)$ por el teorema 5.8 inciso (iii) tenemos que $x_i \,\text{in}(\mathcal{G}_C)$. Además $x_iw_c - w_{c_ic} \in I_C$ luego $x_iw_c \in \text{in}(I_C)$ con

$x_i \in X$ y además por hipótesis si$(x_i w_c) \in \text{std}(\mathcal{G}_C)$. Por el lema 5.7 inciso (ii) tenemos que $w_c \in \text{std}(\mathcal{G}_C)$ entonces por el teorema 5.8 inciso (iii) tenemos que $x_i w_c \in \text{in}(\mathcal{G}_C)$. Por el teorema 5.8 inciso (i) tenemos que los términos iniciales de los binomios tipo I y tipo II generan a $\text{in}(I_C)$.

Por otra parte, por definición tenemos que el coeficiente principal de estos binomios es igual a 1. Sabemos que para toda i tenemos que x_i no puede ser dividido por algún término en $\langle \text{in}(\mathcal{G}_C - \{x_i\})\rangle$ y como para toda $c \in G$ por el lema 5.7 inciso (ii) tenemos que $w_c \in \text{std}(\mathcal{G}_C)$ entonces w_c no puede ser dividido por algún término en $\langle \text{in}(\mathcal{G}_C - \{w_c\})\rangle$, finalmente por el teorema 5.8 inciso (ii) tenemos que para toda $c \in G$ y para toda i, $x_i w_c$ no puede ser dividido por algún término en $\langle \text{in}(\mathcal{G}_C - \{x_i w_c\})\rangle$.

Por la unicidad de la base de Gröbner reducida tenemos que el conjunto de los términos iniciales de los binomios tipo I y tipo II es igual a $\text{in}(\mathcal{G}_C)$. □

El siguiente teorema resume los resultados más importantes obtenidos en este capítulo.

Teorema 5.10.

(i) $\mathcal{G}_\Delta$ *es un sistema de relaciones para* C *de* G*, es decir* $(\mathcal{G}_\Delta, C)$ *es una presentación de* G*.*

(ii) Si Δ *es un sistema de relaciones para* C *de* G*, entonces* $\bar{\Delta}$ *genera al* $\ker(\gamma)$

(iii) Si Δ *es un sistema de relaciones para* C *de* G*, entonces la base de Gröbner reducida del ideal* $I(\Delta) = \left\langle X^{\boldsymbol{u}^+} - X^{\boldsymbol{u}^-} \mid \boldsymbol{u} \in \bar{\Delta} \right\rangle$ *es* $\mathcal{G}_C$*.*

Demostración. El inciso (i) es el teorema 5.5, el inciso (ii) es el teorema 5.4.

El inciso (iii) es consecuencia directa de (ii), y de la proposición 5.3, pues por (ii) sabemos que $\bar{\Delta}$ es un subconjunto finito que genera al $\ker(\gamma)$, por el lema 5.2 y la proposición 5.3 tenemos que $I(\Delta) = I_C$ y por la unicidad de las bases de Gröbner reducidas tenemos que la base de Gröbner reducida de $I(\Delta)$ es $\mathcal{G}_C$. □

Observación. Basándonos en el inciso (iii) del teorema anterior, $\mathcal{G}_C$ puede ser obtenida a partir de un conjunto de relaciones de G.

Teorema 5.11. *Sea G un grupo abeliano finito, $C = \{c_1, \ldots, c_n\}$ un subconjunto generador de G. Para toda $k \in [1,n]$, y para toda $i \in [1, k-1]$, sean m_k y n_{k_i} los exponentes definidos en el teorema 1.5, es decir m_1 es el orden de c_1; para cada $k \in [2,n]$, $m_k c_k = \sum_{i=1}^{k-1} n_{k_i} c_i$, donde $m_k = min\{m > 0 \mid mc_k \in \langle c_1, \ldots, c_{k-1}\rangle\}$, y además $n_{k_i} \in [0, m_i)$. Supongamos además que X esta ordenado de la siguiente forma $x_1 < x_2 < \cdots < x_n$ y que el orden $<$ es el orden lexicográfico, entonces*

$$\mathcal{G}_C = \{x_1^{m_1} - 1, x_2^{m_2} - x_1^{n_{2_1}}, \ldots, x_n^{m_n} - \prod_{i=1}^{n-1} x_i^{n_{n_i}}\}$$

Demostración. Por definición de los exponentes, tenemos que $\mathcal{G} := \{x_1^{m_1} - 1, x_2^{m_2} - x_1^{n_{2_1}}, \ldots, x_n^{m_n} - \prod_{i=1}^{n-1} x_i^{n_{n_i}}\}$ esta contenido en $I_C = \ker(\tilde{\gamma})$, ya que

$$\begin{aligned}\tilde{\gamma}(x_k^{m_k} - \prod_{i=1}^{k-1} x_i^{n_{k_i}}) &= \tilde{\gamma}(x_k^{m_k}) - \tilde{\gamma}(\prod_{i=1}^{k-1} x_i^{n_{k_i}}) \\ &= m_k c_k - \sum_{i=1}^{k-1} n_{k_i} c_i = 0\end{aligned}$$

Por otro lado el término inicial del binomio k-ésimo es igual a $x_k^{m_k}$ por lo que su coeficiente principal es igual a 1, además $x_k^{m_k}$ no es divisible por algún término de $\text{in}(\mathcal{G}) - \{x_k^{m_k}\}$. Ahora nos fijamos en el término $\prod_{i=1}^{k-1} x_i^{n_{k_i}}$ del binomio k-ésimo, es claro que ningún $x_j^{m_j}$ con $j > k$ divide a $\prod_{i=1}^{k-1} x_i^{n_{k_i}}$ pues por hipótesis tenemos que $<$ es el orden lexicográfico con las indeterminadas ordenadas de manera natural, es decir $x_1 < x_2 < \cdots < x_n$. Si $x_j^{m_j}$ con $j < k$ divide a $\prod_{i=1}^{k-1} x_i^{n_{k_i}}$ entonces $m_j \leqslant n_{k_j}$, pero por hipótesis tenemos que $n_{k_j} < m_j$. Luego $\prod_{i=1}^{k-1} x_i^{n_{k_i}}$ no es divisible por algún término de $\text{in}(\mathcal{G} - \{x_k^{m_k} - \prod_{i=1}^{k-1} x_i^{n_{k_i}}\})$.

Solo resta probar que $\text{in}(\mathcal{G})$ genera a $\text{in}(I_C)$, esto lo haremos en la proposición siguiente. □

Notación. Sea $\boldsymbol{u} \in \mathbb{Z}^n$, si $u_k > 0$ para toda $k \in [1,n]$, entonces decimos que $\boldsymbol{u} > 0$.

Proposición 5.12.

(i) Para todo $c \in G$ existe $(u_1, \ldots, u_n)$ tal que $(m_1 - u_1, \ldots, m_n - u_n) > 0$ y $c = \sum_{l=1}^{n} u_l c_l$.

(ii) *Si* $(u_1,\ldots,u_n) \neq (v_1,\ldots,v_n)$, $(m_1-u_1,\ldots,m_n-u_n) > 0$, $(m_1-v_1,\ldots,m_n-v_n) > 0$, *y* $a = \sum_{l=1}^{n} u_l c_l$, $b = \sum_{l=1}^{n} v_l c_l$, *entonces* $a \neq b$.

(iii) *Sea* $c = \sum_{l=1}^{n} u_l c_l$, *entonces* $\prod_{l=1}^{n} x_l^{u_l} = w_c$ *si, y sólo si,* $(m_1-u_1,\ldots,m_n-u_n) > 0$.

(iv) $\mathrm{in}(\mathcal{G})$ *genera a* $\mathrm{in}(I_C)$, *con* $\mathcal{G} = \{x_1^{m_1}-1, x_2^{m_2}-x_1^{n_{21}},\ldots,x_n^{m_n}-\prod_{i=1}^{n-1} x_i^{n_{ni}}\}$.

Demostración. (i) : Como C genera a G entonces existe $(u_1',\ldots,u_n')$ tal que $c = \sum_{l=1}^{n} u_l' c_l$, sea $k = max\{l \mid u_l' \geqslant m_l\}$, es decir $u_k' = qm_k + r$, con $r < m_k$, entonces

$$\begin{aligned} c &= \sum_{l=1}^{k-1} u_l' c_l + qm_k c_k + rc_k + \sum_{l=k+1}^{n} u_l' c_l \\ &= \sum_{l=1}^{k-1} u_l' c_l + q(\sum_{l=1}^{k-1} n_{k_l} c_l) + rc_k + \sum_{l=k+1}^{n} u_l' c_l \\ &= \sum_{l=1}^{k-1} (u_l' + qn_{k_l}) c_l + rc_k + \sum_{l=k+1}^{n} u_l' c_l \end{aligned}$$

Continuamos de la misma manera hasta obtener en un número finito de pasos, $c = \sum_{l=1}^{n} u_l c_l$, con $(m_1-u_1,\ldots,m_n-u_n) > 0$.

(ii) : Supongamos $a = b$, y sea $k = max\{l \mid u_l \neq v_l\}$, suponemos sin perdida de generalidad que $u_k > v_k$, entonces $(u_k - v_k)c_k \in \langle c_1,\ldots,c_{k-1}\rangle$, pero esto no es posible ya que $u_k - v_k \in (0, m_k)$.

(iii) : Supongamos $\prod_{l=1}^{n} x_l^{u_l} = w_c$, si $m_k \leqslant u_k$ para algún $k \in [1,n]$, entonces

$$\prod_{l=1}^{n} x_l^{u_l} > (\prod_{l=1}^{k-1} x_l^{u_l}) x_k^{u_k-m_k} (\prod_{i=1}^{k-1} x_i^{n_{k_i}}) \prod_{l=k+1}^{n} x_l^{u_l} \geqslant w_c$$

Para la otra implicación, supongamos que $\prod_{l=1}^{n} x_l^{u_l} \neq w_c$, entonces por el inciso (i) existe $(v_1,\ldots,v_n) \neq (u_1,\ldots,u_n)$, tal que $(m_1-v_1,\ldots,m_n-v_n) > 0$, más aún $\prod_{l=1}^{n} x_l^{v_l} < \prod_{l=1}^{n} x_l^{u_l}$ y $c = \sum_{l=1}^{n} v_l c_l$, por hipótesis $(m_1-u_1,\ldots,m_n-u_n) > 0$ y $c = \sum_{l=1}^{n} u_l c_l$, entonces por el inciso (ii) tenemos que $c \neq c$, lo cual es una contradicción.

(iv) : Es equivalente a (iii).

Como estamos utilizando $<_{lex}$, entonces por (iii) tenemos que todos los binomios en $\mathcal{G}$ son de tipo I o tipo II. Falta demostrar que cualquier binomio tipo I o tipo II esta en $\mathcal{G}$. Sea $r \in I$, supongamos que $\text{in}(r) \notin \text{in}(\mathcal{G})$ entonces $\text{in}(r) = x_1^{u_1} \cdots x_n^{u_n}$, con $u_j < m_j$ para toda j, pues de lo contrario $\text{in}(r) \in \text{in}(\mathcal{G})$, por el inciso (iii) tenemos que existe $c \in G$ tal que $\text{in}(r) = w_c$, pero w_c no es de tipo I y tampoco es de tipo II, lo cual concluye la demostración. $\square$

Capítulo 6

p-Bases de Gröbner Asociadas Módulos Finitos

En este capítulo definimos el concepto de p-base de Gröbner asociada a un módulo finito. Modelamos el problema de encontrar una p-base de un $\mathbb{Z}_{p^n}C_p$-módulo cadena abierta de la forma $\mathscr{C} = (i, j)$, utilizando la teoría de bases de Gröbner asociadas a grupos abelianos finitos y este nuevo concepto de p-base de Gröbner.

6.1 p-base de Gröbner asociada a un módulo finito

En esta sección definimos el concepto de p-base de Gröbner asociada a un módulo finito, además enunciamos y demostramos algunos resultados acerca de este concepto.

Sea G un p-grupo abeliano finito y C un conjunto generador de G, nuestra meta es encontrar una p-base de G. Observamos que las relaciones de una p-base están dadas por el orden de los elementos en G. Por otro lado, el teorema 5.11 muestra que en la base de Gröbner asociada a este grupo aparecen polinomios de la forma $x_i^{p^{k_i}} - 1$, que bajo $\tilde{\gamma}$ nos da $p^{k_i}c_i = 0$ en G. Esta observación motivó la formulación del siguiente teorema, el cual introduce una propiedad extra a la base de Gröbner encontrada en el teorema 5.11.

Teorema 6.1. *Sea $C = \{c_1, \ldots, c_q\}$ un conjunto generador del p-grupo abeliano finito G, y sean $k_1, \ldots, k_s$ mayores que 1. Entonces*

$$\begin{aligned} \mathcal{G}_C = \{&x_1^{p^{k_1}} - 1, \ldots, x_i^{p^{k_i}} - (\prod_{l=1}^{i-1} x_l^{n'_{i_l}})^{p^{k_i}}, \ldots, x_s^{p^{k_s}} - (\prod_{l=1}^{s-1} x_l^{n'_{s_l}})^{p^{k_s}}, \\ &x_{s+1} - \prod_{l=1}^{s} x_l^{n_{(s+1)_l}}, \ldots, x_q - \prod_{l=1}^{q-1} x_l^{n_{q_l}}\}, \end{aligned} \tag{6.1}$$

si, y sólo si,

$$\mathcal{B} = \{c_1, \ldots, c_i - \sum_{l=1}^{i-1} n'_{i_l} c_l, \ldots, c_s - \sum_{l=1}^{s-1} n'_{s_l} c_l\}$$

es una p-base de G.

Demostración. Por el teorema 5.5 $\mathcal{G}_\Delta$ es un conjunto de relaciones de definición asociado a C de G.

Si $\mathcal{B}$ es una p-base, entonces las relaciones de definición asociadas a $\mathcal{B}$ expresan el orden de cada uno de los elementos y las demás relaciones asociadas a C dicen que los elementos que no están en la p-base son combinaciones lineales con coeficientes enteros de los elementos de $\mathcal{B}$. Entonces por el teorema 5.11 la base de Gröbner asociada a G con respecto a C es

$$\begin{aligned} \mathcal{G}_C = \{&x_1^{p^{k_1}} - 1, \ldots, x_i^{p^{k_i}} - (\prod_{l=1}^{i-1} x_l^{n'_{i_l}})^{p^{k_i}}, \ldots, x_s^{p^{k_s}} - (\prod_{l=1}^{s-1} x_l^{n'_{s_l}})^{p^{k_s}}, \\ &x_{s+1} - \prod_{l=1}^{s} x_l^{n_{(s+1)_l}}, \ldots, x_q - \prod_{l=1}^{q-1} x_l^{n_{q_l}}\}, \end{aligned}$$

Ahora probaremos la primera implicación. Supongamos que $\mathcal{G}_C$ tiene la forma deseada, es decir

$$\begin{aligned} \mathcal{G}_C = \{&x_1^{p^{k_1}} - 1, \ldots, x_i^{p^{k_i}} - (\prod_{l=1}^{i-1} x_l^{n'_{i_l}})^{p^{k_i}}, \ldots, x_s^{p^{k_s}} - (\prod_{l=1}^{s-1} x_l^{n'_{s_l}})^{p^{k_s}}, \\ &x_{s+1} - \prod_{l=1}^{s} x_l^{n_{(s+1)_l}}, \ldots, x_q - \prod_{l=1}^{q-1} x_l^{n_{q_l}}\}, \end{aligned}$$

Entonces aplicando el homomorfismo $\tilde{\gamma}$ obtenemos que los elementos de C satisfacen las siguientes relaciones

$$\begin{aligned} p^{k_1}c_1 &= 0 \\ &\vdots \\ p^{k_i}(c_i - \sum_{l=1}^{i-1} n'_{i_l}c_l) &= 0 \\ &\vdots \\ p^{k_s}(c_s - \sum_{l=1}^{s-1} n'_{s_l}c_l) &= 0 \end{aligned}$$

Por las hipótesis del teorema 5.11 tenemos que los números $p^{k_1}, \ldots, p^{k_s}$ son las mínimas potencias de p que satisfacen estas igualdades, luego son el orden de estos elementos.

Llamamos $b_1 = c_1, \ldots, b_s = c_s - \sum_{l=1}^{s-1} n'_{s_l}c_l$. Demostraremos que $\{b_1, \ldots b_s\}$ es un conjunto linealmente independiente. Sea

$$b \in \langle b_i \rangle \cap \langle b_1, \ldots, b_{i-1} \rangle$$

Entonces $b = d_i b_i = \sum_{l=1}^{i-1} d_l b_l$, como $b_i = c_i - \sum_{l=1}^{i-1} n'_{i_l}c_l$, entonces $d_i c_i - d_i \sum_{l=1}^{i-1} n'_{i_l}c_l = \sum_{l=1}^{i-1} d_l b_l$, de donde

$$d_i c_i - \sum_{l=1}^{i-1} d'_l c_l = 0$$

Sea $d = mcd(d'_1, \ldots, d'_{i-1}, d_i)$. Suponemos que $p^m || d$ (p^m es la máxima potencia de p que divide a d).

Si $p^m \geqslant p^{k_i}$, entonces $b = d_i b_i = 0$.

Si $p^m < p^{k_i}$ entonces por el teorema 5.11 en la base de Gröbner asociada a G, aparecería p^m en vez de p^{k_i} como exponente de x_i. Entonces d no es divisible por alguna potencia de p, pero d es el orden de un elemento en G y G es un p-grupo, por lo tanto $d = 1$. Observamos que $d_i c_i \in \langle c_1, \ldots, c_{i-1} \rangle$, y si $p^r | d_i$ con $p^r \leqslant p^{k_i}$, entonces $p^r c_i \in \langle c_1, \ldots, c_{i-1} \rangle$, pues $d = 1$, pero por el teorema 5.11 tenemos que p^{k_i} es la mínima potencia de p tal que $p^{k_i} c_i \in \langle c_1, \ldots, c_{i-1} \rangle$, por lo tanto $p^r = p^{k_i}$. Entonces $b = d_i b_i = \alpha p^{k_i} b_i = 0$, luego $\langle b_i \rangle \cap \langle b_1, \ldots, b_{i-1} \rangle = \{0\}$,

es decir

$$\langle b_1, \ldots, b_s \rangle = \bigoplus_{l=1}^{s} \langle b_l \rangle$$

Finalmente demostraremos que $\{b_1, \ldots b_s\}$ es un conjunto generador de G. Por hipótesis tenemos que para toda $r \in [s+1, q]$, el coeficiente principal del polinomio r-ésimo en $\mathcal{G}_C$ es igual a 1. Por lo tanto aplicando el homomorfismo $\tilde{\gamma}$ a estos polinomios tenemos que

$$c_r \in \langle b_1, \ldots, b_s \rangle, \quad \text{con } s+1 \leqslant r \leqslant q$$

Como C es un conjunto generador de G, entonces

$$G = \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \cdots \oplus \langle b_s \rangle$$

□

Corolario 6.2. *Los órdenes de los elementos en la p-base $\mathcal{B}$ son los siguientes*

$$o(c_1) = p^{k_1}$$
$$\vdots$$
$$o(c_s - \sum_{l=1}^{s-1} n'_{s_l} c_l) = p^{k_s}$$

Definición. Sea G un p-grupo abeliano finito, y sea $\mathcal{G}$ una base de Gröbner asociada a G. Entonces $\mathcal{G}$ es una *p-base de Gröbner* de G, si $\mathcal{G}$ tiene la forma (6.1), y la denotaremos por $\mathcal{G}_p$.

6.2 p-base de Gröbner de un $\mathbb{Z}_{p^n}C_p$-módulo cadena abierta

En esta sección presentamos la modelación de nuestro problema de calcular una p-base de un $\mathbb{Z}_{p^n}C_p$-módulo cadena abierta de la forma $\mathscr{C} = (i, j)$, utilizando las p-bases de Gröbner asociadas a módulos finitos, definidas en la sección anterior. Finalmente encontramos las p-bases de Gröbner asociadas a nuestros ejemplos de $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de la forma $\mathscr{C} = (i, j)$.

Sea $M = \mathscr{C}(a)$ un Λ-módulo cadena abierta de la forma $\mathscr{C} = (i, j)$, generado por a. Por el teorema 2.8 tenemos que

$$C = \{a, \phi a, \phi^2 a, \ldots, \phi^{i-1} a, \pi a, \pi^2 a, \ldots, \pi^{j-1} a\}$$

es un conjunto generador de M, y además tenemos que

$$\begin{aligned}\Delta = \{&pa = \pi a - \phi^{p-1}\sigma(\phi)a,\ p\phi a = \phi^{p-1}\sigma(\phi)\phi a, \ldots, p\phi^{i-1}a = 0,\\ &p\pi a = \pi^2 a, \ldots, p\pi^{j-2}a = \pi^{j-1}a,\ p\pi^{j-1}a = 0\}.\end{aligned}$$

es un sistema de relaciones asociadas a C de G.

Por el teorema 5.10 inciso (iii), tenemos que la base de Gröbner reducida del ideal $I(\Delta) = \langle X^{\boldsymbol{u}^+} - X^{\boldsymbol{u}^-} \mid \boldsymbol{u} \in \bar{\Delta}\rangle$ es $\mathcal{M}_C$, donde $\mathcal{M}_C$, es la base de Gröbner asociada a M con respecto a C.

Por el teorema 3.1 existe un subconjunto de C que es una p-base de M. Por lo tanto existe un ordenamiento en C tal que $\mathcal{M}_C$ es una p-base de Gröbner de M. Entonces por el teorema 6.1 tenemos que a partir de esta p-base de Gröbner obtenemos otra p-base del Λ-módulo M.

Es importante observar que para asegurar que la base de Gröbner asociada a M con respecto a C, es una p-base de Gröbner (lo cual concluye con esta nueva modelación del problema de encontrar una p-base de M) utilizamos el teorema 3.1, en el cual mostramos explícitamente una p-base de estos Λ-módulos. Sin embargo, tenemos la conjetura de que es posible demostrar, sin hacer uso del teorema 3.1, que para estos Λ-módulos la base de Gröbner asociada siempre es una p-base de Gröbner. Por otro lado, también es importante señalar que esta nueva modelación nos ha permitido encontrar otras p-bases distintas a las dadas en el teorema 3.1. Más aún, a través de esta modelación hemos resuelto el problema para el caso general: Encontrar una p-base de un Λ-módulo cadena abierta o cadena cerrada de la forma $\mathscr{C} = (i_1, j_1; \ldots; i_m, j_m)$ para toda $m \in \mathbb{N}$, lo cual es demasiado complicado de obtener por los métodos usuales, debido a la complejidad que implica el cálculo de los órdenes de todos los elementos de un p-grupo abeliano finito. Este resultado se encuentra en un artículo por publicar, escrito conjuntamente con la *Dra. Ma. A. Aviñó.* En cierta forma el método que proponemos encuentra estos órdenes a través de algoritmos eficientes, implementados en algunos de los más importantes sistemas como: Maple, Macaulay2, CoCoA, Mathematica, REDUCE, AXIOM.

A continuación mostramos algunos ejemplos, que fueron calculados usando el sistema *Macaulay2*[1]. Es importante señalar que la complejidad del algoritmo

[1]Macaulay 2, version 0.8.52

de Buchberger crece considerablemente para este tipo de bases de Gröbner, por lo que la mayoría de estos ejemplos no pudieron calcularse usando otros sistemas como el *MapleV*. Otra observación es que en estos ejemplos se toma como el campo de los coeficientes a los racionales, esto se debe a que todavía no está implementado en *Macaulay2* el algoritmo para calcular una base de Gröbner de un ideal generado por polinomios no homogéneos con coeficientes en los enteros, ni para un ideal generado por polinomios con coeficientes en un anillo finito. Sin embargo, el cálculo de estos ejemplos fué posible gracias a las sugerencias del *Dr. Michael Stillman*.

1. $p = 7$, $n = 3$, $\mathscr{C} = (\overset{i}{6}, \overset{j}{3})$, $i = \overset{t}{0}(p-1) + \overset{r}{6}$, $p = \pi$

$$M \cong \mathbb{Z}_{p^3} \oplus 5\mathbb{Z}_p$$

Por la ecuación (3.1a) tenemos que la p-base de M es

$$Y = \{a, \phi a, \phi^2 a, \phi^3 a, \phi^4 a, \phi^5 a\}$$

Sea γ' el homomorfismo:

$$\gamma'(x_1) = a, \gamma'(x_2) = \phi a, \ldots, \gamma'(x_6) = \phi^5 a,$$
$$\gamma'(x_7) = \pi a, \gamma'(x_8) = \pi^2 a$$

Entonces el conjunto relaciones de definición es

$$\{x_1^7 - x_7, x_2^7 - 1, x_3^7 - 1, x_4^7 - 1, x_5^7 - 1, x_6^7 - 1, x_7^7 - x_8, x_8^7 - 1\}$$

Por lo tanto la p-base de Gröbner asociada a M es

$$\{x_1^{343} - 1, x_2^7 - 1, x_3^7 - 1, x_4^7 - 1, x_5^7 - 1, x_6^7 - 1, x_7 - x_1^7, x_8 - x_1^{49}\}$$

2. $p = 5$, $n = 4$, $\mathscr{C} = (\overset{i}{4}, \overset{j}{4})$, $i = \overset{t}{0}(p-1) + \overset{r}{4}$, $p = \pi$

$$M \cong \mathbb{Z}_{p^4} \oplus 3\mathbb{Z}_p$$

Copyright 1993-1999, all rights reserved, D. R. Grayson and M. E. Stillman
Factory 1.2c from Singular, copyright 1993-1997, G.-M. Greuel, R. Stobbe Factorization and characteristic sets 0.3.1, copyright 1996, M. Messollen GC, copyright 1996, Hans-J. Boehm, Alan J. Demers, Xerox, Silicon Graphics GNU libc and libg++, copyright 1996, Free Software Foundation GNU MP, copyright 1996, Free Software Foundation

Por la ecuación (3.1a) tenemos que la p-base de M es

$$Y = \{a, \phi a, \phi^2 a, \phi^3 a\}$$

Sea γ' el homomorfismo:

$$\gamma'(x_1) = a, \gamma'(x_2) = \phi a, \ldots, \gamma'(x_4) = \phi^3 a,$$
$$\gamma'(x_5) = \pi a, \gamma'(x_6) = \pi^2 a, \gamma'(x_7) = \pi^3 a$$

Entonces el conjunto relaciones de definición es

$$\{x_1^5 - x_5, x_2^5 - 1, x_3^5 - 1, x_4^5 - 1, x_5^5 - x_6, x_6^5 - x_7, x_7^5 - 1\}$$

Por lo tanto la p-base de Gröbner asociada a M es

$$\{x_1^{625} - 1, x_2^5 - 1, x_3^5 - 1, x_4^5 - 1, x_5 - x_1^5, x_6 - x_1^{25}, x_7 - x_1^{125}\}$$

3. $p = 3$, $n = 4$, $\mathscr{C} = (\overset{i}{7}, \overset{j}{3})$, $i = \overset{t}{3}(p-1) + \overset{r}{1}$, $p = \pi + 2\phi^2 + \phi^3$.

$$M \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^4} \oplus \mathbb{Z}_{p^3}$$

Como $p \leqslant i$ y $t \geqslant j$ entonces por la ecuación (3.1b) tenemos que

$$Y = \{a, \phi a, \pi a\}$$

Sea γ' el homomorfismo:

$$\gamma'(x_1) = a, \gamma'(x_2) = \pi a, \gamma'(x_3) = \phi a, \gamma'(x_4) = \pi^2 a,$$
$$\gamma'(x_5) = \phi^2 a, \gamma'(x_6) = \phi^3 a, \ldots, \gamma'(x_9) = \phi^6 a$$

Entonces el conjunto relaciones de definición es

$$\{x_1^3 - x_2 x_5^2 x_6, x_2^3 - x_4, x_3^3 - x_6^2 x_7, x_4^3 - 1, x_5^3 - x_7^2 x_8, x_6^3 - x_8^2 x_9, x_7^3 - x_9^2,$$
$$x_8^3 - 1, x_9^3 - 1\}$$

Por lo tanto la p-base de Gröbner asociada a M es

$$\{x_1^{81} - 1, x_2^9 - 1, x_3^{27} - 1, x_4 - x_2^3, x_5 - x_3^{24} x_2 x_1^{78}, x_6 - x_3^6 x_2^6 x_1^9, x_7 - x_5^6 x_3^9,$$
$$x_8 - x_3^9 x_1^{27}, x_9 - x_8 x_6^3\}$$

4. $p=3$, $n=4$, $\mathscr{C}=(\overset{i}{9},\overset{j}{4})$, $i=\overset{t}{4}(p-1)+\overset{r}{1}$, $p=\pi+2\phi^2+\phi^3$.

$$M\cong\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^5}\oplus\mathbb{Z}_{p^4}$$

Como $p\leqslant i$ y $t\geqslant j$ entonces por la ecuación (3.1b) tenemos que

$$Y=\{a,\phi a,\pi a\}$$

Sea γ' el homomorfismo:

$$\gamma'(x_1)=a,\gamma'(x_2)=\pi a,\gamma'(x_3)=\phi a,\gamma'(x_4)=\pi^2 a,\gamma'(x_5)=\pi^3 a,$$
$$\gamma'(x_6)=\phi^2 a,\gamma'(x_7)=\phi^3 a,\ldots,\gamma'(x_{12})=\phi^8 a$$

Entonces el conjunto relaciones de definición es

$$\{x_1^3-x_2x_6^2x_7,x_2^3-x_4,x_3^3-x_7^2x_8,x_4^3-x_5,x_5^3-1,x_6^3-x_8^2x_9,x_7^3-x_9^2x_{10},$$
$$x_8^3-x_{10}^2x_{11},x_9^3-x_{11}^2x_{12},x_{10}^3-x_{12}^2,x_{11}^3-1,x_{12}^3-1\}$$

Por lo tanto la p-base de Gröbner asociada a M es

$$\{x_1^{243}-1,x_2^{27}-1,x_3^{81}-1,x_4-x_2^3,x_5-x_2^9,x_6-x_3^{78}x_2x_1^{240},x_7-x_6^{78}x_3^{78},$$
$$x_8-x_6^6x_3^9,x_9-x_6^{72}x_3^{63},x_{10}-x_6^9x_3^{27},x_{11}-x_3^{54},x_{12}-x_{11}x_9^3\}$$

5. $p=5$, $n=2$, $\mathscr{C}=(\overset{i}{7},\overset{j}{2})$, $i=\overset{t}{1}(p-1)+\overset{r}{3}$, $p=\pi+4\phi^4+2\phi^5+3\phi^6$.

$$M\cong 3\mathbb{Z}_{p^2}\oplus 2\mathbb{Z}_p$$

Como $p\leqslant i$ y $t<j$ entonces por la ecuación (3.1c) tenemos que

$$Y=\{a,\phi a,\phi^2 a,\phi^3 a,\phi^4 a\}$$

Sea γ' el homomorfismo:

$$\gamma'(x_1)=a,\gamma'(x_2)=\phi a,\ldots,\gamma'(x_7)=\phi^6 a,\gamma'(x_8)=\pi a$$

Entonces el conjunto relaciones de definición es

$$\{x_1^5-x_8x_5^4x_6^2x_7^3,x_2^5-x_6^4x_7^2,x_3^5-x_7^4,x_4^5-1,x_5^5-1,x_6^5-1,x_7^5-1,x_8^5-1\}$$

Por lo tanto la p-base de Gröbner asociada a M es

$$\{x_1^{25}-1,x_2^{25}-1,x_3^{25}-1,x_4^5-1,x_5^5-1,x_6-x_3^{15}x_2^{20},x_7-x_6x_3^5x_2^5,$$
$$x_8-x_5x_3^{10}x_2^{10}x_1^5\}$$

6. $p = 3$, $n = 5$, $\mathscr{C} = (\overset{i}{7}, \overset{j}{5})$, $i = \overset{t}{3}(p-1) + \overset{r}{1}$, $p = \pi + 2\phi^2 + \phi^3$.

$$M \cong \mathbb{Z}_{p^5} \oplus 2\mathbb{Z}_{p^3}$$

Como $p \leqslant i$ y $t < j$ entonces por la ecuación (3.1c) tenemos que

$$Y = \{a, \phi a, \phi^2 a\}$$

Sea γ' el homomorfismo:

$$\gamma'(x_1) = a, \gamma'(x_2) = \phi a, \ldots, \gamma'(x_7) = \phi^6 a,$$
$$\gamma'(x_8) = \pi a, \gamma'(x_9) = \pi^2 a, \gamma'(x_{10}) = \pi^3 a, \gamma'(x_{11}) = \pi^4 a$$

Entonces el conjunto relaciones de definición es

$$\{x_1^3 - x_8 x_3^2 x_4, x_2^3 - x_4^2 x_5, x_3^3 - x_5^2 x_6, x_4^3 - x_6^2 x_7, x_5^3 - x_7^2, x_6^3 - 1, x_7^3 - 1, x_8^3 - x_9,$$
$$x_9^3 - x_{10}, x_{10}^3 - x_{11}, x_{11}^3 - 1\}$$

Por lo tanto la p-base de Gröbner asociada a M es

$$\{x_1^{243} - 1, x_2^{27} - 1, x_3^{27} - 1, x_4 - x_3^{51} x_2^{51}, x_5 - x_3^6 x_2^9, x_6 - x_4^6 x_3^9, x_7 - x_6 x_4^3,$$
$$x_8 - x_3 x_2^3 x_1^3, x_9 - x_8^3, x_{10} - x_8^9, x_{11} - x_8^{27}\}$$

Apéndice A

Algoritmo de $\sigma(\phi)$

Aqui presentamos el algoritmo para calcular $\sigma(\phi)$, que obtuvimos a partir del lema 2.1.

```
#include <iostream.h>

long double* Triangulo_Pascal(unsigned p)  /*Esta funcion
calcula los coeficientes binomiales del
triangulo de Pascal*/
{
    long double *final=new long double[p+1],
 *aux=new long double[p+1];
    for(int i=0; i<=p; i++)
final[i]=aux[i]=0;
    final[0]=aux[0]=aux[2]=1;
    aux[1]=2;
    if(p==2)
return aux;
    for(int i=3; i<=p; i++)
    {
for(int j=1; j<=p; j++)
    final[j]=aux[j-1]+aux[j];
for(int j=0; j<=p; j++)
    aux[j]=final[j];
    }
    return final;
```

```
}

long double Exp(unsigned p , unsigned n)
{
    long double prod=1;
    for(int i=1; i<=n; i++)
prod=prod*p;
    return prod;
}

long double* Sigma(long double *tp, unsigned p ) /*Esta funcion
calcula los coeficientes de sigma(phi)*/
{
    const long double size=2*p-2;
    long double *sigma=new long double[size];
    long double *aux=new long double[size];
    long double *pp=new long double[size];

    for (int i=0; i<size; i++)
sigma[i]=aux[i]=pp[i]=0;
    for (int i=2; i<=p; i++)
sigma[i-1]=pp[i-1]=-tp[i];

    for (int i=1; i<=p-2; i++)
    {
for (int j=1; j<p; j++)
    aux[j+i]=pp[j];

for (int j=i+1; j<p+i; j++)
    aux[j]=(sigma[i]/p)*aux[j];

for (int j=0; j<=i; j++)
    sigma[j]=0;

for (int j=i+1; j<size; j++)
    sigma[j]=sigma[j]+aux[j];
    }
    return sigma;
```

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

```
}

void Modulo(long double* s, unsigned p, unsigned n)
{
    long double pn = Exp(p,n);
    cout << endl;
    cout << "\nEstos son los exponentes de sigma empezando
       por el termino independiente\n"
 << "modulo " << p << '^' << n << '(' << pn << "):\n";
    for(int i=p-1; i<2*p-2; i++)
cout << long(s[i])%long(pn) << ' ';
    cout << endl;
}

main()
{
    unsigned p , n;
    long double *tp, *sigma;
    char resp;

    do
    {
cout << "\nEl siguiente programa corre para primos impares\n";
cout << "\nDame p: ";
cin >> p;
cout << "\nDame n: ";
cin >> n;

tp=Triangulo_Pascal(p);
cout << "\nfila " << p <<" del triangulo de Pascal: ";
for(int i=0; i<=p; i++)
    cout << tp[i] << " ";
cout << endl;
sigma=Sigma(tp,p);
cout << "\nEstos son los coeficientes de sigma "
     << "\nempezando por el termino independiente\n";
for(int i=p-1; i<2*p-2; i++)
    cout << sigma[i] << ' ';
```

```
cout << endl;
Modulo(sigma,p,n);
cout << "\nQuieres volver a correr el programa s/n:";
cin >> resp;

    }while (resp=='s'||resp=='S');
}
```

Bibliografía

[1] W. W. Adams y P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, 1994.

[2] J. L. Alperin y R. B. Bell, *Groups and Representations*, Springer-Verlag, New York-Berlin-Heidelberg, 1995.

[3] F. W. Anderson y K. R. Fuller, *Rings and Categories of Modules*, Springer-Verlag, New York-Berlin-Heidelberg, 1973.

[4] M. A. Aviñó y L. D. García Puente, *Gröbner Bases Associated to Bases of Finite Modules*, por publicar.

[5] M. A. Aviñó Diaz y R. Bautista Ramos, *The Additive Structure of Indecomposable $\mathbb{Z}_{p^n}C_p$-Modules*, Communications in Algebra. **24** (1996), no. 8, 2567–2595.

[6] T. Becker, V. Weispfenning, *Gröbner Bases*, Springer-Verlag, New York-Berlin-Heidelberg, 1993.

[7] M. A. Borges Trenard, *Bases de Groebner Asociadas con Monoides Finitamente Generados*, Tesis Doctoral, Academia de Ciencias de Cuba, Santiago de Cuba, Junio 1992.

[8] H. Cárdenas y E. Lluis, *Módulos Semisimples y Representación de Grupos Finitos*, Serie Sociedad Matemática Mexicana, Trillas, México, 1970.

[9] D. Cox, J. Little, y D. O'Shea, *Ideals, Varieties, and Algorithms*, Segunda ed., Springer-Verlag, New York-Berlin-Heidelberg, 1996.

[10] L. Fuchs, *Abelian Groups*, Tercera ed., Akadémiai Kiadó, Budapest, 1966.

[11] I. Kaplansky, *Infinite Abelian Groups*, University of Michigan Press, Ann Arbor, 1954.

[12] L. A. Nazarova, and A. V. Roiter, *Finitely generated modules over a Dyad of two local Dedekind rings, and finite groups with an abelian normal divisor of index p*, Izv. Akad. Nauk, SSSr. Ser. Mat. Tom 33 (1969) No. 1, 65–86.

[13] J. J. Rotman, *An Introduction to the Theory of Groups*, Cuarta ed., Springer-Verlag, New York-Berlin-Heidelberg, 1994.

[14] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, 1996.

[15] G. Szekeres, *Determination of Certain Family of Finite Metabelian Groups*, Trans. Amer. Math. Soc. 66(1949), 1–43.