Bases de Gröbner Asociadas a Módulos Finitos

LUIS DAVID GARCÍA PUENTE
Licenciado en Matemáticas,
Facultad de Ciencias, UNAM
Director de Tesis: Dra. Maria Alicia Aviñó Diaz

En la teoría de Representaciones de Álgebras interesa describir todos los módulos (espacios vectoriales sobre anillos o más generalmente sobre álgebras, en vez de campos) salvo isomorfísmos.

Si el álgebra estudiada es finita como el caso que nos interesa, tenemos la importante propiedad de que todo módulo generado por un número finito de elementos se puede escribir como suma finita de modulos inescindibles. Un módulo es inescindible si ya no puede descomponerse en la suma de dos o más submódulos no triviales. Por esta razón si conocemos todos los módulos inescindibles de un álgebra podemos construir todos los módulos sobre esta álgebra.

Existen álgebras que tienen un número finito de módulos inescindibles no isomorfos y se llaman álgebras de tipo finito. Otras tienen un número infinito de módulos inescindibles pero estos pueden ser clasificados y reciben el nombre de álgebras mansas. Las que tienen un número infinito de módulos inescindibles y estos no pueden ser clasificados se llaman álgebras salvajes.

Sea $\mathbb{Z}_{p^n}$ los enteros módulo p^n — con p primo, sea $C_p := \langle x \rangle$ el grupo cíclico de orden p. Entonces $\Lambda := \mathbb{Z}_{p^n}C_p = \sum_{i=0}^{p-1} a_i x^i$, con $a_i \in \mathbb{Z}_{p^n}$, forma el álgebra del grupo cíclico de orden p sobre los enteros módulo p^n. Λ es un álgebra mansa.

Los módulos inescindibles sobre Λ son p-grupos abelianos finitos y por esta razón tienen p-bases — conjuntos generadores independientes. Cuando se estudian los módulos sobre un álgebra y esta álgebra es sobre un campo k, tenemos la importante propiedad de que el módulo es un espacio vectorial sobre k y por lo tanto tiene bases y en estas bases se puede estudiar la acción del álgebra mediante matrices. Cuando se estudian las álgebras sobre un anillo como $\mathbb{Z}_{p^n}$ no tenemos esta propiedad dada en una forma sencilla.

El estudio de los $\mathbb{Z}_{p^n}C_p$-módulos finitos fué iniciado por *G. Szekeres* en 1949, en [6]. Szekeres clasificó los Λ-módulos inescindibles, en módulos cadena abierta y módulos cadena cerrada. Sin embargo, en esta clasificación no se tiene la información de como son los módulos sobre el anillo $\mathbb{Z}_{p^n}$ y menos aún una p-base, pero si encontrasemos, a partir de las cadenas, la forma de hallar una p-base entonces podriamos conocer la acción del álgebra sobre esta p-base en forma de matrices. Esta fué nuestra motivación para tratar de calcular una p-base a partir del concepto de cadena.

En esta tesis se demostró por primera vez un teorema donde se describen

p-bases para todos los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de tipo $\mathscr{C} = (i,j)$ (generadas por un sólo elemento, o de dimensión 1). Este es el caso más sencillo, sin embargo, aún en este caso, calcular una p-base puede resultar muy complejo. Además modelamos el problema utilizando Álgebra Computacional, en particular, Bases de Gröbner. Estas no son bases de un módulo sino un conjunto generador con propiedades muy importantes de un ideal de polinomios en varias indeterminadas. A través de las bases de Gröbner, obtuvimos un algoritmo para calcular las p-bases de los módulos en cuestión y además nuevas p-bases de estos módulos no obtenidas en el teorema.

El objetivo general de esta tesis fué iniciar el estudio de las p-bases de los módulos cadena y también utilizar el álgebra computacional para modelar este problema de una forma totalmente nueva. La cual nos permitio resolver el caso general para cualquier Λ-módulo cadena, ver [2].

1 Λ-módulos cadena

Aqui enunciamos algunos resultados que calculan la $\mathbb{Z}_{p^n}$-estructura de los Λ-módulos cadena abierta de tipo $\mathscr{C} = (i,j)$, y además enunciamos un teorema que muestra explícitamente una p-base de estos módulos.

Szekeres describió a los Λ-módulos izquierdos inescindibles 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, con coeficientes enteros no negativos menores que p, que puede ser calculado por medio de un algoritmo descrito en la tesis.

Definición. Decimos que $M := \mathscr{C}(a)$ es un Λ-*módulo cadena abierta de la forma* $\mathscr{C} = (i,j)$ si satisface las siguientes condiciones:
1) $M = \langle a \rangle$, como Λ-módulo,
2) i y j son los mínimos enteros no negativos tales que $\phi^i a = 0$, $\pi^j a = 0$.

Teorema 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:*

$$\begin{aligned} \textit{Si } p > i & \qquad M \cong (i-1)\mathbb{Z}_p \oplus \mathbb{Z}_{p^j}, \\ \textit{si } p \leqslant i \ \textit{ y } \ t \geqslant j & \qquad M \cong \mathbb{Z}_{p^{j-1}} \oplus r\mathbb{Z}_{p^{t+1}} \oplus (p-r-1)\mathbb{Z}_{p^t}, \\ \textit{si } p \leqslant i \ \textit{ y } \ t < j & \qquad M \cong \mathbb{Z}_{p^j} \oplus (r-1)\mathbb{Z}_{p^{t+1}} \oplus (p-r)\mathbb{Z}_{p^t}. \end{aligned}$$

Teorema 2. *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:*

$$\begin{aligned} \textit{Si } p > i & \qquad Y = \{a, \phi a, \ldots, \phi^{i-1}a\}, \\ \textit{si } p \leqslant i \ \textit{ y si } \ t \geqslant j & \qquad Y = \{a, \phi a, \ldots, \phi^{p-2}a, \pi a\}, \\ \textit{si } p \leqslant i \ \textit{ y si } \ t < j & \qquad Y = \{a, \phi a, \ldots, \phi^{p-1}a\}, \end{aligned}$$

es una p-base de M.

Ejemplo. $p = 3$, $n = 4$, $\mathscr{C} = (\overset{i}{9}, \overset{j}{4})$, $i = \overset{t}{4}(p-1) + \overset{r}{1}$, $p = \pi + 2\phi^2 + \phi^3$. Como $p \leqslant i$ y $t \geqslant j$ entonces tenemos que

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

y además que la p-base de M es

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

2 p-bases de Gröbner

Aqui definimos el concepto de p-base de Gröbner asociada a módulos finitos. Modelamos el problema de calcular una p-base de los $\mathbb{Z}_{p^n}C_p$-módulos cadena abierta de la forma $\mathscr{C} = (i, j)$ utilizando este concepto de p-bases de Gröbner.

Sea k un campo y $k[\boldsymbol{x}] = k[x_1, \ldots, x_n]$, el anillo de polinomios en n variables. Los monomios en $k[\boldsymbol{x}]$ son denotados $\boldsymbol{x}^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ e identificados con las n-adas $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ en $\mathbb{N}^n$. Un orden total $\prec$ en $\mathbb{N}^n$ es un orden monomial si el vector cero es el único elemento minimal, y $\boldsymbol{a} \prec \boldsymbol{b}$ implica $\boldsymbol{a} + \boldsymbol{c} \prec \boldsymbol{b} + \boldsymbol{c}$ para todos $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{N}^n$.

Dado un orden monomial $\prec$, todo polinomio no cero en $k[\boldsymbol{x}]$ tiene un único monomio inicial, denotado por $in_\prec(f)$. Si I es un ideal en $k[\boldsymbol{x}]$, entonces su ideal inicial es el ideal monomial $in_\prec(I) := \langle in_\prec(f) \mid f \in I \rangle$.

Un subconjunto finito $\mathcal{G} \subset I$ es una *base de Gröbner* de I con respecto a $\prec$ si $in_\prec(I)$ es generado por $\{in_\prec(g) \mid g \in \mathcal{G}\}$. Es llamada *reducida* si, para cualquier par de elementos distintos $g, g' \in \mathcal{G}$, ningún monomio de g' es divisible por $in_\prec(g)$. La base de Gröbner reducida es única con respecto al orden monomial, con la condición de que todos los polinomios en $\mathcal{G}$ sean mónicos. Además a partir de cualquier conjunto generador de I, podemos calcular la base de Gröbner reducida de I a través del *algoritmo de Buchberger*.

Sea G un p-grupo abeliano finito, y $C = \{c_1, \ldots, c_n\}$ un conjunto generador de G.

Sea $X = \{x_1, \ldots, x_n\}$ el conjunto de n indeterminadas, y sea T el monoide generado por X.

Definimos al homomorfismo γ de la siguiente manera

$$\begin{array}{rccc} \gamma: & T & \to & G \\ & x_i & \mapsto & c_i \end{array}$$

Sea $\tilde{\gamma}$ la extensión natural de γ a un homomorfismo entre las K-álgebras $K[X]$ y $K[G]$.

El núcleo de $\tilde{\gamma}$ es un ideal, el cual denotamos por I_C.

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

El siguiente teorema relaciona esta base de Gröbner, $\mathcal{G}_C$, con una p-base del grupo G.

Teorema 3. *Sea $C = \{c_1, \ldots, c_n\}$ un conjunto generador del p-grupo abeliano finito G, y sean $k_1, \ldots, k_s$ enteros mayores que 1. Entonces $\mathcal{G}_C$ tiene la forma*

$$\begin{aligned}\mathcal{G}_C = \{&x_1^{p^{k_1}} - 1, \ldots, x_{i-1}^{p^{k_{i-1}}} - 1,\\ &x_i^{p^{k_i}} - (\prod_{l=1}^{i-1} x_l^{n'_{i_l}})^{p^{k_i}}, \ldots, x_s^{p^{k_s}} - (\prod_{l=1}^{s-1} x_l^{n'_{s_l}})^{p^{k_s}},\\ &x_{s+1} - \prod_{l=1}^{s} x_l^{n_{(s+1)_l}}, \ldots, x_n - \prod_{l=1}^{n-1} x_l^{n_{n_l}}\},\end{aligned}$$

si, y sólo si,

$$\mathcal{B} = \{c_1, \ldots, c_{i-1}, c_i - \sum_{l=1}^{i-1} n'_{i_l} c_l, \ldots, c_s - \sum_{l=1}^{s-1} n'_{s_l} c_l\}$$

es una p-base de G.

Definición. Sea M un p-grupo abeliano finito, y $\mathcal{G}$ una base de Gröbner asociada a M. Entonces $\mathcal{G}$ es una *p-base de Gröbner* de M, si tiene la forma descrita en el teorema 3.

Sea $M = \mathscr{C}(a)$ un Λ-módulo cadena abierta de la forma $\mathscr{C} = (i, j)$, generado por a. Como consecuencia del teorema 3, para encontrar una p-base de M, basta encontrar una p-base de Gröbner de M visto como p-grupo. Para lo cual desarrollamos un algoritmo en la tesis, que básicamente consiste en definir el morfismo γ, encontrar el ideal I_C asociado a M, calcular la base de Gröbner reducida, con respecto a un orden monomial específico (orden lexicográfico), de I_C, y utilizar el teorema 3 para encontrar los elementos de la p-base de M.

A continuación desarrollamos un ejemplo que muestra la p-base obtenida por el teorema 2 y dos p-bases obtenidas a través de la modelación algorítmica.

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

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

y además por el teorema 2 tenemos que

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

Sea γ el homomorfismo:

$$\begin{aligned}&\gamma(x_1) = a, \gamma(x_2) = \phi a, \ldots, \gamma(x_7) = \phi^6 a,\\ &\gamma(x_8) = \pi a\end{aligned}$$

Entonces algunos teoremas técnicos demostrados en la tesis nos dicen que las relaciones de definición (los generadores del ideal I_C) son

$$\begin{aligned}\{&x_1^5 - x_8 x_5^4 x_6^2 x_7^3, x_2^5 - x_6^4 x_7^2, x_3^5 - x_7^4, x_4^5 - 1,\\ &x_5^5 - 1, x_6^5 - 1, x_7^5 - 1, x_8^5 - 1\}\end{aligned}$$

Por lo tanto la p-base de Gröbner asociada a M (obtenida usando el paquete Macaulay2) es

$$\begin{aligned}&\{x_1^{25}-1, x_2^{25}-1, x_3^{25}-1, x_4^5-1, x_5^5-1,\\ &\ x_6 - x_3^{15}x_2^{20}, x_7 - x_6x_3^5x_2^5,\\ &\ x_8 - x_5x_3^{10}x_2^{10}x_1^5\}\end{aligned}$$

A partir de esta p-base de Gröbner obtenemos la siguiente p-base de M:

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

Si ordenamos las indeterminadas de la siguiente manera

$$x_7 \succ x_6 \succ x_5 \succ x_4 \succ x_8 \succ x_3 \succ x_2 \succ x_1$$

Obtenemos otra p-base de Gröbner asociada a M:

$$\begin{aligned}&\{x_1^{25}-1, x_2^{25}-1, x_3^{25}-1, x_8^5-1, x_4^5-1,\\ &\ x_5 - x_8x_3^{15}x_2^{15}x_1^{20}, x_6 - x_5x_8^4x_2^5x_1^5,\\ &\ x_7 - x_6x_3^5x_2^5\}\end{aligned}$$

A partir de esta p-base de Gröbner obtenemos la siguiente p-base de M:

$$\{a, \phi a, \phi^2 a, \phi^3 a, \pi a\}.$$

Referencias

[1] W. W. Adams y P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, 1994.

[2] M. A. Aviñó y L. D. García Puente, *Gröbner Bases Associated to Bases of Finite Modules*, en preparación.

[3] 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.

[4] M. A. Borges Trenard, *Bases de Groebner Asociadas con Monoides Finitamente Generados*, Tesis Doctoral, Academia de Ciencias de Cuba, Santiago de Cuba, Junio 1992.

[5] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, 1996.

[6] G. Szekeres, *Determination of Certain Family of Finite Metabelian Groups*, Trans. Amer. Math. Soc. 66(1949), 1–43.