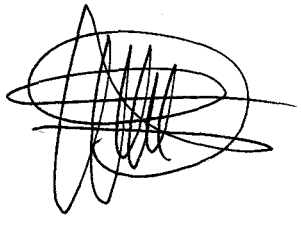
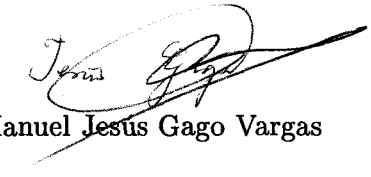
PRESENTACIONES DE MÓDULOS. TEOREMA DE ESTABILIDAD DE SUSLIN EN $\mathbb{Z}[X]$

Memoria presentada por Manuel Jesús Gago Vargas
para optar al grado de DOCTOR EN MATEMÁTICAS
por la UNIVERSIDAD DE SEVILLA



Director de la Memoria:

Francisco J. Castro Jiménez



Doctorando:

Manuel Jesús Gago Vargas

Fecha: **Mayo 1999**

A ILM

Índice de Materias

Agradecimientos

Un trabajo, aunque tenga autor, es el resultado de la ayuda y colaboración de muchas personas en su realización. Mi deuda comienza con Francisco J. Castro Jiménez, que ha compartido esta aventura de principio a fin, y de quien he recibido apoyo continuo. No quiero olvidar el interés de mis compañeros del Departamento de Álgebra, que me han proporcionado un cálido ambiente de trabajo. También deseo mencionar a la Profesora Cynthia Woodburn, por su amabilidad y acertados comentarios.

Introducción

En teoría clásica de nudos, uno de los principales problemas es distinguir nudos por la relación de equivalencia definida por la isotopía ambiente. En [Rei83] Reidemeister probó que dos diagramas de nudos son equivalentes si y solamente si puede transformarse uno en otro mediante tres tipos de movimientos. Se abría así la puerta para la definición de invariantes asociados a los nudos. Uno de esos invariantes fue el polinomio de Alexander, que permitió distinguir un gran número de nudos de una manera simple. Repasemos una de sus formas de cálculo, basada en conceptos topológicos. A partir del diagrama de un nudo, se puede dar una presentación del grupo del nudo, con generadores y relaciones. Recordemos que el grupo del nudo es el primer grupo de homotopía del complemento. A partir de aquí podemos construir, mediante el cálculo diferencial de Fox, la matriz de Alexander, que es la matriz de presentación de un módulo sobre el anillo $\mathbb{Z}[x, x^{-1}]$. El polinomio de Alexander es, entonces, el determinante de esta matriz. Se trata en realidad del generador del primer ideal elemental de la matriz de Alexander, que, en el caso de nudos, es siempre principal.

Si dos nudos son equivalentes, sus grupos son isomorfos, así como sus módulos, y tienen iguales polinomios de Alexander, salvo multiplicación por una unidad del anillo. Este paso desde el complemento del nudo hasta el polinomio establece condiciones necesarias, pero no suficientes para distinguir nudos. Así, encontramos nudos no equivalentes con iguales polinomios de Alexander. Se trata entonces de estudiar qué invariantes podemos extraer a partir de una presentación del módulo.

Uno de ellos es la cadena de ideales elementales. Constituyen una cadena ascendente de

ideales en el anillo, y son una generalización de los divisores elementales de un módulo sobre un dominio de ideales principales. Existen módulos no isomorfos con las mismas cadenas de ideales elementales, aunque en el caso de nudos permiten diferenciar algunos ejemplos (ver [GVCJ93]), o incluso distinguir una familia de nudos con los mismos polinomios de Jones ([Kan86]).

Es natural entonces plantear el problema de la equivalencia de módulos por isomorfismo sobre anillos de polinomios, y como casos más simples estudiar lo que ocurre sobre $\mathbb{Z}[x]$ o $k[x,y]$, con k un cuerpo. En esta situación, consideramos R un anillo conmutativo. Si M es un R-módulo finitamente generado, se puede presentar como

$$R^n \xrightarrow{f} R^m \to M \to 0$$

donde f corresponde a una matriz A con elementos en R de dimensión $m \times n$. Los vectores columna de A son los generadores de $im(f)$. La matriz A se denomina matriz de presentación del módulo M.

En el primer capítulo, definimos diferentes tipos de transformaciones en una matriz, y damos un teorema de clasificación de módulos por isomorfía, que reduce el problema a determinar la equivalencia de unas ciertas matrices de presentación por lo que denominamos transformaciones E-elementales. Este teorema nos permite demostrar el carácter invariante de ciertos objetos que se pueden calcular a partir de la matriz. Consideramos en primer lugar la descomposición primaria de módulos. Sobre anillos de la forma $R[x_1, \ldots, x_m]$, con R un dominio de ideales principales, podemos calcularla con el algoritmo que aparece en [Rut92]. Para evitar el problema de las componentes sumergidas, consideramos una descomposición primaria canónica ([Ort59], [Bou72]). Demostramos que módulos isomorfos tienen componentes primarias canónicas isomorfas. Damos ejemplos que nos permiten distinguir módulos a partir de sus matrices de presentación mediante el cálculo de la descomposición primaria, y otros que no, refutando una conjetura que aparece en [Sna47b].

A partir del teorema de clasificación 1.2.4, se plantea el estudio de la acción de matrices elementales sobre una dada desde un punto de vista algorítmico. Una situación similar la encontramos en el teorema de Estabilidad de Suslin, que establece que una matriz cuadrada A de orden $n \geq 3$ y determinante 1 con coeficientes en $\mathbb{Z}[x_1, \ldots, x_m]$ puede factorizarse en producto de matrices elementales. Las pruebas clásicas son existenciales ([Sus77], [Man97]). En el segundo capítulo se establece una demostración constructiva de este teorema sobre $\mathbb{Z}[x]$, con los métodos desarrollados en [PW95] para el caso $k[x_1, \ldots, x_m]$, con k un cuerpo. En este artículo, la motivación procede de un problema de tratamiento de señales, para descomponer un filtro como concatenación de filtros más sencillos (ver [Par95] para el planteamiento del problema y bibliografía asociada). En nuestro caso, mostramos la posibilidad de trabajar con coeficientes enteros, evitando el uso del teorema de Normalización de Noether del artículo original. Ilustramos, además, la técnica de obtener una solución global a partir del 'pegado' de soluciones locales, mediante el denominado *Proceso de Inducción de Quillen.* Como en el artículo [PW95], se deduce una prueba algorítimica del teorema de Quillen-Suslin para $\mathbb{Z}[x]$.

Como primer paso para dar una prueba constructiva del teorema de Estabilidad de Suslin sobre $\mathbb{Z}[x_1, \ldots, x_m]$ explicitamos un teorema de normalización para vectores unimodulares con coeficientes en $\mathbb{Z}[x_1, \ldots, x_m]$.

Finalizamos el capítulo con unos ejemplos para mostrar las restricciones que tienen los métodos locales para distinguir módulos por isomorfía, a partir de los resultados sobre descomposición primaria del capítulo anterior.

Otra forma de abordar el problema de clasificación de módulos sobre $\mathbb{Z}[x]$ es proyectar sobre otros anillos donde exista un proceso de clasificación. Por ejemplo, se pueden considerar coeficientes sobre $(\mathbb{Z}/\langle p \rangle)[x]$, con p un número primo. Como sabemos, es un dominio euclídeo, y podemos calcular la forma normal de Smith. Sin embargo, este método es más débil que considerar la cadena de ideales elementales, que son una

generalización de los divisores elementales. Por ello, en el capítulo 3 estudiamos la clasificación de módulos sobre el anillo $\mathbb{Z}[x]/\langle px\rangle$, con $p \in \mathbb{Z}$ un número primo, siguiendo la línea de [LS96]. Demostramos que es un anillo pullback, y establecemos un algoritmo para calcular la representación separada de un módulo, que es otro módulo más sencillo, único por isomorfismo. Damos ejemplos en los que podemos distinguir módulos sobre $\mathbb{Z}[x]$ con iguales ideales elementales pasando por un anillo de esta clase y calculando su representación separada. Añadimos algunos resultados destinados a la clasificación algorítmica de módulos sobre este anillo, que enlazan con los resultados de [NRSB75], y objetivo de un trabajo posterior.

En el primer apéndice incluímos el detalle de los cálculos desarrollados para la descomposición primaria de módulos en los ejemplos. En el segundo apéndice incluímos una tabla con los módulos de nudos de hasta 10 cruces que no pueden ser distinguidos por sus polinomios de Alexander. Calculamos bases de Gröbner de sus ideales elementales, que nos permiten distinguir una parte de ellos. Para los restantes, damos diferentes métodos para comprobar que las matrices de presentación encontradas son X-equivalentes.

0.1 Notación

- R es un anillo conmutativo con elemento unidad.
- $\mathcal{M}(m \times n, R)$ es el conjunto de matrices de m filas y n columnas con coeficientes en el anillo R.
- $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{m}$ representan ideales.
- Los módulos los representamos por las letras M, N, Q, etc.

Capítulo 1

Teorema de clasificación y descomposición primaria

1.1 Introducción

En este capítulo damos en primer lugar un conjunto de ejemplos para justificar la introducción de las que denominamos transformaciones X-elementales. Pasamos entonces a la demostracion de un teorema de clasificación que establece una condición necesaria y suficiente basada en dichas transformaciones para que dos matrices presenten módulos isomorfos. Mediante estas transformaciones podemos demostrar el carácter invariante de ciertos objetos extraídos de una presentación.

Asociado a una descomposición primaria de un submódulo de un módulo libre extraemos unos invariantes, que nos permiten distinguir módulos por isomorfía. Damos un ejemplo que refuta una conjetura de E. Snapper, y finalizamos con una discusión de métodos locales para distinguir presentaciones de módulos.

1.2 Teorema de clasificación

Definición 1.2.1. Una presentación finita de un R-módulo M es una sucesión exacta

$$R^n \xrightarrow{\alpha} R^m \xrightarrow{\pi} M \to 0$$

y entonces $M = coker(\alpha)$.

Identificamos la aplicación α con una matriz A de orden $m \times n$ de la siguiente forma: si $f_1, \ldots, f_n$ es una base de R^n y $e_1, \ldots, e_m$ es una base de R^m, entonces $\alpha(f_i) = \sum_{j=1}^{m} a_{ji} e_j$, y

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{n2} & \ldots & a_{mn} \end{pmatrix}.$$

Como π es sobreyectiva, las imágenes de $e_1, \ldots, e_m$ se pueden ver como los generadores de M, y las imágenes de $f_1, \ldots, f_n$ como las relaciones entre dichos generadores. Decimos que A es una matriz de presentación del módulo M. Recíprocamente, dada una matriz A con coeficientes en R, A es una matriz de presentación del módulo $M = R^m/K$, con K el submódulo de R^m generado por las columnas de la matriz A. El problema fundamental es decidir cuándo dos matrices presentan módulos isomorfos. El objetivo de esta sección es presentar un método teórico que resuelve esta cuestión. Por analogía con la clasificación de módulos sobre un dominio de ideales principales, vemos en primer lugar la equivalencia de matrices.

Definición 1.2.2. Sean $A_1, A_2 \in \mathcal{M}(m \times n, R)$. Decimos que son equivalentes si existen matrices P y Q invertibles en R tales que $PA_2Q = A_1$.

Es una relación de equivalencia entre matrices de igual dimensión.

Lema 1.2.1. *Si las matrices A_1 y A_2 son equivalentes, entonces presentan módulos isomorfos.*

Demostración. Sea M_i el módulos presentado por A_i, $i = 1, 2$, y P, Q matrices invertibles en R tales que $PA_2Q = A_1$. Como P es invertible, representa un isomorfismo de R^m, y Q un isomorfismo de R^n. Sea $m_1 = u_1 + im(A_1) \in M_1$. Entonces existe un

único $u_2 \in R^m$ tal $P(u_2) = u_1$. Definimos $\varphi : M_1 \to M_2$ como $\varphi(m_1) = u_2 + im(A_2)$. La aplicación está bien definida, pues si $u_1' + im(A_1) = u_1 + im(A_1)$, y $P(u_2') = u_1'$, existe $v_1 \in R^n$ tal que $A_1(v_1) = u_1 - u_1'$. Entonces $P^{-1}A_1(v_1) = u_2 - u_2'$, y $P^{-1}A_1(v_1) = A_2Q(v_1) \in im(A_2)$. Es inmediato que φ es lineal y biyectiva.

Sobre dominios de ideales principales, el lema 1.2.1 admite la implicación contraria entre matrices de iguales dimensiones. Sin embargo, sobre anillos de polinomios no es así, y existen módulos isomorfos con matrices de presentación no equivalentes.

Ejemplo 1.2.1. Sean

$$A_1 = \begin{pmatrix} 2x^2 + 2x + 1 & 4x + 1 \end{pmatrix}, A_2 = \begin{pmatrix} x - 1 & 5 \end{pmatrix}$$

matrices de presentación sobre $R = \mathbb{Z}[x]$ de los módulos M_1 y M_2.

Consideremos los ideales $K_1 = \langle 2x^2 + 2x + 1, 4x + 1 \rangle, K_2 = \langle x - 1, 5 \rangle$. Mediante el cálculo de sus bases de Gröbner, vemos que $K_1 = K_2$, y por tanto $M_1 \simeq M_2$.

Sin embargo, A_1 y A_2 no son equivalentes. Si lo fueran, existirían $P \in \mathcal{M}(1 \times 1, R), Q \in \mathcal{M}(2 \times 2, R)$ unitarias tales que $PA_2Q = A_1$. Las unidades de $\mathbb{Z}[x]$ son 1 y -1, y podemos tomar P uno de ellos para que $det(Q) = 1$. Escribamos

$$Q = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

con $det(Q) = 1$.

Como las columnas de las matrices A_1 y A_2 generan los mismos ideales en R, podemos calcular una matriz $Q_0 \in \mathcal{M}(2 \times 2, R)$ tal que $A_2Q_0 = A_1$. Por ejemplo,

$$Q_0 = \begin{pmatrix} 2x + 4 & 4 \\ 1 & 1 \end{pmatrix}.$$

Si Q es la matriz que buscamos, entonces $A_2(Q - Q_0) = 0$. En consecuencia, las columnas de la matriz $Q - Q_0$ pertenecen al módulo de sizigias del vector fila definido

por A_2.

Tenemos que $Siz(x-1,5) = \langle(-5, x-1)\rangle$, y entonces

$$Q - Q_0 = \begin{pmatrix} -5k_1 & -5k_2 \\ (x-1)k_1 & (x-1)k_2 \end{pmatrix}$$

para ciertos $k_1, k_2 \in R$. Entonces

$$Q = \begin{pmatrix} 2x+4-5k_1 & 4-5k_2 \\ 1+(x-1)k_1 & 1+(x-1)k_2 \end{pmatrix}.$$

Resulta entonces $det(Q) = 2x + k_1(-4x-1) + k_2(2x^2+2x+1)$.

Si $det(Q) = 1$, entonces $1-2x \in \langle 4x+1, 2x^2+2x+1\rangle = \langle x-1, 5\rangle$, y esto no se verifica. Por tanto, A_1 y A_2 no son equivalentes.

Ejemplo 1.2.2. Sea $R = \mathbb{Q}[x,y,z]$, y consideremos

$$A_1 = \begin{pmatrix} xy+y & xz+1 \end{pmatrix}, A_2 = \begin{pmatrix} yz-y & xz+1 \end{pmatrix}$$

Sea $Q_0 = \begin{pmatrix} z & 0 \\ -y & 1 \end{pmatrix}$ Entonces $A_1Q_0 = A_2$, y buscamos $Q = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ unitaria tal que $A_1Q = A_2$. Entonces las columnas de $Q - Q_0$ están en el módulo de sizigias de $(xy+y, xz+1)$, que es igual a $\langle(xz+1, -(xy+y))\rangle$. Entonces existen $k_1, k_2 \in \mathbb{Q}[x,y,z]$ tales que $Q = \begin{pmatrix} z+k_1(xz+1) & k_2(xz+1) \\ -y-k_1(xy+y) & 1-k_2(xy+y) \end{pmatrix}$. La condición $1 = det(Q)$ implica que $1 - z \in \langle xz+1, y-zy\rangle$, y esto no se verifica.

Es claro que nos encontramos en una situación muy distinta a los dominios de ideales principales, y debemos ampliar las transformaciones. Vamos a construir unas nuevas matrices a partir de unas dadas.

Definición 1.2.3. Sean $A_1 \in \mathcal{M}(m_1 \times n_1, R)$, $A_2 \in \mathcal{M}(m_2 \times n_2, R)$. Llamamos matrices extendidas de A_1 y A_2 a las matrices $A_1^e, A_2^e \in \mathcal{M}((m_1+m_2) \times (m_1+n_1+m_2+n_2), R)$

de la forma

$$A_1^e = \begin{pmatrix} A_1 & 0_{m_1\times m_2} & 0_{m_1\times m_1} & 0_{m_1\times n_2} \\ 0_{m_2\times n_1} & I_{m_2} & 0_{m_2\times m_1} & 0_{m_2\times n_2} \end{pmatrix},$$

$$A_2^e = \begin{pmatrix} A_2 & 0_{m_2\times m_1} & 0_{m_2\times m_1} & 0_{m_2\times n_1} \\ 0_{m_1\times n_2} & I_{m_1} & 0_{m_1\times m_2} & 0_{m_1\times n_1} \end{pmatrix}$$

donde $0_{r\times s}$ es la metriz nula de orden $r \times s$ y I_r es la matriz identidad de orden r.

Nota 1.2.1. Es fácil ver que en los ejemplos anteriores las matrices extendidas son equivalentes.

Definición 1.2.4. Llamamos transformaciones E-elementales sobre una matriz $A \in \mathcal{M}(m \times n, R)$ a las operaciones

- E1: Permutación de filas (columnas).
- E2: Adición de un múltiplo escalar de una fila (columna) a otra fila (columna).
- E3: Multiplicación de una fila (columna) por una unidad del anillo.

Definición 1.2.5. Decimos que dos matrices son E-equivalentes si se puede transformar una en otra mediante transformaciones E-elementales.

Nota 1.2.2. Las transformaciones E-elementales se identifican con el producto por matrices cuadradas invertibles. Sin especificar el tamaño, si $i \neq j$, llamamos e_{ij} a la matriz cuyo elemento (i, j) es 1 y cero en el resto. Si $a \in R$, y $u \in R$ es una unidad, denominamos $P_{ij} = I - e_{ii} - e_{jj} + e_{ij} + e_{ji}$, $E_{ij}(a) = I + a \cdot e_{ij}$ y $D_i(u) = I + (u - 1) \cdot e_{ii}$. Sea A una matriz $m \times n$.

- La multiplicación por la izquierda de una matriz A por una matriz P_{ij} de orden $m \times m$ intercambia la i-ésima y la j-ésima filas de A, y deja inalteradas las restantes. La multiplicación por la derecha por una matriz P_{ij} de orden $n \times n$

hace lo análogo con las columnas i-ésima y j-ésima. Tenemos así la transformación E1.

- La multiplicación por la izquierda de una matriz A por una matriz $E_{ij}(a)$ de orden $m \times m$ produce una matriz cuya i-ésima fila se obtiene multiplicando la j-ésima de A por el escalar a y sumándola a la i-ésima de A, y las restantes permanencen inalteradas. La multiplicación por la derecha por una matriz $E_{ij}(a)$ de orden $n \times n$ da una matriz cuya j-ésima columna es a veces la i-ésima columna de A más la j-ésima columna de A. De esta manera tenemos la transformación E2.

- La multiplicación por la izquierda de una matriz A por una matriz $D_i(u)$ de orden $m \times m$ genera una matriz cuya i-ésima fila es la i-ésima de A multiplicada por u, y las restantes iguales a las de A. La multiplicación por la derecha por una matriz $D_i(u)$ de orden $n \times n$ devuelve una matriz cuya i-esima columna es la i-ésima de A multiplicada por u. Así conseguimos la transformación E3.

Reservamos el nombre de transformación elemental a las de tipo E2, como veremos en el Capítulo 2. Por tanto, si dos matrices son E-equivalentes, entonces son equivalentes.

Nota 1.2.3. Sobre los anillos $\mathbb{Z}[x]$ y $k[x, y]$, existen matrices equivalentes que no son E-equivalentes, tal como aparece en [Coh66].

Definición 1.2.6. Llamamos transformaciones X-elementales sobre una matriz $A \in \mathcal{M}(m \times n, R)$ a las siguientes operaciones y sus inversas:

- Transformaciones E-elementales.
- X1: Sustitución de la matriz A por $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$.
- X2: Adición de una columna de ceros a la matriz A.

Definición 1.2.7. Decimos que dos matrices son X-equivalentes si se puede transformar una en otra mediante transformaciones X-elementales.

Dadas dos matrices A_1 y A_2, es claro que las matrices extendidas A_1^e y A_2^e se obtienen de las originales mediante transformaciones del tipo X1 y X2.

Proposición 1.2.2. *Si dos matrices son X-equivalentes, entonces presentan módulos isomorfos.*

Demostración. Como las transformaciones E-elementales se representan como productos por matrices invertibles, aplicamos el lema 1.2.1. La adición de una columna de ceros no altera el módulo, pues añade un generador trivial. Si K es el submódulo de R^m generado por las columnas de la matriz A, sea K' el submódulo de R^{m+1} generado por $K \times 0$ y $(\mathbf{0}, 1)$. Entonces $R^m/K \simeq R^{m+1}/K'$, y tenemos el resultado para la transformación X1.

Tenemos así nuevas transformaciones que proporcionan otrs matrices de presentación de un módulo. Vamos a ver que son suficientes.

Teorema 1.2.3. *([Lic98]) Dos matrices presentan módulos isomorfos si y solamente si las matrices extendidas son E-equivalentes.*

Demostración. Sean A_1, A_2 matrices de presentación de un módulo M. Tenemos el siguiente diagrama:

$$\begin{array}{ccccccc} R^{n_1} & \xrightarrow{A_1} & R^{m_1} & \xrightarrow{\pi_1} & M & \to & 0 \\ \downarrow \gamma & & \downarrow \beta & & \updownarrow id & & \\ R^{n_2} & \xrightarrow{A_2} & R^{m_2} & \xrightarrow{\pi_2} & M & \to & 0 \end{array}$$

Como R^{m_1} es libre y π_2 es sobreyectiva, podemos construir una aplicación lineal $\beta : R^{m_1} \to R^{m_2}$ tal que $\pi_2\beta = \pi_1$. De igual forma, el carácter libre de R^{n_1} y la exactitud en R^{m_1} y R^{m_2} genera una aplicación lineal $\gamma : R^{n_1} \to R^{n_2}$ tal que $\beta A_1 = A_2\gamma$. Si representamos β y γ por matrices B y C respecto a estas bases, entonces $BA_1 = A_2C$. De forma completamente simétrica se definen aplicaciones $\beta_1 : R^{m_2} \to R^{m_1}$ y $\gamma_1 : R^{n_2} \to$

R^{n_1}, con matrices B_1 y C_1 tales que $B_1A_2 = A_1C_1$. Mediante X-transformaciones,

$$
\begin{aligned}
A_1 &\rightarrow \begin{pmatrix} A_1 & B_1 \\ 0 & I_{m_2} \end{pmatrix} && \text{(por X1 y E2)} \\
&\rightarrow \begin{pmatrix} A_1 & B_1 & B_1A_2 \\ 0 & I_{m_2} & A_2 \end{pmatrix} && \text{(por X2 y E2)} \\
&\rightarrow \begin{pmatrix} A_1 & B_1 & 0 \\ 0 & I_{m_2} & A_2 \end{pmatrix} && \text{(por E2 y } A_1C_1 = B_1A_2\text{)} \\
&\rightarrow \begin{pmatrix} A_1 & B_1 & 0 & B_1B \\ 0 & I_{m_2} & A_2 & B \end{pmatrix} && \text{(por X2 y E2).}
\end{aligned}
$$

Esta matriz es de la misma dimensión que A_1^e, y se obtiene a partir de ella por transformaciones E-elementales. Para cualquier $e \in R^{m_1}$ se tiene que $\pi_1\beta_1\beta(e) = \pi_1(e)$, y por la exactitud en R^{m_1}, la imagen de $(\beta_1\beta - id_{R^{m_1}})$ está contenida en la imagen de A_1. Como R^{m_1} es libre, existe una aplicación $\delta : R^{m_1} \rightarrow R^{n_1}$ tal que $A_1\delta = \beta_1\beta - id_{R^{m_1}}$. Si D es la matriz que representa δ, $A_1D = B_1B - I_{m_1}$. Mediante E2,

$$
\begin{pmatrix} A_1 & B_1 & 0 & B_1B \\ 0 & I_{m_2} & A_2 & B \end{pmatrix} \rightarrow
\begin{pmatrix} A_1 & B_1 & 0 & I_{m_2} \\ 0 & I_{m_1} & A_2 & B \end{pmatrix} \rightarrow
\begin{pmatrix} A_2 & B & 0 & I_{m_2} \\ 0 & I_{m_1} & A_1 & B_1 \end{pmatrix}
$$

y esta última, por los mismos argumentos, es E-equivalente a A_2^e.

Otra forma de ver el teorema anterior es

Corolario 1.2.4. *Dos módulos son isomorfos si y solamente si sus matrices de presentación son X-equivalentes*

Tenemos así un método para analizar si un objeto asociado a una matriz de presentación de un módulo es un invariante de isomorfía. Comenzamos por uno clásico.

Definición 1.2.8. Si $A \in \mathcal{M}(m \times n, R)$ es matriz de presentación de un módulo M, y $0 \leq k < m$, se define el k-ésimo ideal elemental de M como el ideal generado por los menores de orden k de la matriz A, y lo notaremos por $F_k(M)$. Si $k \geq m$, establecemos que $F_k(M) = R$.

Proposición 1.2.5. *Si A_1 y A_2 son matrices de presentación de un módulo, tienen los mismos ideales elementales.*

Demostración. [CF77]

Los ideales elementales clasifican a los módulos sobre dominio de ideales principales, como $\mathbb{Z}$ o $k[x]$. No es así sobre $\mathbb{Z}[x]$ o $k[x, y]$, k un cuerpo.

Ejemplo 1.2.3. Sea $R = \mathbb{Q}[x, y]$, y consideremos los módulos M_1 y M_2 presentados por las matrices respectivas

$$A_1 = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}.$$

Sean $K_1 = \langle (x, 0), (y, 0) \rangle$ y $K_2 = \langle (x, y), (0, 0) \rangle$ los submódulos de R^2 generados por las columnas de estas matrices.

Tenemos que $F_0(M_1) = \langle 0 \rangle = F_0(M_2)$ y $F_1(M_1) = \langle x, y \rangle = F_1(M_2)$. Supongamos que φ es un morfismo entre M_1 y M_2.

$\varphi((1, 0) + K_1) = (a_1, a_2) + K_2$ para ciertos $a_1, a_2 \in R$. Como $x(1, 0) + K_1 = (0, 0) + K_1$, por linealidad, $x(a_1, a_2) \in K_2$. $xa_1 = \alpha x, xa_2 = \alpha y$, para algún $\alpha \in R$, de donde $a_2 x - a_1 y = 0$. Por tanto, $(a_2, -a_1) \in Siz(x, y) = \langle (-y, x) \rangle$, o de otra forma $(a_1, a_2) \in \langle (x, y) \rangle$. Luego $\varphi((1, 0) + K_1) = (0, 0) + K_2$, y φ no puede ser isomorfismo.

Ejemplo 1.2.4. Este ejemplo aparece propuesto como ejercicio en [Eis95]. Sea $R = \mathbb{Q}[x, y, z]$, y consideremos los R-módulos M_1 y M_2 presentados por las matrices

$$A_1 = \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}, A_2 = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$$

respectivamente. Sus ideales elementales son iguales. $F_0(M_1) = \langle xz \rangle = F_0(A_2), F_1(A_1) = \langle x, y, z \rangle = F_1(A_2)$. Sin embargo, no son isomorfos. Sean K_1, K_2 los módulos en R^2 generados por sus columnas. Entonces $M_1 = R^2/K_1, M_2 = R^2/K_2$. Supongamos que existe un tal isomorfismo φ. En el módulo presentado por A_1 la clase de $(0, 1)$ es anulada por z. Por el isomorfismo, se aplicará en un elemento (b_1, b_2) que también es anulado por z en el módulo de A_2. Si $z(b_1, b_2) \in ((x, 0), (y, z))$, entonces $za_1 = \alpha x + \beta y, za_2 = \beta z$, para ciertos $\alpha, \beta \in R$. Entonces $\beta = a_2$, $za_1 = \alpha x + a_2 y$ $(\alpha, b_2, -b_1) \in Siz(x, y, z) = ((-y, x, 0), (-z, 0, x), (0, -z, y))$. De aquí, existen λ_1, λ_2, λ_3 en R tales que $(b_1, b_2) = \lambda_1(0, x) + \lambda_2(-x, 0) + \lambda_3(-y, -z)$, de donde $\varphi((0, 1) + K_1) = (0, ax) + K_2$, para algún $a \in R$ no nulo. Si $\varphi^{-1}((0, 1) + K_2) = (d_1, d_2) + K_1$, entonces $\varphi^{-1}((0, ax) + K_2) = ax(d_1, d_2) + K_1 = (0, 1) + K_1$ $(axd_1, axd_2 - 1) = \alpha(x, y) + \beta(0, z)$ $-1 = -axd_2 + \alpha y + \beta z$ $1 \in (x, y, z)$, lo que es falso. En consecuencia, no puede haber tal isomorfismo.

Más adelante, volveremos sobre este ejemplo.

Ejemplo 1.2.5. Sea $R = \mathbb{Z}[x]$, y consideremos los módulo M_1, M_2 con matrices de presentación respectivas $A_1 = \begin{pmatrix} x & 2 \\ 0 & 0 \end{pmatrix}$ y $A_2 = \begin{pmatrix} x & 0 \\ 2 & 0 \end{pmatrix}$. Entonces $M_1 = R^2/K_1, M_2 = R^2/K_2$, con $K_1 = \langle (x, 0), (2, 0) \rangle \subset R^2$, $K_2 = \langle (x, 2) \rangle \subset R^2$. Se tiene que $F_0(M_1) = F_0(M_2) = 0$, $F_1(M_1) = F_1(M_2) = \langle 2, x \rangle$. Si $\varphi : M_1 \to M_2$ es un morfismo, existen $a_1, a_2, b_1, b_2 \in R$ con $\varphi((1, 0) + K_1) = (a_1, a_2) + K_2, \varphi((0, 1) + K_1) = (b_1, b_2) + K_2$. Por compatibilidad, $x(a_1, a_2) = l_1(x, 2), 2(b_1, b_2) = l_2(x, 2)$ para algunos $l_1, l_2 \in R$. Entonces $l_1 = a_1, b_2 = l_2$, de donde $(a_1, a_2), (b_1, b_2) \in \langle (x, 2) \rangle$, y entonces φ es el morfismo nulo. Como M_1 y M_2 no son nulos, no pueden ser isomorfos.

Nota 1.2.4. En [Vas98], p.40 se establece el siguiente teorema: si R es un anillo íntegramente cerrado, M y M' son R-mdulos tales que $F_j(M) = F_j(M')$, para todo j, los primos asociados de M son de altura menor o igual que 1, y existe un morfismo sobreyectivo φ entre M y M', entonces φ es isomorfismo.

Para el caso $R = \mathbb{Z}[x]$, sabemos que es íntegramente cerrado. Si M' es un módulo cíclico, entonces sus primos asociados tienen altura 1, pues se encuentran entre los factores irreducibles de $F_0(M')$. Si $\varphi : M \to M'$ es un morfismo sobreyectivo, y M' cíclico, entonces los primos asociados de M se tiene que encontrar entre los factores irreducibles de $F_0(M')$, pues $\varphi(F_0(M)) \subset F_0(M')$.

Por tanto, a la hora de establecer condiciones de isomorfía, nos podemos centrar en las condiciones para que exista una aplicación sobreyectiva entre los módulos. Esto se verifica en algunos de los ejemplos del Apéndice II.

Ejemplo 1.2.6. Las condiciones de [Vas98], p.40 no se pueden reducir. Sea $K_1 = ((2,0),(0,2),(x,0),(0,x)) \subset M = \mathbb{Z}[x]^2$. K_1 es $\langle 2,x\rangle$-primario en M. Tenemos que $F_0(K_1) = \langle x,2\rangle^2, F_1(K_1) = \langle 2,x\rangle, F_2(K_2) = R$. La altura del ideal $\langle 2,x\rangle$ es 2. Sea $K_2 = ((x,2),(0,x),(2,0)) \subset M$. Los ideales elementales coinciden con los de K_1. Sea $\varphi : R^2/K_2 \to K_1$ el morfismo definido por $\varphi((1,0)+K_2) = (1,0)+K_1$, $\varphi((0,1)+K_2) = (0,1)+K_1$. Está bien definido y es sobreyectivo. Sin embargo, no es biyectivo, pues $\varphi((0,2)+K_2) = (0,0)+K_1$, y $(0,2)+K_2$ no es nulo. De hecho, no son isomorfos, pues K_2 no es $\langle 2,x\rangle$-primario en M.

En el caso de teoría de nudos, se obtienen ideales sobre el anillo $\mathbb{Z}[x,x^{-1}]$, donde se pueden comparar, pues este anillo se identifica con $\mathbb{Z}[x,y]/\langle xy-1\rangle$. Esta idea se desarrolla en [GVCJ93]. Como hemos visto, los ideales elementales no clasifican. Buscamos otros invariantes de isomorfía que aporten más información. Ese es el objetivo de la siguiente sección.

1.3 Descomposición primaria canónica

Es conocido que en la descomposición primaria de un módulo ([Mat80],[ZS75]), las componentes sumergidas no están unívocamente determinadas. Sin embargo, existe una descomposición primaria canónica que permite establecer una relación de inclusión entre los módulos primarios que intervienen en otra descomposición. Veremos además que módulos isomorfos tienen componentes primarias canónicas isomorfas. En esta sección exigimos que R sea además noetheriano.

Definición 1.3.1. Sea M un R-módulo. Un ideal primo $\mathfrak{p}$ se dice asociado con M si existe $x \in M$ tal que $\mathfrak{p} = Ann(x)$. El conjunto de ideales primos asociados con M se notará por $Ass(M)$.

Definición 1.3.2. Sea M un R-módulo, y Q un submódulo de M. Decimos que Q es primario en M si $Ass(M/Q)$ tiene un único elemento.

Definición 1.3.3. Sea $a \in R$, N un R-módulo y Φ_a el endomorfismo de N definido por $\Phi_a(v) = av$, para $v \in N$.

- Se dice que a es un divisor de cero de N si la aplicación Φ_a no es inyectiva.
- Se dice que a es nilpotente en N si la aplicación Φ_a es nilpotente.

Lema 1.3.1. *Sea Q un submódulo de M. Son equivalentes:*

- *$Q \neq M$ y cada divisor de cero de M/Q es nilpotente.*
- *Q es primario en M.*

Demostración. [Bou72], p. 268.

Nota 1.3.1. Si Q es primario en M, entonces el ideal $(Q : M)$ es primario. En tal caso, si $\mathfrak{p} = rad(Q : M)$, $\mathfrak{p}$ es primo, y decimos que Q es $\mathfrak{p}$-primario en M.

Lema 1.3.2. *Si Q es $\mathfrak{p}$-primario en M, entonces existe un entero $k > 0$ tal que $\mathfrak{p}^k M \subset Q$.*

Demostración. [Bou72] p. 268.

Definición 1.3.4. Sea N un submódulo de M. Una descomposición primaria de N en M es una representación de N como una intersección

$$N = Q_1 \cap \ldots \cap Q_n$$

de submódulos primarios de M. Es una descomposición primaria reducida si los ideales $\mathfrak{p}_i = rad(Q_i : M)$ son todos distintos y si ninguna de las componentes Q_i puede omitirse de la intersección, esto es, si $\bigcap_{j \neq i} Q_j \not\subset Q_i$, para $i = 1, \ldots, n$.

Lema 1.3.3. *Los ideales $\mathfrak{p}_i$ de la definición 1.3.4 dependen únicamente de N y M. Se les denomina los ideales primos pertenenecientes a N en M, o asociados, y lo notaremos por $Ass(M/N)$.*

Proposición 1.3.4. *Sea N un submódulo de M, $N = \bigcap_{i=1}^{r} Q_i$ una descomposición primaria reducida de N en M, y $\mathfrak{p}_i = Ass(M/Q_i)$, $i = 1, \ldots, r$. Si $\mathfrak{p}_i$ es un elemento minimal de $Ass(M/N)$, Q_i es igual a la saturación sobre N de $\mathfrak{p}_i$, y por tanto, no depende de la descomposición.*

Demostración. [Bou72], p. 272.

Definición 1.3.5. Sea Q un submódulo $\mathfrak{p}$-primario de M. El menor de los enteros $n \geq 1$ tal que $\mathfrak{p}^n M \subset Q$ se denomina el exponente de Q en M, y lo notaremos por $e(M/Q)$.

Proposición 1.3.5. *Sea $(Q_\lambda)_{\lambda \in L}$ una familia de submódulos $\mathfrak{p}$-primarios de M. Entonces $Q = \bigcap_{\lambda \in L} Q_\lambda$ es $\mathfrak{p}$-primario si y solamente si la familia $\{e(M/Q_\lambda)_{\lambda \in L}\}$ está acotada superiormente por un valor m. En tal caso, $m \geq e(M/Q) \geq e(M/Q_\lambda)$, para todo $\lambda \in L$.*

Demostración. Si Q es $\mathfrak{p}$-primario, entonces existe un entero k tal que $\mathfrak{p}^k M \subset Q$, por lo que $\mathfrak{p}^k M \subset Q_\lambda$, para todo $\lambda \in L$. Se sigue que $e(M/Q_\lambda) \leq k$ para todo $\lambda \in L$. Si ahora $e(M/Q_\lambda) \leq k$ para cierto $k \in \mathbb{N}$, entonces $\mathfrak{p}^k M \subset Q_\lambda$, para todo $\lambda \in L$, de donde $\mathfrak{p}^k M \subset Q$. Como M es finitamente generado, por [Bou72], proposición 9, p. 266, $\mathfrak{p}$ está contenido en todo primo asociado de M/Q. Si $\mathfrak{p}'$ es un primo asociado de M/Q, entonces $\mathfrak{p}' = Ann(x + Q)$ para algún $x \in M$, y dado que $Q \subset Q_\lambda$, entonces $Ann(x + Q) \subset Ann(x + Q_\lambda) = \mathfrak{p}$, entonces $\mathfrak{p}' \subset \mathfrak{p}$. Por tanto, $Ass(M/Q) = \mathfrak{p}$ y Q es $\mathfrak{p}$-primario en M.

Definición 1.3.6. Sea N un submódulo de M. Una componente primaria de N es un módulo primario que aparece en alguna descomposición primaria minimal de N en M. Un conjunto completo de componentes primarias de N es un conjunto de componentes primarias cuya intersección forman una descomposición primaria minimal de N en M. La intersección de un subconjunto de un conjunto completo de componentes primarias de N se denomina componente de N. Una componente de N se dice aislada si todo primo asociado de N que está contenido en un primo asociado de esa componente es un primo asociado de tal componente.

Proposición 1.3.6. *Una componente aislada de N está unívocamente determinada por sus primos asociados.*

Demostración. [AM80], p.60, [Mat80]

Nota 1.3.2. Si Q es una componente primaria de N, con primo minimal en el conjunto de asociados, entonces es una componente aislada.

Definición 1.3.7. Sea M un R-módulo. Se define el soporte de M como el conjunto de ideales primos de R tales que $M_\mathfrak{p} \neq 0$, y se notará por $Supp(M)$.

Sea M un R-módulo finitamente generado, $\mathfrak{p}$ un elemento de $Ass(M)$ y $\mathcal{C}_\mathfrak{p}$ el conjunto de submódulos Q de M tales que $Ass(M/Q) = \{\mathfrak{p}\}$ y $Ass(Q) = Ass(M) - \{\mathfrak{p}\}$.

Este conjunto es no vacío por [Bou72], p.263, proposición 4. Escribimos $e_{\mathfrak{p}}(M) = inf_{Q \in C_{\mathfrak{p}}} e(M/Q)$.

Proposición 1.3.7. *Sea $n_{\mathfrak{p}}$ un entero mayor o igual que $e_{\mathfrak{p}}(M)$, y sea $\mathcal{F}(n_{\mathfrak{p}})$ el subconjunto de $C_{\mathfrak{p}}$ formado por los submódulos Q tales que $e(M/Q) \leq n_{\mathfrak{p}}$. Entonces $\mathcal{F}(n_{\mathfrak{p}})$ tiene un elemento mínimo, que notaremos por $Q(\mathfrak{p}, n_{\mathfrak{p}})$.*

Demostración. Sea Q la intersección de los módulos de $\mathcal{F}(n_{\mathfrak{p}})$. Es un módulo $\mathfrak{p}$-primario, pues los exponentes de los módulos de $\mathcal{F}(n_{\mathfrak{p}})$ están acotados superiormente por $n_{\mathfrak{p}}$. Resta ver que $Q \in \mathcal{F}(n_{\mathfrak{p}})$. Como $Ass(Q) \subset \bigcap_{Q' \in \mathcal{F}(n_{\mathfrak{p}})} Q' = Ass(M) - \{\mathfrak{p}\}$, $Ass(M/Q) = \mathfrak{p}$ y $e(M/Q) \leq n_{\mathfrak{p}}$, Q es el elemento mínimo.

Proposición 1.3.8. *Sea $(n_{\mathfrak{p}})_{\mathfrak{p} \in Ass(M)}$ una familia de enteros tales que $n_{\mathfrak{p}} \geq e_{\mathfrak{p}}(M)$ para todo $\mathfrak{p} \in Ass(M)$. Entonces los submódulos $Q(\mathfrak{p}, n_{\mathfrak{p}})$ correspondientes a esta familia forman una descomposición primaria reducida de $\{0\}$ en M. Decimos que está canónicamente determinada por la familia $(n_{\mathfrak{p}})$.*

Demostración. Si $x \in \bigcap_{\mathfrak{p} \in Ass(M)} Q(\mathfrak{p}, n_{\mathfrak{p}})$, entonces $Ass(Rx) \subset \bigcap_{\mathfrak{p} \in Ass(M)} Ass(Q(\mathfrak{p}, n_{\mathfrak{p}}) = \emptyset$, de donde $x = 0$ ([Bou72], cor. 1, p.262). Como $Ass(M) = \bigcup_{\mathfrak{p} \in Ass(M)} Ass(M/Q(\mathfrak{p}, n_{\mathfrak{p}}))$ y $Ass(Q(\mathfrak{p}, n_{\mathfrak{p}})) = Ass(M) - \{\mathfrak{p}\}$, por [Bou72], prop. 4, p.271, la descomposición es reducida.

Si se toma $n_{\mathfrak{p}} = e_{\mathfrak{p}}(M)$ para todo $\mathfrak{p} \in Ass(M)$, la descomposición primaria correspondiente de los $Q(\mathfrak{p}) = Q(\mathfrak{p}, e_{\mathfrak{p}}(M))$ se denomina la *descomposición primaria canónica* de $\{0\}$ en M.

Teorema 1.3.9. *Teorema de Ortiz. Sea $\{0\} = \bigcap_{\mathfrak{p} \in Ass(M)} Q'(\mathfrak{p})$ una descomposición primaria reducida de $\{0\}$ en M. Entonces $e(M/Q(\mathfrak{p})) \leq e(M/Q'(\mathfrak{p}))$ para todo $\mathfrak{p} \in Ass(M)$. Si para algún $\mathfrak{p}$ $e(M/Q(\mathfrak{p})) = e(M/Q'(\mathfrak{p}))$ entonces $Q(\mathfrak{p}) \subset Q'(\mathfrak{p})$.*

Demostración. Sea $\mathfrak{p} \in Ass(M)$. Como la descomposición es reducida, se tiene que $Ass(M/Q'(\mathfrak{p})) = \mathfrak{p}$, $Ass(Q'(\mathfrak{p})) = Ass(M) - \{\mathfrak{p}\}$, por lo que que $Q'(\mathfrak{p}) \in C_{\mathfrak{p}}$. Entonces

$e(M/Q(\mathfrak{p}) = e_{\mathfrak{p}}(M) \leq e(M/Q'(\mathfrak{p})$. Si $e(M/Q(\mathfrak{p})) = e(M/Q'(\mathfrak{p}))$, entonces $Q'(\mathfrak{p}) \in \mathcal{F}(e_{\mathfrak{p}})$, y $Q(\mathfrak{p}) \subset Q'(\mathfrak{p})$ por ser elemento mínimo.

Proposición 1.3.10. *$Q(\mathfrak{p}, n_{\mathfrak{p}})$ es la saturación de $\mathfrak{p}^{n_{\mathfrak{p}}}M$ con respecto a $\mathfrak{p}$.*

Demostración. Notemos $r = n_{\mathfrak{p}}$, y sea $M' = M/\mathfrak{p}^r M$. Como $Ass(M) \subset Ass(\mathfrak{p}^r M) \cup Ass(M')$, $Ass(\mathfrak{p}^r M) \subset Ass(Q(\mathfrak{p}, r) = Ass(M) - \{\mathfrak{p}\}$, se tiene que $\mathfrak{p} \in Ass(M')$, y por tanto pertenece a $Supp(M')$. Si $\mathfrak{q} \in Supp(M')$, entonces $\mathfrak{p}^r M_{\mathfrak{q}} \subsetneq M_{\mathfrak{q}}$. Si $\mathfrak{p}$ no está contenido en $\mathfrak{q}$, entonces tal contención no sería estricta. Por tanto, $\mathfrak{p}$ es el menor elemento de $Supp(M')$, y por tanto es un primo minimal de M'. Entonces $Q(\mathfrak{p}, r)/\mathfrak{p}^r M$ es la saturación de 0 respecto de $\mathfrak{p}$ ([Bou72], p.264, 272), y tenemos el resultado.

La saturación de un módulo con respecto a un ideal primo se puede calcular como la intersección de las componentes primarias del módulo cuyo radical está contenido en el ideal ([Bou72], p. 264).

Nota 1.3.3. Sean M_1 y M_2 R-módulos isomorfos, y $\{0\} = \bigcap_{i=1}^{r} Q_i$ una descomposición primaria reducida de $\{0\}$ en M_1, con Q_i módulo $\mathfrak{p}_i$-primario en M_1, y $\{0\} = \bigcap_{i=1}^{r} S_i$ análoga en M_2, con S_i módulo $\mathfrak{p}_i$-primario en M_2 . Por isomorfía, el número de componentes es el mismo. Si $M_1 = R^{m_1}/K_1$ entonces los módulos Q_i los podemos identificar con submódulos $\tilde{Q}_i$ de R^{m_1} que contienen a K_1. De igual forma obtenemos submódulos $\tilde{S}_i$ de R^{m_2} que contienen a K_2. Entonces, las imágenes mediante el isomorfismo de los módulos Q_i, para $i = 1, \ldots, r$ constituyen una descomposición primaria reducida de 0 en M_2. Si Q_j es una componente aislada, su imagen también lo será, y entonces es igual a S_j. Entonces $\tilde{Q}_j/K_1$ es isomorfo a $\tilde{S}_j/K_2$. Nos preguntamos qué relación existe entre $R^{m_1}/\tilde{Q}_j$ y $R^{m_2}/\tilde{S}_j$.

Proposición 1.3.11. *Sean $M_1 = R^{m_1}/K_1$ y $M_2 = R^{m_2}/K_2$ módulos isomorfos, y sea $\{0\} = \bigcap_{i=1}^{r} Q_i$ la descomposición primaria canónica de $\{0\}$ en M_1, con Q_i módulo $\mathfrak{p}_i$-primario en M_1, y $\{0\} = \bigcap_{i=1}^{r} S_i$ M_2 la descomposición primaria canónica de $\{0\}$ en*

M_2, con S_i módulo $\mathfrak{p}_i$-primario en M_2 . Entonces, si para cada $i = 1, \ldots, r$ tenemos que $Q_i = \tilde{Q}_i/K_1, S_i = \tilde{S}_i/K_2$, entonces $R^{m_1}/\tilde{Q}_i$ es isomorfo a $R^{m_2}/\tilde{S}_i$.

Demostración. Sean A_1 y A_2 matrices de presentación respectivas de M_1 y M_2, y K_1 el submódulo de R^{m_1} generado por las columnas de A_1. Las descomposición primaria canónica de $\{0\}$ en M_1 es equivalente a la de K_1 en R^{m_1}. Veamos la acción de las X-transformaciones. La permutación de columnas o la suma a una columna de un múltiplo escalar de otra no altera el módulo, por lo que la intersección es la misma. La permutación de filas se interpreta como un isomorfismo en R^{m_1}, y aplicamos la misma transformación en las componentes primarias canónicas de la intersección. La adición a una fila de un múltiplo escalar de otra está en la misma situación que el caso anterior. La adición de una columna de ceros no altera al módulo. Por último, la transformación X1 sobre A_1 se puede replicar sobre cada una de las componentes de la intersección, respetando la igualdad. Como A_2 se obtiene de A_1 mediante X-transformaciones, y cada una de ellas respeta las componentes canónicas, tenemos el resultado.

Corolario 1.3.12. *Sean M_1 y M_2 módulos isomorfos, con $Q_1, \ldots, Q_r$ las componentes primarias aisladas de $\{0\}$ en M_1, y $Q'_1, \ldots, Q'_r$ las componentes primarias aisladas de $\{0\}$ en M_2. Entonces existe una reordenación de índices tal que Q_i es isomorfo a Q'_i, para $i = 1, \ldots, r$.*

Ejemplo 1.3.1. Consideremos en el anillo $R = \mathbb{Q}[x, y]$ el ideal $I = \langle x^2, xy \rangle$. Desde el punto de vista de módulos, debemos calcular la descomposición primaria de $\{0\}$ en R/I, o bien la descomposición de I en R. Se tiene que $I = \langle x \rangle \cap \langle x^2, y \rangle = \langle x \rangle \cap \langle x, y \rangle^2$. Los primos asociados son $\mathfrak{p}_1 = \langle x \rangle$ y $\mathfrak{p}_2 = \langle x, y \rangle$. $e_{\mathfrak{p}_1}(I) = 1$, $e_{\mathfrak{p}_2}(I) = 2$. Si $e_{\mathfrak{p}_2}(I) = 1$, entonces existiría $\mathfrak{q}_0$ ideal $\langle x, y \rangle$-primario tal que $\langle x, y \rangle \subset \mathfrak{q}_0$, lo que no puede ocurrir porque $\langle x, y \rangle$ es maximal.

Vamos a calcular su descomposición primaria canónica. Con respecto a $\mathfrak{p}_1$, el saturado de $\langle x \rangle$ es $\langle x \rangle$, pues es primario. Con respecto a $\mathfrak{p}_2 = \langle x, y \rangle$, el saturado de $\mathfrak{p}_2^2$ es $\langle x, y \rangle^2$.

Por tanto, la descomposición primaria canónica de I es $\langle x\rangle \cap \langle x,y\rangle^2$. Efectivamente, $\langle x,y\rangle^2 \subset \langle x^2,y\rangle$.

1.4 Comparación de módulos

Aplicamos los resultados de las sección anterior para decidir si dos matrices presentan módulos isomorfos. Para ello, calculamos descomposiciones primarias mediante el algoritmo de [Rut92].

Ejemplo 1.4.1. En $R = \mathbb{Q}[x,y,z]$, consideremos los R-módulos presentados por las matrices

$$A_1 = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}, A_2 = \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}.$$

Tienen las mismas cadenas de ideales elementales, y hemos visto que no son isomorfos (1.2.4).

Sean K_1 y K_2 los submódulos de R^2 generados por las columnas de A_1 y A_2, respectivamente. Una descomposición primaria de K_1 en R^2 es (ver Apéndice I)

$$K_1 = \langle (1,0),(0,z)\rangle \cap \langle (x,0),(y,z),(0,x)\rangle.$$

Si $Q_{11} = \langle (1,0),(0,z)\rangle$, $Q_{12} = \langle (x,0),(y,z),(0,x)\rangle$, entonces Q_{11} es $\langle z\rangle$-primario y Q_{12} $\langle x\rangle$-primario.

Por otro lado, una descomposición primaria de K_2 en R^2 es (ver Apéndice I)

$$K_2 = \langle (x,0),(0,1)\rangle \cap \langle (z,0),(x,y),(0,z)\rangle,$$

con $Q_{21} = \langle (z,0),(x,y),(0,z)\rangle$ submódulo $\langle z\rangle$-primario, y $Q_{22} = \langle (x,0),(0,1)\rangle$ submódulo $\langle x\rangle$-primario.

Vemos que estos módulos tienen los mismos primos asociados. Como son componentes aisladas, se trata ya de las descomposiciones canónicas.

Para comparar las presentaciones de los módulos R^2/K_1 y R^2/K_2, consideremos las componentes $\langle x\rangle$-primarias, por ejemplo. El módulo R^2/Q_{12} tiene matriz de presentación $\begin{pmatrix} x & y & 0 \\ 0 & z & x \end{pmatrix}$, con cadena de ideales elementales $F_0(R^2/Q_{12}) = \langle xz, x^2, xy\rangle$, $F_1(R^2/Q_{12}) = \langle x, yz\rangle$. El módulo R^2/Q_{22} tiene matriz de presentación $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$, con ideales elementales $F_0(R^2/Q_{22}) = \langle x\rangle$, $F_1(R^2/Q_{22}) = R$. Por tanto no presentan módulos isomorfos.

Nota 1.4.1. Se plantea la siguiente cuestión. Sean Q, Q' submódulos $\mathfrak{p}$-primarios de R^n. Supongamos que matrices de presentación asociadas tienen las mismas cadenas de ideales elementales. ¿Presentan entonces módulos isomorfos?. La respuesta es negativa. Consideremos el siguiente ejemplo extraído de [FS64]. Sean $A_1 = \begin{pmatrix} 2x-1 & -5x+5 \\ 11x-11 & -x+2 \end{pmatrix}$, $A_2 = (53x^2 - 105x + 53)$ matrices de presentación de módulos sobre $R = \mathbb{Z}[x, x^{-1}]$. Los ideales elementales son los mismos, y sea $\Delta(x) = 53x^2 - 105x + 53$. Ambos módulos son $\Delta(x)$-primarios (ver Apéndice I), y en dicho artículo se prueba que no son isomorfos.

1.5 Conjetura de Snapper

En [Sna47a], [Sna47b], se definen invariantes de isomorfía de módulos, extraídos de una descomposición primaria, que a partir de ahora siempre entenderemos que es minimal.

Definición 1.5.1. Sea N un submódulo de R^m y $\mathfrak{p}$ un primo asociado. Denominamos $N(\mathfrak{p})$ a la componente aislada de N cuyos primos asociados están contenidos en $\mathfrak{p}$. $N'(\mathfrak{p})$ es la componente aislada de N cuyos primos asociados están estrictamente contenidos en $\mathfrak{p}$.

Lema 1.5.1. *$N(\mathfrak{p})$ es un submódulo $\mathfrak{p}$-primario de $N'(\mathfrak{p})$.*

Demostración. [Sna47a]

Definición 1.5.2. $\mathbf{e}(\mathfrak{p}) = N(\mathfrak{p}) : N'(\mathfrak{p})$ es el $\mathfrak{p}$-divisor elemental de N. Es un ideal $\mathfrak{p}$-primario. $\rho(\mathfrak{p})$ es el exponente de $\mathbf{e}(\mathfrak{p})$ ($\mathfrak{p}$-exponente de N).

Definición 1.5.3. Una sucesión de R-módulos $Q_0 \subset Q_1 \subset \ldots \subset Q_{l-1} \subset V$ se denomina serie de composición $\mathfrak{p}$-primaria de Q_0 a V si cada Q_i es $\mathfrak{p}$-primario en V y no se puede insertar un módulo $\mathfrak{p}$-primario entre dos términos consecutivos de la sucesión.

Lema 1.5.2. *Para todo módulo Q $\mathfrak{p}$-primario en V se puede construir una serie de composición $\mathfrak{p}$-primaria de Q a V. Todas las series de composición tienen la misma longitud.*

Demostración. [Sna47a]

Definición 1.5.4. $\mathbf{l}(\mathfrak{p})$ es la longitud de $N(\mathfrak{p})$ como submódulo primario de $N'(\mathfrak{p})$, y la llamaremos $\mathfrak{p}$-longitud de M.

Nota 1.5.1. Si $\mathfrak{p}$ es minimal (aislado), entonces $N(\mathfrak{p})$ es la componente primaria de ese primo asociado y $N'(\mathfrak{p})$ es el espacio total R^m.

Ejemplo 1.5.1. En $R = \mathbb{Q}[x, y]$, consideremos los siguientes ideales y descomposiciones primarias:

$$I_1 = \langle x \rangle \cap \langle x, y^2 \rangle, I_2 = \langle x \rangle \cap \langle x^2, y \rangle, I_3 = \langle x \rangle \cap \langle x, y^3 \rangle.$$

Llamemos $\mathfrak{q}_{ij}$ a las componentes primarias del ideal I_i, y $\mathfrak{p}_{ij}$ a su primo asociado. Entonces

$\mathfrak{q}_{11} = \langle x \rangle, \mathfrak{p}_{11} = \langle x \rangle,$

$\mathfrak{q}_{12} = \langle x, y^2 \rangle, \mathfrak{p}_{12} = \langle x, y \rangle,$

$\mathfrak{q}_{21} = \langle x \rangle, \mathfrak{p}_{21} = \langle x \rangle.$

$\mathfrak{q}_{22} = \langle x^2, y \rangle, \mathfrak{p}_{22} = \langle x, y \rangle.$

$\mathfrak{q}_{31} = \langle x \rangle, \mathfrak{p}_{31} = \langle x \rangle.$

$\mathfrak{q}_{32} = \langle x, y\rangle^3, \mathfrak{p}_{32} = \langle x, y\rangle$.

Para cada primo asociado, calculamos los invariantes anteriormente definidos. Sea $\mathfrak{p} = \langle x, y\rangle$, primo asociado de I_1, I_2, I_3. $I_1(\mathfrak{p})$ es la componente aislada de I_1 cuyos primos asociados están contenidos en $\mathfrak{p}$. Por tanto, $I_1(\mathfrak{p}) = I_1$. $I_1'(\mathfrak{p})$ es la componente aislada de I_1 cuyos primos asociados están estrictamente contenidos en $\mathfrak{p}$. Por tanto, $I_1'(\mathfrak{p}) = \langle x\rangle$. Análogamente, $I_2(\mathfrak{p}) = I_2$, $I_2'(\mathfrak{p}) = \langle x\rangle$, $I_3(\mathfrak{p}) = I_3$, $I_3'(\mathfrak{p}) = \langle x\rangle$. A partir de aquí, obtenemos $\mathbf{e}_1(\mathfrak{p}) = I_1(\mathfrak{p}) : I_1'(\mathfrak{p}) = \langle x^2, xy\rangle : \langle x\rangle = \langle x, y\rangle$. Entonces se tiene que $\mathbf{e}_2(\mathfrak{p}) = \langle x^2, xy\rangle : \langle x\rangle = \langle x, y\rangle$, $\mathbf{e}_3(\mathfrak{p}) = \langle x^3, x^2y, xy^2\rangle : \langle x\rangle = \langle x, y\rangle^2$, $\rho_1(\mathfrak{p}) = 1$, $\rho_2(\mathfrak{p}) = 1$, $\rho_3(\mathfrak{p}) = 2$.

Sea ahora $\mathfrak{p} = \langle x\rangle$. Entonces

$I_1(\mathfrak{p}) = \langle x\rangle$, $I_1'(\mathfrak{p}) = R$, $\mathbf{e}_1(\mathfrak{p}) = \langle x\rangle$.

$I_2(\mathfrak{p}) = \langle x\rangle$, $I_2'(\mathfrak{p}) = R$, $\mathbf{e}_2(\mathfrak{p}) = \langle x\rangle$.

$I_3(\mathfrak{p}) = \langle x\rangle$, $I_3'(\mathfrak{p}) = R$, $\mathbf{e}_3(\mathfrak{p}) = \langle x\rangle$.

$\rho_1(\mathfrak{p}) = 1$, $\rho_2(\mathfrak{p}) = 1$, $\rho_3(\mathfrak{p}) = 1$.

A partir de la función de Hilbert, en [Sna47b] se incorpora un nuevo invariante. Dado un submódulo de $k[x_1, \ldots, x_n]^m$, se considera el módulo homogeneizado en $k[x_0, x_1, \ldots, x_n]^m$, donde se calcula la función de Hilbert respecto a un módulo que lo contiene. Al coeficiente del término de mayor grado se le denomina grado.

Definición 1.5.5. $a_0(\mathfrak{p})$ es el grado de $N(\mathfrak{p})$ como submódulo primario de $N'(\mathfrak{p})$.

En [Sna47b], p.652 se pregunta si los invariantes que ha definido en los dos artículos determina la matriz de presentación de un módulo sobre $k[x_1, \ldots, x_n]$, con $n > 1$, salvo isomorfismo. Estos invariantes lo son por X-transformaciones. La respuesta a la pregunta es no.

Ejemplo 1.5.2. Consideremos los módulos M_1 y M_2 presentados por las matrices

$$A_1 = \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}, A_2 = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$$

respectivamente. Hemos visto que no son isomorfos en el ejemplo 1.2.4. Sean $K_1 = \langle (x,y),(0,z)\rangle$, $K_2 = \langle (x,0),(y,z)\rangle$ los submódulos de R^2 determinados por las columnas. Entonces $K_1 = Q_{11} \cap Q_{12}$, con $Q_{11} = \langle (1,0),(0,z)\rangle$, $Q_{12} = \langle (x,0),(y,z),(0,x)\rangle$, $K_2 = Q_{21} \cap Q_{22}$, con $Q_{21} = \langle (z,0),(x,y),(0,z)\rangle$ y $Q_{22} = \langle (x,0),(0,1)\rangle$ son descomposiciones primarias en R^2, como hemos calculado anteriormente. Sean $\mathfrak{p}_1 = \langle x\rangle$ y $\mathfrak{p}_2 = \langle z\rangle$ los primos asociados.

Los invariantes de Snapper para K_1 son $e(\mathfrak{p}_1) = \langle x\rangle$, $e(\mathfrak{p}_2) = \langle z\rangle$. $\rho(\mathfrak{p}_1) = 1$, $\rho(\mathfrak{p}_2) = 1$. $l(\mathfrak{p}_1) = 1$, $l(\mathfrak{p}_2) = 1$. $a_0(\mathfrak{p}_1) = 1$, $a_0(\mathfrak{p}_2) = 1$. Los invariantes de Snapper para K_2 son $e(\mathfrak{p}_1) = \langle x\rangle$, $e(\mathfrak{p}_2) = \langle z\rangle$. $\rho(\mathfrak{p}_1) = 1$, $\rho(\mathfrak{p}_2) = 1$. $l(\mathfrak{p}_1) = 1$, $l(\mathfrak{p}_2) = 1$. $a_0(\mathfrak{p}_1) = 1$, $a_0(\mathfrak{p}_2) = 1$. Por tanto, coinciden y no son isomorfos.

Nota 1.5.2. En [Sna47b] aparece la siguiente pregunta:

"Se puede probar fácilmente que si $A = (a_{ij})$ es una matriz $m \times s$, $a_{ij} \in k[x_1, \ldots, x_n]$, los invariantes de A no cambian por transformaciones de semejanza PAQ, donde P y Q son matrices polinomiales cuadradas e invertibles.". Por 'invariantes de A' se refiere a los valores que ha definido en el artículo, y que aquí llamamos invariantes de Snapper. Sigue diciendo

"Si $n = 1$, una descomposición de Noether (descomposición primaria reducida) del espacio de fila (o espacio de columnas) da lugar a invariantes, más concretamente los divisores elementales clásicos de diferente rango, que determinan A completamente salvo transformaciones de semejanza. Si es así para $n > 1$ es un problema no resuelto." Si lo que pregunta es si existen matrices no semejantes con todos los invariantes iguales, tenemos la respuesta en el primer ejemplo de este texto: el mismo ideal expresado de dos formas distintas no semejantes. Para módulos en general, el ejemplo anterior da una respuesta negativa. Continúa diciendo

"Igualmente no resuelto, para $n > 1$, es la cuestión de si invariantes que procedan de una descomposición de Noether de un módulo $M \subset V$ determina al módulo V/M salvo isomorfismo." Vamos a ver en el siguiente ejemplo que podemos tener módulos no

isomorfos con componentes primarias isomorfas.

Ejemplo 1.5.3. En este caso consideramos módulos sobre el anillo $\mathbb{Z}[x]$. En [Hil86] se prueba que los $\mathbb{Z}[x]$-módulos M_1 y M_2 presentados por las respectivas matrices

$$A_1 = \begin{pmatrix} x^2 - x + 1 & 2x + 1 \\ 0 & 5x^2 - 9x + 5 \end{pmatrix}, A_2 = \big((5x^2 - 9x + 5)(x^2 - x + 1)\big)$$

no son isomorfos. Consideremos N_1 el submódulo de $\mathbb{Z}[x]^2$ generado por las columnas de A_1 y N_2 el submódulo de $\mathbb{Z}[x]$ (un ideal) generados por la columna de A_2. Vamos a ver que las componentes primarias canónica de N_1 en $\mathbb{Z}[x]^2$ son isomorfas a las de N_2 en $\mathbb{Z}[x]$.

La descomposición primaria de N_2 en $\mathbb{Z}[x]$ es inmediata, y viene dada por los módulos (en este caso ideales) con matrices de presentación $Q_{21} = (x^2 - x + 1)$ y $Q_{22} = (5x^2 - 9x+5)$. Sea $\mathfrak{p}_1$ el ideal generado por (x^2-x+1), y $\mathfrak{p}_2$ el ideal generado por $(5x^2-9x+5)$. Como se muestra en el Apéndice I, la descomposición primaria de N_1 es

$$\begin{aligned} \langle (x^2 - x + 1, 0), (2x + 1, 5x^2 - 9x + 5) \rangle &= \\ \langle (1, 0), (0, 5x^2 - 9x + 5) \rangle \cap \langle (7, -4x - 8), (0, x^2 - x + 1), (x - 3, 4) \rangle &= \\ = Q_{11} \cap Q_{12} & \end{aligned}$$

Es claro que $\mathbb{Z}[x]^2/Q_{11} \equiv \mathbb{Z}[x]/Q_{21}$, porque sus matrices de presentación están relacionadas mediante una transformación de tipo X2. Veamos ahora que el módulo $\mathbb{Z}[x]^2/Q_{12}$ es isomorfo a $\mathbb{Z}[x]/Q_{21}$.

Sea $\varphi : \mathbb{Z}[x]^2/Q_{12} \to \mathbb{Z}[x]/Q_{21}$ un morfismo, con

$$\begin{aligned} \varphi(\mathrm{e}_1 + Q_{12}) &= (a_{11}x + a_{12}) + Q_{21}, \\ \varphi(\mathrm{e}_2 + Q_{12}) &= (a_{21}x + a_{22}) + Q_{21} \end{aligned}$$

con $a_{ij} \in \mathbb{Z}$, $i, i = 1, 2$. No hace falta tomar términos de mayor grado porque los

podemos reducir mediante $x^2 - x + 1$. Para que φ esté bien definido, se tiene que verificar que

$$7(a_{11}x + a_{12}) + (-4x - 8)(a_{21}x + a_{22}) \in Q_{21},$$
$$(2x + 1)(a_{11}x + a_{12}) + (-x^2 - 3x - 1)(a_{21}x + a_{22}) \in Q_{21}.$$

Entonces existen $\lambda_1, \lambda_2 \in \mathbb{Z}[x]$ tales que $7(a_{11}x+a_{12})+(-4x-8)(a_{21}x+a_{22}) = \lambda_1(x^2-x+1)$ y $(2x+1)(a_{11}x+a_{12})+(-x^2-3x-1)(a_{21}x+a_{22}) = \lambda_2(x^2-x+1)$. Por consideraciones de grado, λ_1 es de grado cero y λ_2 es de grado uno, y escribimos entonces $\lambda_2 = \lambda_{21}x+\lambda_{22}$, con $\lambda_{21}, \lambda_{22} \in \mathbb{Z}$. Al desarrollar e igualar coeficientes queda el sistema en $\mathbb{Z}$

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & -4 & 0 \\ 1 & 0 & 0 & 7 & 0 & -8 & -4 \\ 0 & -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & -1 & 2 & 0 & -3 & -1 \\ 0 & -1 & 1 & 1 & 2 & -1 & -3 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_{21} \\ \lambda_{22} \\ a_{11} \\ a_{12} \\ a_{21} \\ a_{22} \end{pmatrix} = \mathbf{0} \qquad (1.5.1)$$

Resolvemos este sistema diofántico por el algoritmo de Smith, y nos queda que

$$\lambda_1 = -4y_6, \qquad \lambda_{21} = -y_6, \qquad \lambda_{22} = y_7,$$
$$a_{11} = 4y_6 + 4y_7, \quad a_{12} = 4y_6 + 8y_7, \quad a_{21} = y_6, \quad a_{22} = 4y_6 + 7y_7,$$

con $y_6, y_7 \in \mathbb{Z}$. Para que φ sea isomorfismo, hay que exigir que $1 \in \langle x^2 - x + 1, (4y_6 + 4y_7)x+(4y_6+8y_7), y_6x+(4y_6+7y_7)\rangle$, por sobreyectividad. Si tomamos $y_6 = 1, y_7 = -1$, tenemos la condición.

Entonces $\varphi(\mathbf{e}_1 + Q_{12}) = -4 + Q_{21}$, $\varphi(\mathbf{e}_2 + Q_{12}) = (x - 3) + Q_{21}$, y el morfismo inverso es $\psi : \mathbb{Z}[x]/Q_{21} \to \mathbb{Z}[x]^2/Q_{12}$ definido por $\psi(1 + Q_{21}) = (-2, x + 2) + Q_{12}$.

Tenemos así un ejemplo de módulos no isomorfos, con las componentes primarias canónicas del submódulo 0 isomorfas entre sí.

1.6 Localización

Una de las técnicas habituales para estudiar objetos sobre un anillo conmutativo es la localización en ideales primos. En el siguiente capítulo veremos incluso cómo un problema se puede resolver dando soluciones en anillos localizados. Vamos a ver con unos ejemplos que esta técnica no resuelve el problema de la comparación de presentaciones.

Ejemplo 1.6.1. Sea $R = \mathbb{Z}[\sqrt{-5}]$, y consideremos el ideal $I = \langle 2, 1+\sqrt{-5}\rangle$. R es un anillo de Dedekind, y el ideal I no es principal (ver [AW92]). Entonces I no es isomorfo a R como R-módulos, pero para todo ideal maximal $\mathfrak{m}$ de R, se tiene que $I_{\mathfrak{m}}$ es principal, e isomorfo entonces a $R_{\mathfrak{m}}$. Para anillo de polinomios podemos considerar la comparación de $I \otimes R[x] \simeq I[x]$ con $R[x]$. La localización en maximales de R nos da el mismo resultado.

Vamos entonces a exigir que el anillo de coeficientes sea un dominio de ideales principales.

Ejemplo 1.6.2. Retomemos el ejemplo de [Hil86]. Sea M_1 el módulo presentado por la matriz $A_1 = \begin{pmatrix} x^2-x+1 & 2x+1 \\ 0 & 5x^2-9x+5 \end{pmatrix}$ sobre el anillo $\mathbb{Z}[x]$, y M_2 el $\mathbb{Z}[x]$-módulo con matriz de presentación $A_2 = ((5x^2-9x+5)(x^2-x+1))$. Sea $p \in \mathbb{Z}$ un número primo. Queremos estudiar qué ocurre al considerar la proyección sobre $\mathbb{Z}_{\langle p\rangle}[x]$, el anillo de polinomios con coeficientes en el localizado $\mathbb{Z}_{\langle p\rangle}$. Si $p \neq 7$, como $7 \in \langle x^2-x+1, 2x+1\rangle$, podemos añadir columnas nulas y obtener 7 en la posición $(1,3)$. En el anillo localizado, es unidad, y pivotamos sobre él para obtener una matriz equivalente a A_2. Si $p = 7$, entonces operamos de la siguiente forma:

$$43/4 \;=\; (5x^2-9x+5) + (-5/2x + 23/4)(2x+1)$$

Esto se traduce como una operación elemental entre filas. Como $43/4$ es unidad en $\mathbb{Z}_{\langle 7\rangle}$, podemos reducir la matriz a una equivalente a A_2. Por tanto, los módulos son isomorfos sobre $\mathbb{Z}_{\langle p\rangle}[x]$ para todo primo $p \in \mathbb{Z}$.

Ejemplo 1.6.3. Con el mismo ejemplo que en el caso anterior, vamos a considerar el comportamiento sobre anillos locales $\mathbb{Z}[x]_{\mathfrak{p}}$, con $\mathfrak{p}$ un ideal primo de $\mathbb{Z}[x]$. Recordemos que estos módulos tienen componentes primarias isomorfas. Si $\mathfrak{p}$ es un primo que no corta a uno de los asociados y corta al otro, nos queda una componente en M_1, y sabemos que es isomorfa a la correspondiente de M_2. Si $\mathfrak{p}$ es un primo que contiene a los asociados, entonces contiene a $\langle x^2 - x + 1, 5x^2 - 9x + 5\rangle = \langle x^2 - x + 1, 4\rangle$. En tal caso, por su carácter primo, $\mathfrak{p} = \langle x^2 - x + 1, 2\rangle$, que es maximal en $\mathbb{Z}[x]$. Por [Kun85], p. 110, el número mínimo de generadores en el localizado es 1, es decir, es cíclico, y por tanto isomorfo a M_2.

Capítulo 2

Una prueba algorítmica del Teorema de Estabilidad de Suslin sobre $\mathbb{Z}[x]$

2.1 Introducción

En [PW95] se da un algoritmo que descompone una matriz de $SL_n(k[x_1, \ldots, x_m])$, con $n \geq 3$ en producto de matrices elementales. En este capítulo extendemos el resultado, con los mismos métodos, a $SL_n(\mathbb{Z}[x])$, $n \geq 3$. El teorema de estabilidad de Suslin [Sus77] se enuncia así:

> Sea R un anillo conmutativo noetheriano, y $n \geq máx(3, \dim(R) + 2)$. Entonces, toda matriz cuadrada de orden n, $A = (f_{ij})$ de determinante 1, con f_{ij} elementos del anillo de polinomios $R[x_1, \ldots, x_m]$, se puede escribir como producto de matrices elementales sobre $R[x_1, \ldots, x_m]$, para cualquier $m \geq 0$.

Definición 2.1.1. Para un anillo R, una matriz elemental $E_{ij}(a)$ de orden n sobre R

es una matriz de la forma $I + a \cdot e_{ij}$ donde $i \neq j, a \in R$ y e_{ij} es la matriz $n \times n$ cuya (i, j) componente es 1 y las restantes son cero.

Sea $SL_n(R)$ el grupo de todas las matrices $n \times n$ de determinante 1 con entradas en R, y sea $E_n(R)$ el subgrupo de $SL_n(R)$ generado por las matrices elementales. Entonces el *teorema de estabilidad de Suslin* se puede escribir como

$$SL_n(R[x_1, \ldots, x_m]) = E_n(R[x_1, \ldots, x_m]) \tag{2.1.1}$$

para todo $n \geq máx(3, \dim(R) + 2)$.

En este capítulo se siguen los pasos de [PW95] para dar un algoritmo de descomposición en $SL_n(\mathbb{Z}[x])$. Hay que modificar algunas demostraciones del artículo original, como es el uso de la normalización de Noether y la descomposición en ciertos anillos locales. Se darán las demostraciones completas, y se indicará dónde sigue las pruebas de [PW95]. El objetivo es, entonces, desarrollar un algoritmo para que, dada una matriz $A \in SL_n(\mathbb{Z}[x])$ con $n \geq 3$, podamos encontrar matrices elementales $E_1, \ldots, E_t \in E_n(\mathbb{Z}[x])$ tales que $A = E_1 \cdots E_t$.

Nota 2.1.1. Si una matriz A se puede escribir como producto de matrices elementales, diremos que A es *realizable.*

En la primera sección se prueba de forma algorítmica la normalidad de $E_n(\mathbb{Z}[x_1, \ldots, x_m])$ en $SL_n(\mathbb{Z}[x_1, \ldots, x_m])$ para $n \geq 3$. Es la misma que [PW95], pues no interviene para nada el anillo base. Por semejanza, incluímos la matriz de [Coh66] en $SL_2(\mathbb{Z}[x])$.

A continuación, usamos el *Proceso de Inducción de Quillen* para reducir el problema a anillos locales. Se modifica respecto [PW95] la elección de los ideales maximales sobre $\mathbb{Z}$.

En la siguiente sección probamos la transitividad de las matrices elementales sobre las columnas unimodulares en $\mathbb{Z}[x]$. Se altera respecto a [PW95] la exigencia del carácter

mónico de un polinomio por la condición de que el máximo común divisor de sus coeficientes sea 1. Esto permite la reducción del problema a un algoritmo de realización en $SL_3(\mathbb{Z}[x])$ para matrices de la forma

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(\mathbb{Z}[x]),$$

sin exigencias sobre p. Como se comenta en [PW95], esta prueba da una demostración constructiva del *teorema de Quillen-Suslin* en $\mathbb{Z}[x]$, mediante los resultados de [LS92]. Por último, damos un algoritmo para descomponer las matrices de la forma

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

en $R[x]$, donde R es la localización de $\mathbb{Z}$ en un ideal maximal. Se resuelve primero el caso en que el coeficiente líder de p es una unidad, y luego se reduce a éste el caso general.

2.2 Normalidad de $E_n(\mathbb{Z}[x_1, \ldots, x_m])$ en $SL_n(\mathbb{Z}[x_1, \ldots, x_m])$ para $n \geq 3$

Lema 2.2.1. *La matriz de Cohn,* $A = \begin{pmatrix} 1+2x & 4 \\ -x^2 & 1-2x \end{pmatrix} \in SL_2(\mathbb{Z}[x])$ *no es realizable, pero* $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \in SL_3(\mathbb{Z}[x])$ *sí lo es.*

Demostración. El carácter no realizable de A se prueba en [Coh66]. Consideremos

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+2x & 4 & 0 \\ -x^2 & 1-2x & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{2.2.1}$$

Observemos que $\begin{pmatrix} 1+2x & 4 & 0 \\ -x^2 & 1-2x & 0 \\ 0 & 0 & 1 \end{pmatrix} = I + \begin{pmatrix} 2 \\ -x \\ 0 \end{pmatrix} \cdot (x, 2, 0)$. Entonces, la descomposición en matrices elementales se deduce del lema 2.2.2.

Definición 2.2.1. Sea $n \geq 2$. Una **matriz de Cohn** en $\mathbb{Z}[x_1, \ldots, x_m]$ es una matriz de la forma

$$I + a\mathbf{v} \cdot (v_j \mathbf{e}_i - v_i \mathbf{e}_j)$$

donde $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in (\mathbb{Z}[x_1, \ldots, x_m])^n$, $i < j \in \{1, \ldots, n\}$, $a \in \mathbb{Z}[x_1, \ldots, x_m]$, y $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ con 1 en la i-ésima posición.

Lema 2.2.2. *Toda matriz de Cohn con $n \geq 3$ es realizable.*

Demostración. Consideremos el caso $i = 1, j = 2$. Entonces

$$\begin{aligned} B &= I + a \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \cdot (v_2, -v_1, 0, \ldots, 0) \\ &= \begin{pmatrix} 1 + av_1v_2 & -av_1^2 & 0 & \cdots & 0 \\ av_2^2 & 1 - av_1v_2 & 0 & \cdots & 0 \\ av_3v_2 & -av_3v_1 & & & \\ \vdots & \vdots & & I_{n-2} & \\ av_nv_2 & -av_nv_1 & & & \end{pmatrix} \\ &= \begin{pmatrix} 1 + av_1v_2 & -av_1^2 & 0 & \cdots & 0 \\ av_2^2 & 1 - av_1v_2 & 0 & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & I_{n-2} & \\ 0 & 0 & & & \end{pmatrix} \prod_{l=3}^{n} E_{l1}(av_lv_2) E_{l2}(-av_lv_1), \end{aligned}$$

Por tanto, basta probar que

$$A = \begin{pmatrix} 1+av_1v_2 & -av_1^2 & 0 \\ av_2^2 & 1-av_1v_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2.2.2}$$

es realizable para $a, v_1, v_2 \in \mathbb{Z}[x_1, \ldots, x_m]$. Indiquemos por "$\rightarrow$" la aplicación de transformaciones elementales, y consideremos las siguientes:

$$\begin{aligned} A &= \begin{pmatrix} 1+av_1v_2 & -av_1^2 & 0 \\ av_2^2 & 1-av_1v_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1+av_1v_2 & -av_1^2 & v_1 \\ av_2^2 & 1-av_1v_2 & v_2 \\ 0 & 0 & 1 \end{pmatrix} \\ &\rightarrow \begin{pmatrix} 1 & -av_1^2 & v_1 \\ 0 & 1-av_1v_2 & v_2 \\ -av_2 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & v_1 \\ 0 & 1 & v_2 \\ -av_2 & av_1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & v_1 \\ 0 & 1 & v_2 \\ 0 & av_1 & 1+av_1v_2 \end{pmatrix} \\ &\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & v_2 \\ 0 & av_1 & 1+av_1v_2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & v_2 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned} \tag{2.2.3}$$

Anotando todas las transformaciones implicadas, se obtiene

$$A = E_{13}(-v_1)E_{23}(-v_2)E_{31}(-av_2)E_{32}(av_1)E_{13}(v_1)E_{23}(v_2)E_{31}(av_2)E_{32}(-av_1). \tag{2.2.4}$$

En general, para $i < j$,

$$B = I + a \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \cdot (0, \ldots, 0, v_j, 0, \ldots, 0, -v_i, 0, \ldots, 0)$$

(Aquí, v_j aparece en la i-ésima posición y $-v_i$ aparece en la j-ésima posición.)

$$= \begin{pmatrix} 1 & \cdots & av_1v_j & \cdots & -av_1v_i & \cdots & 0 \\ & \ddots & \vdots & & \vdots & & 0 \\ & & 1 + av_iv_j & & -av_i^2 & & \\ & & \vdots & & \vdots & & \\ & & av_j^2 & & 1 - av_iv_j & & \\ & & \vdots & & \vdots & & \\ & & v_nv_j & & -v_nv_i & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ & \ddots & \vdots & & \vdots & & 0 \\ & & 1 + av_iv_j & & -av_i^2 & & \\ & & \vdots & & \vdots & & \\ & & av_j^2 & & 1 - av_iv_j & & \\ & & \vdots & & \vdots & & \\ & & 0 & & 0 & & 1 \end{pmatrix}$$

$$\cdot \prod_{1 \le l \le n, l \ne i,j} E_{li}(av_lv_j)E_{lj}(-av_lv_i)$$

$$= E_{it}(-v_i)E_{jt}(-v_j)E_{ti}(-av_j)E_{tj}(av_i)E_{it}(v_i)E_{jt}(v_j)E_{ti}(av_j)E_{tj}(-av_i)$$

$$\cdot \prod_{1 \le l \le n, l \ne i,j} E_{li}(av_lv_j)E_{lj}(-av_lv_i). \qquad (2.2.5)$$

En lo anterior, $t \in \{1, \ldots, n\}$ se puede elegir cualquier número distinto a i y j.

Como una *matriz de Cohn* es realizable, todo producto de *matrices de Cohn* lo es también. Esta observación permite una generalización del anterior resultado.

Definición 2.2.2. Sea R un anillo y $\mathbf{v} = (v_1, \ldots, v_n)^t \in R^n$ para algún $n \in \mathbb{N}$. Entonces se dice que $\mathbf{v}$ es un *vector columna unimodular* si sus componentes generan R, esto es, si existen $g_1, \ldots, g_n \in R$ tales que $v_1 g_1 + \cdots + v_n g_n = 1$.

Corolario 2.2.3. *Supongamos que* $A \in SL_n(\mathbb{Z}[x_1, \ldots, x_m])$ *con* $n \geq 3$ *admite una escritura de la forma* $A = I + \mathbf{v} \cdot \mathbf{w}$, *con* $\mathbf{v}$ *un vector columna unimodular y* $\mathbf{w}$ *un vector fila en* $\mathbb{Z}[x_1, \ldots, x_m]$, *tales que* $\mathbf{w} \cdot \mathbf{v} = 0$. *Entonces* A *es realizable.*

Demostración. Como $\mathbf{v} = (v_1, \ldots, v_n)^t$ es unimodular, podemos encontrar $g_1, \ldots, g_n \in \mathbb{Z}[x_1, \ldots, x_m]$ tales que $v_1 g_1 + \cdots + v_n g_n = 1$. Esto se puede hacer de manera efectiva mediante el uso de bases de Gröbner ([AL94],[CLO92]). Si lo combinamos con $\mathbf{w} \cdot \mathbf{v} = w_1 v_1 + \cdots + w_n v_n = 0$ nos da una nueva expresión para $\mathbf{w}$:

$$\mathbf{w} = \sum_{i<j} a_{ij}(v_j \mathbf{e}_i - v_i \mathbf{e}_j) \tag{2.2.6}$$

donde $a_{ij} = w_i g_j - w_j g_i$. Ahora,

$$A = \prod_{i<j} (I + \mathbf{v} \cdot a_{ij}(v_j \mathbf{e}_i - v_i \mathbf{e}_j)) \,. \tag{2.2.7}$$

Cada factor del lado derecho de la ecuación es una *matriz de Cohn* y por tanto realizable. Entonces A es también realizable.

Corolario 2.2.4. $BE_{ij}(a)B^{-1}$ *es realizable para toda* $B \in GL_n(\mathbb{Z}[x_1, \ldots, x_m])$ *con* $n \geq 3$ *y* $a \in \mathbb{Z}[x_1, \ldots, x_m]$.

Demostración. Observemos que $i \neq j$, y

$$BE_{ij}(a)B^{-1} = I + (i\text{-ésimo vector columna de } B) \cdot a \cdot (j\text{-ésimo vector fila de } B^{-1}).$$

Sea $\mathbf{v}$ el vector columna i-ésimo de B y sea $\mathbf{w}$ a veces el j-ésimo vector fila de B^{-1}. Entonces (i-ésimo vector fila de B^{-1}) $\cdot\, \mathbf{v} = 1$ implica que $\mathbf{v}$ es unimodular, y $\mathbf{w} \cdot \mathbf{v}$ es

claramente cero, porque $i \neq j$. Así, $BE_{ij}(a)B^{-1} = I + \mathbf{v} \cdot \mathbf{w}$ satisface la condición del corolario anterior, y es realizable.

Nota 2.2.1. Una consecuencia importante de este corolario es que $E_n(\mathbb{Z}[x_1, \ldots, x_m])$ es un subgrupo normal de $SL_n(\mathbb{Z}[x_1, \ldots, x_m])$ para $n \geq 3$, esto es, si $A \in SL_n(\mathbb{Z}[x_1, \ldots, x_m])$ and $E \in E_n(\mathbb{Z}[x_1, \ldots, x_m])$, el corolario anterior nos da un algoritmo para encontrar matrices elementales $E_1, \ldots, E_t$ tales que $A^{-1}EA = E_1 \cdots E_t$. Si $E = F_1 \cdot \ldots \cdot F_r$, con $F_i \in E_n(\mathbb{Z}[x_1, \ldots, x_m])$, entonces $A^{-1}EA = [A^{-1}F_1A] \cdot \ldots [A^{-1}F_rA]$, y cada corchete se descompone en producto de elementales.

2.3 Pegado de las realizaciones locales

Sea $R = \mathbb{Z}$ y $\mathfrak{m} \in \text{Max}(R) = \{$ ideales maximales de $R\}$. Si $A \in SL_n(R[x])$, notamos $A_{\mathfrak{m}} \in SL_n(R_{\mathfrak{m}}[x])$ su imagen bajo el morfismo canónico $SL_n(R[x]) \to SL_n(R_{\mathfrak{m}}[x])$. Sabemos que $SL_n(R) = E_n(R)$ para $n \geq 3$ (incluso para $n = 2$, pues $\mathbb{Z}$ es dominio euclídeo). Consideremos el teorema análogo de Quillen para matrices elementales:

> Supongamos que $n \geq 3$ y $A \in SL_n(R[x])$. Entonces A es realizable sobre $R[x]$ si y solamente si $A_{\mathfrak{m}} \in SL_n(R_{\mathfrak{m}}[x])$ es realizable sobre $R_{\mathfrak{m}}[x]$ para todo $\mathfrak{m} \in \text{Max}(R)$.

Se trata de dar una demostración constructiva. La necesidad de la condición es clara. Queda probar lo siguiente:

Teorema 2.3.1. *(Algoritmo de inducción de Quillen) Dada $A \in SL_n(R[x])$, si $A_{\mathfrak{m}} \in E_n(R_{\mathfrak{m}}[x])$ para todo $\mathfrak{m} \in \text{Max}(R)$, entonces $A \in E_n(R[x])$.*

Demostración. (Teorema 2.3.1.) Sea $p_1 \in \mathbb{Z}$ un primo cualquiera, y llamemos $\mathfrak{m}_1 = \langle p_1 \rangle$, el ideal maximal de $\mathbb{Z}$ generado por p_1. Por la hipótesis, $A_{\mathfrak{m}_1}$ es realizable en $R_{\mathfrak{m}_1}[x]$.

Podemos entonces escribir

$$A_{\mathfrak{m}_1} = \prod_j E_{s_j t_j} \begin{pmatrix} c_j \\ d_j \end{pmatrix} \tag{2.3.1}$$

where $c_j \in R[x]$, $d_j \in R, d_j \notin \mathfrak{m}_1$. Si llamamos $r_1 = \prod_j d_j \notin \mathfrak{m}_1$, podemos reeescribir el producto como

$$A_{\mathfrak{m}_1} = \prod_j E_{s_j t_j} \begin{pmatrix} c_j \prod_{k \neq j} d_k \\ r_1 \end{pmatrix} \in E_n(R_{r_1}[x]) \subset E_n(R_{\mathfrak{m}_1}[x]). \tag{2.3.2}$$

Si r_1 fuera 1, continuamos con el proceso de 'pegado'. Si no es así, sea p_2 un primo que divida a r_1, y llamamemos $\mathfrak{m}_2$ al ideal maximal generado por p_2. Como $A_{\mathfrak{m}_2}$ es realizable en $R_{\mathfrak{m}_2}[x]$, obtenemos de la misma forma un elemento $r_2 \notin \mathfrak{m}_2$. Es claro que $r_1 \in \mathfrak{m}_2$. Como R es un dominio de ideales principales, existe $h_2 \in R$ que genera el ideal $\langle r_1, r_2 \rangle$. Es su máximo común divisor. Si h_2 es 1 vamos al proceso de 'pegado'. En otro caso, tomamos p_3 un primo que divida a h_2, y sea $\mathfrak{m}_3$ el ideal generado por p_3. Tenemos que $r_1, r_2 \in \mathfrak{m}_3$, y calculamos como antes $r_3 \notin \mathfrak{m}_3$. De forma inductiva, definimos $r_j \notin \mathfrak{m}_j$, con

$$A_{\mathfrak{m}_j} \in E_n(R_{r_j}[x]). \tag{2.3.3}$$

y $r_1, \ldots, r_{j-1} \in \mathfrak{m}_j = \langle p_j \rangle$, con p_j un divisor primo de $\mathrm{mcd}(r_1, \ldots, r_{j-1})$. Aquí enlazamos con la construcción de [PW95]. Como R es noetheriano, tras un número finito de pasos encontramos un l tal que $r_1 R + \cdots + r_l R = R$. Mediante bases de Gröbner se puede detectar esta condición. Empezamos entonces el proceso de 'pegado'. Aquí alteramos la exposición de [PW95] para mostrar más claramente el algoritmo. Para simplificar la notación, llamamos $A_i = A_{\mathcal{M}_i}$ e identificamos $A \in SL_n(R[x])$ con $A_i \in SL_n(R_{\mathfrak{m}_i}[x])$

Aserto: Para cualesquiera $c, g \in R$, podemos encontrar un d suficientemente grande tal que $A_i^{-1}(cX)A_i((c + r_i^d g)X) \in E_n(R[x])$ para todo $i = 1, \ldots, l$.

Sea

$$D_i(X, Y, Z) = A_i^{-1}(Y \cdot X)A_i((Y + Z) \cdot X) \in E_n(R_{r_i}[X, Y, Z]) \tag{2.3.4}$$

y escribamos D_i en la forma

$$D_i = \prod_{j=1}^{h} E_{s_j t_j}(b_j + Zf_j) \tag{2.3.5}$$

donde $b_j \in R_{r_i}[X, Y]$ y $f_j \in R_{r_i}[X, Y, Z]$. En adelante, la matriz elemental $E_{s_j t_j}(a)$ se denotará por $E^j(a)$ por conveniencia en la notación. Definimos C_p como

$$C_p = \prod_{j=1}^{p} E^j(b_j) \in E_n(R_{r_i}[X, Y]). \tag{2.3.6}$$

Entonces las matrices C_p satisfacen las relaciones recursivas

$$\begin{aligned} E^1(b_1) &= C_1 \\ E^p(b_p) &= C_{p-1}^{-1} C_p \quad (2 \leq p \leq h) \\ C_h &= I. \end{aligned} \tag{2.3.7}$$

Esta última relación se tiene porque las matrices elementales que aporta $A_i^{-1}(Y \cdot X)$ a C_h son las inversas de las que aporta $A_i((Y + Z) \cdot X)$. Considerando que $E_{ij}(a + b) = E_{ij}(a)E_{ij}(b)$, se tiene

$$\begin{aligned} D_i &= \prod_{j=1}^{h} E^j(b_j + Zf_j) \\ &= \prod_{j=1}^{h} E^j(b_j) E^j(Zf_j) \\ &= [E^1(b_1)E^1(Zf_1)][E^2(b_2)E^2(Zf_2)] \cdots [E^h(b_h)E^h(Zf_h)] \\ &= [C_1 E^1(Zf_1)][C_1^{-1} C_2 E^2(Zf_2)] \cdots [C_{h-1}^{-1} C_h E^h(Zf_h)] \\ &= \prod_{j=1}^{h} C_j E^j(Zf_j) C_j^{-1}. \end{aligned} \tag{2.3.8}$$

De la misma forma que en la pruebas de los corolarios 2.2.4 y 2.2.3, es posible escribir $C_j E^j(Zf_j) C_j^{-1}$ como producto de matrices de Cohn: para todo $j \in \{1, \ldots, h\}$, sea

$\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ la s_j-ésima columna de C_j. Entonces

$$C_j E_{s_j t_j}(Zf_j) C_j^{-1} = \prod_{1 \le \gamma < \delta \le n} [I + \mathbf{v} \cdot Zf_j \cdot a_{\gamma\delta}(v_\gamma \mathbf{e}_\delta - v_\delta \mathbf{e}_\gamma)] \tag{2.3.9}$$

para algunos $a_{\gamma\delta} \in R_{r_i}[X, Y]$. Además, podemos encontrar un número natural d_j tal que

$$v_\gamma = \frac{v'_\gamma}{r_i^{d_j}}, \quad a_{\gamma\delta} = \frac{a'_{\gamma\delta}}{r_i^{d_j}}, \quad f_j = \frac{f'_j}{r_i^{d_j}} \tag{2.3.10}$$

con $v'_\gamma, a'_{\gamma\delta} \in R[X, Y]$, $f'_j \in R[X, Y, Z]$. Si reemplazamos Z por $r_i^{4d_j} g$, todas las matrices de Cohn en la expresión anterior para $C_j E^j(Zf_j) C_j^{-1}$ tienen elementos sin denominadores. Luego

$$C_j E^j(r_i^{4d_j} g f_j) C_j^{-1} \in E_n(R[X, Y]). \tag{2.3.11}$$

Tomando el máximo de tales d_j, para un d suficientemente grande

$$D_i(X, Y, r_i^d g) = \prod_{j=1}^{h} C_j E^j(r_i^d g f_j) C_j^{-1} \in E_n(R[X, Y]). \tag{2.3.12}$$

Tenemos un número d para cada $i \in \{1, \ldots, l\}$. De nuevo consideramos el mayor, y si ponemos $Y = c$, obtenemos el aserto.

Veamos entonces cómo se 'pegan' los resultados locales. Para cada natural m se tiene $r_1^m R + \cdots + r_l^m R = R$. Tomemos m el número d obtenido anteriormente. Entonces podemos encontrar $g_1, \ldots, g_l \in R$ tales que $r_1^d g_1 + \cdots + r_l^d g_l = 1$. Expresemos $A(X) \in$

$SL_n(R[x])$ de la siguiente forma:

$$\begin{aligned} A(X) &= A(X - Xr_1^d g_1) \cdot [A^{-1}(X - Xr_1^d g_1)A(X)] \\ &= A(X - Xr_1^d g_1 - Xr_2^d g_2) \cdot [A^{-1}(X - Xr_1^d g_1 - Xr_2^d g_2)A(X - Xr_1^d g_1)] \\ &\quad \cdot [A^{-1}(X - Xr_1^d g_1)A(X)] \\ &= \cdots \\ &= A(X - \sum_{i=1}^{l} Xr_i^d g_i) \cdot [A^{-1}(X - \sum_{i=1}^{l} Xr_i^d g_i)A(X - \sum_{i=1}^{l-1} Xr_i^d g_i)] \cdots \\ &\quad \cdots [A^{-1}(X - Xr_1^d g_1)A(X)]. \end{aligned} \tag{2.3.13}$$

Notemos que la primera matriz $A(X - \sum_{i=1}^{l} Xr_i^d g_i) = A(0)$ en el lado derecho está en $SL_n(R) = E_n(R)$. Cada expresión entre corchetes es de la forma

$$A_i^{-1}(cX)A_i((c + r_i^d g)X). \tag{2.3.14}$$

y por el aserto cada una de ellas está en $E_n(R[x])$. Por tanto, A también.

Nota 2.3.1. Como consecuencia de este teorema, si $A \in SL_n(R[x])$, basta tener un algoritmo de realización para cada A_m en $R_m[x]$. La reducción de la siguiente sección nos indica que lo necesitaremos en $n = 3$.

2.4 Reducción a $SL_3(\mathbb{Z}[x])$

Sea $A \in SL_n(\mathbb{Z}[x])$ con $n \geq 3$, y $\mathbf{v}$ su última columna. Entonces $\mathbf{v}$ es unimodular, como se puede ver fácilmente al desarrollar el determinante por la última columna. Si pudiéramos reducir $\mathbf{v}$ a $\mathbf{e}_n = (0, 0, \ldots, 0, 1)^t$ mediante la aplicación de operaciones elementales, esto es, si encontramos $B \in E_n(\mathbb{Z}[x])$ tal que $B\mathbf{v} = \mathbf{e}_n$, entonces

$$BA = \begin{pmatrix} & & & 0 \\ & \tilde{A} & & \vdots \\ & & & 0 \\ p_1 & \cdots & p_{n-1} & 1 \end{pmatrix} \tag{2.4.1}$$

para alguna matriz $\tilde{A} \in SL_{n-1}(\mathbb{Z}[x])$ y $p_i \in \mathbb{Z}[x]$ con $i = 1, \ldots, n-1$. Pivotando sobre el 1 podemos hacer ceros en la última fila

$$BAE_{n1}(-p_1)\cdots E_{n(n-1)}(-p_{n-1}) = \begin{pmatrix} \tilde{A} & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.4.2}$$

El problema de expresar $A \in SL_n(\mathbb{Z}[x])$ como producto de matrices elementales se reduce al mismo problema para $\tilde{A} \in SL_{n-1}(\mathbb{Z}[x])$. Repitiendo este proceso, llegamos al problema de expresar $A = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(\mathbb{Z}[x])$ como producto de matrices elementales, que es el objeto de la siguiente sección.

En este apartado se desarrolla un algoritmo para encontrar operaciones elementales que reduzcan un vector unimodular dado $\mathbf{v} \in (\mathbb{Z}[x])^n$ a $\mathbf{e}_n$. También, como corolario a esta *Propiedad de Columna Elemental*, damos una prueba algorítmica de la *Propiedad de Columna Unimodular*, que establece que dado un vector columna unimodular $\mathbf{v} \in (\mathbb{Z}[x])^n$, existe una matriz $B \in SL_n(\mathbb{Z}[x])$ tal que $B\mathbf{v} = \mathbf{e}_n$. Esto proporciona una prueba algorítmica del *Teorema de Quillen-Suslin.*

Definición 2.4.1. Para un anillo R, $\mathrm{Um}_n(R) = \{$vectores columna unimodulares de dimensión n sobre $R\}$.

Nota 2.4.1. Los grupos $GL_n(\mathbb{Z}[x_1, \ldots, x_m])$ y $E_n(\mathbb{Z}[x_1, \ldots, x_m])$ actúan sobre el conjunto $\mathrm{Um}_n(\mathbb{Z}[x_1, \ldots, x_m])$ mediante la multiplicación de matrices.

Sea $R = \mathbb{Z}$. Identificamos $A \in SL_2(R[x])$ con $\begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix} \in SL_n(R[x])$, y consideramos $SL_2(R[x])$ como un subgrupo de $SL_n(R[x])$.

Lema 2.4.1. *Sean $f_1, f_2, b, d \in R[x]$ y r la resultante de f_1 y f_2. Entonces existe existe $B \in SL_2(R[x])$ tal que*

$$B \begin{pmatrix} f_1(b) \\ f_2(b) \end{pmatrix} = \begin{pmatrix} f_1(b+rd) \\ f_2(b+rd) \end{pmatrix}. \tag{2.4.3}$$

Demostración. Es el lema 7.3.3 de [Man97]. Por la propiedad de la resultante de dos polinomios, podemos construir $g_1, g_2 \in R[x]$ tales que $f_1 g_1 + f_2 g_2 = r$ ([CLO92]). Sean $s_1, s_2, t_1, t_2 \in R[X, Y, Z]$ los polinomios definidos por

$$\begin{aligned} f_1(X + YZ) &= f_1(X) + Y s_1(X, Y, Z) \\ f_2(X + YZ) &= f_2(X) + Y s_2(X, Y, Z) \\ g_1(X + YZ) &= g_1(X) + Y t_1(X, Y, Z) \\ g_2(X + YZ) &= g_2(X) + Y t_2(X, Y, Z). \end{aligned} \tag{2.4.4}$$

Definamos entonces

$$\begin{aligned} B_{11} &= 1 + s_1(b, r, d) \cdot g_1(b) + t_2(b, r, d) \cdot f_2(b) \\ B_{12} &= s_1(b, r, d) \cdot g_2(b) - t_2(b, r, d) \cdot f_1(b) \\ B_{21} &= s_2(b, r, d) \cdot g_1(b) - t_1(b, r, d) \cdot f_2(b) \\ B_{22} &= 1 + s_2(b, r, d) \cdot g_2(b) + t_1(b, r, d) \cdot f_1(b). \end{aligned} \tag{2.4.5}$$

Se verifica, mediante un simple cálculo, que $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$ verifica la propiedad del enunciado y $B \in SL_2(R[x])$.

Teorema 2.4.2. *Sea* $\mathbf{v}(X) = \begin{pmatrix} v_1(X) \\ \vdots \\ v_n(X) \end{pmatrix} \in \mathrm{Um}_n(R[x])$, *y* $v_1(X)$ *tal que el máximo común divisor de sus coeficientes es* 1. *Entonces existen* $B_1 \in SL_2(R[x])$ *y* $B_2 \in E_n(R[x])$ *tales que* $B_1 B_2 \cdot \mathbf{v}(X) = \mathbf{v}(0)$.

Demostración. Sea p_1 un primo de $\mathbb{Z}$, y llamamos $\mathfrak{m}_1$ al ideal de $\mathbb{Z}$ generado por p_1. Sea $k_1 = R/\mathfrak{m}_1$ el cuerpo residual. Como $\mathbf{v} \in (R[x])^n$ es un vector columna unimodular, su imagen $\bar{\mathbf{v}}$ en $(k_1[x])^n = ((R/\mathfrak{m}_1)[x])^n$ es también unimodular. Como $k_1[x]$ es un dominio de ideales principales, la base de Gröbner minimal del ideal $\langle \bar{v}_2, \ldots, \bar{v}_n \rangle$ tiene un único

elemento, que llamamos G_1. Entonces $\bar{v}_1$ y G_1 generan el ideal unidad en $k_1[x]$, porque $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n$ generan el ideal unidad. Mediante la división euclídea en $k_1[x]$, podemos encontrar $E_1 \in E_{n-1}(k_1[x])$ tal que

$$E_1 \begin{pmatrix} \bar{v}_2 \\ \vdots \\ \bar{v}_n \end{pmatrix} = \begin{pmatrix} G_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{2.4.6}$$

Consideramos un levantamiento de los elementos de k_1 a R, y entonces podemos ver E_1 como un elemento de $E_n(R[x])$ y G_1 como un elemento de $R[x]$. Entonces

$$\begin{pmatrix} 1 & 0 \\ 0 & E_1 \end{pmatrix} \mathbf{v} = \begin{pmatrix} v_1 \\ G_1 + q_{12} \\ q_{13} \\ \vdots \\ q_{1n} \end{pmatrix} \tag{2.4.7}$$

para algunos $q_{12}, \ldots, q_{1n} \in M_1[x]$. Definimos $r_1 \in R$ como

$$\begin{aligned} r_1 &= \text{Res}(v_1, G_1 + q_{12}) \\ &= \text{la resultante de } v_1 \text{ y } G_1 + q_{12} \end{aligned} \tag{2.4.8}$$

y hallamos $f_1, h_1 \in R[x]$ tales que

$$f_1 \cdot v_1 + h_1 \cdot (G_1 + q_{12}) = r_1. \tag{2.4.9}$$

Como el máximo común divisor de los coeficientes de v_1 es 1, no se anula en $k_1[x]$, y dado que $\bar{v}_1$ y $G_1 \in k_1[x]$ generan el ideal unidad, se tiene que

$$\begin{aligned} \bar{r}_1 &= \text{Res}(v_1, G_1 + q_{12}) \\ &= \text{Res}(\bar{v}_1, G_1) \\ &\neq 0. \end{aligned} \tag{2.4.10}$$

Si $\bar{r}_1 = 0$, entonces $\bar{v}_1$ y G_1 tendrían un factor común en $k_1[x]$, y no generarían el ideal unidad. Por tanto, $r_1 \notin \mathfrak{m}_1$. Si $r_1 = 1$, saltamos a la definición de ciertos b_i. Si no, sea p_2 un divisor de r_1, y $\mathfrak{m}_2$ el ideal generado por p_2. Construímos r_2, que por lo anterior no está en M_2. Si $\langle r_1, r_2 \rangle = \mathbb{Z}$, saltamos a la definición de los b_i. En otro caso, sea d_2 el máximo común divisor de r_1 y r_2, y tomamos p_3 un divisor de d_2. De forma inductiva construímos $r_1, \ldots, r_{j-1} \in \mathfrak{m}_j$, $r_j \notin \mathfrak{m}_j$, y tenemos también las matrices $E_j \in E_{n-1}(k_j[x])$, y los polinomios $G_j \in k_j[x]$ y $f_j, h_j \in R[x]$. y $q_{j2}, \ldots, q_{jn} \in \mathfrak{m}_j[x]$ de forma análoga. Como R es noetheriano, tras un número finito de pasos encontramos un l tal que $r_1R + \cdots + r_lR = R$, y podemos hallar elementos $g_i \in R$ tales que $r_1g_1 + \cdots + r_lg_l = 1$. Definimos $b_0, b_1, \ldots, b_l \in R[x]$ de la siguiente forma:

$$\begin{aligned} b_0 &= 0 \\ b_1 &= r_1g_1x \\ b_2 &= r_1g_1x + r_2g_2x \\ &\vdots \\ b_l &= r_1g_1x + r_2g_2x + \cdots + r_lg_lx = x. \end{aligned} \tag{2.4.11}$$

Estos polinomios b_i satisfacen las relaciones recursivas:

$$\begin{aligned} b_0 &= 0 \\ b_i &= b_{i-1} + r_ig_iX \quad \text{para } i = 1, \ldots, l. \end{aligned} \tag{2.4.12}$$

Aserto: Para cada $i \in \{1, \ldots, l\}$, existe $B_i \in SL_2(R[x])$ y $B_i' \in E_n(R[x])$ tales que $\mathbf{v}(b_i) = B_iB_i'\mathbf{v}(b_{i-1})$.

Supuesto probado el aserto, usamos que $E_n(R[x]) \cdot SL_2(R[x]) \subseteq SL_2(R[x]) \cdot E_n(R[x])$ (Normalidad de $E_n(R[x])$). Recordemos que es posible construir las matrices de este

enunciado. Por inducción nos queda

$$\begin{aligned} \mathbf{v}(x) &= \mathbf{v}(b_l) \\ &= B_l B_l' \mathbf{v}(b_{l-1}) \\ &= B_l B_l' B_{l-1} B_{l-1}' \mathbf{v}(b_{l-2}) \end{aligned} \tag{2.4.13}$$

Como $B_l' \in E_n(R[x])$ y $B_{l-1} \in SL_2(R[x])$, podemos hallar $C_{l-1} \in SL_2(R[x])$ y $D_l' \in E_n(R[x])$ que verifican $B_l' B_{l-1} = C_{l-1} D_l'$. Entonces

$$\begin{aligned} \mathbf{v}(x) &= B_l C_{l-1} D_l' B_{l-1}' \mathbf{v}(b_{l-2}) \\ &= H_l J_{l-1} \mathbf{v}(b_{l-2}) \end{aligned} \tag{2.4.14}$$

con $H_l = B_l C_{l-1} \in SL_2(R[x])$ y $J_{l-1} = D_l' B' l - 1 \in E_n(R[x])$. Entonces

$$\begin{aligned} \mathbf{v}(x) &= BB' \mathbf{v}(b_0) \\ &= BB' \mathbf{v}(0) \end{aligned} \tag{2.4.15}$$

con $B \in SL_2(R[x])$ y $B' \in E_n(R[x])$. Por tanto, resta probar el aserto anterior.

Para ello, sea $\tilde{G}_i = G_i + q_{i2}$. Entonces

$$\begin{pmatrix} 1 & 0 \\ 0 & E_i(x) \end{pmatrix} \mathbf{v}(x) = \begin{pmatrix} v_1(x) \\ \tilde{G}_i(x) \\ q_{i3}(x) \\ \vdots \\ q_{in}(x) \end{pmatrix}. \tag{2.4.16}$$

Para $3 \leq j \leq n$, tenemos

$$\begin{aligned} q_{ij}(b_i) - q_{ij}(b_{i-1}) &\in (b_i - b_{i-1}) \cdot R[x] \\ &= r_i g_i x \cdot R[x]. \end{aligned} \tag{2.4.17}$$

$q_{ij}(b_i) - q_{ij}(b_{i-1})$ tiene en cada sumando una expresión de la forma $b_i^s - b_{i-1}^s$, con s un número natural. Estas expresiones están en el ideal generado por $b_1 - b_{i-1}$. Como $r_i \in R$ no depende de x, tenemos que

$$\begin{aligned} r_i &= f_i(x)v_1(x) + h_i(x)\tilde{G}_i(x) \\ &= f_i(b_{i-1})v_1(b_{i-1}) + h_i(b_{i-1})\tilde{G}_i(b_{i-1}) \\ &= \text{una combinación lineal } de\ v_1(b_{i-1}) \text{ y } \tilde{G}_i(b_{i-1}) \text{ en } R[x]. \end{aligned} \tag{2.4.18}$$

Enotnces vemos que para $3 \leq j \leq n$,

$$q_{ij}(b_i) = q_{ij}(b_{i-1}) + \text{una combinación lineal de } v_1(b_{i-1}) \text{ y } \tilde{G}_i(b_{i-1}) \text{ en} R[x].$$

Entonces podemos construir $C \in E_n(R[x])$ con

$$C \begin{pmatrix} 1 & 0 \\ 0 & E_i(b_{i-1}) \end{pmatrix} \mathbf{v}(b_{i-1}) = C \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \\ q_{i3}(b_{i-1}) \\ \vdots \\ q_{in}(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \\ q_{i3}(b_i) \\ \vdots \\ q_{in}(b_i) \end{pmatrix}.$$

Por el lema 2.4.1, tomando $b = b_{i-1}$, $r = Res(v_1, \tilde{G}_i) = r_i$, $d = g_i x$, encontramos $\tilde{B} \in SL_2(R[x])$ tal que

$$\tilde{B} \begin{pmatrix} v_1(b_{i-1}) \\ \tilde{G}_i(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_i) \\ \tilde{G}_i(b_i) \end{pmatrix}. \tag{2.4.19}$$

Finalmente, definimos $B \in SL_n(R[x])$ como

$$B = \begin{pmatrix} 1 & 0 \\ 0 & E_i(b_i)^{-1} \end{pmatrix} \begin{pmatrix} \tilde{B} & 0 \\ 0 & I_{n-2} \end{pmatrix} \cdot C \cdot \begin{pmatrix} 1 & 0 \\ 0 & E_i(b_{i-1}) \end{pmatrix}. \tag{2.4.20}$$

Esta matriz B verifica

$$B\mathbf{v}(b_{i-1}) = \mathbf{v}(b_i), \tag{2.4.21}$$

De nuevo usamos que $E_n(R[x]) \cdot SL_2(R[x]) \subseteq SL_2(R[x]) \cdot E_n(R[x])$. Como $B = F_1 \cdot \tilde{B} \cdot F_2 \cdot F_3$, con $F_1, F_2, F_3 \in E_n(R[x])$ y $\tilde{B} \in SL_2(R[x])$, podemos encontrar $F_0 \in E_n(R[x])$ y $B_0 \in SL_2(R[x])$ tales que $F_1 \cdot \tilde{B} = B_0 \cdot F_0$. Por tanto

$$B \in SL_2(R[x])E_n(R[x]) \tag{2.4.22}$$

y hemos probado el aserto.

Teorema 2.4.3. *(Propiedad de Columna Elemental) Si $n \geq 3$, el grupo $E_n(\mathbb{Z}[x])$ actúa transitivamente sobre el conjunto* $\mathrm{Um}_n(\mathbb{Z}[x])$.

Demostración. El algoritmo de división euclídea resuelve el problema sobre $\mathbb{Z}$. Sea $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathrm{Um}_n(R[x])$. Como el vector es unimodular, el vector de los términos constantes de cada v_i es también unimodular. Como son elementos de $\mathbb{Z}$, esto significa que el máximo común divisor de esos coeficientes es 1. Mediante la división euclídea en $\mathbb{Z}$ y transformaciones elementales, podemos conseguir que el término contante de v_1 sea igual a 1. Por el teorema 2.4.2, podemos encontrar $B_1 \in SL_2(R[x])$ y $B_2 \in E_n(R[x])$ tales que

$$B_1 B_2 \cdot \mathbf{v}(x) = \mathbf{v}(0) \in R. \tag{2.4.23}$$

Como en R está resuelto el problema, podemos hallar $B' \in E_n(R)$ tal que

$$B' \cdot \mathbf{v}(0) = \mathbf{e}_n. \tag{2.4.24}$$

Entonces tenemos

$$\mathbf{v} = B_2^{-1} B_1^{-1} B'^{-1} \mathbf{e}_n. \tag{2.4.25}$$

Por la normalidad de $E_n(R[x])$ in $SL_n(R[x])$ (corolario 2.2.4), podemos escribir $B_1^{-1} B'^{-1} =$

$B''B_1^{-1}$ para alguna $B'' \in E_n(R[x])$. Como

$$B_1^{-1} = \begin{pmatrix} p & q & 0 & \dots & 0 \\ r & s & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & I_{n-2} & \\ 0 & 0 & & & \end{pmatrix} \tag{2.4.26}$$

para ciertos $p, q, r, s \in R[x]$, se tiene que

$$\begin{aligned} \mathbf{v} &= B_2^{-1}B_1^{-1}B'^{-1}\mathbf{e}_n \\ &= (B_2^{-1}B'')B_1^{-1}\mathbf{e}_n \\ &= (B_2^{-1}B'') \begin{pmatrix} p & q & 0 & \dots & 0 \\ r & s & 0 & \dots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & I_{n-2} & \\ 0 & 0 & & & \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \\ &= (B_2^{-1}B'')\mathbf{e}_n \end{aligned} \tag{2.4.27}$$

donde $B_2^{-1}B'' \in E_n(R[x])$. Ya que esta relación es para cualquier $\mathbf{v} \in \mathrm{Um}_n(R[x])$, obtenemos la transitividad buscada.

Nota 2.4.2. Según el teorema 2.4.3, si $\mathbf{v}, \mathbf{v}'$ son vectores columna de dimensión n y unimodulares en $\mathbb{Z}[x]$, entonces podemos encontrar $B \in E_n(\mathbb{Z}[x])$ tal que $B\mathbf{v} = \mathbf{v}'$. Tomando $\mathbf{v}' = \mathbf{e}_n$ tenemos el algoritmo buscado.

Corolario 2.4.4. *(Propiedad de Columna Unimodular) Si $n \geq 2$, el grupo $GL_n(\mathbb{Z}[x])$ actúa transitivamente sobre el conjunto* $\mathrm{Um}_n(\mathbb{Z}[x])$.

Demostración. Para $n \geq 3$, la *Propiedad de Columna Elemental* implica la *Propiedad de Columna Unimodular* ya que un producto de matrices elementales es unimodular. Si $n =$

2, sean $\mathbf{v} = (v_1, v_2)^t \in \mathrm{Um}_2(\mathbb{Z}[x])$, y calculemos mediante las bases de Gröbner $g_1, g_2 \in \mathbb{Z}[x]$ tales que $v_1 g_1 + v_2 g_2 = 1$. Entonces la matriz unimodular $U_{\mathbf{v}} = \begin{pmatrix} v_2 & -v_1 \\ g_1 & g_2 \end{pmatrix}$ satisface $U_{\mathbf{v}} \cdot \mathbf{v} = \mathbf{e}_2$. Entonces vemos que para cualesquiera $\mathbf{v}, \mathbf{w} \in \mathrm{Um}_2(\mathbb{Z}[x])$, $U_{\mathbf{w}}^{-1} U_{\mathbf{v}} \cdot \mathbf{v} = \mathbf{w}$ donde $U_{\mathbf{w}}^{-1} U_{\mathbf{v}} \in GL_2(\mathbb{Z}[x])$.

2.5 Algoritmo de descomposición en $SL_3(R[x])$

Queremos desarrollar un algoritmo de descomposición en producto de matrices elementales para las matrices de la forma

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(\mathbb{Z}[x]).$$

Existe un argumento en [VS76] que mediante un cambio de variables nos permite reducir este problema a un $p \in \mathbb{Z}[x]$ mónico, que veremos en la sección siguiente. Para el caso de una variable, exponemos un proceso más sencillo. Por la reducción desarrollada en la sección anterior, basta dar un algoritmo para las matrices de la forma $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(R[x])$, donde R es ahora un anillo conmutativo local y principal. No imponemos condiciones sobre p. Daremos en primer lugar el método cuando el coeficiente líder de p es unidad de R, que se reduce al caso mónico, y se resuelve como en [PW95], y a continuación desarrollamos el caso general. El siguiente lema es básico.

Lema 2.5.1. *Sea L un anillo conmutativo y $a, a', b \in L$. Entonces se verifica que:*

1. *(a, b) y (a', b) son unimodulares en L si y solamente si (aa', b) es unimodular en L.*

2. *Dados $c, d \in L$ tales que $aa'd - bc = 1$, existen $c_1, c_2, d_1, d_2 \in L$ que verifican*

$ad_1 - bc_1 = 1$, $a'd_2 - bc_2 = 1$, *y*

$$\begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(L)}.$$

Demostración. (1) Si (aa', b) es unimodular en L, existen $h_1, h_2 \in L$ tales que $h_1 \cdot (aa') + h_2 \cdot b = 1$. Entonces $(h_1 a') \cdot a + h_2 \cdot b = 1$ implica que (a, b) es unimodular, y $(h_1 a) \cdot a' + h_2 \cdot b = 1$ implica que (a', b) es unimodular.

Supongamos ahora que (a, b) y (a', b) son unimodulares en L. Podemos encontrar $h_1, h_2, h_1', h_2' \in L$ tales que $h_1 a + h_2 b = 1$, $h_1' a' + h_2' b = 1$. Sean $g_1 = h_1 h_1'$, $g_2 = h_2' + a' h_2 h_1'$, y consideremos

$$\begin{aligned} g_1 aa' + g_2 b &= h_1 h_1' aa' + (h_2' + a' h_2 h_1') b \\ &= h_1' a' (h_1 a + h_2 b) + h_2' b \\ &= h_1' a' + h_2' b \\ &= 1. \end{aligned} \tag{2.5.1}$$

y tenemos la relación buscada.

(2) Si $c, d \in L$ verifican $aa'd - bc = 1$, entonces (aa', b) es unimodular, que implica que (a, b) y (a', b) son unimodulares. Podemos entonces encontrar $c_1, d_1, d_1, d_2 \in L$ con $ad_1 - bc_1 = 1$ y $a'd_2 - bc_2 = 1$. Por ejemplo, tomemos

$$c_1 = c_2 = c, \quad d_1 = a'd, \quad d_2 = ad. \tag{2.5.2}$$

Consideremos las siguientes transformaciones

$$\begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_{21}(cd_1d_2 - d(c_2 + a'c_1d_2)) \begin{pmatrix} aa' & b & 0 \\ c_2 + a'c_1d_2 & d_1d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= E_{21}(cd_1d_2 - d(c_2 + a'c_1d_2))E_{23}(d_2 - 1)E_{32}(1)E_{23}(-1)$$

$$\begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} E_{23}(1)E_{32}(-1)E_{23}(1) \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$E_{23}(-1)E_{32}(1)E_{23}(a - 1)E_{31}(-a'c_1)E_{32}(-d_1). \qquad (2.5.3)$$

Esta expresión demuestra que

$$\begin{pmatrix} aa' & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} a & b & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a' & b & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(L)}. \qquad (2.5.4)$$

Lema 2.5.2. *Sea L un anillo conmutativo, $A = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$ una matriz de orden 3 con elementos en L, y u una unidad en L. Entonces existe $E \in E_3(L)$ tal que*

$$A = E \cdot \begin{pmatrix} u^{-1}p & uq & 0 \\ u^{-1}r & us & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Demostración. Se tiene que

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad E_{12}(u^{-1}-1)E_{21}(1)E_{12}(u-1)E_{21}(-u^{-1})$$

$$= \begin{pmatrix} u^{-1}p & uq & 0 \\ u^{-1}r & us & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Lema 2.5.3. *Sean $p(x), q(x) \in \mathbb{Z}[x]$, con $p(x)$ mónico, grado$(p(x)) = d > 0$, grado$(q(x)) = l$ y el ideal generado por $p(x)$ y $q(x)$ es igual a $\mathbb{Z}[x]$. Entonces podemos calcular $p'(x), q'(x) \in \mathbb{Z}[x]$ con grado$(p'(x)) < l$, grado$(q'(x)) < d$ y $pp' - qq' = 1$.*

Demostración. Como $1 \in \langle p(x), q(x) \rangle$, entonces podemos hallar $a, b \in \mathbb{Z}[x]$ con $ap+bq = 1$. Si grado$(b(x)) < d$, entonces grado$(b(x)q(x)) < d+l$, y en tal caso grado$(a(x)p(x)) < d+l$ y grado$(a(x)) < l$. Tomamos entonces $p' = a$ y $q' = -b$. Si grado$(b(x)) \geq d$, dividimos por p, dado que es mónico. Entonces existen $q_1(x), r_1(x) \in R[x]$ con $b = pq_1 + r_1$, y grado$(r_1(x)) < d$. Entonces $1 = ap+bq = ap+(pq_1+r_1)q = (a+q_1q)p+qr_1$, y estamos en la situación anterior.

Teorema 2.5.4. *Sea $(R, \mathfrak{m})$ un anillo conmutativo local, $\mathfrak{m}$ su ideal maximal y $A = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(R[x])$ con p mónico. Entonces A es realizable en $R[x]$.*

Demostración. Por inducción sobre el grado(p). Si grado(p)=0, entonces $p = 1$ y A es claramente realizable. Supongamos que grado$(p) = d > 0$ y grado$(q) = l$. Como $p \in R[x]$ es mónico, podemos encontrar $f, g \in R[x]$ tales que

$$q = fp + g, \quad \text{grado(g)} < d. \tag{2.5.5}$$

Entonces

$$AE_{12}(-f) = \begin{pmatrix} p & q-fp & 0 \\ r & s-fr & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} p & g & 0 \\ r & s-fr & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{2.5.6}$$

Podemos suponer que $\deg(q) < d$. Observemos que $p(0)$ o $q(0)$ es una unidad en R. En otro caso, tendríamos que $p(0)s(0) - q(0)r(0) \in \mathfrak{m}$ que contradice $ps - qr = p(0)s(0) - q(0)r(0) = 1$. Consideremos dos casos distintos.

Caso 1: $q(0)$ es una unidad.

Por el carácter invertible de $q(0)$, tenemos que

$$AE_{21}(-q(0)^{-1}p(0)) = \begin{pmatrix} p - q(0)^{-1}p(0)q & q & 0 \\ r - q(0)^{-1}p(0)s & s & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{2.5.7}$$

Entonces podemos suponer que $p(0) = 0$. Escribamos $p = xp'$. Por el lema 2.5.1, podemos encontrar $c_1, d_1, c_2, d_2 \in R[x]$ tales que $xd_1 - qc_1 = 1$, $p'd_2 - qc_2 = 1$ y

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} x & q & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} p' & q & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(R[x])} \tag{2.5.8}$$

Como grado$(p') < d$, la segunda matriz de la parte derecha es realizable por la hipótesis de inducción. Para la primera, podemos suponer que q es unidad en R, pues es posible efectuar reducciones mediante el monomio x. Si q es invertible es fácil encontrar una factorización explícita de $\begin{pmatrix} x & q & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ en matrices elementales. Otra forma de verlo es aplicar el lema 2.5.2 para obtener un 1 en la posición $(1,2)$ y conseguir la descomposición.

Caso 2: $q(0)$ no es unidad.

Por el lema anterior, existen $p', q' \in R[x]$ con $\deg(p') < l, \deg(q') < d$ y $p'p - q'q = 1$. Observemos que las dos relaciones $p'(0)p(0) - q'(0)q(0) = 1$ y $q(0) \in \mathfrak{m}$, implican que $p'(0) \notin \mathfrak{m}$. Esto significa que $q(0) + p'(0)$ es una unidad. Consideremos las siguientes transformaciones

$$\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_{21}(rp' - sq') \begin{pmatrix} p & q & 0 \\ q' & p' & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= E_{21}(rp' - sq')E_{12}(-1) \begin{pmatrix} p+q' & q+p' & 0 \\ q' & p' & 0 \\ 0 & 0 & 1 \end{pmatrix}. \qquad (2.5.9)$$

La última matriz del lado derecho es realizable por el Caso 1, ya que $q(0)+p'(0)$ es una unidad y $\text{grado}(p+q') = d$. Por tanto, $\begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$ es también realizable.

Lema 2.5.5. *Sea* $A = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(R[x])$, *con* $p(0) = 1$, *grado*$(p) = n$, *grado*$(q) = l$. *Entonces* A *es congruente módulo* $E_3(R[x])$ *a una matriz* $A' = \begin{pmatrix} p & q' & 0 \\ r' & s' & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(R[x])$ *con grado*$(q') \leq$ *grado*(p) *y* $q'(0) = 0$.

Demostración. Escribamos $p(x) = 1 + a_1x + \ldots + a_nx^n$, $q(x) = b_0 + b_1x + \ldots + b_lx^l$. Si $b_0 \neq 0$, consideremos $AE_{12}(-b_0)$, y el término constante de q es eliminado. Entonces podemos tomar $q = xq'$, y $\text{grado}(q) \leq \text{máx}\{n, l\}$. Si $l \leq n$, tenemos el resultado. En

otro caso, aplicamos el lema 2.5.1, y

$$A \equiv \begin{pmatrix} p & x & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} p & q' & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(R[x])}.$$

La primera matriz puede ser factorizada como producto de matrices elementales, eliminando los términos de p con grado mayor o igual que 1 mediante el monomio x de la segunda columna. Obtenemos el valor 1 en la posición $(1,1)$, y la matriz es claramente realizable.

Tenemos grado(q') < grado(q), y repitiendo el proceso tenemos el lema.

Teorema 2.5.6. *Sea R un anillo conmutativo local y principal, $\mathfrak{m} = \langle \pi \rangle$ su ideal maximal y* $A = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(R[x])$. *Entonces A es realizable en $R[x]$.*

Demostración. Si $p(0)$ no es una unidad, entonces $q(0)$ tiene que serlo, y también $p(0)+q(0)$. Entonces mediante $AE_{21}(1)$ podemos suponer que $p(0)$ es una unidad, y usando el lema 2.5.2, obtenemos $p(0) = 1$. Por el lema 2.5.5, podemos suponer que

$$A = \begin{pmatrix} p & q & 0 \\ r & s & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

con $p(0) = 1$, $q(0) = 0$ y grado$(q) \leq$ grado(p).

Procedemos por inducción sobre grado(p). Si grado$(p) = 0$, entonces $p = 1$, y tenemos el resultado. Supongamos entonces que grado$(p) = n > 0$, grado$(q) = l \leq n$, y $p(x) = 1 + a_1x + \ldots + a_nx^n, q(x) = b_1x + \ldots + b_lx^l, a_n, b_l \neq 0$. Si $a_n \notin \mathfrak{m}$, entonces por el lema 2.5.2 podemos conseguir p mónico, y entonces aplicar el teorema 2.5.4. Supongamos que $a_n \in \mathfrak{m}$. Si todo $b_i \in \mathfrak{m}$, entonces existe un entero $k > 0$ con $q = \pi^k q'$,

y al menos uno de los coeficientes de q' no está en $\mathfrak{m}$. Por el lema 2.5.1,

$$A \equiv \begin{pmatrix} p & \pi^k & 0 \\ c_1 & d_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} p & q' & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{E_3(R[x])}.$$

Aplicamos k veces el lema 2.5.1 a la primera matriz, y la reducimos a

$$A_1 = \begin{pmatrix} p & \pi & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Recordemos que $a_n = \pi^e a'_n$, con $e > 0$ y $a'_n \notin \mathfrak{m}$, por lo que podemos eliminar el término líder de p.

$$A_1 \cdot E_{21}(-\pi^{e-1} a'_n x^n) = \begin{pmatrix} p' & \pi & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

y $p'(0) = 1$, grado(p') < grado(p). Por la hipótesis de inducción, esta matriz es realizable. Sea

$$A_2 = \begin{pmatrix} p & q' & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

con $q'(x) = b'_1 x + \ldots + b'_l x^l$, y sea j el menor número tal que $b'_j \notin \mathfrak{m}$. Consideremos dos casos:

Caso 1: $b'_1 \notin \mathfrak{m}$. Entonces b'_1 es una unidad, y la matriz es equivalente mediante transformaciones elementales a

$$\begin{pmatrix} -{b'_1}^{-1} q' & b'_1 p & 0 \\ -{b'_1}^{-1} d_2 & b'_1 c_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(se intercambian primera y segunda columna y se aplica el lema 2.5.2). Tenemos $-{b'_1}^{-1}q' = xg_2$, y grado(g_2) < grado$(q') \leq n$. Por el lema 2.5.1, es congruente módulo $E_3(R[x])$ a

$$\begin{pmatrix} g_2 & b'_1 p & 0 \\ s_1 & t_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x & b'_1 p & 0 \\ s_2 & t_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

La segunda matriz es realizable. Para la primera, observemos que $g_2(0) = 1$, grado$(g_2) < l \leq n$. Aplicamos el lema 2.5.5, y esta matriz es equivalente a

$$\begin{pmatrix} g_2 & p' & 0 \\ s_3 & t_3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

con $g_2(0) = 1$, grado$(p') \leq$ grado$(g_2) < n$, y por la hipótesis de inducción, la matriz es realizable.

Caso 2: $b'_1 \in \mathfrak{m}$. Apliquemos las siguientes transformaciones:

$$\begin{pmatrix} p & q' & 0 \\ c_2 & d_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot E_{12}(-b'_1 x) = \begin{pmatrix} p & q' - b'_1 xp & 0 \\ c_2 & d_2 - b'_1 xc_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} q' - b'_1 xp = & \\ & x((b_2 - b'_1 a_1)x + \ldots + (b'_l - b'_1 a_l)x^{l-1} + \\ & +(-b'_1 a_{l+1})x^l + \ldots + (-b'_1 a_n)x^n) \\ = xq'' & \end{aligned}$$

Por el lema 2.5.1, es congruente módulo $E_3(R[x])$ a

$$\begin{pmatrix} p & x & 0 \\ s_1 & t_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} p & q'' & 0 \\ s_2 & t_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

La primera matriz en el producto es realizable, y en la segunda tenemos que grado$(q'') \leq n$, con el coeficiente del término de grado $j-1$ igual a $b'_j - b_1 a_{j-1} \notin \mathfrak{m}$. Repitiendo este proceso podemos conseguir como coeficiente del término de grado 1 un elemento que no está en $\mathfrak{m}$. Aplicamos el Caso 1, y la prueba está completa.

2.6 Normalización de vectores unimodulares

Uno de los problemas a salvar para extender el resultado de [PW95] al anillo $\mathbb{Z}[x_1, \ldots, x_m]$ es el uso que se hace del teorema de Normalización de Noether para, mediante un cambio de variables, conseguir un polinomio mónico en x_m. En esta sección damos una versión constructiva de un teorema de normalización para vectores unimodulares sobre el anillo $\mathbb{Z}[x_1, \ldots, x_m]$.

Definición 2.6.1. Una sucesión finita de elementos $a_1, \ldots, a_r$ de un anillo R se dice regular si la imagen del elemento a_i en $R/\langle a_1, \ldots, a_{i-1}\rangle$ no es un divisor de cero, para $i = 1, \ldots, r-1$. Para $i = 1$, esto significa que a_1 no es divisor de cero en R. Establecemos que 0 no es divisor de cero en un anillo R' si y solamente si $R' = 0$.

Definición 2.6.2. Sea R un anillo. La altura de un ideal primo $\mathfrak{p}$ de R, que notaremos por $ht_R(\mathfrak{p})$, es el supremo de las longitudes $n-1$ de cadenas estrictamente crecientes

$$\mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$

de ideales primos de R. La altura de un ideal I arbitrario, $ht_R(I)$, es el ínfimo de las alturas de los ideales primos que contienen a I.

Lema 2.6.1. *Sea $a_1, \ldots, a_r$ una sucesión regular en un anillo noetheriano R. Entonces $ht_R(Ra_1 + \ldots + Ra_r) \geq r$.*

Demostración. [VS76] p.961

Proposición 2.6.2. *Sea I un ideal en $R = \mathbb{Z}[x_1, \ldots, x_m]$, $R' = R/I$, y $f_1, f_2 \in R$ tales que $\langle f_1 + I, f_2 + I\rangle = R'$. Entonces existe $h \in R$ tal que $(f_1 + hf_2) + I$ no es divisor de cero en R'.*

Demostración. Calculemos una descomposición primaria de I en R ([GTZ88]), y de los primos asociados tomamos los maximales por la relación de inclusión en $Ass(I)$. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ tales ideales, y construyamos $h_{ij} \in \mathfrak{p}_i - \mathfrak{p}_j$ para $i \neq j$, $i, j \in \{1, \ldots, s\}$. Podemos suponer el conjunto ordenado de forma que $f_1 \in \mathfrak{p}_1, \ldots, \mathfrak{p}_t$, $t \leq s$. Sea $\tilde{\mathfrak{p}}_i$ la imagen de $\mathfrak{p}_i$ en R'. Observemos que el conjunto de divisores de cero de R' es $\cup_{i=1}^{s} \tilde{\mathfrak{p}}_i$. Si $t = 0$, entonces $f_1 + I$ no es divisor de cero, y tomamos $h = 0$. Si $t \neq 0$, sea $h = \sum_{j=1}^{t} \prod_{i \neq j}^{s} h_{ij}$. Un producto vacío se toma igual a 1. Tal es el caso si $s = t = 1$. Notemos que $h \in \mathfrak{p}_k$ para $t + 1 \leq k \leq s$. Entonces $(f_1 + I) + (h + I)(f_2 + I)$ no está contenido en ningún $\tilde{\mathfrak{p}}_i$, para $1 \leq i \leq s$. Si $(f_1 + hf_2) + I \in \tilde{\mathfrak{p}}_i$, para $1 \leq i \leq t$, entonces $hf_2 \in \mathfrak{p}_i$. Como las clases de f_1 y f_2 generan el anillo R', no puede ocurrir que f_2 pertenezca a $\mathfrak{p}_i$. Entonces $h \in \mathfrak{p}_i$. Todos los sumandos de h, menos uno están en $\mathfrak{p}_i$, y ese sumando es producto de elementos que no pertenecen a $\mathfrak{p}_i$. Para los restantes i entre $t + 1$ y s recordemos que f_1 no pertenece a $\mathfrak{p}_i$, y tenemos el resultado.

Corolario 2.6.3. *Sea $R = \mathbb{Z}[x_1, \ldots, x_m]$, r un número natural y $\mathbf{b} = (b_1, \ldots, b_r)^t \in \mathrm{Um}_r(R)$. Entonces existe una matriz $B \in E_r(R)$ triangular superior con valores 1 en la diagonal principal tal que $B \cdot \mathbf{b} = (d_1, \ldots, d_r)^t$, con $\{d_1, \ldots, d_r\}$ una sucesión regular.*

Demostración. Por inducción sobre r. El caso $r = 2$ es trivial, pues es la proposición anterior con $I = 0$. Entonces, si $b_1 = 0$, $b_2 = 1$ tomamos $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Si $b_1 \neq 0$, consideramos B igual a la identidad. Sea $R_0 = R$. Como el vector $\mathbf{b}$ es unimodular, existen $a_1, \ldots, a_r \in A_0$ con $a_1 b_1 + \ldots + a_r b_r = 1$. Sea $b_0 = a_2 b_2 + \ldots + a_r b_r$. Entonces existe $z \in R_0$ tal que $d_1 = b_1 + z b_0$ no es divisor de cero. Sea $I_1 = d_1 R_0$. Sea ahora $R_1 = R_0/I_1$, y notemos $b_i^{(1)}$ las imágenes de b_i en R_1, para $i = 2, \ldots, r$. Se tiene que el

vector $(b_2^{(1)}, \ldots, b_r^{(1)})^t$ es unimodular en R_1.

$$d_1 = b_1 + za_2b_2 + \ldots za_rb_r, 1 = a_1b_1 + a_2b_2 + \ldots a_rb_r$$

$$a_1d_1 = a_1b_1 + za_1a_2b_2 + \ldots za_1a_rb_r$$

Restando queda $1 - a_1d_1 = (a_2 - za_1a_2)b_2 + \ldots + (a_r - za_1a_r)b_r$ y tomando imágenes en R_1 tenemos la unimodularidad.

Aplicamos ahora la hipótesis de inducción. Observemos que en cada paso usamos un anillo $R_k = R/I_k$ para cierto ideal I_k. Existe una matriz $B_1^{(1)} \in E_{r-1}(R_1)$ triangular superior con valores 1 en la diagonal tal que

$$B_1^{(1)} \begin{pmatrix} b_2^{(1)} \\ \vdots \\ b_r^{(1)} \end{pmatrix} = \begin{pmatrix} d_2^{(1)} \\ \vdots \\ d_r^{(1)} \end{pmatrix}$$

y la sucesión $d_2^{(1)}, \ldots, d_r^{(1)}$ es regular en R_1. Levantamos $B_1^{(1)}$ a una matriz $B_1 \in E_{r-1}(R)$ que se aplique en ella, y sea

$$B = \begin{pmatrix} 1 & za_2 & \ldots & za_r \\ 0 & & B_1 & \end{pmatrix}.$$

Entonces $B \in E_r(R)$, pues los elementos de la fila 1 se pueden eliminar mediante transformaciones elementales. B es triangular superior, tiene elementos igual a 1 en la diagonal principal, y

$$B \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{pmatrix} = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix}$$

con $d_1, d_2, \ldots, d_r$ sucesión regular.

Sea $R' = R_0[y_1, \ldots, y_n]$, con R_0 un anillo noetheriano, y definimos $\mathbb{T}^n = \{Y^\alpha = y_1^{\alpha_1} \cdots y_n^{\alpha_n} | \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$ el conjunto de los productos de potencias. Sea $<$ un orden en $\mathbb{T}^n$. Si $f \in R'$, podemos escribir $f = \sum_{i=i}^{r} a_i Y^{\alpha_i}$, con $a_i \in R_0 - \{0\}$, $\alpha_i \in \mathbb{N}^n$ y $\alpha_r < \ldots < \alpha_1$. Con esta notación, definimos

Definición 2.6.3.

- $lc(f) = c_1$, el coeficiente líder de f.
- $lp(f) = Y^{\alpha_1}$, el producto de potencias líder de f.
- $lt(f) = c_1 Y^{\alpha_1}$, el término líder de f.

Observemos que el anillo $R = \mathbb{Z}[x_1, \ldots, x_m]$ lo podemos ver como también como $R' = \mathbb{Z}[x_1, \ldots, x_{m-1}][x_m]$. Si $<$ es un orden en $\mathbb{T}^m$ para el que x_m es mayor que las demás variables, lo denominamos orden de eliminación en x_m. Sea $<'$ el orden en R' determinado por el grado en x_m. Tenemos el siguiente resultado:

Proposición 2.6.4. *Sea $\mathcal{G} = \{g_1, \ldots, g_t\}$ base de Gröbner en $\mathbb{Z}[x_1, \ldots, x_m]$ con respecto a un orden de eliminación en x_m. Entonces $\mathcal{G}$ es base de Gröbner en $\mathbb{Z}[x_1, \ldots, x_{m-1}][x_m]$ con respecto al orden determinado por el grado en x_m.*

Demostración. [GTZ88].

Nota 2.6.1. Sea $f \in \mathbb{Z}[x_1, \ldots, x_m]$. Por una parte tenemos $lc(f)$ que es un elemento de $\mathbb{Z}$, y por otra $lc_{<'}(f)$; es el coeficiente del término de mayor grado en x_m. Es un polinomio en $\mathbb{Z}[x_1, \ldots, x_{m-1}]$.

Lema 2.6.5. *Sea I un ideal de $\mathbb{Z}[x_1, \ldots, x_m]$. El conjunto $lc_{<'}(I) = \{lc_{<'}(f) | f \in I\}$ es un ideal de $\mathbb{Z}[x_1, \ldots, x_{m-1}]$.*

Demostración. Sean $g_1, g_2 \in lc_{<'}(I)$, con $f_1, f_2 \in I$ tales que $lc_{<'}(f_i) = g_i$, para $i = 1, 2$. Si, por ejemplo, $\text{grado}_{x_m}(f_1) - \text{grado}_{x_m}(f_2) = k \geq 0$, entonces $g_1 + g_2 = lc_{<'}(f_1 + x_m^k f_2)$. Si $g \in \mathbb{Z}[x_1, \ldots, x_{m-1}]$, entonces $gg_1 = lc_{<'}(gf_1)$.

Lema 2.6.6. *Sea I un ideal de $R = \mathbb{Z}[x_1, \ldots, x_m]$ y $\mathcal{G} = \{g_1, \ldots, g_r\}$ una base de Gröbner de I respecto a un orden de eliminación en x_m. Entonces*

1. $lc_{<'}(I) = \langle lc_{<'}(g_1), \ldots, lc_{<'}(g_r)\rangle$.

2. *Dado $h \in lc_{<'}(I)$, podemos calcular $f \in I$ tal que $lc_{<'}(f) = h$.*

Demostración. Sea $h \in lc_{<'}(I)$ y $f \in I$ tal que $lc_{<'}(f) = h$. Entonces $lt_{<'}(f) = hx_m^k$ para algún $k \geq 0$. Por la proposición 2.6.4, $hx_m^k = \sum_{i=1}^r h_i lt_{<'} g_i$, donde podemos suponer que para cada i $h_i = 0$ o $lp(h_i)lp(g_i) = x_m^k$. Entonces $h = lc_{<'}(h_1)lc_{<'}(g_1) + \ldots + lc<'(h_r)lc_{<'}(g_r)$, y tenemos la primera parte. Dado $h \in lc_{<'}(I)$, sean $h_1, \ldots, h_r \in \mathbb{Z}[x_1, \ldots, x_{m-1}]$ tales que $h = \sum_{i=i}^r h_i lc_{<'}(g_i)$. Entonces, si $f = \sum_{i=1}^r h_i g_i$ se tiene que $lc_{<'}(f) = h$, pues $lc_{<'}(h_i) = h_i$ para $i = 1, \ldots, r$.

Lema 2.6.7. *Sea R_0 un anillo noetheriano, $R = R_0[x]$, I un ideal de R y J el ideal de R_0 formado por los coeficientes de los términos de mayor grado de polinomios en I. Entonces $ht_{R_0}(J) \geq ht_A(I)$.*

Demostración. [VS76] p.964

Lema 2.6.8. *Sea $R = \mathbb{Z}[x_1, \ldots, x_m]$, I un ideal de R, con $ht_R(I) \geq 2$. Entonces existe un cambio invertible de variables $x_1, \ldots, x_m \leftrightarrow y_1, \ldots, y_m$ en el anillo R tal que I contiene un polinomio que es unitario en y_1.*

Demostración. Sea J el ideal en $R_0 = \mathbb{Z}[x_1, \ldots, x_{m-1}]$ formado por los coeficientes de los términos de mayor grado en x_m de polinomios del ideal I, que es calculable. Entonces $ht_{R_0}(J) \geq ht_R(I) \geq 2$. Si $m = 1$, entonces $J = \mathbb{Z}$, y el ideal I contiene un polinomio que es unitario en x_1. Para $n \geq 2$, procedemos por inducción sobre n, y suponemos que existe un cambio de variables $x_1, \ldots, x_{m-1} \leftrightarrow y_1, \ldots, y_{m-1}$ en R_0 que hace que el ideal J contenga un polinomio g unitario en y_1. Entonces, I contiene un polinomio f de la forma $gx_m^s + h$, donde $\text{grado}_{x_m}(h) < s$. Para un n suficientemente grande, el cambio $y_m = x_m - y_1^n$ hace que el polinomio f sea unitario en y_1.

Lema 2.6.9. *Sea* $R = \mathbb{Z}[x_1, \ldots, x_m]$, $r \geq 3$, *y* $\mathbf{b} \in \mathrm{Um}_r(R)$. *Entonces existe* $A \in E_r(R)$ *y un cambio de variables* $x_1, \ldots, x_m \leftrightarrow y_1, \ldots, y_m$ *tal que* $A \cdot \mathbf{b} = (c_i)$, *donde* c_r *es unitario en* y_1 *como polinomio en* $y_1, \ldots, y_m$.

Demostración. Podemos calcular una matriz $B \in E_r(R)$ tal que $B \cdot \mathbf{b} = (d_i)$, con $d_1, \ldots, d_r$ una sucesión regular. Entonces $ht_R(Rd_1 + \ldots + Rd_{r-1}) \geq r - 1 \geq 2$. Por el lema anterior, existe un cambio de variables $x_1, \ldots, x_m \leftrightarrow y_1, \ldots, y_m$ tal que el ideal $Rd_1 + \ldots + Rd_{r-1}$ contiene un polinomio f que es unitario en y_1. Sea $f = a_1 d_1 + \ldots + a_{r-1} d_{r-1}$, y consideremos el vector $\mathbf{u} = (a_1 y_1^n, \ldots, a_{r-1} y_1^n)$, donde $n-1$ es el grado en y_1 del polinomio d_r en $y_1, \ldots, y_m$. Entonces el polinomio $c_r = d_r + d_1 a_1 y_1^n + \ldots + d_{r-1} a_{r-1} y_1^n$ es unitario en y_1. Por tanto, podemos tomar

$$A = \begin{pmatrix} I_{r-1} & 0 \\ u & 1 \end{pmatrix} \cdot B$$

que pertenece a $E_r(R)$.

Nota 2.6.2. La prueba de la *Propiedad de Columna Elemental* y la realización de matrices en $SL_3(R[x])$ de [PW95] usan el Lema de Normalización de Noether. En ambos casos se aplican sobre vectores unimodulares, por lo que es posible usar el lema 2.6.9 para anillos más generales como $\mathbb{Z}[x_1, \ldots, x_m]$.

Capítulo 3

Módulos sobre $\mathbb{Z}[x]/(px)$.

3.1 Introducción

El problema de la clasificación de módulos finitamente generados sobre $\mathbb{Z}[x]$ no está resuelto, y menos aún su resolución algorítmica. En el Capítulo 1 hemos visto algunos métodos generales, que nos proporcionan condiciones necesarias para diferenciar dos presentaciones. Otra manera es considerar la proyección sobre un anillo donde tengamos un algoritmo de clasificación. En este caso, consideramos $R = \mathbb{Z}[x]/\langle px \rangle$, con $p \in \mathbb{Z}$ un número primo. Extendemos parte del algoritmo de [LS96] para el anillo R.
La base teórica es la misma, y en primer lugar probamos que este anillo es de tipo pullback. Por tanto, los resultados de Levy ([Lev81b] y [Lev81a]) dan la clasificación de los módulos sobre R. El objetivo es dar una versión algorítmica de estos resultados, hasta la reducción al caso local resuelto en [NR69] y [NRSB75].

Suponemos que el R-módulo viene dado por una matriz de presentación. El primer paso reduce la clasificación al estudio de matrices $A(x)$ con coeficientes en R tales que $A(0)$ sea la matriz nula, considerando sus entradas con valores en el cuerpo $\mathbb{Z}/\langle p \rangle$. Pasamos entonces al cálculo de la denominada representación separada del módulo. Es un módulo asociado al original, único por isomorfismo. Esto nos permite diferenciar una familia de módulos sobre $\mathbb{Z}[x]$, tomando un primo p adecuado.

Las secciones siguientes se encargan de efectuar las reducciones necesarias hasta llegar a los tipos de módulos estudiados en [NR69] y [NRSB75].

3.2 R es un anillo pullback

Sea $R_1 = \mathbb{Z}$, $R_2 = (\mathbb{Z}/\langle p\rangle)[x]$, $\pi_1 : R_1 \to \mathbb{Z}/\langle p\rangle$ la proyección canónica y $\pi_2 : R_2 \to \mathbb{Z}/\langle p\rangle$ el morfismo definido por $\pi_2(q(x)) = q(0)$.

Definición 3.2.1. $R = \{(r_1, r_2) \in R_1 \times R_2 | \pi_1(r_1) = \pi_2(r_2)\}$ se denomina el anillo pullback de π_1 y π_2.

Nota 3.2.1. A los anillos R_1 y R_2 los denominaremos anillos coordenados de R.

Lema 3.2.1. *Sean $\pi_1 : R_1 \to R_0$, $\pi_2 : R_2 \to R_0$ epimorfismos de anillos. Entonces el conjunto $R = \{(r_1, r_2) \in R_1 \times R_2 | \pi_1(r_1) = \pi_2(r_2)\}$ tiene estructura de anillo.*

Demostración. Las operaciones están definidas por

$$(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2'), (r_1, r_2) \cdot (r_1', r_2') = (r_1 r_1', r_2 r_2').$$

El elemento unidad es $(1, 1)$.

Lema 3.2.2. $R \simeq \mathbb{Z}[x]/\langle px\rangle$.

Demostración. Sea $\varphi : R \to \mathbb{Z}[x]/\langle px\rangle$ definida por $\varphi((q(x), r)) = (q(x) - q(0)) + r$. La idea es la identificación de los elementos sin término constante de $(\mathbb{Z}/\langle p\rangle)[x]$ y $\mathbb{Z}[x]/\langle px\rangle$. Es fácil ver que $((q_1(x) - q_1(0)) + r_1) \cdot ((q_2(x) - q_2(0)) + r_2) = (q_1(x)q_2(x) - q_1(0)q_2(0)) + r_1 r_2$, considerando que $r_2(q_1(x) - q_1(0)) = \bar{r}_2(q_1(x) - q_1(0) = q_2(0)(q_1(x) - q_1(0))$, siendo $\bar{r}_2$ la clase de r_2 en $\mathbb{Z}/\langle p\rangle$.

Nota 3.2.2. En lo que sigue, R identificará al anillo $\mathbb{Z}[x]/\langle px\rangle$.

Nota 3.2.3. Recordemos que $E_n(R)$ es el grupo de las matrices elementales con coeficientes en R (ver 2.1.1).

3.3 Primera reducción

El primer paso consiste en reducir el problema a una matriz $A(x)$ tal que $A(0)$ sea nula en $\mathbb{Z}/\langle p\rangle$, es decir, que sus términos constantes sean múltiplos de p.

Lema 3.3.1. *Sea $(g_1, g_2, \ldots, g_n)$ un vector fila sobre R tal que al menos un g_i tiene un término constante no nulo módulo p ($g_i(0) \not\equiv 0 \pmod{p}$). Entonces el ideal $\langle g_1, g_2, \ldots, g_n\rangle$ es principal, su generador g tiene un término constante no nulo módulo p y se puede construir $V \in E_n(R)$ con*

$$(g, 0, \ldots, 0) \;=\; (g_1, g_2, \ldots, g_n) \cdot V \tag{3.3.1}$$

Demostración. Si $f \in R$, lo podemos considerar como un polinomio con coeficientes en $\mathbb{Z}[x]$, y llamamos $in(f)$ al término de mayor grado en x. Consideramos el siguiente algoritmo:

1) **Mientras** existan índices i, j tales que $in(g_i) = c_i x^{e_i}$, $in(g_j) = c_j x^{e_j}$, con $e_i \geq e_j > 0$, **reemplaza** g_i por $g_i' = g_i - c_i c_j' x^{e_i - e_j} g_j$, donde $c_j' \in \mathbb{Z}$ y $c_j c_j' \equiv 1 \pmod{p}$.

Esta operación reduce el grado de g_i, y en el vector transformado sigue habiendo un elemento cuyo término constante es no nulo módulo p. Si g_i tiene el término constante no nulo módulo p y $e_i > e_j$, entonces es claro. Si $e_i = e_j$, y $g_j(0) \equiv 0 \pmod{p}$, entonces g_i' verifica la condición. Si $e_i = e_j$ y $g_j(0) \not\equiv 0 \pmod{p}$, entonces lo tenemos con g_j.

2) **Mientras** existan índices i, j tales que $in(g_i) = c_i$, $in(g_j) = c_j$, no nulos, **reemplaza** (g_i, g_j) por $(d_{ij}, 0)$, con $d_{ij} = mcd(c_i, c_j)$ mediante

$$\begin{pmatrix} g_i & g_j \end{pmatrix} \begin{pmatrix} \alpha_i & -c_j/d_{ij} \\ \alpha_j & c_i/d_{ij} \end{pmatrix} = \begin{pmatrix} d_{ij} & 0 \end{pmatrix} \tag{3.3.2}$$

donde $d_{ij} = \alpha_i c_i + \alpha_j c_j$.

Como $\mathbb{Z}$ es dominio euclídeo, esta matriz se puede descomponer en producto de matrices elementales. Con esta operación queda un único término constante en el vector.

3) Tras las operaciones 1) y 2), el vector queda de la forma $(f(x), d, 0, \ldots, 0)$, con

$in(f) = cx^e$, $e > 0$. Si d es no nulo módulo p, podemos reducir el grado de f mediante $f - cd'dx^e$, con $d'd \equiv 1 \pmod{p}$. Si $d \equiv 0 \pmod{p}$, entonces el término constante de f es no nulo módulo p. Dado que $mcd(d, f(0)) = 1$, existen $\alpha, \beta \in \mathbb{Z}$ con $\alpha d + \beta f(0) = 1$ y

$$\begin{pmatrix} f(x) & d \end{pmatrix} \begin{pmatrix} \beta & -d \\ \alpha & f(0) \end{pmatrix} = \begin{pmatrix} f'(x) & -df(x) + df(0) \end{pmatrix} \tag{3.3.3}$$

con $f'(0) = 1$.

Observemos que $-df(x) + df(0)$ no tiene término constante, y los restantes aparecen multiplicados por d, que es múltiplo de p. Entonces es cero en R. Como antes, la matriz unimodular se puede descomponer en producto de matrices elementales, pues $\mathbb{Z}$ es dominio euclídeo.

Al final, queda una única entrada no nula, y mediante transformaciones elementales podemos poner a ella o su opuesta en la primera posición

Teorema 3.3.2. *Sea $A(x)$ una matriz $m \times n$ con coeficientes en el anillo R, y $r = rango(A(0))$ en el anillo $\mathbb{Z}/\langle p \rangle$. Entonces existen $U(x) \in E_m(R)$, $V(x) \in E_n(R)$ tales que*

$$U(x) \cdot A(x) \cdot V(x) = \begin{pmatrix} f_1(x) & 0 & \dots & 0 & 0 \\ 0 & f_2(x) & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & f_r(x) & 0 \\ 0 & 0 & \dots & 0 & B(x) \end{pmatrix} \tag{3.3.4}$$

donde $f_i \in R$ con $f_i(0) \neq 0$ en $\mathbb{Z}/\langle p \rangle$, para $i = 1, \dots, r$, y B una matriz $(m-r) \times (n-r)$ con coeficientes en R tal que $B(0) = 0$ en $\mathbb{Z}/\langle p \rangle$.

Demostración. Por inducción sobre r. Para $r = 0$ es trivial. Si $r \geq 1$ podemos suponer que en la posición $(1, 1)$ tenemos un elemento $a_{11}(x)$ con $a_{11}(0) \not\equiv 0 \pmod{p}$, tras

realizar permutaciones de filas y columnas. Esto puede provocar cambios de signo, pero no afecta a nuestro resultado. Aplicamos el algoritmo del lema 3.3.1 a la primera fila de la matriz $A(x)$. Entonces

$$B = A \cdot V = \begin{pmatrix} b_{11}(x) & 0 & \dots & 0 \\ b_{21}(x) & b_{22}(x) & \dots & b_{2n}(x) \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1}(x) & b_{m2}(x) & \dots & b_{mn}(x) \end{pmatrix} \tag{3.3.5}$$

con $b_{11}(0) \not\equiv 0 \pmod{p}$. Sea I el ideal generado por la primera columna de B. Es principal, de nuevo por el lema 3.3.1. Si I está generado por $b_{11}(x)$, existe $U \in E_m(R)$ tal que

$$U \cdot A \cdot V = \begin{pmatrix} b_{11}(x) & 0 & \dots & 0 \\ 0 & b_{22}(x) & \dots & b_{2n}(x) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m2}(x) & \dots & b_{mn}(x) \end{pmatrix} \tag{3.3.6}$$

y tenemos el resultado por inducción. Si $b_{11}(x)$ no es generador, existe $c_{11}(x)$ factor propio de $b_{11}(x)$ que genera I. Aplicando de nuevo el lema, obtenemos

$$C = U \cdot A \cdot V = \begin{pmatrix} c_{11}(x) & c_{12}(x) & \dots & c_{1n}(x) \\ 0 & c_{22}(x) & \dots & c_{2n}(x) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{m2}(x) & \dots & c_{mn}(x) \end{pmatrix} \tag{3.3.7}$$

con $c_{11}(0) \not\equiv 0 \pmod{p}$. Sea J el ideal principal generado por la primera fila de C. Si J está generado por $c_{11}(x)$, usamos el mismo argumento que antes, y por la hipótesis de inducción habríamos terminado. En otro caso, el ideal J está generado por un factor propio $d_{11}(x)$ de $c_{11}(x)$, y aplicamos el algoritmo del lema 3.3.1 a la primera fila de la matriz C. La cadena de factores propios no puede ser infinita, y el proceso termina.

Ahora nos hace falta llevar la forma diagonal obtenida a otra única salvo unidades.

Proposición 3.3.3. *Sea*

$$A = \begin{pmatrix} f_1(x) & 0 & \dots & 0 & 0 \\ 0 & f_2(x) & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & f_r(x) & 0 \\ 0 & 0 & \dots & 0 & B(x) \end{pmatrix}$$

matriz $m \times n$ con coeficientes en R, tal que $f_i(0) \not\equiv 0 \pmod{p}$, para $i = 1, \dots, r$. Entonces existen $U \in E_m(R)$, $V \in E_n(R)$ tales que

$$U(x) \cdot A \cdot V(x) = \begin{pmatrix} g_1(x) & 0 & \dots & 0 & 0 \\ 0 & g_2(x) & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & g_r(x) & 0 \\ 0 & 0 & \dots & 0 & B(x) \end{pmatrix}$$

con g_i dividiendo a g_{i+1} para $i = 1, \dots, r-1$.

Demostración. El proceso es similar al algoritmo de la forma normal de Smith sobre dominio de ideales principales. Podemos suponer, mediante permutaciones de filas y columnas, que $f_1(x)$ es de grado minimal entre los $f_i(x)$. Si $f_1(x)$ no divide a $f_2(x)$, sumamos a la primera fila la segunda. Mediante el lema 3.3.1, hacemos ceros en la primera fila, y por idéntico razonamiento al teorema anterior, llegamos a una matriz de

la forma

$$\begin{pmatrix} f_1'(x) & 0 & \dots & 0 & 0 \\ 0 & f_2'(x) & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & f_r(x) & 0 \\ 0 & 0 & \dots & 0 & B(x) \end{pmatrix}$$

con $f_1'(x)$ dividiendo a $f_2'(x)$. Si $f_1'(x)$ no divide a $f_3'(x)$, repetimos el proceso anterior. Tras un número finito de pasos, el elemento en la posición $(1,1)$ divide a los restantes de la diagonal. El resultado se tiene entonces por inducción.

Lema 3.3.4. *Las unidades de R son 1 y -1.*

Demostración. Si $u \in R$ es unidad, por razones de grado tiene que ser un elemento de $\mathbb{Z}$, y las unidades en este anillo son 1 y -1.

Corolario 3.3.5. *Sean $A_1 = diag(f_1, \dots, f_r)$, $A_2 = diag(g_1, \dots, g_r)$ matrices diagonales con coeficientes en R, tales que:*

- *f_i divide a f_{i+1}, g_i divide a g_{i+1}, para $i = 1, \dots, r-1$.*
- *Presentan el mismo módulo.*
- *$f_i(0) \neq 0$ en $\mathbb{Z}/\langle p \rangle$, $g_i(0) \neq 0$ en $\mathbb{Z}/\langle p \rangle$, para $i = 1, \dots, r$.*

Entonces $g_i = \epsilon f_1$ para todo $i = 1, \dots, r$, con $\epsilon = 1, -1$.

Demostración. Consideremos los ideales elementales $F_r(A_1) = \langle f_1 \rangle$, $F_r(A_2) = \langle g_1 \rangle$. Entonces existen $\alpha, \beta \in R$ tales que $g_1 = \alpha f_1$, $f_1 = \beta g_1$, de donde $(1 - \alpha\beta)g_1 = 0$. Llevando la igualdad a $\mathbb{Z}[x]$, existe $h \in \mathbb{Z}[x]$ tal que $(1 - \alpha\beta)g_1 = hpx$. No puede ocurrir que p divida a g_1 ni que x divida a g_1, pues $g_1(0)$ no es nulo en $\mathbb{Z}/\langle p \rangle$. Por tanto, px divide a $(1 - \alpha\beta)$, de donde $-\alpha\beta$ es unidad en R. Por el lema 3.3.4, son 1 o -1. Los demás elementos se obtienen por inducción, y considerando los siguientes ideales elementales.

Nota 3.3.1. Si una matriz A con coeficientes en R tiene rango máximo, el corolario 3.3.5 da una forma normal similar a la de Smith.

Corolario 3.3.6. *Teorema de Estabilidad de Suslin en R. Toda matriz unimodular* $A \in SL_n(R)$, $n \geq 1$, *puede ser factorizada como producto de matrices elementales sobre R.*

Demostración. Si $A \in SL_n(R)$, entonces $A(0) \in SL_n(\mathbb{Z}/\langle p \rangle)$, y tenemos $r = m = n$ en el Teorema 3.3.2. Existen $U, V \in E_n(R)$ tales que UAV es una matriz diagonal con determinante $f_1(x) \cdot \ldots \cdot f_n(x) = 1$. Esto implica que cada polinomio es 1 o -1, y lo podemos ver como una matriz unitaria en $\mathbb{Z}$. Como es un dominio euclídeo, existe $E \in E_n(\mathbb{Z})$ tal que $UAV = E$, de donde $A = U^{-1}EV^{-1} \in E_n(R)$.

Nota 3.3.2. Estos resultados se pueden extender a anillos $D[x]/\langle ax \rangle$ con D dominio euclídeo, $a \in D$ irreducible.

3.4 Cálculo de una representación separada

Sea N un submódulo de R^m, y sean $\mathbf{a}_1(x), \ldots, \mathbf{a}_n(x)$ en $\mathbb{Z}[x]^m$ cuyas clases generan N. Si $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ es la base canónica de $\mathbb{Z}[x]^m$, entonces representamos N como el submódulo N' de $\mathbb{Z}[x]^m$ generado por $\mathbf{a}_1(x), \ldots, \mathbf{a}_n(x), px\mathbf{e}_1, \ldots, px\mathbf{e}_m$. Según [AL94] y [KRK84] podemos calcular $\mathcal{G}'$ una base de Gröbner *reducida* de N', con el orden TOP, el orden en $\mathbb{Z}$ definido por el valor absoluto, con los positivos menores que los negativos y $\mathbf{e}_1 < \ldots < \mathbf{e}_m$.

Definición 3.4.1. En la situación anterior, al conjunto $\mathcal{G}$ formado por los elementos de $\mathcal{G}'$ menos los elementos $px\mathbf{e}_i$ lo denominamos base estándar de N.

Sea $A(x)$ una matriz $m \times n$ con coeficientes en R, tal que $A(0) = 0$ en $\mathbb{Z}/\langle p \rangle$, y sea N el submódulo de R^m generado por sus columnas. Sea $\mathcal{G}$ una base estándar de N, y

definimos $N_1 = N \cap \langle p \rangle \cdot R^m$, $N_2 = N \cap \langle x \rangle \cdot R^m$. Estos módulos podemos calcularlos a partir de $N' \cap ip\mathbb{Z}[x]^m$ y $N' \cap \langle x \rangle \mathbb{Z}[x]^m$. Sea $\mathcal{G}_1$ base estándar de N_1 y $\mathcal{G}_2$ base estándar de N_2. N_2 lo podemos ver como un submódulo de $(\mathbb{Z}/\langle p \rangle)[x]^m$. Entonces $\mathcal{G}_1 \subset \mathcal{G}$, porque el orden TOP nos dará los elementos de grado cero en cualquier componente y los elementos de la matriz tienen términos constantes múltiplos de p.

Sea $\mathcal{G}_3 = \mathcal{G} - (\mathcal{G}_1 \cup \mathcal{G}_2)$, y llamemos N_3 al submódulo de R^m generado por los vectores de $\mathcal{G}_3$. Sean $A_1, A_2(x), A_3(x)$ las matrices cuyas columnas son los elementos de $\mathcal{G}_1$, $\mathcal{G}_2$, $\mathcal{G}_3$, respectivamente. Entonces $M = \operatorname{coker}(A(x)) = \operatorname{coker}(A_1, A_2(x), A_3(x))$, pues lo único que hemos hecho ha sido añadir generadores.

Lema 3.4.1. *Sea N_i el submódulo de R^m generado por las columnas de A_i, para $i = 1, 2, 3$. Entonces*

$$N_3 \cap \langle p \rangle \cdot R^m \subset N_1, N_3 \cap \langle x \rangle \cdot R^m \subset N_2 \tag{3.4.1}$$

Demostración. Inmediato porque $N_3 \subset N$.

Vamos a ver que esta construcción permite el cálculo de una representación separada de un R-módulo M.

Definición 3.4.2. Un R-módulo S se dice separado si es un R-submódulo de una suma directa $S_1 \bigoplus S_2$, donde S_1 es un módulo sobre $\mathbb{Z}$ y S_2 es un módulo sobre $(\mathbb{Z}/\langle p \rangle)[x]$.

Definición 3.4.3. Una representación separada de un R-módulo M es un epimorfismo de R-módulos $\varphi : S \twoheadrightarrow M$ tal que S es separado, y si φ admite una factorización

$$\varphi : S \to S' \twoheadrightarrow M \tag{3.4.2}$$

con S' un R-módulo separado, entonces f es inyectiva.

Teorema 3.4.2. *Un R-módulo M' es separado si y solamente si $\langle x \rangle \cdot M' \cap \langle p \rangle \cdot M' = 0$.*

Demostración. Tenemos que $ker(\pi_1) = \langle p \rangle$ y $ker(\pi_2) = \langle x \rangle$. El lema 2.9 de [Lev81b] estable que M' es un R-módulo separado si y solamente si $ker(\pi_1) \cdot M' \cap ker(\pi_2) \cdot M' = 0$.

Nota 3.4.1. Por la definición de anillo pullback del inicio, se tiene que $R \cap \mathbb{Z} = (ker(\pi_1), 0)$ y $R \cap (\mathbb{Z}/\langle p \rangle)[x] = (0, ker(\pi_2))$.

Teorema 3.4.3. *Sea $\varphi : M' \to M$ un epimorfismo de R-módulos, con M' un módulo separado. Son equivalentes:*

1. *φ es una representación separada de M.*
2. *φ es inyectiva en $(R \cap \mathbb{Z})M'$ y en $(R \cap (\mathbb{Z}/\langle p \rangle)[x])M'$, y además $ker(\varphi) \subset \langle p, x \rangle M'$.*

Demostración. Es la proposición 2.3(ii) de [Lev81b].

Teorema 3.4.4. *Todo R-módulo tiene una representación separada, única salvo isomorfismo.*

Demostración. ([Lev81b], teorema 2.8)

La prueba anterior es existencial y no constructiva. Vamos a ver que con las matrices A_1, A_2 que hemos definido podemos dar una matriz de presentación de la representación separada.

Teorema 3.4.5. *Sean A_1, $A_2(x)$, $A_3(x)$ las matrices construídas anteriormente. Entonces:*

- *El módulo $M' = \text{coker}(A_1, A_2(x))$ es separado.*
- *La aplicación canónica de M' sobre $M = \text{coker}(A_1, A_2(x), A_3(x))$ es una representación separada de M.*

Demostración. Aplicamos el teorema 3.4.2 para la primera parte. Sea $m' \in \langle p \rangle \cdot M' \cap \langle x \rangle \cdot M'$. Entonces existen $u(x), v(x) \in R^m$ tales que $m' = pu(x)$ y $m' = xv(x)$ en M'. Entonces $pu(x) - xv(x)$ es 0 en M', o lo que es lo mismo, existen $a(x), b(x) \in R^m$ con

$$pu(x) - xv(x) = A_1 a(x) + A_2(x) b(x).$$

Recordemos que los elementos de A_2 no tienen términos constantes. Entonces, tomando $x = 0$ en la anterior igualdad queda que $pu(0) = A_1 a(0) \in N_1$. Pero en R^m, $pu(x) = pu(0)$, luego m' es el elemento nulo de M'.

Para la segunda parte aplicamos el teorema 3.4.3. Sea φ la aplicación canónica de M' en M, definida por $\varphi(a + (N_1 + N_2)) = a + N$. Es sobreyectiva, y $ker(\varphi)$ está generado por las columnas de $A_3(x)$ módulo $N_1 + N_2$. Recordemos que $A_3(0)$ es nula considerada en $\mathbb{Z}/\langle p \rangle$, por lo que todas sus entradas están en el ideal $\langle p, x \rangle$. Tenemos así una de las condiciones. Para la inyectividad, calculamos $ker(\varphi) \cap (R \cap \mathbb{Z})M' = ker(\varphi) \cap \langle p \rangle \cdot M'$. Como $N_3 \cap \langle p \rangle \cdot R^m \subset N_1$ (3.4.1), entonces la intersección es el cero de M'. Análogamente se tiene que $ker(\varphi) \cap \langle x \rangle M' = 0$.

Ejemplo 3.4.1. Sea M el módulo presentado por la matriz $\begin{pmatrix} 2 & 0 \\ x & 12 \end{pmatrix}$ sobre el anillo $R = \mathbb{Z}[x]/\langle 2x \rangle$. Una base estándar del módulo N generado por las columnas es $\mathcal{G} = \{(2, x), (0, 12), (4, 0)\}$, y una base reducida de $N \cap \langle x \rangle R$ está formada por $\{(0, x^2)\}$. Entonces

$$M = \operatorname{coker} \begin{pmatrix} 4 & 0 & 0 & 2 \\ 0 & 12 & x^2 & x \end{pmatrix}$$

y una representación separada es

$$M' = \operatorname{coker} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 12 & x^2 \end{pmatrix}.$$

Ejemplo 3.4.2. Consideremos los $\mathbb{Z}[x]$-módulos M_i, $i = 1, 2$ presentados por las matrices A_i, con $A_1 = \begin{pmatrix} p & 0 \\ x & ap^2 \end{pmatrix}$, y $A_2 = \begin{pmatrix} p & x \\ 0 & ap^2 \end{pmatrix}$, con $a, p \in \mathbb{Z}$, p un número primo. Vamos a usar los resultados anteriores para probar que M_1 y M_2 no son isomorfos como $\mathbb{Z}[x]$-módulos. Sea $R = \mathbb{Z}[x]/\langle px \rangle$, y consideremos los módulos M_1' y M_2' definidos sobre este anillo por las matrices anteriores. Una representación separada de M_1' es el R-módulo S_1 con matriz de presentación $\begin{pmatrix} p^2 & 0 & 0 \\ 0 & kp^2 & x^2 \end{pmatrix}$. Una representación separada de M_2' es el R-módulo S_2 con matriz de presentación $\begin{pmatrix} p & 0 & x^2 \\ 0 & kp^3 & 0 \end{pmatrix}$. S_1 y S_2 no son isomorfos como R-módulos pues, por ejemplo, $F_1(S_1) = \langle p^2, x^2 \rangle$ y $F_1(S_2) = \langle p, x^2 \rangle$, y $p \notin F_1(S_1)$. Tenemos así una familia de módulos en $\mathbb{Z}[x]$, con iguales cadenas de ideales elementales, que podemos distinguir mediante el paso a $\mathbb{Z}[x]/\langle px \rangle$.

Nota 3.4.2. Podemos encontrar módulos sobre $\mathbb{Z}[x]/\langle px \rangle$ no isomorfos cuyas representaciones separadas sí son isomorfas. Por ello, es interesante dar una clasificación completa de estos módulos. Las siguientes secciones se encargan de llevar la matriz de presentación a una forma donde se pueda aplicar [NR69] y [NRSB75].

3.5 Reducción a matrices con doble diagonal

El objetivo de esta sección es diagonalizar la parte separada del módulo, para que si las posteriores modificaciones de la matriz $A_3(x)$, que serán operaciones entre filas, afectan a la parte separada, podamos restaurar el carácter diagonal.

Proposición 3.5.1. *Sean $A_1 \in \mathcal{M}(m \times n_1; \mathbb{Z})$, $A_2(x) \in \mathcal{M}(m \times n_2; (\mathbb{Z}/\langle p \rangle)[x])$ matrices con el mismo número de filas tales que $A_1 = 0$ en $\mathbb{Z}/\langle p \rangle$, $A_2(0) = 0$ en R. Entonces*

existen $U \in SL_m(R)$, $V_1 \in SL_{n_1}(\mathbb{Z})$, $V_2 \in SL_{n_2}((\mathbb{Z}/\langle p\rangle)[x])$ *con*

$$U \cdot \begin{pmatrix} A_1 & A_2(x) \end{pmatrix} \cdot \begin{pmatrix} V_1 & 0 \\ 0 & V_2(x) \end{pmatrix} =$$

$$\begin{pmatrix}
f_1 & 0 & \dots & 0 & 0 & \dots & 0 & g_1(x) & 0 & \dots & 0 & 0 & \dots & 0 \\
0 & f_2 & \dots & 0 & 0 & \dots & 0 & 0 & g_2(x) & \dots & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \dots & f_r & 0 & \dots & 0 & 0 & 0 & \dots & g_s(x) & 0 & \dots & 0 \\
0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0
\end{pmatrix}$$

tales que $f_i \in \langle p\rangle\mathbb{Z}$, f_{i+1} *divide a* f_i *para* $i = 1, \dots, r-1$, *y* $g_j(x) \in (\mathbb{Z}/\langle p\rangle)[x]$, $g_j(0) = 0$, *para* $j = 1, \dots, s$.

Demostración. Si $A_1 = 0$ o $A_2(x) = 0$, el problema se reduce a calcular la forma normal de Smith sobre $(\mathbb{Z}/\langle p\rangle)[x]$ o sobre $\mathbb{Z}$, respectivamente. Supongamos entonces que $A_1 \neq 0$. Calculamos la forma normal de Smith sobre $\mathbb{Z}$, y obtenemos matrices $U' \in E_m(\mathbb{Z})$, $V' \in E_{n_1}(\mathbb{Z})$ tales que

$$U' \cdot \begin{pmatrix} A_1 & A_2(x) \end{pmatrix} \cdot \begin{pmatrix} V' & 0 \\ 0 & I \end{pmatrix} =$$

$$\begin{pmatrix}
f_1 & 0 & \dots & 0 & 0 & \dots & 0 & h_{11}(x) & h_{12}(x) & \dots & h_{1n_2}(x) \\
0 & f_2 & \dots & 0 & 0 & \dots & 0 & h_{21}(x) & h_{22}(x) & \dots & h_{2n_2}(x) \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\
0 & 0 & \dots & f_r & 0 & \dots & 0 & h_{s1}(x) & h_{s2}(x) & \dots & h_{sn_2}(x) \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \dots & 0 & 0 & \dots & 0 & h_{m1}(x) & h_{m2}(x) & \dots & h_{mn_2}(x)
\end{pmatrix}$$

donde f_{i+1} divide a f_i para $i = 1, \ldots, r-1$. Claramente, p divide a cada f_i.

Una operación de la forma "reeamplaza la entrada $h_{i1}(x)$ por $h_{i1}(x) - c \cdot x^{\alpha} \cdot h_{j1}(x)$" se dice *permitida* si $\alpha > 0$ o bien $i > j$.

Si $\alpha > 0$ esta operación entre filas no altera la matriz diagonal a la izquierda, pues $p \cdot x = 0$ en R, y p es factor de cada elemento diagonal.

Si $\alpha = 0$ y $i > j$, en la parte izquierda tendríamos en la posición $(i, 1)$ el valor $-cf_j$, que podemos reducir a 0, dado que f_i divide a f_j.

El siguiente paso es diagonalizar la zona de la matriz que contiene polinomios en x, sin cambiar la forma normal de Smith sobre $\mathbb{Z}$ que tenemos a la izquierda. Esto se consigue aplicando operaciones permitidas en la parte derecha.

Sea $j := 1$. **Mientras** $j \leq n_2$ **realiza**:

1. Si la columna j de la parte en $(\mathbb{Z}/\langle p \rangle)[x]$ es cero, **ir** a paso 4. En otro caso, seleccionamos, entre los elementos de menor grado, la que tenga un índice menor. Si pivotamos sobre este elemento, podemos realizar transformaciones permitidas, pues las entradas con mayor grado están en el caso $\alpha > 0$, y las de igual grado tienen un índice de posición mayor. Estas operaciones anulan entradas o reducen el grado. Por repetición de este proceso, conseguimos que en la columna quede un único elemento no nulo. Esto lo podemos hacer porque $\mathbb{Z}/\langle p \rangle[x]$ es un dominio euclídeo.

2. Si esta entrada no nula tiene grado mínimal entre los elementos de su fila, mediante operaciones con columnas, que no afectan a la parte izquierda, podemos reducir el grado de todos los elementos de esa fila. Si se anulan todos, **ir** al paso 3. En otro caso, localizamos la primera columna a la derecha de j con una entrada en esa fila de grado mínimo, e intercambiamos las dos columnas. Si queremos mantener operaciones elementales, debemos cambiar el signo, y no altera al módulo. **Volver** al paso 1.

3. Realiza operaciones elementales entre columnas en la parte izquierda para restaurar la forma diagonal.

4. $j := j + 1$ y **volver** al paso 1.

5. Permuta las columnas de la parte derecha para conseguir la forma diagonal.

Notemos que en este proceso se pueden generar entradas diagonales nulas en la parte derecha de la matriz, por encima de la fila s. Por ejemplo, si la parte de la derecha queda como $\begin{pmatrix} 0 & 0 \\ g(x) & 0 \end{pmatrix}$, permutamos las columnas para dejarla en forma diagonal, y queda $\begin{pmatrix} 0 & 0 \\ 0 & g(x) \end{pmatrix}$.

Seguimos con el algoritmo principal, tras la reducción efectuada en 3.3.2. A partir de la submatriz $B(x)$ que nos quedaba, calculamos las matrices A_1, $A_2(x)$, $A_3(x)$ del lema 3.4.1. Como sabemos, las dos primeras matrices definen una representación separada del R-módulo

$$M = \operatorname{coker} \begin{pmatrix} A_1, & A_2(x), & A_3(x) \end{pmatrix} \tag{3.5.1}$$

Aplicamos el algoritmo de la proposición 3.5.1 a la matriz $\begin{pmatrix} A_1, & A_2(x) \end{pmatrix}$, y calculamos las matrices U, V_1 y $V_2(x)$. Consideramos entonces

$$U \cdot \begin{pmatrix} A_1, & A_2(x), & A_3(x) \end{pmatrix} \cdot \begin{pmatrix} V_1 & 0 & 0 \\ 0 & V_2(x) & 0 \\ 0 & 0 & I \end{pmatrix}$$

Esto es aplicar las operaciones de fila definidas por U sobre $A_3(x)$, y que no tengan efecto las operaciones entre columnas. Tenemos una nueva matriz de presentación del módulo M, en la forma $\begin{pmatrix} F, & G(x), & H(x) \end{pmatrix}$.

Proposición 3.5.2. *El módulo M tiene una matriz de presentación de la forma*

$$\begin{pmatrix} F, & G(x), & H(x) \end{pmatrix}$$

con

1. $F = diag(f_1, f_2, \ldots, 0, \ldots, 0)$.

2. $G(x) = diag(g_1(x), g_2(x), \ldots, 0, \ldots, 0)$.

3. *Cada elemento de la fila i-ésima de* $H(x)$ *es una combinación lineal de* f_i/p *y* $g_i(x)/x$ *con coeficientes enteros no múltiplos de* p.

Demostración. Recordemos que cada f_i es divisible por p, y los $g_j(x)$ son nulos o tienen grado estrictamente positivo. El elemento (i, j) de $H(x)$ se puede escribir como

$$h_{ij}(x) = u_{ij} + v_{ij}(x),$$

con $v_{ij}(0) = 0$. Denominemos grado de un elemento de $\mathbb{Z}$ a la mayor potencia de p que lo divide. Mediante operaciones elementales con columnas, podemos conseguir que u_{ij} menor que f_i, en valor absoluto. Veamos que además grado(u_{ij}) < grado(f_i). Lo haremos considerando el siguiente caso, que se generaliza fácilmente. Tomemos la matriz de presentación en la forma

$$\begin{pmatrix} f_1 & 0 & g_1(x) & 0 & u_{11} + v_{11}(x) \\ 0 & f_2 & 0 & g_2(x) & u_{21} + v_{21}(x) \end{pmatrix}.$$

Si $u_{ij} = u'_{ij}p^k$ y $f_i = f'_i p^k$, con u'_{ij} y f'_i no divisibles por p, añadimos una columna de ceros, y le sumamos la columna de $h_{11}(x)$ multiplicada por p. Resulta entonces la matriz

$$\begin{pmatrix} f_1 & 0 & g_1(x) & 0 & u_{11} + v_{11}(x) & pu_{11} \\ 0 & f_2 & 0 & g_2(x) & u_{21} + v_{21}(x) & pu_{21} \end{pmatrix}.$$

Por el lema 3.4.1, existen $a_1, a_2 \in R$ tales que $pu_{11} = a_1 f_1$, $pu_{21} = a_2 f_2$. Como mcd$(u_{11}, f_1) = dp^k$, con d =mcd(u'_{11}, f'_1), existen $\alpha, \beta \in \mathbb{Z}$ tale que $dp^k = \alpha f_1 + \beta u_{11}$. Obtendríamos entonces una matriz de la forma

$$\begin{pmatrix} f_1 & 0 & g_1(x) & 0 & u_{11} + v_{11}(x) & pu_{11} & dp^k \\ 0 & f_2 & 0 & g_2(x) & u_{21} + v_{21}(x) & pu_{21} & \beta pu_{21} \end{pmatrix}.$$

Mediante f_2 podemos hacer ceros en las últimas columnas de la segunda fila. De nuevo, por el lema 3.4.1, se tiene que verificar que f_1 divide a dp^k. Entonces son iguales, de donde $u_{11} \geq f_1$.

Por otro lado, podemos hacer $v(x) = 0$ o grado$(v(x)) <$ grado$(g_i(x))$. Por ser $\begin{pmatrix} F, & G(x) \end{pmatrix}$ una representación separada del módulo, se sigue que $p \cdot u$ es un múltiplo de f_i, con coeficiente no múltiplo de p, y $x \cdot v$ es múltiplo escalar de $g_i(x)$, con coeficiente no nulo en $\mathbb{Z}/\langle p \rangle$.

Si en la matriz $\begin{pmatrix} F, & G(x), & H(x) \end{pmatrix}$ hay filas de ceros al final, las podemos quitar, considerando que quitamos al módulo original una suma directa de R^k. Podemos entonces suponer que no existen filas nulas, y que máx$(r, s) = t = m$.

3.6 Reducción a forma local

En este apartado descomponemos el módulo que tenemos de la sección anterior como suma directa de módulos sobre $\mathbb{Z}$ y $(\mathbb{Z}/\langle p \rangle)[x]$ y de módulos sobre R con unas propiedades especiales. Estos últimos admiten el tratamiento de [NRSB75]. Como en [LS96], usamos la notación $[r_i]$ para indicar una matriz diagonal diag$(r_1, \ldots, r_m)$ de orden m. Después del proceso de la sección anterior, el módulo M admite una presentación de la forma

$$\begin{pmatrix} [p^{a_i+1} f_i], & [x^{b_i+1} g_i(x)], & [p^{a_i} f_i] \cdot A + [x^{b_i} g_i(x)] \cdot B \end{pmatrix},$$

donde hemos extraído las potencias de p y x, y renombrado los elementos de la matriz por simplicidad en la notación. Si todos los f_i son cero, lo que nos queda se puede reducir a la forma normal de Smith sobre $(\mathbb{Z}/\langle p \rangle)[x]$. Por tanto, suponemos que existen entradas con términos constantes no nulos. Podemos imponer las siguientes condiciones:

1. La matriz no tiene filas nulas, y $f_i \not\equiv 0 \pmod{p}$ para todo $i = 1, \ldots, r$. Si $g_i(x) \neq 0$, entonces $g_i(0) \neq 0$.

2. Las matrices A y B son de dimensión $m \times n$, tienen entradas en $\mathbb{Z}$, y las que son no nulas no son múltiplo de p.

3. Los tres bloques de la matriz satifacen las propiedades del lema 3.4.1.

4. Los exponentes $a_1, \ldots, a_m, b_1, \ldots, b_m$ son enteros no negativos tales que $a_{i+1} \leq a_i$, y si $a_{i+1} = a_i$, entonces $b_{i+1} \geq b_i$.

Esta última condición se consigue mediante permutaciones de filas y columnas, y se renuncia a la relación de divisibilidad que existía entre los f_i. La descomposición del módulo M viene dada por la siguiente proposición.

Proposición 3.6.1. *Existe una serie de transformaciones E-elementales sobre R que transforma la matriz*

$$U = \begin{pmatrix} [1] & 0 & 0 & 0 & 0 \\ 0 & [1] & 0 & 0 & 0 \\ 0 & 0 & [p^{a_{i+1}} f_i] & [x^{b_{i+1}} g_i(x)] & [p^{a_i} f_i] \cdot A + [x^{b_i} g_i(x)] \cdot B \end{pmatrix}$$

en la matriz

$$V = \begin{pmatrix} [f_i] & 0 & 0 & 0 & 0 \\ 0 & [g_i(x)] & 0 & 0 & 0 \\ 0 & 0 & [p^{a_{i+1}}] & [\delta_i x^{b_{i+1}}] & [p^{a_i} \bar{f}_i] \cdot A + [x^{b_i} g_i(0)] \cdot B \end{pmatrix},$$

donde $\delta_i = 1$ si $g_i(x) \neq 0$, $\delta_i = 0$ en otro caso, y en la matriz diagonal $[g_i(x)]$ eliminamos los ceros.

Demostración. Observemos que la matriz U se obtiene de nuestra matriz original mediante transformaciones del tipo X1, por lo que representa un módulo isomorfo. Supongamos

que $g_1(0) \neq 0$. Aplicamos dos veces la transformación X1 en la esquina superior izquierda, y permutamos columnas para conseguir la matriz

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & p^{a_1+1}f_1 & x^{b_1+1}g_1(x) & a_{11}f_1 + b_{11}x^{b_1}g_1(x) & \dots & * \\ 0 & 0 & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \end{pmatrix}.$$

Si multiplicamos esta matriz a la izquierda por $E_{32}(-x^{b_1+1})E_{31}(-p^{a_1+1})$ y a la derecha por $E_{13}(f_1)E_{14}(g_1(x))$ nos queda

$$\begin{pmatrix} 1 & 0 & f_1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & g_1(x) & 0 & \dots & 0 \\ -p^{a_1+1} & -x^{b_1+1} & 0 & 0 & a_{11}f_1 + b_{11}x^{b_1}g_1(x) & \dots & * \\ 0 & 0 & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \end{pmatrix}.$$

Solamente han intervenido las cuatro primeras filas y columnas. Como f_1 no es múltiplo de p, existen $u, u' \in \mathbb{Z}$ tales que $uf_1 + u'p^{a_1+1} = 1$. Igualmente, como $g_1(0) \in \mathbb{Z}/\langle p\rangle - \{0\}$, existen $v(x), v'(x) \in (\mathbb{Z}/\langle p\rangle)[x])$ tales que $v(x)g_1(x) + v'(x)x^{b_1+1} = 1$ en $(\mathbb{Z}/\langle p\rangle)[x])$. Además, $u \not\equiv 0 \pmod{p}$ y $v(0) \neq 0$ en $\mathbb{Z}/\langle p\rangle$. Realizamos las siguientes transformaciones sobre la matriz anterior:

1. A la primera fila le sumamos la tercera multiplicada por u'.

2. A la segunda fila le sumamos la tercera multiplicada por $v'(x)$.

3. A la primera columna le sumamos la tercera multiplicada por $-u$.

4. A la segunda columna le sumamos la cuarta multiplicada por $-v(x)$.

Teniendo en cuenta que $px = 0$ en R, resulta

$$\begin{pmatrix} 0 & -u'x^{b_1+1} & f_1 & 0 & a_{11}p^{a_1}f_1u' + b_{11}x^{b_1}g_1(x)u' & * \\ -v'(0)p^{a_1+1} & 0 & 0 & g_1(x) & a_{11}p^{a_1}f_1v'(0) + b_{11}x^{b_1}g_1(x)v'(x) & * \\ -p^{a_1+1} & -x^{b_1+1} & 0 & 0 & a_{11}p^{a_1}f_1 + b_{11}x^{b_1}g_1(x) & * \\ 0 & 0 & 0 & 0 & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Recordamos que f_1 y $g_1(0)$ son unidades en $\mathbb{Z}/\langle p\rangle$. Además, f_1 divide al primer sumando de los elementos que se encuentran a su derecha. Lo mismo ocurre con $g_1(x)$ con respecto a los segundos sumandos. Mediante transformaciones E-elementales entre columnas obtenemos la matriz

$$\begin{pmatrix} f_1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & g_1(x) & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & p^{a_1+1} & x^{b_1+1} & a_{11}p^{a_1}f_1 + b_{11}x^{b_1}g_1(0) & \dots & a_{1n}p^{a_1}f_1 + b_{1n}x^{b_1}g_1(0) \\ 0 & 0 & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & * & \dots & * \end{pmatrix}.$$

Si $g_1(x) = 0$, entonces únicamente se efectúa una transformación X1, y se realiza un proceso similar.

A continuación, se repite el algoritmo a la fila de la matriz que contiene los exponentes a_2, b_2, hasta a_m, b_m.

Análogamente, si $f_i = 0$, que se tiene para $i > r$, se efectúa solamente una transformación X1 y se sigue el procedimiento análogo. Por último, se permutan las columnas para conseguir la matriz V.

Nota 3.6.1. Esta proposición expresa M como suma directa de los módulos $\mathbb{Z}/\langle f_i\rangle$,

$(\mathbb{Z}/\langle p\rangle)[x]/\langle g_i(x)\rangle$, $i = 1, \ldots, m$ y el conúcleo de la matriz

$$\left(\; [p^{a_i+1}], \;\; [\delta_i x^{b_i+1}], \;\; [p^{a_i}] \cdot A + [x^{b_i}] \cdot B \; \right).$$

Si $\delta_i = 0$, se deja para mantener la forma diagonal. En las matrices A y B se han incorporado las constantes f_i y $g_i(0)$. Las hipótesis de 3.6 siguen siendo válidas. El tratamiento posterior de la matriz de la derecha se puede hacer a través de los resultados de [NRSB75], objeto de un futuro trabajo.

Apéndice I

3.7 Ejemplo de Eisenbud

En este apartado aparecen detallados los cálculos de las descomposiciones primarias de los módulos que intervienen en 1.2.4, y que nos permiten distinguirlos. El proceso sigue los pasos de [Rut92]. Para algunos cálculos, usamos el programa *CoCoa* ([CNR98]).

- Descomposición de $N = \langle (x,0),(y,z)\rangle$ en $M = \langle (1,0),(0,1)\rangle$ sobre el anillo $\mathbb{Q}[x,y,z]$. En este caso, el anillo R es el cuerpo $\mathbb{Q}$ y tomamos $x_1 = x, x_2 = y, x_3 = z$. El primer paso es el cálculo de $Ann(M/N)$. Tenemos que $Ann(M/N) = (N : M) = \langle xz\rangle$. Como $Ann(M/N) \cap \mathbb{Q} = 0$, que es 0-primario, estamos en las condiciones del algoritmo MPDC. Dado que $dim_{\mathbb{Q}[x,y,z]}(Ann(M/N)) > 0$, hallamos i tal que $dim_{\mathbb{Q}[x_i]}(Ann(M/N) \cap \mathbb{Q}[x_i]) \neq 0$. Para $i = 1$ es claro que $\langle xz\rangle \cap \mathbb{Q}[x] = 0$, y $dim_{\mathbb{Q}[x]}(0) > 0$. Sea $\mathfrak{p} = 0 \subset \mathbb{Q}[x]$. Hay que calcular la extensión de N en el anillo $\mathbb{Q}[x]_{(0)}[y,z]$. Como el anillo de coeficientes $\mathbb{Q}[x]_{(0)}$ es el cuerpo de fracciones $\mathbb{Q}(x)$, el polinomio x es unidad, y entonces $N^e = N\mathbb{Q}[x]_{(0)}[y,z] = \langle (1,0),(y,z)\rangle)$. La contracción a $\mathbb{Q}[x,y,z]$ es $N^{ec} = \langle (1,0),(y,z)\rangle \cap M$, que es igual a $\langle (1,0),(0,z)\rangle$. Existe un $g \in \mathbb{Q}[x] - 0$ tal que $N = (N + gM) \cap N^{ec}$. Es fácil ver que se tiene para $g = x$. Definimos $N' = N + gM = \langle (x,0),(y,z),(0,x)\rangle)$. Se tiene que $Ann(M/N') = \langle x\rangle$, que es maximal en $\mathbb{Q}[x]$. Entonces, el algoritmo continúa con el cálculo de la descomposición primaria de N' en $\mathbb{Q}[x,y,z]$ y la de N^{ec} en $\mathbb{Q}[x]_{(0)}[y,z]$.

Descomposición primaria de $N_1 = \langle(1,0),(0,z)\rangle)$ en $M_1 = \langle(1,0),(0,1)\rangle)$ sobre el anillo $\mathbb{Q}[x]_{(0)}[y,z]$. En este caso, $Ann(M_1/N_1) = \langle z\rangle$ y $dim\langle z\rangle > 0$. Hay que encontrar una variable x_i tal que $\langle z\rangle \cap \mathbb{Q}[x]_{(0)}[x_i]$ tenga dimensión no nula. Vemos que $\langle z\rangle \cap \mathbb{Q}[x]_{(0)}[y] = (0)$, y entonces y es la variable buscada. El ideal primo en donde hay que localizar es 0. Calculamos el ideal extendido de N_1 en $\mathbb{Q}[x]_{(0)}[y]_{(0)}[z]$. Se tiene que $N_1^e = \langle(1,0),(0,z)\rangle$, y $N_1^{ec} = N_1$. Por ello, el valor de g_1 tal que $N_1 = (N_1 + g_1M_1) \cap M_1$ puede ser $g_1 = 1$ y $N_1 + g_1M_1 = M_1$. Entonces hay que calcular la descomposición primaria de $\langle(1,0),(0,z)\rangle$ en $\langle(1,0),(0,1)\rangle$ sobre el anillo $\mathbb{Q}[x]_{(0)}[y]_{(0)}[z]$, y contraerla.

Como $\langle z\rangle$ es maximal en $\mathbb{Q}[x]_{(0)}[y]_{(0)}[z]$, que es un DIP, es un módulo primario. La contracción a $\mathbb{Q}[x]_{(0)}[y,z]$ es $\langle(1,0),(0,z)\rangle$, y por tanto, $\langle(1,0),(0,z)\rangle$ es un módulo $\langle z\rangle$-primario en $\mathbb{Q}[x,y,z]^2$.

Descomposición primaria de $N_2 = \langle(x,0),(y,z),(0,x)\rangle$ en $M_2 = \langle(1,0),(0,1)\rangle$ sobre el anillo $\mathbb{Q}[x,y,z]$. Repitiendo la secuencia de pasos anteriores, vemos en primer lugar que $Ann(M/N) = \langle x\rangle$. En $\mathbb{Q}[y]$, $\langle x\rangle \cap \mathbb{Q}[y] = 0$, de dimensión mayor que cero. El ideal en el que localizamos es 0, y $N_2^e = N_2\mathbb{Q}[y]_{(0)}[x,z] = \langle(x,0),(1,y^{-1}z),(0,x)\rangle$. La contracción nos da que $N_2^{ec} = N_2^e \cap M_2 = N_2$. En tal caso, $g = 1$. De forma análoga al cálculo anterior, se tiene que N_2 es $\langle x\rangle$-primario en M_2.

- Descomposición de $N = \langle(x,y),(0,z)\rangle$ en $M = \langle(1,0),(0,1)\rangle$ sobre el anillo $\mathbb{Q}[x,y,z]$. Por simetría con el caso anterior, resulta que $N = \langle(z,0),(x,y),(0,z)\rangle \cap \langle(x,0),(0,1)\rangle$.

3.8 Ejemplo de Hillman

Se trata de calcular la descomposición primaria del módulo $N = \langle (x^2 - x + 1, 0), (2x + 1, 5x^2 - 9x + 5) \rangle$ en $M = \langle (1,0), (0,1) \rangle$ sobre el anillo $\mathbb{Z}[x]$. Aplicamos el algoritmo MPD.

Para el cálculo de $Ann(M/N)$, tenemos la siguiente cadena de igualdades:

$$Ann(M/N) = (N : M) = (N : (1,0)) \cap (N : (0,1)),$$

y $N : (1,0)$ se obtiene mediante la 'división' de una base de $N \cap (1,0)R$ por el vector $(1,0)$. Análogamente conseguimos una base de $N : (0,1)$. Como resultado final, queda que $Ann(M/N) = \langle (5x^2 - 9x + 5)(x^2 - x + 1) \rangle$. Esto se podía haber obtenido a partir de un resultado de [BE77] que nos dice que en este caso $Ann(M/N) = F_0(M/N) : F_1(M/N)$. Es claro que $Ann(M/N) \cap \mathbb{Z} = (0)$, y $dim_{\mathbb{Z}}(0) \neq 0$. Hay que proceder ahora al cómputo de $N^{ec} = N\mathbb{Z}_{(0)}[x] \cap M$. Por un resultado de [Rut92], $N = N\mathbb{Z}_{(0)}[x] \cap M = NR_s[x] \cap M$, con s el mínimo común múltiplo de los coeficientes líder de una base de Gröbner de N. Tenemos que con respecto al orden TOP y $\mathbf{e}_1 < \mathbf{e}_2$, una base es $G = \{(x^2 - x + 1, 0), (2x + 1, 5x^2 - 9x + 5)\}$. Tomamos $s = 5$. Queda entonces

$$N^{ec} = NR_5[x] \cap M = (N, (5t - 1, 0), (0, 5t - 1))R[x,t] \cap M.$$

Con respecto a TOP, y $x < t$ (orden de eliminación), una base de Gröbner está formada por los elementos

$\mathbf{f}_1 = (x^2 - x + 1, 0)$

$\mathbf{f}_2 = (2x + 1, 5x^2 - 9x + 5)$

$\mathbf{f}_3 = (5t - 1, 0)$

$\mathbf{f}_4 = (0, 5t - 1)$

$\mathbf{f}_5 = (2tx + t, tx + 5t + x^2 - 2x)$

$\mathbf{f}_6 = (3tx - 2t, tx^2 + 5tx + x^3 - 2x^2$

$\mathbf{f}_7 = (-tx + 2t + x, 2tx + 10t + 2x^2 - 4x)$

Por tanto, $N^{ec} = N$.

Existe $a \in \mathbb{Z} - (0)$ tal que $N = (N + aM) \cap N^{ec}$. Como $N = N^{ec}$, podemos tomar $a = 1$, $N + aM = \mathbb{Z}[x]^2$.

Hay que proceder al cálculo de la descomposición primaria de $N\mathbb{Z}_{(0)}[x] = N\mathbb{Q}[x]$ en $\mathbb{Q}[x]^2$. En este caso, se puede obtener fácilmente a partir de la forma normal de Smith, pues $\mathbb{Q}[x]$ es DIP. Sabemos que los primos asociados son $\mathfrak{p}_1 = (x^2 - x + 1)$ y $\mathfrak{p}_2 = (5x^2 - 9x + 5)$. La forma diagonal es

$$D = \begin{pmatrix} 1 & 0 \\ 0 & (5x^2 - 9x + 5)(x^2 - x + 1) \end{pmatrix}$$

La descomposición primaria de la matriz D tiene como matrices de presentación

$$D_2 = \begin{pmatrix} 1 & 0 \\ 0 & x^2 - x + 1 \end{pmatrix}, D_1 = \begin{pmatrix} 1 & 0 \\ 0 & 5x^2 - 9x + 5 \end{pmatrix}.$$

Las matrices de paso son

$$Q = \begin{pmatrix} 6/7x + 1 & -2x - 1 \\ -3/7x^2 + 1/7x & x^2 - x + 1 \end{pmatrix}$$

y

$$P = \begin{pmatrix} 1 & 0 \\ 15/7x^4 - 32/7x^3 + 24/7x^2 - 5/7x & 1 \end{pmatrix}.$$

Por tanto, las componentes primarias del módulo original tienen como matrices de presentación

$$Q_1 = P^{-1}D_1Q^{-1} = \begin{pmatrix} x^2 - x + 1 & 2x + 1 \\ a_{21}(x) & a_{22}(x) \end{pmatrix},$$

$$Q_2 = P^{-1}D_2Q^{-1} = \begin{pmatrix} x^2 - x + 1 & 2x + 1 \\ b_{21}(x) & b_{22}(x) \end{pmatrix},$$

con $a_{21}(x) = -15/7x^6 + 47/7x^5 - 8x^4 + 29/7x^3 - 5/7x^2$, $a_{22}(x) = -30/7x^5 + 7x^4 + 2x^3 - 33/7x^2 - 4x + 5$, $b_{21}(x) = -15/7x^6 + 47/7x^5 - 68/7x^4 + 57/7x^3 - 25/7x^2 + 4/7x$, $b_{22}(x) = -30/7x^5 + 7x^4 - 10/7x^3 - 13/7x^2 + 4/7x + 1$. Llamemos Q_1 y Q_2 a los módulos

generados por las columnas de estas matrices. Las componentes primarias buscadas son las contracciones de estos módulos a $\mathbb{Z}[x]^2$.

Veamos en primer lugar $Q_1^c = Q_1 \cap \mathbb{Z}[x]^2$. Si consideramos $S_1 = 7Q_1 \subset \mathbb{Z}[x]^2$, entonces $S_1^e = Q_1$ y $Q_1^c = S_1\mathbb{Q}[x] \cap \mathbb{Z}[x]^2$, y este módulo podemos calcularlo tal como hemos hecho antes. No apartamos un poco del método de Rutman, pero llegamos a los mismos resultados. Para hallar esta intersección, debemos tener en primer lugar una base de Gröbner de S_1, que tiene los elementos

$\mathbf{h}_1 = (49, -105x^4 + 224x^3 - 98x^2 - 91x + 70)$

$\mathbf{h}_2 = (0, 35x^2 - 63x + 35)$

$\mathbf{h}_3 = (49, 0)$.

El mínimo común múltiplo de los coeficientes líder es 735. Entonces $Q_1^c = (S_1, (735t - 1, 0), (0, 735t - 1)) \cap \mathbb{Z}[x]^2$. Esta expresión es calculable en $\mathbb{Z}[x, t]$, y nos queda al final que $Q_1^c = \langle (1, 0), (0, 5x^2 - 9x + 5) \rangle$.

Procedamos al cálculo de Q_2^c. Sea $Q_{21} = \langle (7(x^2 - x + 1), -15x^6 + 47x^5 - 68x^4 + 57x^3 - 25x^2 + 4x), (7(2x + 1), -30x^5 + 49x^4 - 10x^3 - 13x^2 + 4x + 7) \rangle$. Entonces $Q_2^c = Q_{21}\mathbb{Q}[x] \cap \mathbb{Z}[x]^2$. Como antes, precisamos una base de Gröbner de Q_{21} en $\mathbb{Z}[x]^2$. Si tomamos el orden TOP, tal base es

$\mathbf{h}_2 = (0, 7x^2 - 7x + 7)$,

$\mathbf{h}_3 = (-7x + 21, 15x^5 - 77x^4 + 117x^3 - 67x^2 + 5x + 7)$,

$\mathbf{h}_4 = (49, -28x - 56)$,

$\mathbf{h}_6 = (49x - 147, 196)$

El mínimo común múltiplo de los coeficientes de los términos de mayor grado es 420. Por tanto, $Q_2^c = (Q_{21}, (420t - 1, 0), (0, 420t - 1)) \cap \mathbb{Z}[x]^2$, y entonces $Q_2^c = ((49, -28x - 56), (0, x^2 - x + 1), (-x + 3, -4), (-21, 12x + 24)) = ((7, -4x - 8), (0, x^2 - x + 1), (-x + 3, -4)) = ((7, -4x - 8), (2x + 1, -x^2 - 3x - 1))$, como se comprueba fácilmente.

3.9 Ejemplo de Fox-Smythe

Sea $N = \langle (2x-1, 11x-11), (-5x+5, -x+2) \rangle$ submódulo de $M = \mathbb{Z}[x]^2$. Para el cálculo de la descomposición primaria de N en M, aplicamos el algoritmo de Rutman, como en los ejemplos anteriores. Se tiene que $Ann(M/N) = \langle 53x^2 - 105x + 53 \rangle$, que es un ideal primo $\mathfrak{p}$ en $\mathbb{Z}[x]$. Es claro que $Ann(M/N) \cap \mathbb{Z} = 0$. Hay que proceder al cálculo de $N^{ec} = N\mathbb{Z}[x]_{(0)} \cap M = N\mathbb{Z}[x]_a \cap M$, para un $a \in \mathbb{Z}[x]$ no nulo. Este valor se calcula como el mínimo común múltiplo de los coeficientes de los términos líder de una base de Gröbner de N. Entonces $a = 55$, y $N\mathbb{Z}[x]_a \cap M = (N\mathbb{Z}[x,t] + (at-1)\mathbb{Z}[x,t]^2) \cap M$. Efectuando estos cálculos resulta que $N^{ec} = N$. Como $N^e = N\mathbb{Z}[x]_{\mathfrak{p}}$ es $\mathfrak{p}$-primario en $\mathbb{Z}[x]^2_{\mathfrak{p}}$, tenemos que N es primario en M.

Apéndice II

En este apéndice se explicitan las matrices de presentación de los módulos de nudos de hasta 10 crúces que presentan iguales polinomios de Alexander. El anillo base es $R = \mathbb{Z}[x, x^{-1}]$. Esta información está basada en [BZ85] tabla I del Apéndice. El objetivo es diferenciarlos y como primer método, se calculan los ideales elementales. Si coinciden, se intenta verificar el carácter isomorfo de las presentaciones.

El cálculo de la matriz de Alexander se realiza a partir de la matriz de Seifert del nudo, según el teorema 8.8 de [BZ85]. Si V es una matriz de Seifert, entonces la matriz de Alexander de presentación del módulo es $M(x) = V^t - xV$. Estas matrices aparecen calculadas en la misma referencia, y las usamos como punto de partida. Sobre ellas, efectuamos operaciones X-elementales, hasta reducirlas a una matriz 2×2 o incluso 1×1. En este último caso, el polinomio que queda es el polinomio de Alexander, que notamos por $\Delta_1(x)$. La numeración de los nudos se hace según la tabla de [Rol76], y si K es el código del nudo, $M(K)$ identifica su matriz de Alexander.

Las siguientes parejas se diferencian por sus ideales elementales:

$$(8_9, 10_{155}),\quad (8_{18}, 9_{24}),\quad (8_{20}, 10_{140}),\quad (9_{28}, 10_{163}),\quad (9_{29}, 10_{163}),\quad (9_{38}, 10_{63}),$$
$$(9_{40}, 10_{59}),\quad (10_{40}, 10_{103}),\quad (10_{42}, 10_{75}),\quad (10_{65}, 10_{77}),\quad (10_{67}, 10_{74}),\quad (10_{87}, 10_{98}).$$

En los casos en que tienen iguales cadenas de ideales elementales probamos que los módulos son isomorfos.

1. $10_{67}, 10_{74}$

$$M(10_{67}) = \begin{pmatrix} 0 & x-2 \\ (2x-1)(-2+3x-2x^2) & 5 \end{pmatrix},$$
$$M(10_{74}) = \begin{pmatrix} 1-2x & 0 \\ 0 & 4-8x+7x^2-2x^3 \end{pmatrix}.$$

$F_1(M(10_{67})) = R, F_1(M(10_{74})) = \langle x+1, 3\rangle$. Se distinguen por sus ideales elementales.

2. $10_{103}, 10_{40}$

$$M(10_{103}) = \begin{pmatrix} 0 & 1-2x+2x^2 \\ -2+4x-5x^2+3x^3-x^4 & -x+3x^2-x^3 \end{pmatrix},$$
$$M(10_{40}) = (\Delta_1(x)).$$

$F_1(M(10_{103})) = \langle x+1, 5\rangle, F_1(M(10_{40})) = R$. Los ideales elementales distinguen los módulos.

3. $9_{38}, 10_{63}$

$$M(9_{38}) = \begin{pmatrix} 4x-4 & -3x^2+7x-5 \\ -3x^2+7x-5 & x^3-6x^2+9x-5 \end{pmatrix},$$
$$M(10_{63}) = \begin{pmatrix} 5x^2+x-5 & 2x-1 \\ -6x+10 & x^2-3x+3 \end{pmatrix}.$$

$F_1(M(9_{38})) = \langle x+1, 2\rangle, F_1(M(10_{63})) = \langle x^2+x+1, 2\rangle$. Los ideales elementales distinguen los módulos.

4. $8_{21}, 10_{136}$

$$M(8_{21}) = (\Delta_1(x)),$$
$$M(10_{136}) = (\Delta_1(x)).$$

Los módulos son isomorfos.

5. $10_{59}, 9_{40}$

$$M(10_{59}) = \left((x^2-x+1)(x^2-3x+1)^2 \right),$$
$$M(9_{40}) = \begin{pmatrix} -1+4x-5x^2+4x^3-x^4 & -x+3x^2-x^3 \\ 0 & 1-3x+x^2 \end{pmatrix}.$$

$F_1(M(10_{59})) = R, F_1(M(9_{40})) = \langle x^2-3x+1 \rangle$. Se distinguen por sus ideales elementales.

6. $10_{141}, 8_5$

$$M(10_{141}) = (\Delta_1(x)),$$
$$M(8_5) = (\Delta_1(x)).$$

Los módulos son isomorfos.

7. $10_{163}, 9_{28}, 9_{29}$

$$M(9_{28}) = \left((x^2-x+1)(x^4-4x^3+7x^2-4x+1)\right),$$
$$M(9_{29}) = \begin{pmatrix} 1-2x+2x^2 & 1-x+x^2-x^3 \\ -1+3x-4x^2+x^3 & -x+2x^2 \end{pmatrix},$$
$$M(10_{163}) = \begin{pmatrix} 2-2x & -1+x+x^2 \\ -27+40x-19x^2+6x^3-x^4 & 14-22x \end{pmatrix}.$$

$F_1(M(9_{28})) = R, F_1(M(9_{29})) = R, F_1(M(10_{163})) = \langle x^2-x+1, 2 \rangle$. De esta forma diferenciamos 10_{163}. Los módulos presentados por las matrices $M(9_{28})$ y $M(9_{29})$ son isomorfos, pues $PM(9_{29})Q = M(9_{28})$, con

$$P = \begin{pmatrix} -2x^2+6x+1 & 4x \\ 1-3x+4x^2-x^3 & 1-2x+2x^2 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & -1-5x+11x^2-15x^3+8x^4-2x^5 \\ 0 & 1 \end{pmatrix}.$$

Estas matrices se han obtenido al aplicar el método de descomposición primaria, y resultar matrices de equivalencia sobre el anillo $\mathbb{Q}[x, x^{-1}]$.

8. $8_{20}, 10_{140}$

$$\begin{aligned} M(8_{20}) &= \left((1-x+x^2)^2\right), \\ M(10_{140}) &= \begin{pmatrix} -1+x-x^2 & 0 \\ -2x & 1-x+x^2 \end{pmatrix} \end{aligned}$$

$F_1(M(8_{20})) = R, F_1(M(10_{140})) = (x^2-x+1, 2)$. Son distinguibles por sus ideales elementales.

9. $10_{65}, 10_{77}$ $F_1(10_{65}) = \langle x^2+x+1, 2\rangle, F_1(10_{77}) = R$. Son distinguibles por sus ideales elementales (ver [GVCJ93]).

10. $10_{87}, 10_{98}$

$$\begin{aligned} M(10_{87}) &= (\Delta_1(x)), \\ M(10_{98}) &= \begin{pmatrix} (-1+2x)(-1+x-x^2) & -5(1-x+x^2) \\ 0 & (-2+x)(1-x+x^2) \end{pmatrix}. \end{aligned}$$

$F_1(M(10_{87})) = R, F_1(M(10_{98})) = \langle x^2-x+1\rangle$. Son distinguibles por sus ideales elementales.

11. $9_{24}, 8_{18}$

$$\begin{aligned} M(9_{24}) &= (\Delta_1(x)), \\ M(8_{18}) &= \begin{pmatrix} (1-3x+x^2)(1-x+x^2) & 0 \\ 0 & (-1+x-x^2) \end{pmatrix}. \end{aligned}$$

$F_1(M(9_{24})) = R, F_1(M(8_{18})) = \langle x^2-x+1\rangle$. Son distinguibles por sus ideales elementales.

12. $8_{11}, 10_{147}$

$$\begin{aligned} M(8_{11}) &= \begin{pmatrix} \Delta_1(x) \end{pmatrix}, \\ M(10_{147}) &= \begin{pmatrix} 2-4x & 1-x-x^2 \\ -4+9x-2x^2 & -3+4x \end{pmatrix}. \end{aligned}$$

$F_1(M(8_{11})) = R, F_1(M(10_{147})) = R$. Los ideales elementales coinciden. Además, los módulos son isomorfos, pues $E_{21}(-2)M(10_{147})E_{12}(1) = \begin{pmatrix} 4x-2 & x^2-3x+1 \\ -2x^2+x & x-1 \end{pmatrix}$. Reduciendo sobre $x-1$ obtenemos una unidad en la posición $(1,2)$, y por tanto el módulo es isomorfo a $M(8_{11})$.

13. $8_{10}, 10_{143}$

$$\begin{aligned} M(8_{10}) &= (\Delta_1(x)), \\ M(10_{143}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

14. $6_1, 9_{46}$

$$\begin{aligned} M(6_1) &= (\Delta_1(x)), \\ M(9_{46}) &= \begin{pmatrix} 7 & 2x-1 \\ x-2 & 0 \end{pmatrix}. \end{aligned}$$

Los ideales elementales coinciden. Además, los módulos son isomorfos. Sean $K_1 = ((7, x-2), (2x-1, 0)) \subset R^2$, y $K_2 = (2x-1)(x-2) \subset R$. Consideremos la aplicación $\varphi : R^2/K_1 \to R/K_2$ definida por $\varphi(\mathbf{e}_1 + K_1) = (x-2) + K_2$, $\varphi(\mathbf{e}_2 + K_1) = (4x-9) + K_2$. El origen de esta definición viene de considerar los morfismos entre estos módulos, que asigna $\mathbf{e}_1 + K_1$ en $a + K_2$, $\mathbf{e}_2 + K_1$ en $b + K_2$. Se obtiene entonces que $a = \lambda_2(x-2)$, $b = \lambda_1(2x-2) - 7\lambda_2$, con $\lambda_1, \lambda_2 \in R$. Si se considera el ideal $(z(x-2), y(2x-1) - 7z, 2x^2 - 5x + 2) \cap \mathbb{Z}[y,z]$, se obtiene el ideal generado por $-3yz + 7z^2$. Para $y = 2, z = 1$ se obtienen los valores del morfismo elegido. Es fácil ver que $1 = 4(-2x+1) - (4x-9)$, con lo que garantizamos el carácter sobreyectivo de φ. Sea $\psi : R/K_2 \to R^2/K_1$ definido por $\psi(1 + K_2) = (-5, -2) + K_1$. φ y ψ están bien definidos. Se tiene que $\psi(\varphi(\mathbf{e}_1 + K_1)) = (1,0) + K_1$ y $\psi(\varphi(\mathbf{e}_2 + K_1)) = (0,1) + K_1$. Por tanto, φ es inyectivo.

15. $10_{165}, 9_{15}$

$$\begin{aligned} M(10_{165}) &= \begin{pmatrix} 1-2x & -1+4x-x^2 \\ -2+4x-2x^2 & -2x+x^2 \end{pmatrix}, \\ M(9_{15}) &= (\Delta_1(x)). \end{aligned}$$

Los ideales elementales coinciden. Por columnas, se tiene que el ideal $\langle -2+4x-2x^2, -2x+x^2 \rangle$ contiene a x^2, que es unidad en el anillo. Por tanto, se puede reducir a una matriz de orden 1×1.

16. $10_{130}, 7_5$

$$\begin{aligned} M(10_{130}) &= (\Delta_1(x)), \\ M(7_5) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

17. $8_8, 10_{129}$

$$\begin{aligned} M(8_8) &= (\Delta_1(x)), \\ M(10_{129}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

18. $10_{131}, 8_{14}, 9_8$

$$\begin{aligned} M(10_{131}) &= (\Delta_1(x)), \\ M(8_{14}) &= (\Delta_1(x)), \\ M(9_8) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

19. $10_{12}, 10_{54}$

$$\begin{aligned} M(10_{12}) &= (\Delta_1(x)), \\ M(10_{54}) &= \begin{pmatrix} x-5 & -x^2+x-1 \\ -3-3x+9x^2-8x^3-2x^4 & -1+x-x^3 \end{pmatrix}. \end{aligned}$$

$F_1(M(10_{12})) = R, F_1(M(10_{54})) = R$. Los ideales elementales coinciden. Los módulos son isomorfos, pues si a la segunda fila se le suma la primea multiplicada por $-(x+1)$ se obtiene la matriz $\begin{pmatrix} x-5 & -x^2+x-1 \\ 2+x+8x^2-8x^3-2x^4 & x \end{pmatrix}$, y tenemos una unidad en la posición $(2,2)$.

20. $10_{52}, 10_{23}$

$$\begin{aligned} M(10_{52}) &= (\Delta_1(x)), \\ M(10_{23}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

21. $10_{56}, 10_{25}$

$$\begin{aligned} M(10_{56}) &= \begin{pmatrix} 4-6x+3x^2 & -7+13x-14x^2+5x^3 \\ -2+4x-3x^2+x^3 & 3-7x+9x^2-5x^3+x^4 \end{pmatrix}, \\ M(10_{25}) &= (\Delta_1(x)). \end{aligned}$$

$F_1(M(10_{56})) = R, F_1(M(10_{25})) = R$. Los ideales elementales coinciden. Vamos a ver que presentan módulos isomorfos, considerando las siguientes transformaciones sobre $A = M(10_{56})$.

$$A_1 = E_{21}(1)AE_{12}(-x) = \begin{pmatrix} 3x^2-6x+4 & 2x^3-8x^2+9x-7 \\ x^3-2x+2 & -3x^2+4x-4 \end{pmatrix}.$$

Mediante una X1-transformación, y una operación elemental por columnas, llegamos a

$$A_3 = \begin{pmatrix} 3x^2-6x+4 & 2x^3-8x^2+9x-7 & 0 \\ x^3-2x+2 & -3x^2+4x-4 & 0 \\ 0 & x & 1 \end{pmatrix}.$$

Entonces

$$\begin{aligned} A_4 &= E_{12}(-2)E_{13}(-(2x^2-8x+9))E_{23}(-(-3x+4))A_3 \\ &= \begin{pmatrix} -2x^3+3x^2-2x & 1 & -2x^2+2x-1 \\ -7x^3+12x^2-10x+2 & 0 & -8x^2+11x-8 \\ 2x^4-3x^3+2x^2 & 0 & 2x^3-2x^2+x+1 \end{pmatrix}. \end{aligned}$$

Por transformaciones elementales entre columnas, hacemos ceros en la primera fila, y eliminamos entonces la primera fila y segunda columna, mediante una X1-transformación. Queda entonces

$$A_5 = \begin{pmatrix} -7x^3+12x^2-10x+2 & -8x^2+11x-8 \\ 2x^4-3x^3+2x^2 & 2x^3-2x^2+x+1 \end{pmatrix}.$$

Si calculamos una base de Gröbner del ideal formado por los elementos de la segunda fila, vemos que generan el total. Entonces podemos obtener una unidad en la segunda fila, y pivotar sobre él para obtener una presentación igual a la de $M(10_{56})$.

22. $10_{10}, 10_{164}$

$$\begin{aligned} M(10_{10}) &= (\Delta_1(x)), \\ M(10_{164}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

23. $10_{162}, 10_{20}$

$$\begin{aligned} M(10_{162}) &= \begin{pmatrix} -1-x+x^2 & 3-x \\ -5x+3x^2 & 3+3x-3x^2 \end{pmatrix}, \\ M(10_{20}) &= (\Delta_1(x)). \end{aligned}$$

Tenemos que $F_1(M(10_{162})) = R, F_1(M(10_{20})) = R$. Los ideales elementales coinciden, y los módulos son isomorfos, pues $x \in \langle -5x+3x^2, 3+3x-3x^2 \rangle$, por lo que añadiendo una columna de ceros podemos obtener una unidad, y pivotar sobre ese elemento para conseguir una matriz X-equivalente a $M(10_{20})$.

24. $10_{34}, 10_{135}$

$$\begin{aligned} M(10_{34}) &= (\Delta_1(x)), \\ M(10_{135}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

25. $9_2, 7_4$

Este es un ejemplo que aparece en [CF77]. Sus módulos son isomorfos.

26. $8_3, 10_1$

$$\begin{aligned} M(8_3) &= (\Delta_1(x)), \\ M(10_1) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

27. $10_{37}, 10_{28}$

$$\begin{aligned} M(10_{37}) &= (\Delta_1(x)), \\ M(10_{28}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

28. $10_{24}, 10_{18}$

$$\begin{aligned} M(10_{24}) &= (\Delta_1(x)), \\ M(10_{18}) &= \begin{pmatrix} 2-4x+4x^2-2x^3 & -x \\ x-2x^2+2x^3 & -2+3x \end{pmatrix}. \end{aligned}$$

Como x es una unidad en R, los módulos son isomorfos.

29. $10_{68}, 10_{31}$

$$\begin{aligned} M(10_{68}) &= \begin{pmatrix} 3-3x & -1+2x \\ -2+x^3 & 2-4x+3x^2-2x^3 \end{pmatrix}, \\ M(10_{31}) &= \begin{pmatrix} -2+9x-10x^2+4x^3 & -x \\ -6+8x-4x^2 & 2-x \end{pmatrix}.. \end{aligned}$$

Como antes, el elemento de la posición $(1,2)$ nos permite establecer que $M(10_{31}) \simeq (\Delta_1(x))$. Como $F_1(M(10_{68})) = R, F_1(M(10_{31})) = R$, efectuamos transformaciones sobre $M(10_{68})$. La matriz $E_{12}(2)E_{21}(1)E_{12}(-x)M(10_{68})$ tiene una unidad en la posición $(1,2)$, por lo que son módulos isomorfos.

30. $7_6, 10_{133}$

$$\begin{aligned} M(7_6) &= (\Delta_1(x)), \\ M(10_{133}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

31. $10_{132}, 5_1$

$$\begin{aligned} M(10_{132}) &= (\Delta_1(x)), \\ M(5_1) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

32. $8_9, 10_{155}$

$$\begin{aligned} M(8_9) &= (\Delta_1(x)), \\ M(10_{155}) &= \begin{pmatrix} 1-2x+x^2-x^3 & -2+2x-x^2 \\ 0 & -1+x-2x^2+x^3 \end{pmatrix}. \end{aligned}$$

Como $F_1(M(8_9)) = R$, $F_1(M(10_{155})) = \langle x+1, 5 \rangle$, los ideales elementales distinguen los módulos.

33. $10_{127}, 10_{150}$

$$\begin{aligned} M(10_{127}) &= (\Delta_1(x)), \\ M(10_{150}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

34. $8_{16}, 10_{156}$

$$\begin{aligned} M(8_{16}) &= (\Delta_1(x)), \\ M(10_{156}) &= (\Delta_1(x)). \end{aligned}$$

Los módulos son isomorfos.

35. $10_{149}, 9_{20}$

$$\begin{aligned} M(10_{149}) &= \begin{pmatrix} -1+2x-2x^2+x^3 & x^2 \\ 2-3x+2x^2 & (x-1)^3 \end{pmatrix}, \\ M(9_{20}) &= (\Delta_1(x)). \end{aligned}$$

En $\mathbb{Z}[x, x^{-1}]$, el módulo $M(10_{149})$ es isomorfo a $(\Delta_1(x))$, pues tiene una unidad del anillo en la posición $(1, 2)$.

36. $10_{42}, 10_{75}$

$$\begin{aligned} M(10_{42}) &= (\Delta_1(x)), \\ M(10_{75}) &= \begin{pmatrix} -8+28x-36x^2+24x^3-8x^4+x^5 & 3 \\ 3-9x+9x^2-5x^3+x^4 & -1-x \end{pmatrix}. \end{aligned}$$

$F_1(M(10_{42})) = R, F_1(M(10_{75})) = \langle x+1, 3 \rangle$. Los ideales elementales distinguen a los módulos.

Bibliografía

[AL94] W.W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, 1994.

[AM80] M.F. Atiyah and I.G. Macdonald. *Introducción al Álgebra Conmutativa*. Reverté, Barcelona, 1980.

[AW92] W.A. Adkins and S.H. Weintraub. *Algebra. An Approach via Module Theory*, volume 136 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[BE77] D.A. Buchsbaum and D. Eisenbud. What annihilates a module? *J. Algebra*, 47:231–243, 1977.

[Bou72] N. Bourbaki. *Commutative Algebra*. Addison-Wesley, Reading, Massachusetts, 1972.

[BZ85] G. Burde and H. Zieschang. *Knots*, volume 5 of *de Gruyter Studies in Mathematics*. Walter de Gruyter, Berlin and New York, 1985.

[CF77] R.H. Crowell and R.H. Fox. *Introduction to Knot Theory*, volume 57 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms*. Springer-Verlag, New York, 1992.

[CNR98] A. Capani, G. Niesi, and L. Robbiano. Cocoa: a system for doing computations in commutative algebra. *Available via anonymous ftp from: cocoa.dima.unige.it*, 1998.

[Coh66] P.M. Cohn. On the structure of the GL_2 of a ring. *Inst. Hautes Études Sci. Publ. Math.*, 30:365–413, 1966.

[Eis95] D. Eisenbud. *Commutative algebra. With a view toward algebraic geometry.*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[FS64] R.H. Fox and N. Smythe. An ideal class invariant of knots. *Proc. Amer. Math. Soc.*, 15:707–709, 1964.

[GTZ88] P. Giani, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomials ideals. *J. Symb. Comput.*, 6:149–167, 1988.

[GVCJ93] J. Gago-Vargas and F. Castro-Jiménez. Gröbner bases and the comparison of knots and links. Prepublicaciones de la Univ. de Sevilla, Depto. de Álgebra, núm. 24, 1993.

[Hil86] J.A. Hillman. Knot modules and the elementary divisor theorem. *J. of Pure and Applied Algebra*, 40:115–124, 1986.

[Kan86] T. Kanenobu. Infinitely many knots with the same polynomial invariant. *Trans. Amer. Math. Soc.*, 97:158–162, 1986.

[KRK84] A. Kandri-Rody and D. Kapur. Algorithms for computing Gröbner bases of polynomial ideals over various Euclidean rings. In *Proceedings of EUROSAM 84*, volume 174 of *Lect. Notes in Computer Science*, pages 195–206. Springer-Verlag, 1984.

[Kun85] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, Boston, 1985.

[Lev81a] L.S. Levy. Mixed modules over $\mathbb{Z}G$, G cyclic of prime order, and over related Dedekind pullbacks. *J. Algebra*, 71:62–114, 1981.

[Lev81b] L.S. Levy. Modules over pullbacks and subdirect sums. *J. Algebra*, 71:50–61, 1981.

[Lic98] W.B.R. Lickorish. *An introduction to knot theory*, volume 175 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.

[LS92] A. Logar and B. Sturmfels. Algorithms for the Quillen-Suslin theorem. *J. Algebra*, 145:231–239, 1992.

[LS96] R.C. Laubenbacher and B. Sturmfels. A normal form algorithm for modules over $k[x,y]/\langle xy\rangle$. *J. Algebra*, 184:1001–1024, 1996.

[Man97] S. Mandal. *Projective Modules and Complete Intersections*, volume 1672 of *Lecture Notes in Mathematics*. Springer-Verlag, New York, 1997.

[Mat80] H. Matsumura. *Commutative Algebra*. Benjamin/Cummings, Reading, 1980.

[NR69] 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. *Math. USSR Izv.*, 3:65–86, 1969.

[NRSB75] L.A. Nazarova, A.V. Roiter, V.V. Sergeichuk, and V.M. Bondarenko. Application of modules over a dyad for the classifcation of finite p-groups possesing an Abelian subgroup of index p and of pairs of mutually annihilating operators. *J. Soviet Math.*, 3:636–653, 1975.

[Ort59] V. Ortiz. Sur une certaine decomposition canonique d'un ideal en intersection d'ideaux primaires dans un anneau noetherien commutatif. *C. R. Acad. Sci. Paris*, 248:3385–3387, 1959.

[Par95] H. Park. *A Computational Theory of Laurent Polynomial Rings and Multidimensional FIR Systems*. PhD thesis, University of California at Berkeley, 1995.

[PW95] H. Park and C. Woodburn. An algorithmic proof of Suslin's stability theorem for polynomial rings. *J. Algebra*, 178:277–298, 1995.

[Rei83] K. Reidemeister. *Knot Theory (Translation of Knotentheorie).* BSC Associates, Idaho, 1983.

[Rol76] D. Rolfsen. *Knots and Links.* Publish or Perish, 1976.

[Rut92] E.W. Rutman. Gröbner bases and primary decomposition of modules. *J. Symbolic Computation*, 14:483–503, 1992.

[Sna47a] E. Snapper. Polynomial matrices in one variable, differential equations and module theory. *Amer. J. of Mathematics*, 69:299–326, 1947.

[Sna47b] E. Snapper. Polynomial matrices in several variables. *Amer. J. of Mathematics*, 69:622–652, 1947.

[Sus77] A.A. Suslin. On the structure of the special linear group over polynomial rings. *Math. USSR, Izv.*, 11:221–238, 1977.

[Vas98] W.V. Vasconcelos. *Computational Methods in Commutative Algebra and Algebraic Geometry*, volume 2 of *Algorithms and Computation in Mathematics.* Springer-Verlag, Berlin, 1998.

[VS76] L.N. Vaserstein and A.A. Suslin. Serre's problem on projective modules over polynomial rings and algebraic K-theory. *Math. USSR, Izv.*, 40:937–1001, 1976.

[ZS75] O. Zariski and P. Samuel. *Commutative Algebra. Vol. I*, volume 28 of *Graduate Texts in Mathematics.* Springer-Verlag, Heidelberg, 1975.

Manuel Jesús Gago Vargas

Presentación de módulos. Tercera de exhibidad de Sufín en $\mathbb{Z}[\bar{x}]$.

Sobresaliente cum laude

por unanimidad

5 Octubre 99