Divisores Libres y Configuraciones de Hiperplanos





Sixto José Martínez Gan

Trabajo de fin de grado de Matemáticas
Universidad de Zaragoza

Junio de 2025

Resumen

Índice general

Resumen III

1. Introducción 1

2. Módulos 3
2.1. Conceptos básicos . . . 3
2.2. Homomorfismos . . . 4

3. Bases de Gröbner y Sicigias 9
3.1. Órdenes monomiales . . . 10
3.2. Bases de Gröbner . . . 14
3.3. Sicigias . . . 16

4. El Criterio de Saito 19
4.1. Producto Exterior . . . 20
4.2. Demostración del Criterio de Saito . . . 22
4.2.1. El papel del rango . . . 22
4.2.2. Comienzo de la demostración . . . 24
4.2.3. Der(f) libre implica $\det\left(\delta_1, \delta_2, \ldots, \delta_n\right) = uf$ . . . 24
4.2.4. $\det\left(\delta_1, \delta_2, \ldots, \delta_n\right) = uf$ implica que Der(f) es libre . . . 26

A. Un ejemplo completo de cálculo 29
A.1. A mano . . . 29
A.2. Con ordenador . . . 33

B. Demostración del Criterio de Buchberger 35

Capítulo 1

Introducción

Supongamos que tenemos un polinomio en varias variables, por ejemplo $f(x,y,z) := x^2 + y^2 + xz$, y estamos trabajando intensivamente con combinaciones lineales polinómicas de sus derivadas parciales de primer orden, es decir, expresiones como

$$y^2\frac{\partial f}{\partial x} + xy\frac{\partial f}{\partial y} - x^3\frac{\partial f}{\partial z}, \quad \frac{\partial f}{\partial x} - \frac{\partial f}{\partial z}, \quad \text{o} \quad \left(x^2 - y^2\right)\frac{\partial f}{\partial x} + (xy - yz)\frac{\partial f}{\partial y}.$$

Entre las muchas preguntas que podemos hacernos se encuentra saber cuáles son aquellas cuyo valor es un múltiplo escalar de la propia f. Por ejemplo,

$$x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y} + z\frac{\partial f}{\partial z} = x\cdot(2x+z) + y\cdot 2y + z\cdot x = 2x^2 + 2y^2 + 2xz = 2f.$$

¿Cuáles son estas? ¿Qué estructura siguen? ¿Y cómo podemos calcularlas?

¿Cómo de larga debería ser esta introducción? ¿Tiene que «desvelar» ya los funcionamientos o solo plantear los problemas que queremos resolver?

Capítulo 2

Módulos

2.1. Conceptos básicos

Los conjuntos con los que trabajaremos son una generalización de los espacios vectoriales donde los coeficientes pertenecen a un anillo en vez de a un cuerpo. A esta generalización la llamamos módulo. En este capítulo veremos solo algunas de las propiedades y definiciones necesarias para nuestros propósitos. Sin embargo, la teoría de módulos se extiende mucho más allá de esta exigua presentación, por lo que recomendamos que se consulte un texto introductorio como [3] o [4].

Definición 2.1. Sea A un anillo y M un conjunto sobre el que hay definidas dos operaciones: una suma, $+ : M \times M \to M$; y una multiplicación escalar, $\cdot : A \times M \to M$. El conjunto M es un *A-módulo* si

- $(M, +)$ es un grupo abeliano y
- se cumple que $\begin{cases} (a+b)\cdot m = a\cdot m + b\cdot m, \\ a\cdot(m+n) = a\cdot m + a\cdot n, \\ (ab)\cdot m = a\cdot(b\cdot m) \ \text{ y} \\ 1\cdot m = m \end{cases}$ para todo a y b en A y m y n en M.

Ejemplo 2.2. El producto cartesiano $\mathbb{Z}^n$ es un $\mathbb{Z}$-módulo con las operaciones naturales. En general, dado cualquier anillo A, A^n es también un A-módulo con las operaciones componente a componente. Trivialmente, el propio A es un A-módulo.

Un módulo sobre un cuerpo es un espacio vectorial pero no todas las propiedades de espacios vectoriales se trasladan a módulos.

A lo largo de este trabajo será de gran importancia el anillo de polinomios $K\left[x_1, x_2, \ldots, x_n\right]$ sobre un cuerpo K, al que denotaremos $K[\mathbf{x}]$. Sobre todo porque a partir de este construiremos el conjunto de vectores de polinomios $K[\mathbf{x}]^n$, que es un $K[\mathbf{x}]$-módulo.

De aquí en adelante, para todos los resultados, daremos por sentado que A sea un anillo y M un A-módulo.

Definición 2.3. Un subconjunto no vacío $N \subseteq M$ se dice que es un *A-submódulo* de M si es un A-módulo con las operaciones de M restringidas.

Ejemplo 2.4. Si pensamos en $\mathbb{Z}$ como un $\mathbb{Z}$-módulo, $2\mathbb{Z}$ es un $\mathbb{Z}$-submódulo. Esto debería recordarnos a los ideales de $\mathbb{Z}$. De hecho, un ideal de un anillo A es un A-submódulo del propio A.

Consideremos el $\mathbb{R}[x, y]$-módulo $\mathbb{R}[x, y]^2$ y tomemos un par de elementos, como pueden ser $\mathbf{u} := \begin{pmatrix} x^2y + xy^2 \\ x + y \end{pmatrix}$

y $\mathbf{v} := \begin{pmatrix} y^3 \\ x^3 \end{pmatrix}$. El conjunto de combinaciones lineales de estos vectores,

$$\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{R}[x,y]} := \{ a\mathbf{u} + b\mathbf{v} \,|\, a, b \in \mathbb{R}[x,y] \} = \left\{ \begin{pmatrix} a\left(x^2y + xy^2\right) + by^3 \\ a(x+y) + bx^3 \end{pmatrix} |\, a, b \in \mathbb{R}[x,y] \right\}.$$

es un $\mathbb{R}[x,y]$-submódulo. De hecho, a este tipo de módulos los llamaremos submódulos generados por $\mathbf{u}$ y $\mathbf{v}$.

Definición 2.5. Sea N un A-submódulo de M y G un subconjunto cualquiera de N. Diremos que N *está generado por* G y lo denotaremos como $N = \langle G \rangle_A$ si

$$N = \left\{ a_1 g_1 + a_2 g_2 + \cdots + a_k g_k \,\middle|\, a_i \in A, g_i \in G, k \in \mathbb{N} \right\}.$$

En el caso que exista algún $G = \left\{ g_1, g_2, \ldots, g_n \right\}$ de forma que $N = \langle G \rangle_A$ diremos que N está finitamente generado y lo escribiremos como $N = \langle g_1, g_2, \ldots, g_n \rangle_A$. Cuando el anillo con el que estamos trabajando esté claro, omitiremos el subíndice.

Análogamente a los espacios vectoriales, existe un concepto de base.

Definición 2.6. Diremos que $B \subseteq M$ es una *base* de M si $M = \langle B \rangle$ y además, para cada m existe una única representación como combinación lineal de elementos de B.

Definición 2.7. Sea N un A-submódulo de M. Diremos que N es *libre* si admite una base.

Por último, damos las dos nociones más básicas relacionadas con la divisibilidad en los módulos.

Definición 2.8. Sean m y l dos elementos de un A-módulo M. Diremos que *m divide a l* si existe $a \in A$ de forma que $am = l$.

Definición 2.9. Sea N un A-submódulo de M y $\sim$ la siguiente relación de equivalencia sobre M: $m \sim m' \Leftrightarrow m - m' \in N$. Definimos el *cociente de un módulo por un submódulo* como ${}^{M}\!/_{N} := {}^{M}\!/_{\sim}$, que es un A-módulo con las operaciones heredadas. Los elementos de este cociente se denotarán por $m + N$.

2.2. Homomorfismos

Definición 2.10. Sean M y N dos A-módulos. Una aplicación $\phi : M \longrightarrow N$ se dice que es un *homomorfismo de A-módulos* si respeta las operaciones de módulo, es decir, si

- $\phi\left(m + m'\right) = \phi(m) + \phi\left(m'\right)$ y
- $\phi(am) = a\phi(m)$

para todo $m, m' \in M$ y $a \in A$. En ocasiones, nos referiremos a los homomorfismos de A-módulos como a aplicaciones A-lineales.

Ejemplo 2.11. La inclusión de $\mathbb{Z}^n$ en $\mathbb{Q}^n$ es un homomorfismo de $\mathbb{Z}$-módulos, sin embargo, no es un homomorfismo de $\mathbb{Q}$-módulos ya que $\mathbb{Z}^n$ no es un $\mathbb{Q}$-módulo. Por otro lado, la aplicación $\phi : \mathbb{C}[x,y] \longrightarrow \mathbb{C}$ que envía a cada polinomio $p(x,y)$ a $p(0,1)$ es un homomorfismo de $\mathbb{C}$-módulos.

Lema 2.12. *Sean dos A-módulos M y N y un homomorfismo ϕ de A-módulos. El núcleo* $\ker\phi$ *es un submódulo de M y la imagen* $\operatorname{im}\phi$ *es un submódulo de N.*

Con estas definiciones, ya podemos empezar a expresar los objetos que nos encontrábamos al principio en un lenguaje más formal. Para abreviar la notación, escribiremos ∂_i cuando nos refiramos a la aplicación

$$\begin{aligned} K[\mathbf{x}] &\xrightarrow{\partial_i} K[\mathbf{x}] \\ p &\longmapsto \frac{\partial p}{\partial x_i}. \end{aligned}$$

Observamos que ∂_i no es un homomorfismo de $K[\mathbf{x}]$-módulos.

Con estas aplicaciones, pasamos a definir el módulo de derivaciones, el conjunto de todas las posibles combinaciones lineales de derivadas parciales:

$$\mathrm{Der}(K[\mathbf{x}]) := \left\{ a_1\partial_1 + a_2\partial_2 + \cdots + a_n\partial_n \,\middle|\, a_i \in K[\mathbf{x}]\ \forall i \right\}.$$

Es un $K[\mathbf{x}]$-módulo. Y para cada $\delta \in \mathrm{Der}(K[\mathbf{x}])$ definimos $\delta \cdot p := \delta(p)$. Observemos que ∂_i no es un homomorfismo de $K[\mathbf{x}]$-módulos debido al comportamiento con el producto de la derivada. De hecho, los elementos $\delta \in K[\mathbf{x}]$ se comportan como sigue:

$$\begin{cases} \delta(f_1+f_2) = \delta(f_1)+\delta(f_2), \\ \delta(f_1f_2) = \delta(f_1)\,f_2 + f_1\delta(f_2) \\ \delta(af_1) = a\delta(f_1) \end{cases} \quad \text{y}$$

para f_1 y f_2 polinomios de $K[\mathbf{x}]$ y a una constante de K.

Tomando $f \in K[\mathbf{x}]$, aquellas derivaciones —elementos de $\mathrm{Der}(K[\mathbf{x}])$— que cuando se aplican a f devuelven un múltiplo escalar de f forman el submódulo de derivaciones tangentes a f:

$$\mathrm{Der}(f) := \{\delta \in \mathrm{Der}(K[\mathbf{x}]) \,|\, \delta(f) \in \langle f \rangle\}. \tag{2.1}$$

Puede verse que si identificamos ∂_i con $\mathbf{e}_i$, tenemos que $\mathrm{Der}(K[\mathbf{x}])$ es isomorfo a $K[\mathbf{x}]^n$ y, por esta misma razón, $\mathrm{Der}(f)$ puede verse como un $K[\mathbf{x}]$-submódulo de $K[\mathbf{x}]^n$.

Definición 2.13. Diremos que un anillo A es *noetheriano* si todos sus ideales son finitamente generados. Diremos también que un A-módulo M es *noetheriano* si todo submódulo $N \subseteq M$ está finitamente generado. Es decir, si existen $n_1, n_2, \ldots, n_k$ en N de forma que $N = \langle n_1, n_2, \ldots, n_k \rangle$.

De aquí en adelante, salvo que se indique lo contrario, asumiremos que A siempre es un anillo noetheriano.

Lema 2.14. *Sea M un A-módulo noetheriano. Los submódulos y módulos cocientes de M son también noetherianos.*

Lema 2.15. *Que M sea noetheriano es equivalente a que toda cadena ascendente de submódulos $N_1 \subseteq N_2 \subseteq \ldots$ sea eventualmente estacionaria.*

Definición 2.16. Sea M un A-módulo. Diremos que M es *libre de torsión* si el único $m \in M$ tal que $am = 0$ para todo $a \in A$ es 0.

¿Esta definición cerca de libre junto con algún ejemplo sencillo de no libre y libre de torsión y de no libre de torsión.

Definición 2.17. Sean M y N dos A-módulos. El *conjunto de homomorfismos de A-módulos* de M a N es también un A-módulo y se denota por

$$\mathrm{Hom}_A(M,N) := \{\phi : M \longrightarrow N \,|\, \phi \text{ es un homomorfismo de } A\text{-módulos}\}.$$

Definición 2.18. Se define el módulo dual M^* como el conjunto de homomorfismos de A-módulos de M en A:

$$M^* := \mathrm{Hom}_A(M,A).$$

Hago una propuesta alternativa que creo que simplifica y aclara.

Definición 2.19. Dados dos A-módulos M, N, una forma *bilineal* $\Phi : M \times N \to A$ es una aplicación tal que

- $\Phi(am + a'm', n) = a\Phi(m,n) + a'\Phi(m',n)$ y
- $\Phi(m, an + a'n') = a\Phi(m,n) + a'\Phi(m,n')$

$\forall a, a' \in A$, $\forall m, m' \in M$, $\forall n, n' \in N$. Una forma bilineal induce homomorfismos $\Phi_1 : M \to N^*$, $\Phi_2 : N \to M^*$, dados por $\Phi_1(m)(n) := \Phi(m,n) =: \Phi_2(n)(m)$.

Por la definición de espacio dual tenemos una forma bilineal $\Phi^M : M \times M^* \to A$, definida mediante evaluación, que induce un homomorfismo natural $\Psi := \Phi_1^M : M \to M^{**}$.

Definición 2.20. Sea $\psi : M \to M^{**}$ el homomorfismo de A-módulos que envía un elemento m de M a la función $\psi(m) : M^* \to A$ que a cada $\phi \in M^*$ le asigna el valor $\phi(m)$:

$$\begin{aligned} \psi : M &\longrightarrow \mathrm{Hom}_A\big(\mathrm{Hom}_A(M,A), A\big) \\ m &\longmapsto \psi(m) : \mathrm{Hom}_A(M,A) \longrightarrow A \\ &\qquad\qquad \phi \longmapsto \phi(m) \end{aligned}$$

Diremos que M es un A-módulo *reflexivo* si M es isomorfo a M^{**} por medio de esta aplicación ψ.

Ejemplo 2.21. Veamos que todo espacio vectorial de dimensión finita es reflexivo. Sea V un K-espacio vectorial de dimensión n y con base $\{v_1, v_2, \dots, v_n\}$. El conjunto $\mathrm{Hom}_K(V,K)$ se compone de las aplicaciones lineales de V en K. Cada elemento ϕ de $\mathrm{Hom}_K(V,K)$ puede representarse como la multiplicación por una matriz, puesto que

$$\phi(v) = \big(\phi(v_1), \phi(v_2), \dots, \phi(v_n)\big) \cdot v;$$

y viceversa, es decir, para cualquier vector w de V, $v \mapsto w \cdot v$ es un elemento de $\mathrm{Hom}_K(V,K)$. Esta biyección es un isomorfismo de K-módulos, por lo que V es isomorfo a V^* y, por consiguiente, a V^{**} también. Con esto hemos demostrado que V^{**} es un K-espacio vectorial de la misma dimensión de V, pero para verificar que V sea reflexivo debemos cerciorarnos de que la aplicación ψ sea un isomorfismo. Basta darse cuenta que el kernel de ψ es necesariamente el vector nulo, que se corresponde con evaluar todas las aplicaciones de V^* en el $\mathbf{0}$, y por lo tanto ψ es inyectiva; como V y V^{**} son de la misma dimensión, concluimos que ψ es un isomorfismo.

Ejemplo 2.22. Consideremos ahora el $\mathbb{Z}$-módulo $\mathbb{Z}/p\mathbb{Z}$ donde p es un número primo. Sabemos que $\mathbb{Z}/p\mathbb{Z} = \langle 1 \rangle$; por lo tanto, cualquier $\phi \in (\mathbb{Z}/p\mathbb{Z})^*$ está unívocamente determinado por la imagen de 1. Supongamos que $\phi(1) = x \in \mathbb{Z}$, se debe cumplir que

$$px = p\phi(1) = \phi(p \cdot 1) = \phi(0) = 0 \;\Leftrightarrow\; px = 0 \;\Leftrightarrow\; x = 0.$$

Es decir, que $(\mathbb{Z}/p\mathbb{Z})^* = \{\mathbf{0}^*\}$ donde $\mathbf{0}^*$ envía cualquier elemento de $\mathbb{Z}/p\mathbb{Z}$ al 0 de $\mathbb{Z}$. Al estar $(\mathbb{Z}/p\mathbb{Z})^*$ solo compuesto por la aplicación que todo lo lleva al cero, su dual, $(\mathbb{Z}/p\mathbb{Z})^{**}$, solo estará compuesto por la aplicación $\mathbf{0}^{**}$ que envía todo al 0 de $\mathbb{Z}$ también. Al ser todos estos conjuntos finitos, podemos ver que la cardinalidad de $(\mathbb{Z}/p\mathbb{Z})^{**}$ y $\mathbb{Z}/p\mathbb{Z}$ no coinciden y por lo tanto no pueden ser isomorfos, impidiendo esto a su vez que $\mathbb{Z}/p\mathbb{Z}$ sea un $\mathbb{Z}$-módulo reflexivo.

Más propiedades acerca de los módulos reflexivos pueden encontrarse en [8, Tag 0AUY].

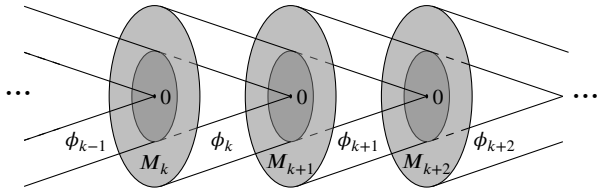
En ocasiones, encadenaremos homomorfismos y podemos necesitar expresar las relaciones entre las imágenes y los núcleos de las distintas aplicaciones. Para expresar esto, utilizaremos las sucesiones exactas.

Definición 2.23. Diremos que una expresión del siguiente estilo:

$$\dots \xrightarrow{\phi_{k-1}} M_k \xrightarrow{\phi_k} M_{k+1} \xrightarrow{\phi_{k+1}} M_{k+2} \xrightarrow{\phi_{k+2}} \dots$$

es una *sucesión exacta* si se cumple que $\mathrm{im}\,\phi_i = \ker \phi_{i+1}$ para todo i, como ilustra este diagrama:

Para indicar que una aplicación $\phi : M \to N$ es inyectiva, escribiremos $0 \to M \xrightarrow{\phi} N$; y para indicar que es sobreyectiva, $M \xrightarrow{\phi} N \to 0$.



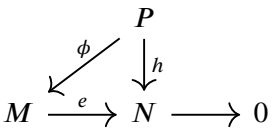
Con las sucesiones exactas, podemos resumir nuestro problema en una sola expresión. Recordemos que estamos estudiando el $K[\mathbf{x}]$-módulo $\mathrm{Der}(f)$, que es un $K[\mathbf{x}]$-submódulo de $\mathrm{Der}(K[\mathbf{x}])$. Por otro lado, cada derivación δ, cuando se aplica a f nos da lugar a un elemento en el $K[\mathbf{x}]$-submódulo $J := \langle \partial_1 f, \ldots, \partial_n f \rangle \subseteq K[\mathbf{x}]$. Finalmente, a nosotros los elementos que nos interesan son aquellos que sean múltiplos de f, es decir, que pertenezcan al $K[\mathbf{x}]$-submódulo $\langle f \rangle$ o más exactamente a $J \cap \langle f \rangle$. Esto último es equivalente a decir que nos interesan aquellos elementos que son 0 cuando hacemos el cociente de J por $J \cap \langle f \rangle$. Este cociente se puede hacer de dos formas que son isomorfas: $J+\langle f \rangle / \langle f \rangle$ o $J / J \cap \langle f \rangle$. Todo esto lo podemos expresar como una secuencia exacta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Der}(f) & \xrightarrow{\Phi} & \mathrm{Der}(K[\mathbf{x}]) & \xrightarrow{\pi\circ\xi} & \frac{J}{J\cap\langle f\rangle} & \longrightarrow & 0 \\ & & & & \updownarrow & & & & \\ & & & & K[\mathbf{x}]^n & & & & \end{array} \tag{2.2}$$

La función Φ es una inclusión, ξ envía una derivación δ a su evaluación en f —$\delta(f)$— y π es simplemente la aplicación canónica de J a $J/J\cap\langle f\rangle$.

Definición 2.24. Un A-módulo P es *proyectivo* si para cada epimorfismo de A-módulos $e : M \to N$ y cada homomorfismo de A-módulo $h : P \to N$ existe un homomorfismo de A-módulos $\phi : P \to M$ de forma que $h = e \circ \phi$.

Suele ser común referirse a esto diciendo que todo homomorfismo h puede ser «elevado» a través de cualquier epimorfismo e a un homomorfismo ϕ y queda ilustrado por el diagrama de la derecha.



Ejemplo 2.25. Sean $M = \mathbb{Z}/4\mathbb{Z}$, $N = \mathbb{Z}/2\mathbb{Z}$ y $P = \mathbb{Z}/2\mathbb{Z}$ vistos como $\mathbb{Z}$-módulos. Como e es un epimorfismo de $\mathbb{Z}$-módulos, necesariamente tendremos que $e(0) = e(2) = 0$ y $e(1) = e(3) = 1$. Como h simplemente tomaremos la identidad. Sea ahora $\phi : P \to M$ un homomorfismo de $\mathbb{Z}$-módulos cualquiera; existen dos posibilidades para $\phi(1)$:

- si $\phi(1) \in \{0, 2\}$, entonces $e(\phi(1)) = 0 \neq h(1)$;
- si por el contrario $\phi(1) \in \{1, 3\}$, entonces $\phi(0) = \phi(2 \cdot 1) = 2\phi(1) = 2$ y de nuevo llegamos a que $e(\phi(1)) = 0 \neq h(1)$.

En conclusión, $\mathbb{Z}/2\mathbb{Z}$ no es un $\mathbb{Z}$-módulo proyectivo.

Damos ahora dos propiedades que nos permitirán relacionar los módulos proyectivos con los libres.

Lema 2.26. *Todo módulo libre es proyectivo.*

Demostración. Sea P un A-módulo libre con base $\{p_1, p_2, \ldots, p_k\}$ y tomemos el resto de premisas como en la Definición 2.24. Al ser P un módulo libre, cualquier homomorfismo de A-módulos $\phi : P \to N$ está unívocamente determinado por las imágenes de la base de P. Sean $m_1, m_2, \ldots, m_k$ elementos de M de forma que $e(m_i) = h(p_i)$, cuya existencia está garantizada por ser e un epimorfismo. Definiendo $\phi(p_i) := m_i$ tenemos que $e(\phi(p_i)) = h(p_i)$ por lo que $e \circ \phi = h$. □

Una introducción a los módulos proyectivos puede encontrarse en [5, sección 1.2].

Capítulo 3

Bases de Gröbner y Sicigias

A partir de este momento solo trabajaremos con módulos $K[\mathbf{x}]^n$ ya que son los involucrados en el módulo de derivaciones.

Uno de los principales problemas que tienen los módulos en general es que describirlos es más complicado que en el caso de los espacios vectoriales. Con los espacios vectoriales, sabemos que siempre existe una base y que, dándola, describimos por completo este espacio. En el caso de los módulos, sin embargo, dar una base en el sentido de base de espacio vectorial no siempre es posible. Esto se materializa en el problema de ser capaz de determinar si un elemento en particular se encuentra dentro del módulo.

Veamos cómo se afronta este problema a distintos niveles.

Ejemplo 3.1. Consideremos el $\mathbb{R}$-módulo $\mathbb{R}[x]$ —solo una variable— y a $f := x^3 - 6x^2 + 11x - 6$ y $g := x^3 - 9x^2 + 26x - 24$ dos elementos de este. Queremos determinar si un polinomio cualquiera, por ejemplo $p = 3x^7 + 4x^5 - 3x^2 + x + 1$, pertenece al submódulo —o en este caso, ideal— $\langle f, g\rangle$. Como $\mathbb{R}[x]$ es un dominio euclídeo, es dominio de ideales principales y, por lo tanto,

Es una tontería, pondría los racionales en lugar de los reales, también para otros ejemplos.

$$\langle f, g\rangle = \langle \operatorname{mcd}(f, g)\rangle = \left\langle x^2 - 5x + 6\right\rangle.$$

Ahora responder la pregunta es mucho más sencillo, ya que $p \in \langle f, g\rangle$ si y solo si p es un múltiplo de $x^2 - 5x + 6$. Y eso podemos saberlo utilizando el algoritmo de la división para polinomios de una variable que conocemos:

$$p = \underbrace{\left(3x^5 + 15x^4 + 61x^3 + 215x^2 + 709x + 2252\right)}_{\text{cociente } q}\underbrace{\left(x^2 - 5x + 6\right)}_{\text{divisor } d} + \underbrace{7007x - 13511}_{\text{resto } r}.$$

Por el Teorema de la División, sabemos que este resto es el único polinomio de $\mathbb{R}[x]$ que satisface $p = qd + r$ con grado menor que d. Por lo tanto, al no ser 0, podemos afirmar que p no está en $\langle f, g\rangle$.

Este ejemplo también ilustra un cambio de perspectiva que será muy importante a lo largo de toda esta sección: la división deja de ser importante por los valores exactos que arroja y su relevancia es más bien cualitativa. Con esto nos referimos a que, como tal, los valores concretos del cociente y el resto no tienen ninguna relevancia a la hora de determinar si p pertenece o no a $\langle f, g\rangle$. Conocidas las propiedades de este algoritmo de la división en $\mathbb{R}[x]$, solo nos interesa si el resto es 0 o no, puesto que es lo que determina si p pertenece o no a $\langle f, g\rangle$. En base a esto, nuestra motivación para la división debe cambiar de ser «obtener q y r de forma que $p = qd + r$ donde grado $r <$ grado d» a un más abstracto «obtener un representante r que satisfaga algunas condiciones de la clase de p en $\mathbb{R}[x]/\langle f,g\rangle$».

En realidad con este lenguaje, r es importante ya que determina la clase de p en el cociente.

Visto así, el Ejemplo 3.1 supone una situación idílica: por ser un dominio de ideales principales, sabemos que vamos a poder representar a cualquier conjunto generador con un solo elemento; por lo tanto, sobre cualquier conjunto generador siempre habrá definida una división, que consistirá en dividir como

ya conocemos por el elemento generador. Además, por el Teorema de la División, conocemos que el representante r que satisfaga grado $r <$ grado d es único, lo cual nos permite discernir si p está en $\langle f, g\rangle$ viendo si $r = 0$ o no.

En espacios más complicados, muchas de estas buenas propiedades desaparecen e impiden extender el proceso anterior.

Más variables: Consideremos ahora el anillo de polinomios $\mathbb{R}[x, y, z]$, un elemento $f := 4x^2y + 12xy^2 + \frac{5}{2}xz^3 + x^2yz$ y el ideal $I := \langle f\rangle$. Si bien este espacio no tiene por qué ser un dominio de ideales principales, al solo haber un generador podemos obviar de momento esa parte. Siguiendo la línea del Ejemplo 3.1, para ver si $p \in \mathbb{R}[x, y, z]$ deberíamos dividir por f y ver si el resto es 0 o no. Pero llegados a este punto, ¿cómo deberíamos dividir? Podemos intentar imitar el algoritmo usual de la división, pero este necesita siempre una noción de orden entre los términos del divisor y también del dividendo. En este caso, ¿deberíamos tomar $4x^2y$ como «término líder» de f o igual sería mejor tomar a uno de mayor grado como $\frac{5}{2}xz^3$? Pero $\frac{5}{2}xz^3$ y x^2yz tienen el mismo grado, ¿cuál escoger, entonces? La elección de este «término líder» en dividendo y divisor cambiará el funcionamiento del algoritmo, así que debemos cerciorarnos de cuáles de estas opciones son válidas y también revisar si el algoritmo tradicional adaptado de esta manera sirve su propósito.

Más generadores: Sin cambiar de espacio, consideremos ahora el ideal $I := \left\langle x + y, xyz, x^2 + y^2 + z^2\right\rangle$. En este caso, el que $\mathbb{R}[x, y, z]$ no sea un dominio de ideales principales es un problema. ¿Cómo podemos dividir siquiera? Otra dificultad a la que nos enfrentamos aquí una vez hayamos entendido cómo dividir será saber si nuestro sistema de generadores es compatible con la división ya que, por ejemplo, a $x^2 + y^2 + z^2$ se le puede restar $(x + y)^2$ e I podría expresarse como $\left\langle x + y, xyz, -2xy + z^2\right\rangle$. ¿Sirven ambas representaciones?

Más «dimensiones»: Por último, también debemos tener en cuenta que por lo general trabajaremos en $K[\mathbf{x}]^r$, lo cual hará que los elementos tengan más de una componente. ¿Cómo integrar las componentes en las divisiones?

En resumen, para poder construir un algoritmo de la división más general necesitaremos tener un orden total dentro de los monomios para saber cómo ir construyendo el cociente, ver cómo dividir por más de un generador e integrar a las distintas componentes.

3.1. Órdenes monomiales

El concepto de orden monomial nos permite construir un orden total sobre los monomios de $K[\mathbf{x}]$. Para poder definirlo bien, debemos identificar un monomio en n variables con un vector en $\mathbb{N}^n$ que represente sus exponentes, es decir,

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \longleftrightarrow \left(\alpha_1, \alpha_2, \dots, \alpha_n\right).$$

Tomando $\alpha \in \mathbb{N}^n$, notaremos $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ como x^α. Así pues, un orden monomial se corresponde con un orden total en $\mathbb{N}^n$ de forma que sea compatible con la estructura de monoide que posee el conjunto de monomios.

Definición 3.2. Un *orden monomial* $>$ es un orden total sobre los monomios en n variables que respeta la multiplicación, es decir, que satisface

$$x^\alpha > x^\beta \implies x^\gamma x^\alpha > x^\gamma x^\beta$$

para todo α, β y γ en $\mathbb{N}^n$.

Sin embargo esta propiedad deja en el aire el papel del 1. ¿Cómo debemos ordenarlo?

Definición 3.3. Sea $>$ un orden monomial. Si para todo $\alpha \in \mathbb{N}^n$

- $x^\alpha > 1$, diremos que el orden es global;
- $x^\alpha < 1$, diremos que el orden es local;
- si no son ninguna de las dos anteriores, diremos que el orden es mixto.

Ejemplo 3.4 (Orden lexicográfico)**.** Una posibilidad de ordenar los monomios es como si estos fueran palabras en el diccionario. Por ejemplo, podemos ver $x^3y^2z^4$ como $xxxyyzzzz$ y en $x^2y^4z^4$ como $xxyyyyzzzz$. Así, $x^3y^2z^4 > x^2y^4z^4$. De manera más formal, $x^\alpha > x^\beta$ si la primera componente no nula por la izquierda de $\alpha - \beta$ es positiva. Con los valores de antes, $x^3y^2z^4 > x^2y^4z^4$ ya que la primera componente de $(3,2,4)-(2,4,4) = (1,-2,0)$ es positiva.

Es fácil ver que este orden es, en efecto, un orden monomial ya que si $x^\alpha > x^\beta$, tendremos que la primera componente de $\alpha - \beta$ será positiva, y lo mismo ocurrirá con la de $\alpha+\gamma-(\beta+\gamma) = \alpha-\beta$ por lo que $x^\gamma x^\alpha > x^\gamma x^\beta$.

Para referirnos a este orden en concreto utilizaremos $>_{\texttt{LEX}}$.

Ejemplo 3.5 (Orden graduado-lexicográfico)**.** En ocasiones no nos interesará ordenar los monomios con el orden lexicográfico puesto que no tiene en cuenta el grado: $x^2 > xy^{129}z^{34}$. Por lo tanto, podemos definir un orden que tenga en cuenta el grado; en particular, que primero ordene por el grado y, en caso de empate, utilice el orden lexicográfico:

$$x^\alpha > x^\beta \iff \begin{cases} \operatorname{grado} x^\alpha > \operatorname{grado} x^\beta & \text{o} \\ \operatorname{grado} x^\alpha = \operatorname{grado} x^\beta \text{ y } x^\alpha >_{\texttt{LEX}} x^\beta. \end{cases}$$

Este orden monomial es el graduado-lexicográfico y se denota por $>_{\texttt{GRAD-LEX}}$.

Para poder generalizar estos órdenes a un módulo como $K[\mathbf{x}]^r$ primero tenemos que aclarar qué es un monomio en este anillo. La elección es bastante natural cuando consideramos que un elemento de, por ejemplo, $\mathbb{R}[x,y]^3$ como puede ser $\begin{pmatrix} 2xy+y^2 \\ x^3 \\ y \end{pmatrix}$ puede escribirse como $2xy\mathbf{e}_1 + y^2\mathbf{e}_1 + x^3\mathbf{e}_2 + y\mathbf{e}_3$.

Definición 3.6. A las expresiones de la forma $x^\alpha \mathbf{e}_i$ con $i \in \{1,\dots,n\}$ las llamaremos *monomios* de $K[\mathbf{x}]$.

Definición 3.7. Sea $>$ un orden monomial en $K[\mathbf{x}]$. Un *orden monomial de módulos* $>_{\text{mód}}$ es un orden total sobre los monomios de $K[\mathbf{x}]^r$ que es compatible con la estructura de $K[\mathbf{x}]$-módulo de $K[\mathbf{x}]^r$ y con el orden $>$, es decir, que satisface

- $x^\alpha \mathbf{e}_i >_{\text{mód}} x^\beta \mathbf{e}_j \implies x^\alpha x^\gamma \mathbf{e}_i >_{\text{mód}} x^\beta x^\gamma \mathbf{e}_j$ y
- $x^\alpha > x^\beta \implies x^\alpha \mathbf{e}_i >_{\text{mód}} x^\beta \mathbf{e}_i$

para todo α, β y γ en $\mathbb{N}^n$ e i y j en $\{1,\dots,r\}$. Por lo general, omitiremos el subíndice «mód» ya que se sobreentenderá que estamos tratando con módulos.

Ejemplo 3.8. Una manera de extender el orden monomial $>_{\texttt{LEX}}$ a los monomios de $K[\mathbf{x}]^n$ es ordenar primero en función de la posición, haciendo que las primeras posiciones vayan antes que las últimas —por ejemplo $\mathbf{e}_2 > \mathbf{e}_3$—, y si hubiese un empate, entonces se utilizase el orden $>_{\texttt{LEX}}$. Así definimos el siguiente orden monomial de módulos:

$$x^\alpha \mathbf{e}_i > x^\beta \mathbf{e}_j \iff \begin{cases} i < j & \text{o} \\ i = j \text{ y } x^\alpha >_{\texttt{LEX}} x^\beta. \end{cases} \tag{3.1}$$

Sin embargo, podríamos haber tomado la decisión de que primero se comparasen x^α y x^β y, en caso de empate, se hubiesen mirado las posiciones. Ambas posibilidades dan lugar a distintos órdenes monomiales de módulos: Vemos pues que es necesario aclarar si la posición de los monomios debe ser evaluada antes o después, así que denotamos a estos órdenes como $>_{(\texttt{POS,LEX})}$ para el correspondiente a (3.1) y $>_{(\texttt{LEX,POS})}$

para aquel que primero compara según el orden lexicográfico y después según la posición. Por ver un caso concreto, $xy\mathbf{e}_2 >_{(\texttt{LEX},\texttt{POS})} y^3\mathbf{e}_1$ pero $y^3\mathbf{e}_1 >_{(\texttt{POS},\texttt{LEX})} xy\mathbf{e}_2$.

Esta generalización que hemos hecho no está limitada a $>_{\texttt{LEX}}$, también se podría realizar con otros órdenes como $>_{\texttt{GRAD-LEX}}$. Incluso se podrían permutar las posiciones para obtener todavía más órdenes.

Con el concepto de orden monomial de módulos damos el primer paso en dirección a la generalización del algoritmo de la división formalizando esa noción de «término líder» que mencionábamos.

Definición 3.9. Sea $p := c_1 x^{\mathbf{s_1}}\mathbf{e}_{i_1} + c_2 x^{\mathbf{s_2}}\mathbf{e}_{i_2} + \cdots + c_m x^{\mathbf{s_m}}\mathbf{e}_{i_m}$ un polinomio de $K[\mathbf{x}]^r$ y $>$ un orden monomial de módulos. Sea $k \in \{1, \ldots, m\}$ de forma que $x^{\mathbf{s_k}}$ sea el máximo del conjunto de monomios de p según el orden $>$, entonces

- el *monomio líder* de p se denomina $\mathrm{LM}(p) := x^{\mathbf{s_k}}\mathbf{e}_{i_k}$;
- el *coeficiente líder* de p es el coeficiente que acompaña al monomio líder en p y se define como $\mathrm{LC}(p) := c_k$;
- el *término líder* de p es $\mathrm{LT}(p) := \mathrm{LC}(p)\mathrm{LM}(p)$.

Necesitamos también concretar la noción de divisibilidad para poder integrar las distintas componentes que puedan tener los elementos dentro de la división. Según la Definición 2.8, para $x^\alpha\mathbf{e}_i$ y $x^\beta\mathbf{e}_j$ dos monomios de $K[\mathbf{x}]$ tenemos que $x^\alpha\mathbf{e}_i$ divide a $x^\beta\mathbf{e}_j$ si $i = j$ y $x^\alpha | x^\beta$.

Con todo esto, ya podemos definir un algoritmo de la división de un elemento por otro en $K[\mathbf{x}]^r$. En esencia, imitaremos al algoritmo tradicional solo que, en este caso, nos guiaremos por los monomios líderes y no por el grado.

Definición 3.10. El *algoritmo de división simple* se aplica a dos elementos f y g de $K[\mathbf{x}]^n$ junto con un orden monomial sobre este.

1: Definimos $D \leftarrow f$, $d \leftarrow g$, $c \leftarrow 0$ y $r \leftarrow \mathbf{0}$ como las variables que representan el dividendo, divisor, cociente y resto, respectivamente. Nótese que D, d y r son vectores de $K[\mathbf{x}]^r$ mientras que c es un polinomio de $K[\mathbf{x}]$.
2: **repite**
3: ▏ **mientras** $\mathrm{LM}(d) | \mathrm{LM}(D)$ **haz**
4: ▏ ▏ Sea $m \in K[\mathbf{x}]$ de forma que $\mathrm{LM}(D) = m\mathrm{LM}(d)$.
5: ▏ ▏ $D \leftarrow D - md$, $c \leftarrow c + m$
6: ▏ $D \leftarrow D - \mathrm{LM}(D)$, $r \leftarrow r + \mathrm{LM}(D)$
7: **hasta que** $D = \mathbf{0}$

Al finalizar este algoritmo, tendremos que $f = cg + r$ donde ninguno de los términos de r es divisible por $\mathrm{LM}(g)$.

La única novedad de este algoritmo con respecto al que ya conocemos de polinomios en una sola variable es la instrucción de la línea 6. En ella, le sustraemos a D su término líder, lo añadimos al resto y repetimos todo el proceso otra vez con el resto de términos de D. Esto lo hacemos para reducir todo lo posible el resto, garantizando que ninguno de sus términos sea divisible por $\mathrm{LM}(g)$. De no hacer esto, solo podríamos garantizar que, al final de la ejecución, $\mathrm{LT}(D)$ no es divisible por $\mathrm{LT}(g)$.

Ejemplo 3.11. Sean $f := 3x^4\mathbf{e}_1 + 2x^3\mathbf{e}_1 + 2x^2y\mathbf{e}_2 + x^2\mathbf{e}_1$ y $g := x^2\mathbf{e}_1 + 2y\mathbf{e}_3$ dos elementos de $\mathbb{R}[x, y]^3$ con el orden monomial $>_{(\texttt{GRAD-LEX},\texttt{POS})}$. Aunque hayamos expresado en la definición todo de una forma muy «programable», en esencia, lo que hacemos es bastante similar a una división usual:

$$
\begin{array}{rllll|l}
3x^4\mathbf{e}_1 & +2x^3\mathbf{e}_1 & +2x^2y\mathbf{e}_2 & & +x^2\mathbf{e}_1 & & x^2\mathbf{e}_1+2y\mathbf{e}_3 \\
-(3x^4\mathbf{e}_1 & & & +6x^2y\mathbf{e}_3) & & & 3x^2+2x+1 \\
\hline
 & +2x^3\mathbf{e}_1 & +2x^2y\mathbf{e}_2 & -6x^2y\mathbf{e}_3 & +x^2\mathbf{e}_1 & & \\
 & -(2x^3\mathbf{e}_1 & & & & +4xy\mathbf{e}_3) & \\
\hline
 & \text{1ª iteración:} & \cancel{2x^2y\mathbf{e}_2} & \cancel{-6x^2y\mathbf{e}_3} & +x^2\mathbf{e}_1 & -4xy\mathbf{e}_3 & \\
 & & \uparrow \text{1ª iteración} & \uparrow \text{2ª iteración} & -(x^2\mathbf{e}_1 & & +2y\mathbf{e}_3) \\
\hline
 & & & & \text{3ª iteración:} & \cancel{-4xy\mathbf{e}_3} & \cancel{-2y\mathbf{e}_3} \\
 & & & & & \uparrow \text{3ª iteración} & \uparrow \text{4ª iteración}
\end{array}
$$

1ª iteración: reducimos D dos veces, lo cual se corresponde con dos ejecuciones del bucle interno o las dos primeras restas que aparecen arriba. Después, eliminamos el término líder de D, $2x^2y\mathbf{e}_2$, ya que no es divisible por $\mathrm{LM}\left(x^2\mathbf{e}_1+2y\mathbf{e}_3\right)=x^2\mathbf{e}_1$ y se lo añadimos a r. Esto deja $D=-6x^2y\mathbf{e}_3+x^2\mathbf{e}_1-4xy\mathbf{e}_3$, $c=3x^2+2x$ y $r=2x^2y\mathbf{e}_2$.

2ª iteración: el término líder de D, $-6x^2y\mathbf{e}_3$, sigue sin ser divisible por $x^2\mathbf{e}_1$, por lo que no reducimos. Después, eliminamos este de D y se lo añadimos a r. Esto deja $D=x^2\mathbf{e}_1-4xy\mathbf{e}_3$, $c=3x^2+2x$ y $r=2x^2y\mathbf{e}_2-6x^2y\mathbf{e}_3$.

3ª iteración: reducimos una vez. Después, eliminamos el término líder de D, $-4xy\mathbf{e}_3$, ya que no es divisible por $x^2\mathbf{e}_1$ y se lo añadimos a r. Esto deja $D=-2y\mathbf{e}_3$, $c=3x^2+2x+1$ y $r=2x^2y\mathbf{e}_2-6x^2y\mathbf{e}_3-4xy\mathbf{e}_3$.

4ª iteración: el término líder de D, $-2y\mathbf{e}_3$, el último que queda, no es divisible por $x^2\mathbf{e}_1$, por lo que no reducimos. Después, eliminamos el término líder de D y se lo añadimos a r. Esto deja $D=0$, $c=3x^2+2x+1$ y $r=2x^2y\mathbf{e}_2-6x^2y\mathbf{e}_3-4xy\mathbf{e}_3-2y\mathbf{e}_3$. Al ser ya $D=0$, el algoritmo para.

Queda por lo tanto

$$f=\left(3x^2+2x+1\right)g+\underbrace{2x^2y\mathbf{e}_2-6x^2y\mathbf{e}_3-4xy\mathbf{e}_3-2y\mathbf{e}_3}_{\text{resto } r}$$

donde ninguno de los términos en r es divisible por $\mathrm{LT}(g)$.

A partir de este algoritmo, podemos generalizar más para afrontar un número finito de divisores. La clave para esta generalización será buscar entre estos divisores a alguno que pudiera reducir D y, caso de encontrarlo, reducir por ese. Puede que haya casos donde haya más de un divisor que pueda reducir, en cuyo caso se puede escoger el que se prefiera.

Definición 3.12. Sean f un elemento y $N=\langle g_1,\dots,g_k\rangle$ un $K[\mathbf{x}]$-submódulo de $K[\mathbf{x}]^r$. Definimos el *algoritmo de división compuesta* de f entre N como sigue:

1: Definimos $D\leftarrow f$, $d_i\leftarrow g_i$, $c_i\leftarrow 0$ y $r\leftarrow 0$ como las variables que representan el dividendo, los divisores, los cocientes y el resto, respectivamente.
2: **repite**
3: **mientras** haya algún i de forma que $\mathrm{LM}\left(d_i\right)|\mathrm{LM}(D)$ **haz**
4: Sea i de forma que $\mathrm{LM}\left(d_i\right)|\mathrm{LM}(D)$.
5: Sea $m\in K[\mathbf{x}]$ de forma que $\mathrm{LM}(D)=m\mathrm{LM}\left(d_i\right)$.
6: $D\leftarrow D-md_i$, $c_i\leftarrow c_i+m$
7: $D\leftarrow D-\mathrm{LM}(D)$, $r\leftarrow r+\mathrm{LM}(D)$
8: **hasta que** $D=0$

Un ejemplo como el de (A.1) muestra cómo funciona este algoritmo. Ahora, haría falta generalizar todavía más para ser capaces también de dividir por un número infinito de divisores, pero los siguientes resultado nos permitirán ver que esto no es necesario.

Teorema 3.13 (de la base de Hilbert)**.** *Sea A un anillo noetheriano. Entonces el anillo de polinomios $A\left[x_1,\dots,x_n\right]$ es también noetheriano.*

Di algo más.

Proposición 3.14. *Sea A un anillo noetheriano y M un A-módulo finitamente generado. Entonces, M es un A-módulo noetheriano.*

Como K es un cuerpo, todos sus ideales son principales, así que es noetheriano. Por el teorema de la base de Hilbert, $K[\mathbf{x}]$ es noetheriano también. Y por último, por la Proposición 3.14, $K[\mathbf{x}]^r$ es igualmente noetheriano. Esto nos asegura que es suficiente con tener un algoritmo de la división para un número finito de divisores.

Con respecto a los problemas que se presentaban al principio, ya hemos resuelto varios: tenemos un orden para los monomios que nos permite tener un convenio de cuáles son los términos principales de los polinomios, hemos integrado las distintas componentes de un vector de $K[\mathbf{x}]^r$ al concepto de monomio y sabemos cómo dividir por ellas, y también sabemos cómo afrontar la división con más de un divisor. Sin embargo, todavía podemos encontrarnos con casos como el siguiente.

Ejemplo 3.15. Supongamos que $N := \langle x\mathbf{e}_1 + y\mathbf{e}_2, y\mathbf{e}_1 + x\mathbf{e}_2\rangle$ es un $\mathbb{R}[x,y]$-submódulo de $\mathbb{R}[x,y]^2$ y queremos saber si $f := x^2\mathbf{e}_2 - y^2\mathbf{e}_2$ pertenece a N. Al aplicar el algoritmo de la división siguiendo el orden $>_{(\mathtt{POS},\mathtt{LEX})}$ de 3.12 nos encontramos que ninguno de los dos generadores de N puede reducir a f, por lo tanto el resto es el propio f. Como el resto es distinto de 0, estaríamos tentados a decir que f no pertenece a N, pero démonos cuenta de que $f = -y\left(x\mathbf{e}_1 + y\mathbf{e}_2\right) + x\left(y\mathbf{e}_1 + x\mathbf{e}_2\right)$ y, por ende, sí que pertenece.

Para entender bien lo que ocurre en este ejemplo, necesitamos el siguiente objeto.

Definición 3.16. Sea G un subconjunto de $K[\mathbf{x}]^r$ con un orden monomial de módulos $>$. El $K[\mathbf{x}]$-*submódulo de los monomios líderes* de G lo denotaremos por

$$\mathrm{LM}(N) := \langle \mathrm{LM}(g) \,|\, g \in N\rangle.$$

¿Qué es lo que ocurre en el Ejemplo 3.15? Si nos fijamos, en la operación $f = -y\left(x\mathbf{e}_1 + y\mathbf{e}_2\right) + x\left(y\mathbf{e}_1 + x\mathbf{e}_2\right)$, los términos líderes de sendos generadores —$x\mathbf{e}_1$ e $y\mathbf{e}_1$— se anulan, por lo que el término líder de esta combinación es menor que los términos líderes de los generadores. En general, esto lo que nos muestra es que $\mathrm{LM}(N)$ no tiene que ser igual a $\left\langle \mathrm{LM}\left(x\mathbf{e}_1 + y\mathbf{e}_2\right), \mathrm{LM}\left(y\mathbf{e}_1 + x\mathbf{e}_2\right)\right\rangle$.

Esto supone un duro golpe para nuestros algoritmos de la división, ya que cuando para un $K[\mathbf{x}]$-submódulo $N = \langle g_1, \ldots, g_k\rangle$ tengamos que $\mathrm{LM}(N) \neq \left\langle \mathrm{LM}\left(g_1\right), \ldots, \mathrm{LM}\left(g_k\right)\right\rangle$, aunque el resto sea distinto de 0, no podremos garantizar que el elemento esté fuera de N. Por supuesto, si el resto es 0 sí que podemos garantizar que sí está. Para solucionar este problema, necesitamos encontrar una representación de los submódulos que sí sea compatible con el algoritmo de la división. Es decir, que cuando dividamos por los generadores y el resto sea distinto de 0, podamos decir que el elemento no pertenece.

3.2. Bases de Gröbner

Para conseguir esta mejor representación, simplemente exigimos la condición que discutíamos en la sección anterior.

Definición 3.17. Sea N un $K[\mathbf{x}]$-submódulo de $K[\mathbf{x}]^r$ con un orden monomial de módulos $>$ y G un subconjunto de N. Este subconjunto G es una *base de Gröbner* de N si $N = \langle G\rangle$ y $\langle \mathrm{LM}(G)\rangle = \mathrm{LM}(\langle G\rangle)$.

Para verificar si esta clase de conjuntos generadores soluciona de una vez por todas estos problemas, necesitamos unos resultados intermedios.

Lema 3.18 (de Dickson)**.** *Sea $N \subseteq \mathbb{N}^n$ e $I := \langle x^\alpha \mid \alpha \in N\rangle$ un ideal monomial. Entonces existen $\alpha_1, \ldots, \alpha_k$ en N de forma que $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_k}\rangle$.*

Aunque el lema de Dickson habla de ideales monomiales dentro del anillo de polinomios $K[\mathbf{x}]$, extenderlo a submódulos es inmediato. Si pensamos en un $K[\mathbf{x}]$-submódulo N de $K[\mathbf{x}]^r$ generado por monomios,

es decir $N := \left\langle x^\alpha \mathbf{e}_{i_\alpha} | \alpha \in J \right\rangle$ donde $J \subset \mathbb{N}^n$, podemos expresarlo como

$$N = \langle x^\alpha | \alpha \in J \text{ e } i_\alpha = 1 \rangle \mathbf{e}_1 + \langle x^\alpha | \alpha \in J \text{ e } i_\alpha = 2 \rangle \mathbf{e}_2 + \cdots + \langle x^\alpha | \alpha \in J \text{ e } i_\alpha = r \rangle \mathbf{e}_r;$$

por el lema anterior, cada uno de estos «coeficientes» que acompañan a los vectores $\mathbf{e}_i$ es un ideal monomial finitamente generado;

$$\begin{aligned} &= \left\langle x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_{k_1}} \right\rangle \mathbf{e}_1 + \left\langle x^{\beta_1}, x^{\beta_2}, \ldots, x^{\beta_{k_2}} \right\rangle \mathbf{e}_2 + \cdots + \langle x^{\gamma_1}, x^{\gamma_2}, \ldots, x^{\gamma_{k_r}} \rangle \mathbf{e}_r \\ &= \left\langle x^{\alpha_1}\mathbf{e}_1, x^{\alpha_2}\mathbf{e}_1, \ldots, x^{\alpha_{k_1}}\mathbf{e}_1, x^{\beta_1}\mathbf{e}_2, x^{\beta_2}\mathbf{e}_2, \ldots, x^{\beta_{k_2}}\mathbf{e}_2, \ldots, x^{\gamma_1}\mathbf{e}_r, x^{\gamma_2}\mathbf{e}_r, \ldots, x^{\gamma_{k_r}}\mathbf{e}_r \right\rangle. \end{aligned}$$

Este resultado nos permite ver una condición más fuerte sobre los $K[\mathbf{x}]$-submódulos monomiales de $K[\mathbf{x}]^r$: no solo son finitamente generados, como ya sabíamos gracias a la Proposición 3.14, sino que además admiten conjuntos generadores finitos formados por algunos monomios del conjunto generador original.

Lema 3.19. *Sea N un $K[\mathbf{x}]$-submódulo monomial de $K[\mathbf{x}]^r$ de forma que $N = \left\langle x^{\alpha_1}\mathbf{e}_{i_1}, x^{\alpha_2}\mathbf{e}_{i_2}, \ldots, x^{\alpha_k}\mathbf{e}_{i_k} \right\rangle$. Un monomio $x^\beta \mathbf{e}_i$ pertenece a N si y solo si es un múltiplo de alguno de los monomios generadores. En otras palabras, existe $j \in \{1, \ldots, k\}$ de forma que $x^{\alpha_j}\mathbf{e}_{i_j} | x^\beta \mathbf{e}_i$.*

Este pequeño resultado nos da una forma bastante rápida de determinar si un monomio pertenece o no a un $K[\mathbf{x}]$-submódulo monomial de $K[\mathbf{x}]^r$. Démonos cuenta de que esto es justo lo que hacemos cuando intentamos reducir el término líder de f en el algoritmo de la división de la Definición 3.12. Con todo esto, ya damos la respuesta final a la pregunta que abre el capítulo.

Teorema 3.20. *Sea N un $K[\mathbf{x}]$-submódulo de $K[\mathbf{x}]^r$ y sea $G = \{g_1, g_2, \ldots, g_k\}$ una base de Gröbner de N. Un elemento f de $K[\mathbf{x}]^r$ pertenece a N si y solo si el resto de f dividido por G según el algoritmo 3.12 es* 0*.*

Demostración. Como ya mencionamos antes, si el resto es 0 sabemos que $f \in N$. Asumamos ahora que el resto no es 0. Eso quiere decir que en alguna iteración nos hemos encontrado con que $\mathrm{LM}(D)$ no es divisible por ninguno de los $\mathrm{LM}(g_i)$. En todo momento, D es de la forma $f - g$ donde g es una combinación lineal de los elementos de G —los cocientes por los divisores—. Por lo tanto, si $\mathrm{LM}(D)$ no pertenece a $\langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_k) \rangle$, como G es una base de Gröbner, tampoco pertenecerá a $\mathrm{LM}(N)$ y, por lo tanto, $f - g = D \notin N$ lo cual, como g sí que pertenece a N, es equivalente a decir que $f \notin N$. □

Con todo esto, ya tenemos una solución al problema de la pertenencia de un elemento a un submódulo: obtener la base de Gröbner del submódulo y dividir por ella para ver si el resto es nulo o no. Sin embargo, no tenemos garantías de que existan bases de Gröbner para todos los submódulos y, en caso de que sí las haya, tampoco sabemos cómo calcularlas.

Recordemos el problema que nos habíamos encontrado en el Ejemplo 3.15. En este ejemplo, había monomios líderes ocultos en los términos de los generadores. Para desenmascararlos, lo que haremos será lo que vimos en ese ejemplo: anular los términos libres para forzar a que estos aparezcan. Para eso, dados $f = x^\alpha \mathbf{e}_i$ y $g = x^\alpha \mathbf{e}_j$ elementos de $K[\mathbf{x}]^r$ y a y b elementos de $K[\mathbf{x}]$ de forma que $a\mathrm{LM}(f) = b\mathrm{LM}(g) = \mathrm{mcm}(\mathrm{LM}(f), \mathrm{LM}(g))$[1], definimos la siguiente expresión:

$$\mathrm{S}(f,g) = \begin{cases} \frac{a}{\mathrm{LC}(f)} f - \frac{b}{\mathrm{LC}(g)} g & \text{si } i = j; \\ 0 & \text{si } i \neq j. \end{cases}$$

[1] Aquí podría haber un pequeño malentendido con la noción de mínimo común múltiplo: por ejemplo, ¿cuál es el mínimo común múltiplo de xy^2 y x^2y en $\mathbb{R}[x, y]$? Lo natural sería decir x^2y^2, que es nuestra convención, pero también sería válido decir $3x^2y^2$ ya que ambos tienen el mismo orden monomial. Por simplicidad, siempre nos referiremos a aquel que no está multiplicado por constante.

Ejemplo 3.21. Sean $f = 3x^2y\mathbf{e}_1 + 2x\mathbf{e}_2$ y $g = 13x\mathbf{e}_1 + y^5\mathbf{e}_2$ elementos de $\mathbb{R}[x,y]^2$ con el orden $>_{(\mathtt{LEX},\mathtt{POS})}$. Como $\mathrm{LM}(f) = x^2y\mathbf{e}_1$ y $\mathrm{LM}(g) = x\mathbf{e}_1$ están en la misma componente —$\mathbf{e}_1$—, y $\mathrm{mcm}(\mathrm{LM}(f), \mathrm{LM}(g)) = x^2y = \mathrm{LM}(f) = xy\mathrm{LM}(g)$, tenemos que

$$\mathrm{S}(f,g) = \frac{1}{3}\left(3x^2y\mathbf{e}_1 + 2x\mathbf{e}_2\right) + \frac{xy}{13}\left(13x\mathbf{e}_1 + y^5\mathbf{e}_2\right) = \frac{2}{3}x\mathbf{e}_2 + \frac{1}{13}xy^6\mathbf{e}_2.$$

Nótese que esto desvela a $x\mathbf{e}_2$ como un monomio líder en $\mathrm{LM}(\langle f, g\rangle)$.

En esencia, lo que buscaremos hacer es evaluar las parejas de polinomios en el conjunto generador a través de esta expresión, si nos descubren un monomio líder nuevo, lo incorporamos a la base y, si no, seguimos.

Definición 3.22. Sea $G := \{g_1, \ldots, g_k\}$ y $N := \langle G\rangle$. El algoritmo que utilizaremos para obtener una base de Gröbner para N, llamado el *Algoritmo de Buchberger*, se define como sigue:

1: Definimos $d_i \leftarrow g_i$ para $i \in \{1, \ldots, k\}$ y $t \leftarrow k$.
2: **mientras** hayan i y j en $\{1, \ldots, t\}$ de forma que el resto de $\mathrm{S}(g_i, g_i)$ entre $d_1, \ldots, d_t$ no sea 0 **haz**
3: Sean i y j una de esas posibles parejas.
4: Sea r el resto de dividir $\mathrm{S}(g_i, g_j)$ entre $d_1, \ldots, d_t$.
5: $d_{t+1} \leftarrow r$
6: $t \leftarrow t+1$

Al final del algoritmo, $\{d_1, \ldots, d_t\}$ es una base de Gröbner de N.

El funcionamiento de este algoritmo se sustenta en dos pilares. El primero es que, como cada vez que añadimos un nuevo elemento este es un resto cuyo término líder por definición no es múltiplo de ningún $\mathrm{LM}(d_i)$, tenemos que los $K[\mathbf{x}]$-submódulo $\langle \mathrm{LM}(d_1), \ldots, \mathrm{LM}(d_t)\rangle$ forman una cadena ascendente la cual, por ser $K[\mathbf{x}]^r$ noetheriano, debe finalizar en algún momento. Por esto mismo, el algoritmo termina. El segundo es el Teorema 3.23, que nos garantiza que cuando este algoritmo pare, el conjunto que tendremos será una base de Gröbner.

Teorema 3.23 (criterio de Buchberger)**.** *Sea G un subconjunto de $K[\mathbf{x}]^r$, este último equipado con un orden monomial de módulos $>$. G es una base de Gröbner de $\langle G\rangle$ si y solo si para toda pareja de elementos f y g en G se tiene que el resto de $\mathrm{S}(f,g) = 0$ entre G es 0.*

Demostración. Véase el apéndice B. □

Un ejemplo de cálculo de base de Gröbner puede encontrarse en apéndice A.1.

3.3. Sicigias

En la sección anterior hemos solucionado el problema de pertenencia a un $K[\mathbf{x}]$-submódulo de $K[\mathbf{x}]^r$, pero necesitamos conocer los generadores de este submódulo. Por lo tanto, hasta el momento solo hemos resuelto la mitad del problema ya que para $\mathrm{Der}(f)$ todavía no sabemos calcular todavía un conjunto de generadores. Para poder hacer esto, introducimos el concepto de sicigia, una noción que extiende el concepto de solución de un sistema lineal en el caso de un espacio vectorial.

Definición 3.24. Sean A un anillo, M un A-módulo y $f_1, f_2, \ldots, f_k$ elementos de M. Una sicigia de los elementos $f_1, f_2, \ldots, f_k$ es una k-tupla $(g_1, g_2, \ldots, g_k)$ de A^k de forma que $f_1g_1 + f_2g_2 + \cdots + f_kg_k = 0$.

Nótese que el conjunto de sicigias de $f_1, f_2, \ldots, f_k$ forma un A-submódulo de A^k puesto que es el kernel del homomorfismo de A-módulos

$$\begin{aligned} A^k &\xrightarrow{\ \sigma\ } M \\ a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \cdots + a_k\mathbf{e}_k &\longmapsto a_1f_1 + a_2f_2 + \cdots + a_kf_k \end{aligned} \tag{3.2}$$

Definición 3.25. Sean A un anillo, M un A-módulo y $f_1, f_2, \dots, f_k$ elementos de M. Denotaremos por $\operatorname{syz}(f_1, f_2, \dots, f_k)$ *al A-submódulo de A^k formado por todas las sicigias de $f_1, f_2, \dots, f_k$.*

Dale un poco más de bombo a este resultado

Véase que $\operatorname{Der}(f)$, tal y como está definido en (2.1) puede expresarse en términos de sicigias:

$$\operatorname{Der}(f) = \left\{ a_1\partial_1 + a_2\partial_2 + \cdots + a_n\partial_n \,\middle|\, a_1\partial_1 f + a_2\partial_2 f + \cdots + a_n\partial_n f = pf, p \in K[\mathbf{x}] \right\};$$

recordemos que podemos ver ∂_i como $\mathbf{e}_i$;

$$\begin{aligned} &\simeq \left\{ (a_1, a_2, \dots, a_n) \in K[\mathbf{x}]^n \,\middle|\, a_1\partial_1 f + a_2\partial_2 f + \cdots + a_n\partial_n f - pf = 0, p \in K[\mathbf{x}] \right\} \\ &= \left\{ (a_1, a_2, \dots, a_n) \in K[\mathbf{x}]^n \,\middle|\, (a_1, a_2, \dots, a_n, p) \in \operatorname{syz}(\partial_1 f, \partial_2 f, \dots, \partial_n f, f), p \in K[\mathbf{x}] \right\}. \end{aligned}$$

Por lo tanto, para calcular $\operatorname{Der}(f)$ obtendremos primero $\operatorname{syz}(\partial_1 f, \partial_2 f, \dots, \partial_n f, f)$ y nos olvidaremos de la última componente. Ahora nuestro objetivo será calcular sicigias, para lo cual necesitaremos dos resultados. El primero nos permite restringir una base de Gröbner a solamente unas coordenadas.

Lema 3.26. *Sea $>$ un orden monomial de módulos que satisface*

$$x^\alpha \mathbf{e}_i > x^\beta \mathbf{e}_j \Leftrightarrow \begin{cases} i < j & o \\ i = j & y\ x^\alpha >' x^\beta \end{cases} \quad \text{donde } >' \text{ es un orden monomial.} \tag{3.3}$$

Es decir, un orden que mira primero la posición en el orden usual. Sea M un $K[\mathbf{x}]$-submódulo de $K[\mathbf{x}]^n$ y G una base de Gröbner de este con respecto al orden $>$. Entonces, para el módulo restringido a las componentes a partir de la s-ésima, es decir,

$$M_s := \left\{ (m_s, m_{s+1}, \dots, m_n) \,\middle|\, (\underbrace{0, 0, \dots, 0}_{s-1}, m_s, m_{s+1}, \dots, m_n) \in M \right\},$$

el conjunto G_s es una base de Gröbner con respecto al orden $>$.

Demostración. Tomemos un $f_s = (f_s, f_{s+1}, \dots, f_n)$ en M_s. Por definición, este tiene un elemento asociado en M, $f = (0, 0, \dots, 0, f_s, f_{s+1}, \dots, f_m)$. Al ser G una base de Gröbner de M, tendremos que habrá algún $g \in G$ de forma que $\operatorname{LM}(g) | \operatorname{LM}(f)$. Ahora bien, por la condición que satisface el orden, sabemos que todos los términos de g deben encontrarse en la s-ésima componente o por debajo, lo cual nos garantiza que $g = (0, 0, \dots, 0, g_s, g_{s+1}, \dots, g_n)$. Gracias a esto, sabemos que también se cumplirá que $\operatorname{LM}(g_s) | \operatorname{LM}(f_s)$ y, como $G_s \subseteq M_s$, esto es equivalente a que $\operatorname{LM}(M_s) = \langle \operatorname{LM}(G) \rangle$ lo cual nos garantiza que G_s es base de Gröbner con respecto a este orden. □

Démonos cuenta de que esto nos permite calcular bases de Gröbner a M_s con respecto a cualquier orden: escogemos un orden que satisfaga la condición que impone el Lema 3.26 con el cual G_s. Pero démonos cuenta de que G_s es un conjunto generador de M_s independientemente del orden escogido, así que cambiamos el orden y calculamos la base de Gröbner a partir de G_s con respecto a este nuevo orden.

Teorema 3.27. *Sean $f_1, f_2, \dots, f_k$ elementos de $K[\mathbf{x}]^r$ y sean $f_1^+, f_2^+, \dots, f_k^+$ los correspondientes elementos en $K[\mathbf{x}]^{r+k}$ pero en este caso por el principio, es decir, si $f_i = (a_1, a_2, \dots, a_r)$ entonces*

$$f_i^+ = (a_1, a_2, \dots, a_r, \underbrace{0, 0, \dots, 0}_{k}).$$

Entonces, si G es una base de Gröbner de $M := \langle f_1^+ + \mathbf{e}_{r+1}, f_2^+ + \mathbf{e}_{r+2}, \dots, f_k^+ + \mathbf{e}_{r+k} \rangle$ con respecto a un orden $>$ que satisfaga la condición (3.3)*, se tiene que —siguiendo la notación introducida en el Lema 3.26—*

$$\operatorname{syz}(f_1, f_2, \dots, f_k) = \langle G_{r+1} \rangle.$$

En particular, G_{r+1} es una base de Gröbner de $\operatorname{syz}(f_1, f_2, \dots, f_k)$ con respecto al orden $>$.

Demostración. Por el lema anterior sabemos que G_{r+1} es una base de Gröbner de M_{r+1}. Queda pues comprobar que $M_{r+1} = \operatorname{syz}\left(f_1, f_2, \ldots, f_k\right)$. Supongamos[2] que $m_{r+1} = \left(\mu_{r+1}, \mu_{r+2}, \ldots, \mu_{r+k}\right) \in M_{r+1}$, entonces existe un elemento asociado $m = \left(0, 0, \ldots, 0, \mu_{r+1}, \mu_{r+2}, \ldots, \mu_{r+k}\right) \in M$. Podemos expresar m de dos formas, una en términos de los vectores de la base canónica y otra en términos de los $f_i^+ + \mathbf{e}_{r+i}$ que generan M:

$$\begin{aligned}\mu_{r+1}\mathbf{e}_{r+1} + \mu_{r+2}\mathbf{e}_{r+2} + \cdots + \mu_{r+k}\mathbf{e}_{r+k} &= b_1\left(f_1^+ + \mathbf{e}_{r+1}\right) + b_2\left(f_2^+ + \mathbf{e}_{r+2}\right) + \cdots + b_k\left(f_k^+ + \mathbf{e}_{r+k}\right), \quad b_j \in K[\mathbf{x}]; \\ &= \left(b_1 f_1^+ + b_2 f_2^+ + \cdots + b_k f_k^+\right) \; + \; \left(b_1\mathbf{e}_{r+1} + b_2\mathbf{e}_{r+2} + \cdots + b_k\mathbf{e}_{r+k}\right).\end{aligned}$$

Como todas las componentes de f_i^+ desde la $r+1$-ésima —incluida— son 0, podemos extraer dos conclusiones. La primera es que $b_i = \mu_i$ ya que son los únicos coeficientes que acompañan a las últimas componentes; y la segunda es que

$$\mu_1 f_1 + \mu_2 f_2 + \cdots + \mu_k f_k = b_1 f_1 + b_2 f_2 + \cdots + b_k f_k = 0.$$

Por ende, $m_{r+1} \in \operatorname{syz}\left(f_1, f_2, \ldots, f_k\right)$. En el otro sentido, si tenemos que $m_{r+1} := \left(\mu_1, \mu_2, \ldots, \mu_k\right)$ pertenece a $\operatorname{syz}\left(f_1, f_2, \ldots, f_k\right)$, entonces existe

$$m := \mu_{r+1}\left(f_1^+ + \mathbf{e}_{r+1}\right) + \mu_{r+2}\left(f_2^+ + \mathbf{e}_{r+2}\right) + \cdots + \mu_{r+k}\left(f_k^+ + \mathbf{e}_{r+k}\right) \in M$$

con sus primeras r componentes nulas y las últimas k coinciden con las de m_{r+1}. Por lo tanto, $m_{r+1} \in M_{r+1}$. Concluimos, pues, que $M_{r+1} = \operatorname{syz}\left(f_1, f_2, \ldots, f_k\right)$. □

Por lo tanto, para calcular $\operatorname{syz}\left(f_1, f_2, \ldots, f_k\right)$, primero calcularemos una base de Gröbner G de

$$\left\langle f_1^+ + \mathbf{e}_{r+1}, f_2^+ + \mathbf{e}_{r+2}, \ldots, f_k^+ + \mathbf{e}_{r+k} \right\rangle.$$

Por este último teorema, sabemos que G_{k+1} es un conjunto generador de $\operatorname{syz}\left(f_1, f_2, \ldots, f_k\right)$ y en particular una base de Gröbner con respecto al orden que hayamos escogido. Si deseamos una base de Gröbner con respecto a otro orden, como decíamos antes de este teorema, basta con aplicar el algoritmo de Buchberger sobre G_{k+1}.

[2]Para que el lector sepa en todo momento cuándo un elemento está en $K[\mathbf{x}]^{r+k}$ o $K[\mathbf{x}]^k$, utilizamos el subíndice en el elemento dándole consistencia con la notación utilizada en el lema anterior. Pero este no debe ser interpretado de forma distinta que si pusiéramos m' o $\overline{m}$; es decir, el subíndice sobre un elemento no debe verse como el resultado de una «proyección».

Capítulo 4

El Criterio de Saito

En el capítulo anterior concluíamos con un método para calcular $\mathrm{Der}(f)$ utilizando las sicigias, una herramienta que hemos derivado de las bases de Gröbner. Con estas, podemos obtener un conjunto generador de $\mathrm{Der}(f)$ e incluso una base de Gröbner de este mismo que nos permita determinar si una derivación está o no en el conjunto. Pero otra pregunta de gran importancia aparece cuando consideramos una gran diferencia entre módulos y espacios vectoriales: así como para estos últimos siempre tenemos que los subespacios admiten una base, en el caso de los módulos no tiene por qué ser así.

Ejemplo 4.1. Consideremos el $K[x,y]$-módulo $\langle x, y\rangle$. Por ser noetheriano, sabemos que, de existir alguna base para $\langle x, y\rangle$, esta debe de ser finita. Supongamos que existe y es $\{a_1, a_2, \ldots, a_k\}$. Entonces, existirán unos únicos $p_1, p_2, \ldots, p_k$ y $q_1, q_2, \ldots, q_k$ en $K[x,y]$ de forma que

$$p_1a_1 + p_2a_2 + \cdots + p_ka_k = x \quad \text{y} \quad q_1a_1 + q_2a_2 + \cdots + q_ka_k = y.$$

Esto nos permite llegar a la siguiente igualdad:

$$yp_1a_1 + yp_2a_2 + \cdots + yp_ka_k = xy = xq_1a_1 + xq_2a_2 + \cdots + xq_ka_k.$$

Ahora bien, por ser $\{a_1, a_2, \ldots, a_k\}$ una base, necesariamente tendremos que $yp_i = xq_i$ para todo i. Como $\mathrm{mcd}(x,y) = 1$, es necesario que $p_i = xp_i'$. Esto nos lleva a que

$$\begin{aligned} xp_1'a_1 + xp_2'a_2 + \cdots + xp_k'a_k &= x \\ x\left(p_1'a_1 + p_2a_2' + \cdots + p_k'a_k\right) &= x, \end{aligned}$$

El anillo $K[\mathbf{x}]$ es un dominio de integridad por lo que podemos simplificar,

$$p_1'a_1 + p_2a_2' + \cdots + p_k'a_k = 1.$$

Esto último es una contradicción, ya que $1 \notin \langle x, y\rangle$.

Antes de poder enunciar el criterio de Saito, necesitamos una definición más.

Definición 4.2. Un polinomio $p \in K[\mathbf{x}]$ se dice libre de cuadrados si, en caso de poder expresarlo de la forma $p = a^2b$, se tiene que a es una unidad de $K[\mathbf{x}]$.

Lema 4.3. *Un polinomio $p \in K[\mathbf{x}]$ es libre de cuadrados si y solo si* $\mathrm{mcd}\left(p, \frac{\partial p}{\partial x_1}, \frac{\partial p}{\partial x_2}, \ldots, \frac{\partial p}{\partial x_n}\right)$ *es una unidad de $K[\mathbf{x}]$.*

El criterio de Saito nos da una forma bastante rápida de determinar si $\mathrm{Der}(f)$ es o no libre. Nos permitimos la licencia de denotar por δ_i tanto a la derivación como al vector de coeficientes asociado en $K[\mathbf{x}]^n$.

Teorema 4.4 (Criterio de Saito)**.** *Sea f un polinomio libre de cuadrados de $K[\mathbf{x}]$ y $\delta_1, \delta_2, \ldots, \delta_n$ derivaciones de* $\mathrm{Der}(f)$*. Entonces,* $\mathrm{Der}(f)$ *es libre si y solo si* $\det\left(\delta_1, \delta_2, \ldots, \delta_n\right) = uf$ *donde u es una unidad de K, es decir, un elemento de $K \setminus \{0\}$.*

En este capítulo explicaremos la demostración de este resultado que aparecen en [2]. Pero primero, deberemos ilustrar algunas construcciones que se utilizan en dicha demostración.

4.1. Producto Exterior

De cara a la demostración del Criterio de Saito, utilizaremos una operación que nos será de gran ayuda: el producto exterior. Para entender esta, necesitaremos entender primero el producto tensorial. En esencia, el producto tensorial aparece en el siguiente contexto: supongamos que M, N y O son A-módulos y tenemos una aplicación $b : M \times N \to O$ que es bilineal, o sea, que $b(\bullet, n)$ y $b(m, \bullet)$ son homorfismos de A-módulos para cualquier $m \in M$ y $n \in N$; nos gustaría encontrar un A-módulo E a partir de $M \times N$ en el cual exista un homomorfismo de A-módulos $b' : E \to O$ que se comporte como b. En resumen, queremos que para cada (m,n) en $M \times N$ exista un elemento $m * n$ en E de forma que $b'(m * n) = b(m,n)$. Esta es la motivación de la construcción del producto tensorial.

Definición 4.5. Sea A un anillo y M y N dos A-módulos. Tomemos como E al A-módulo definido como $\bigoplus_{\substack{m\in M\\ n\in N}} A \cdot \mathbf{e}_{m,n}$ donde $\mathbf{e}_{m,n}$ debe entenderse como la tupla (m,n) sin ningún tipo de operación asociada, es decir, no debemos pensar que $\mathbf{e}_{m,n} + \mathbf{e}_{m',n'} = \mathbf{e}_{m+m',n+n'}$ al igual que no pensamos que $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{e}_3$. Ahora, consideremos dentro de E el A-submódulo S definido por

$$S = \left\langle \begin{matrix} \mathbf{e}_{m+m',n} - \mathbf{e}_{m,n} - \mathbf{e}_{m',n}, & \mathbf{e}_{m,n+n'} - \mathbf{e}_{m,n} - \mathbf{e}_{m,n'}, \\ \mathbf{e}_{am,n} - a\mathbf{e}_{m,n}, & \mathbf{e}_{m,an} - a\mathbf{e}_{m,n} \end{matrix} \middle| \, a \in A, m \in M, n \in N \right\rangle.$$

Definimos el producto tensorial de M por N como $M \otimes N := {}^{E}\!/_{S}$ y denotaremos a la clase de equivalencia de cada $\mathbf{e}_{m,n}$ como $m \otimes n$.

Ejemplo 4.6. Quizás el ejemplo más natural sea el producto escalar. Así pues, tomemos la aplicación $\langle \bullet, \bullet \rangle : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$, que es bilineal. En este caso, todo elemento de $\mathbb{R}^3 \otimes \mathbb{R}^3$ es de la siguiente forma —entendiendo S como en la definición de antes—:

$$\begin{aligned} \begin{pmatrix} a \\ b \\ c \end{pmatrix} \otimes \begin{pmatrix} d \\ e \\ f \end{pmatrix} + S &= \left(a\mathbf{e}_1 + b\mathbf{e}_2 + c\mathbf{e}_3\right) \otimes \left(d\mathbf{e}_1 + e\mathbf{e}_2 + f\mathbf{e}_3\right) + S \\ &= ad\,\mathbf{e}_1 \otimes \mathbf{e}_1 + ae\,\mathbf{e}_1 \otimes \mathbf{e}_2 + af\,\mathbf{e}_1 \otimes \mathbf{e}_3 + bd\,\mathbf{e}_2 \otimes \mathbf{e}_1 \\ &\quad + be\,\mathbf{e}_2 \otimes \mathbf{e}_2 + bf\,\mathbf{e}_2 \otimes \mathbf{e}_3 + cd\,\mathbf{e}_3 \otimes \mathbf{e}_1 + ce\,\mathbf{e}_3 \otimes \mathbf{e}_2 + cf\,\mathbf{e}_3 \otimes \mathbf{e}_3 + S \end{aligned} \tag{4.1}$$

(De aquí en adelante omitiremos los «$+S$» o similares sumas por el A-submódulo que estemos haciendo el cociente.)

Vemos pues que $\left\{ \mathbf{e}_i \otimes \mathbf{e}_j \,|\, i,j \in \{1,2,3\} \right\}$ es una base de $\mathbb{R}^3 \otimes \mathbb{R}^3$. Por lo tanto, para encontrar una aplicación lineal $\phi : \mathbb{R}^3 \otimes \mathbb{R}^3 \to \mathbb{R}$ que coincida con el producto escalar debemos dar las imágenes de la base. En este caso,

$$\phi\left(\mathbf{e}_i \otimes \mathbf{e}_j\right) = \left\langle \mathbf{e}_i, \mathbf{e}_j \right\rangle = \begin{cases} 1 & \text{si } i = j; \\ 0 & \text{si } i \neq j. \end{cases}$$

Si evaluamos esta aplicación lineal f en el producto anterior veremos que, en efecto, nos devuelve el valor que queremos. Por lo tanto, gracias al producto tensorial hemos convertido una aplicación bilineal en una aplicación lineal a costa de tener un dominio algo más complicado.

Ahora supongamos que aquello en lo que queremos trabajar son aplicaciones bilineales alternadas, es decir, $b : M \times M \to N$ donde $b\left(m,m'\right) = -b\left(m',m\right)$. En esta situación tendremos que imponer que $m \otimes n = -n \otimes m$.

Definición 4.7. Sea A un anillo y M un A-módulo. Consideremos el A-submódulo T de $M \otimes M$ definido como

$$T = \left\langle m \otimes m' - m' \otimes m | m, m' \in M \right\rangle.$$

Definiremos el producto exterior de M por M como $M \wedge M := {}^{(M\otimes M)}/_{T}$ y denotaremos la clase de equivalencia de cada (m, m') como $m \wedge m'$.

Nótese que ahora $m \wedge m = 0$.

Ejemplo 4.8. El ejemplo natural en el caso de aplicaciones bilineales alternadas es el producto vectorial $\bullet\times\bullet : \mathbb{R}^3 \times \mathbb{R} \to \mathbb{R}^3$. Podemos aplicar el mismo proceso que en (4.1).

$$\begin{aligned}\begin{pmatrix} a \\ b \\ c \end{pmatrix} \wedge \begin{pmatrix} d \\ e \\ f \end{pmatrix} &= \left(a\mathbf{e}_1 + b\mathbf{e}_2 + c\mathbf{e}_3\right) \wedge \left(d\mathbf{e}_1 + e\mathbf{e}_2 + f\mathbf{e}_3\right) \\ &= ad\mathbf{e}_1 \wedge \mathbf{e}_1 + ae\mathbf{e}_1 \wedge \mathbf{e}_2 + af\mathbf{e}_1 \wedge \mathbf{e}_3 + bd\mathbf{e}_2 \wedge \mathbf{e}_1 \\ &\quad + be\mathbf{e}_2 \wedge \mathbf{e}_2 + bf\mathbf{e}_2 \wedge \mathbf{e}_3 + cd\mathbf{e}_3 \wedge \mathbf{e}_1 + ce\mathbf{e}_3 \wedge \mathbf{e}_2 + cf\mathbf{e}_3 \wedge \mathbf{e}_3;\end{aligned}$$

suprimimos los elementos de la forma $\mathbf{e}_i \wedge \mathbf{e}_i$ y ponemos todas las parejas $\mathbf{e}_i \wedge \mathbf{e}_j$ de forma que $i < j$;

$$\begin{aligned}&= ae\mathbf{e}_1 \wedge \mathbf{e}_2 + af\mathbf{e}_1 \wedge \mathbf{e}_3 - bd\mathbf{e}_1 \wedge \mathbf{e}_2 + bf\mathbf{e}_2 \wedge \mathbf{e}_3 - cd\mathbf{e}_1 \wedge \mathbf{e}_3 - ce\mathbf{e}_2 \wedge \mathbf{e}_3 \\ &= (ae - bd)\mathbf{e}_1 \wedge \mathbf{e}_2 + (af - cd)\mathbf{e}_1 \wedge \mathbf{e}_3 + (bf - ce)\mathbf{e}_2 \wedge \mathbf{e}_3.\end{aligned}$$

Vemos por lo tanto que $\mathbb{R}^3 \wedge \mathbb{R}^3$ tiene como base $\left\{\mathbf{e}_1 \wedge \mathbf{e}_2, \mathbf{e}_1 \wedge \mathbf{e}_3, \mathbf{e}_2 \wedge \mathbf{e}_3\right\}$ y las imágenes de estos son

$$\phi\left(\mathbf{e}_1 \wedge \mathbf{e}_2\right) = \mathbf{e}_1 \times \mathbf{e}_2 = \mathbf{e}_3, \quad \phi\left(\mathbf{e}_1 \wedge \mathbf{e}_3\right) = \mathbf{e}_1 \times \mathbf{e}_3 = -\mathbf{e}_2 \text{ y } \phi\left(\mathbf{e}_2 \wedge \mathbf{e}_3\right) = \mathbf{e}_2 \times \mathbf{e}_3 = \mathbf{e}_1.$$

Vemos de nuevo que la aplicación ϕ es lineal y nos devuelve el producto vectorial.

Estas mismas ideas pueden extenderse a aplicaciones n-lineales para construir productos como $\bigotimes^n M = M \otimes M \otimes \cdots \otimes M$ y, consecuentemente a aplicaciones n-lineales alternadas para construir $\bigwedge^n M := M \wedge M \wedge \cdots \wedge M$.

Aunque pueda parecer que los productos exteriores hacen un espacio «más grande», esto no tiene por qué ser así.

Ejemplo 4.9. Consideremos $\mathbb{R}^3 \wedge \mathbb{R}^3 \wedge \mathbb{R}^3$. Los elementos son de la forma

$$\begin{aligned}\begin{pmatrix} a \\ b \\ c \end{pmatrix} \wedge \begin{pmatrix} d \\ e \\ f \end{pmatrix} \wedge \begin{pmatrix} g \\ h \\ i \end{pmatrix} &= aei\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3 + afh\mathbf{e}_1 \wedge \mathbf{e}_3 \wedge \mathbf{e}_2 + bdi\mathbf{e}_2 \wedge \mathbf{e}_1 \wedge \mathbf{e}_3 \\ &\quad + bfg\mathbf{e}_2 \wedge \mathbf{e}_3 \wedge \mathbf{e}_1 + cdh\mathbf{e}_3 \wedge \mathbf{e}_1 \wedge \mathbf{e}_2 + ceg\mathbf{e}_3 \wedge \mathbf{e}_2 \wedge \mathbf{e}_1;\end{aligned}$$

donde podemos ver que, por ejemplo, $\mathbf{e}_2 \wedge \mathbf{e}_3 \wedge \mathbf{e}_1 = -\mathbf{e}_2 \wedge \mathbf{e}_1 \wedge \mathbf{e}_3 = \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3$ y así expresamos todos estos productos en términos de $\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3$;

$$= (aei + bfg + cdh - (ceg + afh + bdi))\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3. \tag{4.2}$$

Vemos, por lo tanto, que $\mathbb{R}^3 \wedge \mathbb{R}^3 \wedge \mathbb{R}^3$ es en realidad $\mathbb{R}\left(\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3\right)$, un espacio isomorfo a $\mathbb{R}$.

Lo que ocurre en estos casos es que los distintos órdenes en los que pongamos los elementos de un producto exterior $v_1 \wedge v_2 \wedge \cdots \wedge v_k$ solo lo cambian en signo. Podemos resumir lo que ocurre en el siguiente lema.

Lema 4.10. *Sea V un espacio vectorial de dimensión n. Entonces,* $\dim \bigwedge^k V = \binom{n}{k}$. *En particular, nótese que si $k > n$, entonces $\bigwedge^k V = \{0\}$.*

Por otro lado, podemos extender los homomorfismos de A-módulos que ya conocemos a productos exteriores de una forma natural.

Definición 4.11. Sea A un anillo, M y N dos A-módulos y $\phi : M \to N$ un homomorfismo de A-módulos. Definimos la aplicación $\bigwedge^k \phi : \bigwedge^k M \to \bigwedge^k N$ como sigue:

$$m_1 \wedge m_2 \wedge \cdots \wedge m_k \longmapsto \phi(m_1) \wedge \phi(m_2) \wedge \cdots \wedge \phi(m_k).$$

Un fenómeno relevante ocurre cuando tenemos dos espacios vectoriales V y W de la misma dimensión cada uno con una base $\{v_1, v_2, \ldots, v_n\}$ y $\{w_1, w_2, \ldots, w_n\}$ y una aplicación lineal $\phi : V \to W$ entre ellos. Escribiendo las coordenadas en función de estas bases, la aplicación lineal ϕ tiene asociada una matriz P de forma que las coordenadas de la imagen de v_i a través de ϕ son la i-ésima columna de P. Ahora bien, $\bigwedge^n V$ y $\bigwedge^n W$ son espacios vectoriales de dimensión 1 con base $v_1 \wedge v_2 \wedge \cdots \wedge v_n$ y $w_1 \wedge w_2 \wedge \cdots \wedge w_n$, respectivamente. Por lo tanto, la aplicación $\bigwedge^n \phi : \bigwedge^n V \to \bigwedge^n W$ simplemente será multiplicar por un escalar. Qué escalar es este nos lo dice el siguiente lema.

Proposición 4.12. *Sea $\phi : V \to W$ como en el párrafo anterior. Entonces, la aplicación lineal $\bigwedge^n \phi : \bigwedge^n V \to \bigwedge^n W$ envía*

$$v_1 \wedge v_2 \wedge \cdots \wedge v_n \mapsto \det \Phi w_1 \wedge w_2 \wedge \cdots \wedge w_n.$$

Demostración. Es suficiente con el razonamiento del párrafo anterior y un desarrollo similar al de (4.2), que como puede verse, es el determinante de una matriz 3×3:

$$\bigwedge^n \phi(v_1 \wedge v_2 \wedge \cdots \wedge v_n) = P_1 \wedge P_2 \wedge \cdots \wedge P_n = (\det P)\, w_1 \wedge w_2 \wedge \cdots \wedge w_n. \tag{4.3}$$

□

4.2. Demostración del Criterio de Saito

A lo largo de esta demostración, utilizaremos fuertemente el hecho de que $\mathrm{Der}(f)$ es un $K[\mathbf{x}]$-módulo reflexivo. Esto se debe a que podemos encontrar ciertas relaciones entre los módulos reflexivos y los módulos libres. Por un lado, tenemos la siguiente relación:

$$M \text{ módulo libre} \xRightarrow{\text{lema 2.26}} M \text{ módulo proyectivo} \Longrightarrow M \text{ módulo reflexivo}$$

$$M \text{ módulo libre} \xLeftarrow[\substack{\text{Teorema de Quillen-Suslin} \\ [6]}]{\text{si } M \text{ es un } K[\mathbf{x}]\text{-módulo}} M \text{ módulo proyectivo} \xLeftarrow{\text{si } M \text{ es un } K[x,y]\text{-módulo}} M \text{ módulo reflexivo}$$

Gracias a estas implicaciones podemos asegurar que todo módulo libre es reflexivo. Sin embargo, solo podemos asegurar que los módulos reflexivos sean libres cuando son $K[x, y]$-módulo, es decir, cuando admitan la estructura de módulo asociada a un anillo de polinomios en dos variables. Esto, por lo tanto, nos garantiza que $\mathrm{Der}(f)$ es siempre libre cuando $f \in K[x, y]$. Más que solucionar nuestro problema, estos resultados nos sirven para ilustrar la gran dificultad que supone garantizar que un módulo reflexivo sea libre.

4.2.1. El papel del rango

En un módulo libre, la noción de rango es simplemente la cantidad de elementos que tiene la base. Pero como ya hemos visto a lo largo de este trabajo, hay módulos que no tienen por qué ser libres. Por ende, necesitamos generalizar la noción de rango para poder tratar con estos.

Definición 4.13. Sea A un dominio de integridad y $\sim$ la relación de equivalencia sobre $A \times (A \setminus \{0\})$ dada por $(a, b) \sim (\alpha, \beta) \iff a\beta = \alpha b$. A la clase de equivalencia de (a, b) la denotaremos $\frac{a}{b}$. El conjunto

$$\mathrm{Q}(A) := {}^{A \times (A \setminus \{0\})}\!/_{\sim}$$

junto con las operaciones

$$\frac{a}{b}+\frac{\alpha}{\beta} := \frac{a\beta+\alpha b}{b\beta} \quad \text{y} \quad \frac{a}{b}\cdot\frac{\alpha}{\beta} := \frac{a\alpha}{b\beta}$$

forma un cuerpo al cual llamaremos cuerpo de fracciones de A. El homomorfismo natural $A \hookrightarrow \mathrm{Q}(A)$ es inyectivo.

El cuerpo de fracciones de un anillo nos permite llevar un A-módulo a un $\mathrm{Q}(A)$-espacio vectorial.

Definición 4.14. Llamaremos extensión de escalares del A-módulo M al conjunto $M \otimes \mathrm{Q}(A)$.

Lema 4.15. *La extensión de escalares de un A-módulo M es un $\mathrm{Q}(A)$-espacio vectorial. Además, la aplicación $\varphi : M \to M \otimes \mathrm{Q}(A)$ dada por $m \mapsto m \otimes 1$ es inyectiva si y solo si M es libre de torsión.*

Demostración. Para la primera afirmación, vemos que $M \otimes \mathrm{Q}(A)$ es un $\mathrm{Q}(A)$-módulo y, como $\mathrm{Q}(A)$ es un cuerpo, tenemos un espacio vectorial.

Para la segunda, véase que

$$\begin{aligned} \ker\varphi = 0 &\iff m\otimes 1 \neq 0 \quad \forall m \in M\setminus\{0\} \\ &\iff am\otimes\frac{1}{a} \neq 0 \quad \forall a \in A\setminus\{0\} \\ &\implies am \neq 0 \end{aligned}$$

La otra implicación.

□

Definición 4.16. Sea M un A-módulo finitamente generado. Diremos que M tiene rango r si $M \otimes \mathrm{Q}(A)$ es un $\mathrm{Q}(A)$-espacio vectorial de dimensión r.

Recordemos que ya en 4.10 había un resultado sobre el rango del producto exterior de los espacios vectoriales. Generalizamos esto a los módulos.

Lema 4.17. *Sea M un A-módulo de rango n y $s \in \mathbb{N}$. Entonces, $\bigwedge^s M$ es un A-módulo de rango $\binom{n}{s}$.*

Demostración. Consideremos $\left(\bigwedge^s M\right) \otimes \mathrm{Q}(A)$. Hay un isomorfismo de $\mathrm{Q}(A)$-módulos entre $\bigwedge^s M \otimes \mathrm{Q}(A)$ y $\bigwedge^s (M \otimes \mathrm{Q}(A))$:

$$\begin{aligned} \bigwedge^s M \otimes \mathrm{Q}(A) &\longleftrightarrow \bigwedge^s (M \otimes \mathrm{Q}(A)) \\ \left(m_1 \wedge m_2 \wedge \cdots \wedge m_s\right) \otimes \frac{a}{b} &\longrightarrow \left(m_1 \otimes \frac{a}{b}\right) \wedge \left(m_2 \otimes 1\right) \wedge \cdots \wedge \left(m_s \otimes 1\right) \\ \left(m_1 \wedge m_2 \wedge \cdots \wedge m_s\right) \otimes \frac{a_1 a_2 \ldots a_s}{b_1 b_2 \ldots b_s} &\longleftarrow \left(m_1 \otimes \frac{a_1}{b_1}\right) \wedge \left(m_2 \otimes \frac{a_2}{b_2}\right) \wedge \cdots \wedge \left(m_s \otimes \frac{a_s}{b_s}\right) \end{aligned}$$

Aunque pudiera parecer que no es un isomorfismo puesto que los lados derechos no lucen iguales, recordemos que por las propiedades del producto tensorial y exterior y por ser ambos conjuntos $\mathrm{Q}(A)$-módulo tenemos que

$$\begin{aligned} \left(m_1 \otimes \frac{a_1}{b_1}\right) \wedge \left(m_2 \otimes \frac{a_2}{b_2}\right) \wedge \cdots \wedge \left(m_s \otimes \frac{a_s}{b_s}\right) &= \left[\frac{a_1}{b_1}\left(m_1 \otimes 1\right)\right] \wedge \left[\frac{a_2}{b_2}\left(m_2 \otimes 1\right)\right] \wedge \cdots \wedge \left[\frac{a_s}{b_s}\left(m_s \otimes 1\right)\right] \\ &= \frac{a_1 a_2 \ldots a_s}{b_1 b_2 \ldots b_s}\left(m_1 \otimes 1\right) \wedge \left(m_2 \otimes 1\right) \wedge \cdots \wedge \left(m_s \otimes 1\right) \\ &= \left(m_1 \otimes \frac{a_1 a_2 \ldots a_s}{b_1 b_2 \ldots b_s}\right) \wedge \left(m_2 \otimes 1\right) \wedge \cdots \wedge \left(m_s \otimes 1\right). \end{aligned}$$

Ahora bien, por hipótesis $M \otimes \mathrm{Q}(A)$ es un $\mathrm{Q}(A)$-espacio vectorial de rango n así que $\bigwedge^n (M \otimes \mathrm{Q}(A))$ será también un $\mathrm{Q}(A)$-espacio vectorial, en este caso de rango $\binom{n}{s}$. Gracias al isomorfismo, $\left(\bigwedge^s M\right) \otimes \mathrm{Q}(A)$ es igualmente otro $\mathrm{Q}(A)$-espacio vectorial de rango $\binom{n}{s}$ lo cual quiere decir que M es de rango $\binom{n}{s}$. □

Esta cadena de implicaciones que recogemos aquí nos será muy útil a lo largo de la demostración del Criterio de Saito:

$$\left.\begin{array}{l} M \text{ módulo reflexivo} \xRightarrow{[8,\ \text{Tag 0AV0}]} M \text{ libre de torsión} \\ \qquad\qquad\qquad\qquad\quad M \text{ de rango } 1 \end{array}\right\} \Longrightarrow M \text{ es un ideal de } K[\mathbf{x}] \left.\begin{array}{l} \\ \\ M \text{ es reflexivo} \end{array}\right\} \Longrightarrow M \text{ es un módulo libre} \tag{4.4}$$

4.2.2. Comienzo de la demostración

Puede encontrarse en [7, corolario 1.7] una demostración de que $\mathrm{Der}(f)$ es un módulo reflexivo de rango n. Siguiendo el esquema, tenemos que $\mathrm{Der}(f)$ es libre de torsión, pero necesitaríamos que tuviese rango 1 para continuar hacia delante. Lo que haremos será estudiar el módulo $\bigwedge^n \mathrm{Der}(f)$ para reducir este rango y poder continuar.

El Lema 4.17 nos garantiza que $\bigwedge^n \mathrm{Der}(f)$ es un $K[\mathbf{x}]$-módulo reflexivo de rango 1. Siguiendo el esquema en 4.4, tenemos que $\bigwedge^n \mathrm{Der}(f)$ es también libre de torsión y, por lo tanto, $\bigwedge^n \mathrm{Der}(f)$ es isomorfo a un ideal de $K[\mathbf{x}]$. Por último, aplicando la última de las implicaciones, tenemos que $\bigwedge^n \mathrm{Der}(f)$ es un $K[\mathbf{x}]$-módulo libre y además de rango 1. Sumado a esto tenemos que $\bigwedge^n \mathrm{Der}(f)$ es un $K[\mathbf{x}]$-submódulo de $\bigwedge^n \mathrm{Der}(K[\mathbf{x}]) = \langle \partial_1 \wedge \partial_2 \wedge \cdots \wedge \partial_n \rangle$, por lo tanto, $\mathrm{Der}(f) = \langle p\partial_1 \wedge \partial_2 \wedge \cdots \wedge \partial_n \rangle$ para algún p. Nótese que este p está bien definido salvo por alguna unidad de $K[\mathbf{x}]$, es decir, tanto nos daría poner p que kp siempre y cuando exista $k^{-1} \in K[\mathbf{x}]$.

Ahora bien, recordemos la sucesión exacta de 2.2. Podemos aplicar productos exteriores a los elementos, pero esto hace que la sucesión pueda dejar de ser exacta. Sin embargo, habrá un homomorfismo

$$\bigwedge^n \mathrm{Der}(f) \xrightarrow{\bigwedge^n \Phi} \bigwedge^n \mathrm{Der}(K[\mathbf{x}]).$$

Recordemos lo que ocurría en 4.12. De forma similar, aquí tendremos que $\bigwedge^n \Phi$ se corresponde con multiplicar por el escalar p —o up donde u es una unidad de $K[\mathbf{x}]$—. Sin embargo, el hecho de que no tengamos base de $\mathrm{Der}(f)$ impide que se pueda ver Φ como una matriz. Aun así, nos permitimos el abuso de notación de llamar $\det \Phi := p$, pero no es más que una convención, no se trata de un determinante de una matriz como ocurre en el caso de las aplicaciones entre espacios vectoriales. Tenemos pues que $\bigwedge^n \mathrm{Der}(f) = \langle \det \Phi \partial_1 \wedge \partial_2 \wedge \cdots \wedge \partial_n \rangle$.

4.2.3. $\mathrm{Der}(f)$ libre implica $\det\left(\delta_1, \delta_2, \ldots, \delta_n\right) = uf$

Ahora, por un lado, definamos $N := \langle \delta_1, \delta_2, \ldots, \delta_n \rangle$ como un $K[\mathbf{x}]$-submódulo de $\mathrm{Der}(f)$ donde los δ_i forman una base de $\mathrm{Der}(f)$ y consideremos la inclusión $N \xrightarrow{\iota} \mathrm{Der}(f)$. Para aclararnos algo más, escribimos el siguiente esquema de los homomorfismos —¡ojo!, esto no es una sucesión exacta—:

$$N = \langle \delta_1, \delta_2, \ldots, \delta_n \rangle \xrightarrow{\iota} \mathrm{Der}(f) \xrightarrow{\Phi} \mathrm{Der}(K[\mathbf{x}]). \tag{4.5}$$

Como los $\delta_i \in \mathrm{Der}(K[\mathbf{x}]) = \langle \partial_1, \partial_2, \ldots, \partial_n \rangle$, tenemos que existe alguna matriz $A \in \mathrm{Mat}(n \times n, K[\mathbf{x}])$ de forma que

$$\left(\delta_1, \delta_2, \ldots, \delta_n\right) = \left(\partial_1, \partial_2, \ldots, \partial_n\right) A \tag{4.6}$$

Por lo tanto, podemos pensar en que la aplicación $\Phi \circ \iota$ envía a cada δ_i a $\left(\partial_1, \partial_2, \ldots, \partial_n\right) A_i$ donde A_i es la i-ésima columna de A. Es decir, que las columnas de A se entienden como las coordenadas de los δ_i en función de la base $\left\{\partial_1, \partial_2, \ldots, \partial_n\right\}$[1]. Pensemos ahora en la aplicación

$$N \xrightarrow{\bigwedge^n (\Phi \circ \iota)} \mathrm{Der}(K[\mathbf{x}])$$

$$\delta_1 \wedge \delta_2 \wedge \cdots \wedge \delta_n \longmapsto \partial_1 \wedge \partial_2 \wedge \cdots \wedge \partial_n \det A$$

[1] Es decir, que $\det\left(\delta_1, \delta_2, \ldots, \delta_n\right) = \det A$.

Vemos[2] por ella que $\det(\Phi\circ\imath) = \det\Phi\det\imath = \det A$. Como $\imath$ es un monomorfismo, puede representarse como una matriz que tiene inversa en $\mathrm{Mat}(n\times n, K[\mathbf{x}])$ y por la regla de Cramer[3] para la matriz inversa, $\det i$ debe ser unidad de $K[\mathbf{x}]$.

El valor del determinante

Por un lado, fijamos $f\partial_i \in \mathrm{Der}(f)$; y por otro, definimos $\theta_{i,j} := \frac{\partial f}{\partial x_i}\partial_j - \frac{\partial f}{\partial x_j}\partial_i \in \mathrm{Der}(f)$. Así,

$$\theta_{i,1}\wedge\theta_{i,2}\wedge\cdots\wedge\theta_{i,i-1}\wedge f\partial_i\wedge\theta_{i,i+1}\wedge\cdots\wedge\theta_{i,n-1}\wedge\theta_{i,n} \in \bigwedge^n \mathrm{Der}(f).$$

Pero, simplificando todos los productos exteriores nulos nos queda

$$f\left(\frac{\partial f}{\partial x_i}\right)^{n-1}\partial_1\wedge\partial_2\wedge\cdots\wedge\partial_n \in \bigwedge^n \mathrm{Der}(f) = \langle \det\Phi\,\partial_1\wedge\partial_2\wedge\cdots\wedge\partial_n\rangle.$$

Esto quiere decir que $\det\Phi \mid f\left(\frac{\partial f}{\partial x_i}\right)^{n-1}$ para todo i. Asimismo, el máximo común divisor de todos ellos también será divisible por $\det\Phi$:

$$\det\Phi \,\Big|\, f\,\mathrm{mcd}\left(f^{n-1}, \left(\frac{\partial f}{\partial x_1}\right)^{n-1}, \left(\frac{\partial f}{\partial x_2}\right)^{n-1}, \ldots, \left(\frac{\partial f}{\partial x_n}\right)^{n-1}\right).$$

No nos olvidemos de que gracias al Lema 4.3 sabemos que ese máximo común divisor es 1. Por esta razón, $\det\Phi$ debe dividir a f.

En el caso de que f ya sea irreducible, $\det\Phi$ solo puede ser 1 o f. Supongamos que es 1, entonces como hemos dicho algo más arriba, $\det A = 1\cdot\det\imath$, que es una unidad de $K[\mathbf{x}]$. Nuevamente por la regla de Cramer, tendremos que A^{-1} es una matriz con elementos en $K[\mathbf{x}]$. Pero esto implicaría que la expresión 4.6 es bidireccional y que podemos expresar

$$\left(\delta_1,\delta_2,\ldots,\delta_n\right)A^{-1} = \left(\partial_1,\partial_2,\ldots,\partial_n\right).$$

Esto es lo mismo que decir $\mathrm{Der}(f) = \mathrm{Der}(K[\mathbf{x}])$, algo que en general no es cierto salvo que f sea una constante. Descartamos tal situación por ser muy aislada.

Necesitamos un pequeño resultado para poder trabajar el caso en el que f no es irreducible.

Lema 4.18. *Sea f un polinomio libre de cuadrados de $K[\mathbf{x}]$ que puede ser descompuesto en factores irreducibles como $f = f_1f_2\cdots f_r$. Entonces,* $\mathrm{Der}(f) = \bigcap_{i=1}^r \mathrm{Der}\left(f_i\right)$.

Demostración. Sea $\delta\in\mathrm{Der}(f)$ y llamemos $f_{-i} := f_1f_2\cdots f_{i-1}f_{i+1}\cdots f_{r-1}f_r$. Por la regla del producto tenemos que

$$\begin{aligned}
\delta(f) &= \delta\left(f_1f_2\cdots f_r\right)\\
pf_1f_2\cdots f_r &= \delta\left(f_i\right)f_{-i} + f_i\delta\left(f_{-i}\right)\\
pf_1f_2\cdots f_r - f_i\delta\left(f_{-i}\right) &= \delta\left(f_i\right)f_{-i}\\
\left(pf_{-i} - \delta\left(f_{-i}\right)\right)f_i &= \delta\left(f_i\right)f_{-i}.
\end{aligned}$$

Como además $\mathrm{mcd}\left(f_i, f_{-i}\right) = 1$ por ser f libre de cuadrados, podemos decir que $\delta\left(f_i\right)\mid f_i$. Este argumento nos garantiza que $\mathrm{Der}(f)\subseteq\bigcap_{i=1}^r\mathrm{Der}\left(f_i\right)$. En el otro sentido, supongamos que $\delta\in\bigcap_{i=1}^r\mathrm{Der}\left(f_i\right)$.

[2] De nuevo, recordemos que $\det\Phi$ no es el determinante de una matriz, sino una convención que hemos explicado antes. Por otro lado, $\det(\Phi\circ\imath)$ sí que es el determinante de una matriz ya que tanto N como $\mathrm{Der}(K[\mathbf{x}])$ son módulos libres.

[3] Por si no la recordamos, esta dice que toda matriz C inversible cumple que $C^{-1} = \frac{1}{\det C}\mathrm{adj}(C)$, con $\mathrm{adj}(C)$ la matriz de adjuntos.

Está claro que $f_1 | \delta(f_1)$. Ahora asumamos que $f_1 f_2 \cdots f_k | \delta(f_1 f_2 \cdots f_k)$ para algún $k \in \{1, 2, \ldots, r-1\}$, cambiemos sutilmente la expresión f_{-i} a $f_1 f_2 \cdots f_{i-1} f_{i+1} \cdots f_k f_{k+1}$ y veamos que

$$\begin{aligned} \delta(f_1 f_2 \cdots f_{k+1}) &= \delta(f_{k+1})\, f_{-(k+1)} + f_{k+1}\delta(f_{-(k+1)}) \\ &= p f_{k+1} f_{-(k+1)} + f_{k+1}\delta(f_{-(k+1)}), \quad \text{donde } p \in K[\mathbf{x}], \\ &= pf + f_{k+1}\delta(f_{-(k+1)}); \end{aligned}$$

por la hipótesis de inducción, $\delta(f_{-(k+1)}) = q f_{-(k+1)}$ con $q \in K[\mathbf{x}]$;

$$\begin{aligned} &= pf + f_{k+1} q f_{-(k+1)} \\ &= (p+q) f. \end{aligned}$$

Por lo tanto, concluimos $\bigcap_{i=1}^{r} \mathrm{Der}(f_i) \subseteq \mathrm{Der}(f)$ y, por ende, $\mathrm{Der}(f) = \bigcap_{i=1}^{r} \mathrm{Der}(f_i)$. □

A partir de este lema podemos decir que $\bigwedge^n \mathrm{Der}(f) \subseteq \bigwedge^n \mathrm{Der}(f_i)$, lo cual nos lleva a que $\langle \det \Phi \rangle \subseteq \langle f_i \rangle$ como ideales de $K[\mathbf{x}]$. Pero esto no es más que decir $f_i \,|\, \det \Phi$ para todo i, por lo tanto $f \,|\, \det \Phi$. Junto con el resultado anterior, tenemos que $\det \Phi = u' f$ donde u' es una unidad de $K[\mathbf{x}]$.

Por todo esto,

$$\det(\delta_1, \delta_2, \ldots, \delta_n) = \det A = \det(\Phi \circ \imath) = \det \Phi \det \imath = u' f \det \imath = uf, \quad \text{con } u \text{ una unidad de } K[\mathbf{x}].$$

4.2.4. $\det(\delta_1, \delta_2, \ldots, \delta_n) = uf$ implica que $\mathrm{Der}(f)$ es libre

Antes de embarcarnos en la otra implicación, necesitaremos un resultado auxiliar.

Lema 4.19. *Si M es un $K[\mathbf{x}]$-módulo finitamente generado, entonces M^* es reflexivo.*

$$\begin{array}{ccccc} (M^*)_{\mathrm{Q}} \times M_{\mathrm{Q}} & \xrightarrow{\text{eval}} & \mathrm{Q}(K[\mathbf{x}]) \\ \uparrow & \uparrow & \uparrow \\ M^* \times M & \xrightarrow{\text{eval}} & K[\mathbf{x}] \\ \uparrow & \uparrow & \uparrow \\ 0 & 0 & 0 \end{array}$$

Demostración. Para cualquier A-módulo B, denotaremos $B_{\mathrm{Q}} := B \otimes \mathrm{Q}(A)$. Consideremos el diagrama de homomorfismos de $K[\mathbf{x}]$-módulo que aparece a la derecha. Las inyecciones que aquí mostramos son las naturales: en el caso de las de la izquierda, mandan los elementos m bien de M o M^* a los correspondientes $m \otimes 1$; y en el de la derecha se manda p a $\frac{p}{1}$. Estas son inyecciones si y solo si M es libre de torsión ya que en caso de que no, un elemento como $m \otimes 1 = fm \otimes \frac{1}{f}$ podría ser 0 si $fm = 0$. Con el mapa eval cometemos un abuso de notación y lo reutilizamos en ambos casos aunque no sea la misma aplicación. Esta envía un par (f, m) a $f(m)$ en ambos casos, es decir, evalúa la aplicación en el punto que se le dé.

Podemos ver los conjuntos de la parte baja del diagrama como subconjuntos de los de arriba. Así, pensaremos en M^* como en

$$\left\{ h \in (M^*)_{\mathrm{Q}} \,|\, \mathrm{eval}(h, m) \in K[\mathbf{x}] \ \forall m \in M \right\},$$

o en otras palabras, como todos aquellos homomorfismos en el conjunto ampliado a las fracciones que «restringidos» a M funcionan como un elemento de M^*.

Esto terminarlo.

□

Ahora asumamos que existen $\delta_1, \delta_2, \ldots, \delta_n$ de forma que $\det(\delta_1, \delta_2, \ldots, \delta_n) = uf$ con u una unidad de $K[\mathbf{x}]$ y volvamos al esquema de 4.5. A partir de este, sabemos que tenemos

$$\begin{array}{ccccc} \bigwedge^n N & \longrightarrow & \bigwedge^n \mathrm{Der}(f) & \subseteq & \bigwedge^n \mathrm{Der}(K[\mathbf{x}]) \\ \langle \delta_1 \wedge \cdots \wedge \delta_n \rangle & \longrightarrow & \langle f\partial_1 \wedge \cdots \wedge \partial_n \rangle & \subseteq & \langle \partial_1 \wedge \cdots \wedge \partial_n \rangle \end{array}$$

Ahora bien, recordemos que

$$\delta_1 \wedge \delta_2 \wedge \cdots \wedge \delta_n = \det\left(\delta_1, \delta_2, \ldots, \delta_n\right) \partial_1 \wedge \partial_2 \wedge \cdots \wedge \partial_n = uf\, \partial_1 \wedge \partial_2 \wedge \cdots \wedge \partial_n.$$

Al ser u simplemente una unidad, hemos llegado a que $\bigwedge^n N = \bigwedge^n \mathrm{Der}(f)$. Lo que buscamos ahora es quitar ese producto exterior. Ya sabemos que $N \subseteq \mathrm{Der}(f)$, por lo que solo nos hace falta ver la otra implicación. Sea $\delta \in \mathrm{Der}(f)$, que por ser $\mathrm{Der}(f)$ un subconjunto de $\mathrm{Der}(K[\mathbf{x}])$, lo podemos escribir como

$$\delta = p_1\partial_1 + p_2\partial_2 + \cdots + p_n\partial_n.$$

Fijémonos ahora en la relación 4.6. Recordando la regla de Cramer, sabemos que

$$A^{-1} = \frac{1}{\det A}\mathrm{adj}(A) = \frac{1}{uf}\mathrm{adj}(A) = \frac{1}{f}B$$

donde $\mathrm{adj}(A)$ es la matriz adjunta de A. A^{-1} está en $\mathrm{Mat}(n\times n, \mathrm{Q}(K[\mathbf{x}]))$ pero los adjuntos de la matriz A están en $K[\mathbf{x}]$, por lo que podemos expresar A^{-1} como vemos al final de la igualdad con $B \in \mathrm{Mat}(n\times n, K[\mathbf{x}])$. Como

$$\left(\partial_1, \partial_2, \ldots, \partial_n\right) = \left(\delta_1, \delta_2, \ldots, \delta_n\right) A^{-1} = \frac{1}{f}\left(\delta_1, \delta_2, \ldots, \delta_n\right) B,$$

reescribimos δ como

$$\begin{aligned} \delta &= \frac{b_1}{f}\delta_1 + \frac{b_2}{f}\delta_2 + \cdots + \frac{b_n}{f}\delta_n, \quad \text{donde } b_i \in K[\mathbf{x}], \text{ o también} \\ &= \overline{b}_1\delta_1 + \overline{b}_2\delta_2 + \cdots + \overline{b}_n\delta_n, \quad \text{donde } \overline{b}_i \in \mathrm{Q}(K[\mathbf{x}]). \end{aligned}$$

En este último paso vamos garantizar que estos $\overline{b}_i$ están[4] en $K[\mathbf{x}]$. Para ello, acordémonos de que $\delta \in \mathrm{Der}(f)$ y $\bigwedge^n \mathrm{Der}(f) = \bigwedge^n N$, por lo que si en $\delta_1 \wedge \delta_2 \wedge \cdots \wedge \delta_n$ sustituimos δ_i por δ nos queda

$$\delta_1 \wedge \delta_2 \wedge \cdots \wedge \delta_{i-1} \wedge \delta \wedge \delta_{i+1} \wedge \cdots \wedge \delta_{n-1} \wedge \delta_n \in \bigwedge^n N.$$

Percatémonos de que esta expresión, una vez eliminamos todos los productos exteriores nulos, queda como $\overline{b}_i\delta_1 \wedge \delta_2 \wedge \cdots \wedge \delta_n \in \bigwedge^n N$, lo cual es solo posible si $\overline{b}_i \in K[\mathbf{x}]$. Con esto concluimos que $\delta \in N$ y, por tanto, que $N = \mathrm{Der}(f)$.

Para poner un ejemplo espero a la introducción, para que case con el ejemplo que allí pongamos.

[4] Más bien, se pueden ver como elementos de $K[\mathbf{x}]$. Como por ejemplo $\frac{f^2}{f} \in \mathrm{Q}(K[\mathbf{x}])$, que realmente puede verse como f en $K[\mathbf{x}]$.

Apéndice A

Un ejemplo completo de cálculo

El algoritmo para calcular las sicigias que nos permite obtener $\mathrm{Der}(f)$, en esencia el algoritmo de Buchberger, tienen un alto coste computacional que hace impracticable ejecutarlos «a mano». En la práctica, se utilizan sistemas de Álgebra Computacional que ya vienen preparados con estos algoritmos en sus versiones más óptimas. Sin embargo, como ocurre con muchas otras operaciones a lo largo de nuestra experiencia matemática, conviene saber cómo hacerlas a mano para tener una mayor intuición. En muchos textos que tratan sobre estos asuntos se suelen omitir los ejemplos a este tipo de operaciones o se dan algunos en casos demasiado sencillos —ideales de $K[\mathbf{x}]$ en vez de $K[\mathbf{x}]$-módulo de $K[\mathbf{x}]^n$ donde da la casualidad que todo se anula a la primera— por lo que creemos conveniente desarrollar en este apéndice por completo un caso no trivial para que el lector se lleve una imagen realista de qué ocurre detrás de la pantalla. Además, ilustraremos también después cómo se resuelve utilizando un sistema dedicado a este tipo de cálculos.

A.1. A mano

En concreto, intentaremos calcular $\mathrm{Der}(f)$ donde $f = x^2z + y^3$ en el anillo $\mathbb{C}[x,y,z]$ con el orden $>_{(\mathtt{POS},\mathtt{GRAD\text{-}LEX})}$. Recordemos que lo que buscamos es una descripción total del conjunto

$$\mathrm{Der}(f) = \left\{ (a,b,c) \in \mathbb{C}[x,y,z]^3 \,\middle|\, a\frac{\partial f}{\partial x} + b\frac{\partial f}{\partial y} + c\frac{\partial f}{\partial z} = kf,\ k \in \mathbb{C}[x,y,z] \right\}.$$

Esto lo podíamos reescribir como

$$\mathrm{Der}(f) = \left\{ (a,b,c) \in \mathbb{C}[x,y,z]^3 \,\middle|\, (a,b,c,k) \in \mathrm{syz}\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}, f\right),\ k \in \mathbb{C}[x,y,z] \right\}.$$

Lo primero que tendremos que hacer será calcular el submódulo de sicigias $\mathrm{syz}\left(2xz, 3y^2, x^2, x^2z + y^3\right)$ siguiendo el método indicado en 3.27. Comenzamos ampliando los distintos elementos a vectores para que sus componentes extra «mantengan el registro» de las anulaciones que hacemos. Así, tomamos

$$g_1 := \begin{pmatrix} 2xz \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ g_2 := \begin{pmatrix} 3y^2 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},\ g_3 := \begin{pmatrix} x^2 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \text{ y } \ g_4' := \begin{pmatrix} x^2z + y^3 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Calculamos ahora una base de Gröbner a partir de estos elementos. Para empezar con el mejor pie posible, lo que haremos será convertir este conjunto en un conjunto reducido, es decir, que buscaremos garantizar

que ninguno de los términos de g_i sea divisible por algún $\mathrm{LM}\left(g_j\right)$ donde $j \neq i$. En este caso, vemos que g_1, g_2 y g_3 no tienen ningún termino divisible, sin embargo g_4' sí, así que lo reducimos:

$$\begin{array}{rrrrr|l|l}
x^2z\mathbf{e}_1 & +y^3\mathbf{e}_1 & & & +\mathbf{e}_5 & 2xz\mathbf{e}_1+\mathbf{e}_2 \ \ (g_1) & x^2\mathbf{e}_1+\mathbf{e}_4 \ \ (g_3) \\
-(x^2z\mathbf{e}_1 & & +\frac{1}{2}x\mathbf{e}_2) & & & \frac{1}{2}x & \\
\hline
 & y^3\mathbf{e}_1 & -\frac{1}{2}x\mathbf{e}_2 & & +\mathbf{e}_5 & & \\
 & -(y^3\mathbf{e}_1 & & +\frac{1}{3}y\mathbf{e}_3) & & 3y^2\mathbf{e}_1+\mathbf{e}_3 \ \ (g_2) & \\
\hline
 & \text{1ª iteración:} & \cancel{-\frac{1}{2}x\mathbf{e}_2} & \cancel{-\frac{1}{3}y\mathbf{e}_3} & \cancel{+\mathbf{e}_5} & \frac{1}{3}y & \\
 & & \uparrow \text{1ª iteración} & \uparrow \text{2ª iteración} & \text{3ª iteración} \uparrow & &
\end{array} \tag{A.1}$$

Por ser esta la primera división con más de un divisor que hacemos, la desglosaremos algo más siguiendo la notación del algoritmo en 3.12.

1ª iteración: $\mathrm{LT}(D) = x^2z\mathbf{e}_1$ es divisible por $\mathrm{LM}\left(g_1\right)$ y $\mathrm{LM}\left(g_3\right)$. Escogemos, por pura preferencia personal, g_1 y reducimos —la primera resta—. Después de reducir, $\mathrm{LT}(D) = y^3\mathbf{e}_1$ es divisible por $\mathrm{LM}\left(g_2\right)$ así que reducimos por este. Tras esta reducción, $\mathrm{LT}(D) = -\frac{1}{2}x\mathbf{e}_2$, que no es divisible por ninguno de los monomios líderes de g_1, g_2 y g_3. Se lo sustraemos a D y lo añadimos al resto. Esto deja $D = -\frac{1}{3}y\mathbf{e}_3 + \mathbf{e}_5$, $c_1 = \frac{1}{2}x$, $c_2 = \frac{1}{3}y$, $c_3 = 0$ y $r = -\frac{1}{2}x\mathbf{e}_2$.

2ª iteración: $\mathrm{LT}(D) = -\frac{1}{3}y\mathbf{e}_3$ no es divisible por ninguno de los términos líderes de los divisores. Así pues, no reducimos y sustraemos este término de D para pasarlo a r. Esto deja $D = \mathbf{e}_5$, $r = -\frac{1}{2}x\mathbf{e}_2 - \frac{1}{3}y\mathbf{e}_3$ y los cocientes como antes.

3ª iteración: $\mathrm{LT}(D) = \mathbf{e}_5$ y nos encontramos con la misma situación que antes. Al sustraer este de D, D pasa a ser 0, por lo que el algoritmo termina. Nos queda $r = -\frac{1}{2}x\mathbf{e}_2 - \frac{1}{3}y\mathbf{e}_3 + \mathbf{e}_5$.

De aquí en adelante, no escribiremos todas las «cajas de división» desde el principio, sino que las iremos añadiendo conforme las necesitemos. Tampoco seguiremos tachando ni indicando hasta dónde alcanza cada iteración para descargar las divisiones.

El resto de la anterior división es irreducible por los demás elementos, así que lo usaremos como elemento g_4. Multiplicar por un escalar un elemento no afecta al resultado, por lo tanto, intentamos obtener la expresión más sencilla para este y así

$$g_4 := -6\left(-\frac{1}{2}x\mathbf{e}_2 - \frac{1}{3}y\mathbf{e}_3 + \mathbf{e}_5\right) = \begin{pmatrix} 0 \\ 3x \\ 2y \\ 0 \\ -6 \end{pmatrix}.$$

Ahora sí, comenzamos a calcular la base de Gröbner. La primera pareja, g_1 y g_2, nos da

$$\mathrm{S}\left(g_1, g_2\right) = 3y^2g_1 - 2xzg_2 = \begin{pmatrix} 6xy^2z \\ 3y^2 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 6xy^2z \\ 0 \\ 2xz \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 3y^2 \\ -2xz \\ 0 \\ 0 \end{pmatrix};$$

cuyo término líder se encuentra en la segunda componente. Como no hay ningún otro g_i con término líder en la segunda componente, este elemento es irreducible y, por ello, lo añadimos como g_5 a la lista

de elementos de la base. Pasamos ahora a la siguiente pareja, g_1 y g_3; aquí tenemos que

$$\mathrm{S}(g_1,g_3) = xg_1 - 2zg_3 = \begin{pmatrix} 2x^2z \\ x \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 2x^2z \\ 0 \\ 0 \\ 2z \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ x \\ 0 \\ -2z \\ 0 \end{pmatrix}.$$

Este elemento sí que es reducible, por lo que le aplicamos el algoritmo de la división por $\{g_1,g_2,g_3,g_4,g_5\}$:

$$\begin{array}{llll|l} x\mathbf{e}_2 & & -2z\mathbf{e}_4 & & 2xz\mathbf{e}_1+\mathbf{e}_2 \\ \hline -(x\mathbf{e}_2 & +\frac{2}{3}y\mathbf{e}_3 & & -2\mathbf{e}_5) & \frac{1}{3} \\ \hline & -\frac{2}{3}y\mathbf{e}_3 & -2z\mathbf{e}_4 & +2\mathbf{e}_5 & \end{array}$$

De nuevo, al no ser 0 lo añadiremos a nuestra lista de generadores como g_6 pero antes lo multiplicamos por un escalar para hacer la expresión lo más sencilla posible:

$$g_6 := \frac{-3}{2}\left(-\frac{2}{3}y\mathbf{e}_3 - 2z\mathbf{e}_4 + 2\mathbf{e}_5\right) = \begin{pmatrix} 0 \\ 0 \\ y \\ 3z \\ -3 \end{pmatrix}.$$

El resto de emparejamientos en los que esté g_1 cumplirán $\mathrm{S}(g_1,g_i) = 0$ ya que los términos líderes no estarán en la misma componente. Lo mismo ocurre con las parejas formadas por g_2 o g_3 y g_4, g_5 o g_6; y lo mismo podemos razonar con aquellas formadas por g_4 o g_5 y g_6. A la hora de realizar este proceso a mano, conviene mantener un registro de cuáles son los elementos de la base y qué parejas hace falta evaluar. En este momento, la situación es la siguiente: la lista de generadores es

$$g_1 = \begin{pmatrix} 2xz \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ g_2 = \begin{pmatrix} 3y^2 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},\ g_3 = \begin{pmatrix} x^2 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},\ g_4 = \begin{pmatrix} 0 \\ 3x \\ 2y \\ 0 \\ -6 \end{pmatrix},\ g_5 = \begin{pmatrix} 0 \\ 3y^2 \\ -2xz \\ 0 \\ 0 \end{pmatrix} \text{ y } g_6 = \begin{pmatrix} 0 \\ 0 \\ y \\ 3z \\ -3 \end{pmatrix}.$$

y entre estos las parejas ya evaluadas se muestran en la tabla a la derecha marcadas con el símbolo ✓. Démonos cuenta de que $\mathrm{S}(g_i,g_i) = 0$ y que $\mathrm{S}(g_i,g_j) = -\mathrm{S}(g_j,g_i)$, por lo que no hace falta prestar atención por debajo de la diagonal la cual indicamos con el símbolo •. En blanco dejamos las parejas que sí están pendientes de ser evaluadas. Así pues, continuamos con la pareja formada por g_2 y g_3:

	1	2	3	4	5	6
1	•	✓	✓	✓	✓	✓
2		•		✓	✓	✓
3			•	✓	✓	✓
4				•		✓
5					•	✓

$$\mathrm{S}(g_2,g_3) = x^2g_1 - 3y^2g_3 = \begin{pmatrix} 3x^2y^2 \\ 0 \\ x^2 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 3x^2y^2 \\ 0 \\ 0 \\ 3y^2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x^2 \\ -3y^2 \\ 0 \end{pmatrix}.$$

Al tener su término líder en la tercera componente, solo podría ser reducido por g_6 y, como $\mathrm{LM}(g_6)$ no divide a su término líder, no se puede reducir y, por ello, lo tomamos como g_7. Proseguimos con la otra

pareja que nos quedaba en la tabla anterior:

$$\mathrm{S}\left(g_4, g_5\right) = y^2 g_4 - x g_5 = \begin{pmatrix} 0 \\ 3xy^2 \\ 2y^3 \\ 0 \\ -6y^2 \end{pmatrix} - \begin{pmatrix} 0 \\ 3xy^2 \\ -2x^2 z \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 2x^2 z + 2y^3 \\ 0 \\ -6y^2 \end{pmatrix}.$$

Este sí puede reducirse:

$$\begin{array}{rrrr|l} 2x^2 z\mathbf{e}_3 & +2y^3\mathbf{e}_3 & & -6y^2\mathbf{e}_5 & x^2\mathbf{e}_3 - 3y^2\mathbf{e}_4 \\ \cline{4-4} -(2x^2 z\mathbf{e}_1 & & -6y^2 z\mathbf{e}_4) & & 2z \\ \hline & 2y^3\mathbf{e}_3 & +6y^2 z\mathbf{e}_4 & -6y^2\mathbf{e}_5 & \\ & -(2y^3\mathbf{e}_1 & +6y^2 z\mathbf{e}_4 & -6y^2\mathbf{e}_5) & y\mathbf{e}_3 + 3z\mathbf{e}_4 - 3\mathbf{e}_5 \\ \cline{4-4} & & & 0 & 2y^2 \end{array}$$

	1	2	3	4	5	6	7
1	•	✓	✓	✓	✓	✓	✓
2		•	✓	✓	✓	✓	✓
3			•	✓	✓	✓	✓
4				•	✓	✓	✓
5					•	✓	✓
6						•	

De hecho, como puede verse, se reduce al cero, así que no hay nada que añadir. Tras dar por evaluadas todas las parejas con términos líderes en componentes distintas nos queda la tabla actualizada que vemos a la izquierda. Solo queda por lo tanto una pareja por evaluar:

$$\mathrm{S}\left(g_6, g_7\right) = x^2 g_6 - y g_7 = \begin{pmatrix} 0 \\ 0 \\ x^2 y \\ 3x^2 z \\ -3x^2 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ x^2 y \\ -3y^3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 3x^2 z + 3y^3 \\ -3x^2 \end{pmatrix}.$$

Al tener el término líder en la cuarta componente, concluimos que no será divisible por ningún otro monomio líder. Lo multiplicamos por $\frac{1}{3}$ y lo añadimos a la lista como g_8. Por 3.23, sabemos que

$$g_1 = \begin{pmatrix} 2xz \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ g_2 = \begin{pmatrix} 3y^2 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},\ g_3 = \begin{pmatrix} x^2 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},\ g_4 = \begin{pmatrix} 0 \\ 3x \\ 2y \\ 0 \\ -6 \end{pmatrix},\ g_5 = \begin{pmatrix} 0 \\ 3y^2 \\ -2xz \\ 0 \\ 0 \end{pmatrix},\ g_6 = \begin{pmatrix} 0 \\ 0 \\ y \\ 3z \\ -3 \end{pmatrix},\ g_7 = \begin{pmatrix} 0 \\ 0 \\ x^2 \\ -3y^2 \\ 0 \end{pmatrix} \text{ y } g_8 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ x^2 z + y^3 \\ -x^2 \end{pmatrix}$$

forma una base de Gröbner. Para dar un resultado más «canónico», vamos a reducirla. En este caso hay poco que hacer ya que el único elemento que es reducible es g_4:

$$\begin{array}{rrrr|l} 3x\mathbf{e}_2 & 2y\mathbf{e}_3 & & -6\mathbf{e}_5 & y\mathbf{e}_3 + 3z\mathbf{e}_4 - 3\mathbf{e}_5 \\ \cline{4-4} & -(2y\mathbf{e}_3 & 6z\mathbf{e}_4 & -6\mathbf{e}_5) & 2 \\ \hline 3x\mathbf{e}_2 & & -6z\mathbf{e}_4 & & \end{array}$$

Cambiando g_4 a $3x\mathbf{e}_2 - 6z\mathbf{e}_4$ ya sí que obtenemos una base de Gröbner reducida. Terminada de calcular esta base de Gröbner, pasamos a restringirla a las últimas cuatro componentes, ya que recordemos que a nosotros lo que nos interesaba era el «registro» que iban llevando estas componentes de los coeficientes de $\mathrm{S}\left(g_i, g_j\right)$ que nos daban las anulaciones. Debemos eliminar a g_1, g_2 y g_3 ya que estos tienen primera componente no nula y así llegamos a la solución de la sicigia:

$$\operatorname{syz}\left(2xz, 3y^2, x^2, x^2 z + y^3\right) = \left\langle \begin{pmatrix} 3x \\ 2y \\ 0 \\ -6 \end{pmatrix}, \begin{pmatrix} 3y^2 \\ -2xz \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ 3z \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ x^2 \\ -3y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ x^2 z + y^3 \\ -x^2 \end{pmatrix} \right\rangle.$$

Por último, recordemos que en $\mathrm{Der}(f)$ lo que buscamos son los coeficientes que acompañan a las derivadas, no buscamos saber cuales son los factores por los que queda multiplicado f. Esta información nos la da la última componente y, como por el orden monomial de módulos elegido esta última componente no juega ningún papel a la hora de garantizar que el conjunto sea base de Gröbner, podemos eliminarla sin más para obtener una base de Gröbner reducida de $\mathrm{Der}(f)$:

$$\mathrm{Der}\left(x^2z+y^3\right) = \left\langle \begin{pmatrix} 3x \\ 2y \\ 0 \end{pmatrix}, \begin{pmatrix} 3y^2 \\ -2xz \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ 3z \end{pmatrix}, \begin{pmatrix} 0 \\ x^2 \\ -3y^2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ x^2z+y^3 \end{pmatrix} \right\rangle.$$

A.2. Con ordenador

Con el ejemplo anterior queda suficientemente ilustrado que realizar este procedimiento a mano puede ser tedioso y en casos con expresiones más enrevesadas y con más términos puede llegar a ser impracticable. Como ya decíamos antes, se suele utilizar software especializado para realizar estas operaciones. En nuestro caso, utilizamos el programa [1] el cual entre sus muchas funciones, tiene algunas dedicadas exclusivamente al cómputo de sicigias y bases de Gröbner. Mostramos aquí cómo realizar el mismo procedimiento que hemos visto antes a través de esta herramienta.

Lo primero de todo es definir el anillo sobre el que estamos trabajando:

```
ring A = 0, (x,y,z), (c,Dp);
```

Esta instrucción define no solo `A` como un anillo sino que también lo activa de cara al resto de operaciones; es decir, de aquí en adelante el programa asume que los ideales, módulos, etcétera son en función a este anillo. También observamos que hay tres elementos diferenciados en el valor que asignamos al anillo: `0`, `(x,y,z)` y `(c,Dp)`. El primero da la característica del anillo en el que estemos trabajando, el segundo indica el número y nombre de variables que tiene —como $[x,y,z]$ en $K[x,y,z]$— y el último especifica el orden monomial de módulos a utilizar, que en este caso será $>_{(\mathtt{POS,GRAD\text{-}LEX})}$.

Después de esto, ya podemos definir el polinomio f:

```
poly f = x2z + y3;
```

Nótese que aunque podríamos utilizar la notación `x^2*z + y^3` la sintaxis de Singular nos permite escribir los exponentes simplemente a la derecha de las variables y omitir el símbolo de multiplicación.

Tras esto, construimos los vectores para poder hallar su base de Gröbner:

```
module M = [diff(f,x), 1, 0, 0, 0], [diff(f,y), 0, 1, 0, 0],
  [diff(f,z), 0, 0, 1, 0], [f, 0, 0, 0, 1];
```

Implícitamente estamos diciendo que `M` es el A-módulo generado por esos elementos, no solo le estamos asignando la lista.

Ya por último le pedimos que nos calcule la base de Gröbner de dichos generadores:

```
module G = std(M); // Guardamos la base como el modulo engendrado
                   // por esta.
print(G);
```

y el programa nos devuelve

```
0,     0, 0,   0,  0,   3y2,2xz,x2,
0,     0, 0,   x,  3y2, 0,  1,  0,
0,     y, x2,  0,  -2xz,1,  0,  0,
x2z+y3,3z,-3y2,-2z,0,   0,  0,  1,
-x2,   -3,0,   0,  0,   0,  0,  0
```

que son los mismos elementos que habíamos obtenido antes a mano pero ordenados en orden ascendente.

Alternativamente, puede usarse la instrucción dedicada al cómputo de sicigias, `syz`:

```
ideal I = diff(f,x), diff(f,y), diff(f,z), f;
S = syz(I);
print(S);
```

Esto devuelve

```
0, 0,   x,  3y2,
y, x2,  0,  -2xz,
3z,-3y2,-2z,0,
-3,0,   0,  0
```

Démonos cuenta de que esto no es el mismo resultado que antes y eso se debe a que la función `syz` nos devuelve solo un conjunto generador, no una base de Gröbner. Pero eso tiene fácil solución:

```
module GS = std(S);
print(GS);
```

Y esto sí que ya nos devuelve la base de Gröbner que buscamos:

```
0,     0, 0,   x,  3y2,
0,     y, x2,  0,  -2xz,
x2z+y3,3z,-3y2,-2z,0,
-x2,   -3,0,   0,  0
```

Apéndice B

Demostración del Criterio de Buchberger

Si G es una base de Gröbner, entonces, como $\mathrm{S}(f,g) \in \langle G \rangle$, por el Teorema 3.20 tenemos que el resto de su división entre los elementos de G será 0.

La implicación contraria es la que conlleva más trabajo. Lo primero que debemos hacer es introducir un orden monomial nuevo en función del conjunto generador. Como $K[\mathbf{x}]^r$ es noetheriano, podemos asumir desde el principio que $G = \{g_1, g_2, \ldots, g_k\}$. Definimos, por tanto, el siguiente orden monomial de módulos en $K[\mathbf{x}]^k$:

$$x^\alpha \mathbf{e}_i >_{\text{Schreyer}} x^\beta \mathbf{e}_j \iff \begin{cases} \mathrm{LM}\left(x^\alpha g_i\right) > \mathrm{LM}\left(x^\beta\right) & \text{o} \\ \mathrm{LM}\left(x^\alpha g_i\right) = \mathrm{LM}\left(x^\beta\right) & \text{e} \quad \text{i <j.} \end{cases}$$

Ahora, para dos generadores g_i y g_j de forma que $\mathrm{LM}\left(g_i\right)$ y $\mathrm{LM}\left(g_j\right)$ estén en la misma componente, tomamos $c_j m_{ji}$ y $c_i m_{ij}$ elementos de $K[\mathbf{x}]$ de forma que $c_i, c_j \in K$ y m_{ji}, m_{ij} son monomios de $K[\mathbf{x}]$y cumplen

$$\mathrm{S}\left(g_i, g_j\right) = c_j m_{ji} g_i - c_i m_{ij} g_j.$$

Esto último lo podemos expresar en términos de los elementos de G como

$$c_j m_{ji} g_i - c_i m_{ij} g_j = \sum_{\nu=1}^{k} a_\nu^{(ij)} g_\nu.$$

Con todo esto, definimos la expresión

$$s_{ij} := c_j m_{ji} \mathbf{e}_i - c_i m_{ij} \mathbf{e}_j - \sum_{\nu=1}^{k} a_\nu^{(ij)} \mathbf{e}_\nu \in K[\mathbf{x}]^k .$$

Que puede entenderse como un vector que registra una combinación lineal que anula los generadores, es decir, $s_{ij} \in \mathrm{syz}\left(g_1, g_2, \ldots, g_k\right)$. Además, con respecto al orden de Schreyer, $\mathrm{LM}\left(s_{ij}\right) = m_{ji}\mathbf{e}_i$. Esto se debe por un lado a que $\mathrm{LM}\left(m_{ij} g_j\right) = \mathrm{LM}\left(m_{ji} g_i\right)$ pero $i < j$; y por otro a que

$$\mathrm{LM}\left(a_\nu^{(ij)} g_\nu\right) \leq \mathrm{LM}\left(c_j m_{ji} g_i - c_i m_{ij} g_j\right) < \mathrm{LM}\left(m_{ji} g_i\right).$$

Con los preliminares terminados, pasamos a demostrar que si el resto de $\mathrm{S}\left(g_i, g_j\right)$ entre G es 0 para todo i y j, entonces tenemos una base de Gröbner. Lo primero es tomar un $f \in \langle G \rangle$ y un $a = \left(a_1, a_2, \ldots, a_k\right) \in K[\mathbf{x}]^k$ de forma que $f = \sum_{i=1}^{k} a_i g_i$. Ahora consideremos la expresión

$$a = h + \sum$$

Completar la demostración.

Bibliografía

[1] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. SINGULAR 4-4-0 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2024.

[2] Daniele Faenzi, Marcos Jardim, and Jean Vallès. Saito criterion and its avatars, 2024.

[3] Gert-Martin Greuel and Gerhard Pfister. *A Singular Introduction to Commutative Algebra*. Springer, 2 edition, 2007.

[4] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Springer Berlin, Heidelberg, 1 edition, 2000.

[5] T. Y. Lam. *Lectures on Modules and Rings*. Graduate Texts in Mathematics. Springer New York, 1 edition, 1998.

[6] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 3 edition, 2002.

[7] Kyoji Saito. Theory of logarithmic differential forms and logarithmic vector fields. *Journal of the Faculty of Science (sección 1A)*, 27(2):265–291, 01 1980.

[8] The Stacks Project Authors. *Stacks Project*, 2025.