Una plantilla en LaTeX para el trabajo de fin de grado





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 Syzygias 9
3.1. Graduación de Módulos . . . 10
3.2. Órdenes monomiales . . . 10
3.3. Bases de Gröbner . . . 14
3.4. Sicigias . . . 16

4. El Criterio de Saito 19
4.1. Producto Exterior . . . 19
4.2. Demostración del Criterio de Saito . . . 22

A. Un ejemplo completo de cálculo 25

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 estamos trabajando 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.

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* $\begin{cases} (a+b)\cdot m = a\cdot m + b\cdot m, \\ a\cdot(m+n) = a\cdot m + a\cdot n, \\ (ab)\cdot m = a\cdot(b\cdot m) \quad y \\ 1\cdot m = m \end{cases}$ *para todo a y b en A y m y n en M.*

Ejemplo 2.2. $\mathbb{Z}^n$ 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.

La definición de espacio vectorial es más restrictiva que la de módulo, por lo que todo C-espacio vectorial donde C es un cuerpo es también un C-módulo. Por ejemplo, $\mathbb{R}^n$ es un $\mathbb{R}$-módulo.

A lo largo de este trabajo será de gran importancia el anillo de polinomios sobre un cuerpo, $K[x_1, x_2, \ldots, x_n]$, al que denotaremos $K[\mathbf{x}]$. Sobre todo porque a partir de este construimos 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 **u** y **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*

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

En el caso que exista algún $G = \{g_1, g_2, \ldots, g_n\}$ 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.

Definición 2.6. *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 2.7. *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 2.8. *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*

- $\phi(m + m') = \phi(m) + \phi(m')$ *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 2.9. 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 2.10. *Sean dos A-módulos M y N y un homomorfismo ϕ de A-módulos.* $\ker\phi$ *es un submódulo de M e* $\operatorname{im}\phi$ *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

$$\begin{aligned} \partial_i : K[\mathbf{x}] &\to K[\mathbf{x}] \\ p &\mapsto \frac{\partial p}{\partial x_i}. \end{aligned}$$

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

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

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

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

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

Definición 2.11. *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 2.12. *Sea M un A-módulo noetheriano. Los submódulos y módulos cocientes de M son también noetherianos.*

DEMOSTRACIÓN. □

Lema 2.13. *Que M sea noetheriano es equivalente a que toda cadena ascendente de submódulos $N_1 \subseteq N_2 \subseteq \ldots$ sea eventualmente estacionaria.*

DEMOSTRACIÓN. □

Definición 2.14. *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.*

Definición 2.15. *Sean M y N dos A-módulos. El conjunto de homomorfismos de A-módulos de M a N se denota por*

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

Definición 2.16. *Se define el módulo dual M^* como el conjunto de homomorfismos de A-módulos de M en A:*

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

Definición 2.17. *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 $\phi(m)$:*

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

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

Ejemplo 2.18. Veamos que todo espacio vectorial de dimensión finita es reflexivo. Sea V un K-espacio vectorial de dimensión n y con base $\{v_1, v_2, \ldots, v_n\}$. Podemos ver a V como un K-módulo y, entonces, $\mathrm{Hom}_K(V,K)$ son simplemente 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

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

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 tenemos 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 este sea reflexivo debemos cerciorarnos de que la aplicación ψ sea un isomorfismo. Para ello, basta darse cuenta que el kernel de esta 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 2.19. 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 $\mathbb{Z}$. 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.

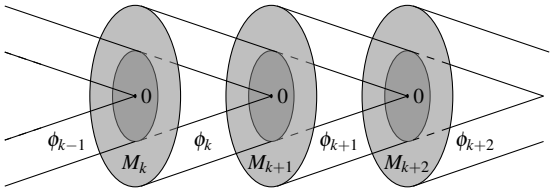
Una discusión más profunda acerca de los módulos reflexivos y sus propiedades puede encontrarse en [Stacks, Tag 0AUY].

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 2.20. *Diremos que una expresión del siguiente estilo:*

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

es una sucesión exacta si se cumple que $\operatorname{im}\phi_i = \ker\phi_{i+1}$ *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 secuencias exactas, podemos resumir nuestro problema en una sola expresión. Recordemos que estamos estudiando el $K[\mathbf{x}]$-módulo $\operatorname{Der}(f)$, que es un $K[\mathbf{x}]$-submódulo de $\operatorname{Der}(K[\mathbf{x}])$. Por otro lado, cada derivación δ, cuando se aplica a f nos da lugar a un elemento en el $K[\mathbf{x}]$-submódulo $J := \langle \partial_1 f, \ldots, \partial_n f \rangle$. Finalmente, a nosotros los elementos que nos interesan son aquellos que sean múltiplos de f, es decir, que pertenezcan al $K[\mathbf{x}]$-submódulo $\langle f \rangle$; para poder identificarlo, haremos el cociente de J por $\langle f \rangle$ para que así todas las expresiones de J que sean múltiplos de f vayan al cero. Todo esto lo podemos expresar como sigue:

$$0 \to \operatorname{Der}(f) \xrightarrow{\Phi} \operatorname{Der}(K[\mathbf{x}]) \xrightarrow{\kappa} K[\mathbf{x}]^n \xrightarrow{\xi} J \xrightarrow{\pi} \frac{J}{J \cap \langle f \rangle} \to 0. \tag{2.2}$$

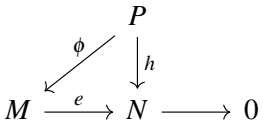
La función Φ es una inclusión, la función κ es el isomorfismo que envía ∂_i a $\mathbf{e}_i$, ξ envía una derivación δ a su evaluación en f —$\delta(f)$— y π es simplemente la aplicación canónica.

Un tipo de módulo muy importante en la demostración del Criterio de Saito es el módulo proyectivo, que nos sirve en muchos casos como tipo de módulo intermedio para algunos razonamientos.

Definición 2.21. *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 siguiente diagrama de secuencias

exactas:



Ejemplo 2.22. 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 2.23. *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 2.21. 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 discusión más exhaustiva acerca de los módulos proyectivos en [LectMoRi].

Capítulo 3

Bases de Gröbner y Syzygias

A partir de este momento nos fijaremos en $K[\mathbf{x}]^n$ ya que sus elementos son los involucrados en el módulo de derivaciones. En particular nos fijaremos en sus submódulos.

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. Supongamos que tenemos $\mathbb{R}[x]$ —solo una variable— como módulo de sí mismo, $f := x^3 - 6x^2 + 11x - 6$ y $g := x^3 - 9x^2 + 26x - 24$ dos elementos de este y queremos determinar si el polinomio $p = 3x^7 + 4x^5 - 3x^2 + x + 1$ 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,

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

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:

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

El resto es distinto de 0, por lo que p no pertenece a $\langle f, g \rangle$.

Este ejemplo nos señala el camino para investigar la pertenencia a un módulo: primero, debemos encontrar una representación de los generadores para los que un «algoritmo de la división» tenga sentido; después, realizamos esta división que debe estar definida de forma que si el «resto» es distinto de cero, sepamos que el elemento no pertenece, y si es cero, entonces sí.

Visto así, el ejemplo (3.1) supone una situación idílica: por ser un dominio de ideales principales, sabemos que vamos a poder representar al conjunto generador con un solo elemento, para el cual tenemos el algoritmo de la división usual definido. Además, sabemos que el resto de este algoritmo de la división arroja la conclusión que buscamos.

El problema aparece cuando empezamos a investigar conjuntos más complicados.

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 $I := \langle f \rangle$. Aquí, no hay problema en conseguir un sistema de generadores que nos permita «dividir» puesto que solo hay un elemento. Sin embargo, a la hora de intentar dividir, nos encontramos dudando

sobre cómo hacerlo. Tal y como está escrito, podríamos inclinarnos por tomar como el término principal a $4x^2y$ e intentar dividir como lo hacemos en $\mathbb{R}[x]$, pero hay términos que tienen mayor grado, así que puede que esta forma no nos termine llevando a un resto como buscamos. Pero si decidimos poner a un término de grado máximo, al principio, ¿cuál de los dos deberíamos elegir, xz^3 o x^2yz? ¿son los dos válidos y nos llevarán al mismo resultado? En resumen, ¿cómo debemos tomar el valor que tenemos que tomar como «líder» para dirigir la división?

En el mismo anillo que el ejemplo anterior, consideremos el ideal $I := \langle x+y, xyz, x^2+y^2+z^2 \rangle$. Con este ideal la situación es todavía peor que con el anterior. ¿Nos sirven estos generadores? ¿Y cómo hacemos para dividir con ellos?

Vemos por lo tanto que en el momento en el que introducimos más variables, perdemos la capacidad de resolver el problema de una forma razonable. Para poder solucionar este problema, deberemos generalizar el algoritmo de la división para que este pueda aplicarse a estos nuevos objetos y, asimismo, deberemos trabajar en una representación del ideal que sea compatible con nuestro nuevo algoritmo.

3.1. Graduación de Módulos

Pensemos con detalle en el algoritmo de la división en un anillo de polinomios familiar como es $\mathbb{R}[x]$. Al dividir $p = x^3+2x^2-x+1$ entre $q = x^2-1$, buscamos anular el término de mayor grado de p —x^3— haciendo al mayor término de q —x^2— alcanzar a este. Esto es básicamente en lo que pensamos en todo momento mientras realizamos el algoritmo de la división «con caja»:

$$\begin{array}{rrrr|l} x^3 & +2x^2 & -x & +1 & x^2-1 \\ \cline{5-5} -(x^3 & & -x) & & x+2 \\ \cline{1-4} \text{1ª iteración:} \quad & +2x^2 & & +1 & \\ & -(2x^2 & & -2) & \\ \cline{2-4} & & \text{2ª iteración:} & +3 & \end{array}$$

Como puede apreciarse, el funcionamiento de este algoritmo depende muy fuertemente de la noción de grado de un polinomio. Al estar generalizando todo, es oportuno que generalicemos también la noción de grado a anillos y módulos.

Definición 3.2. *Sea A un anillo. Se dice que es un anillo graduado si existe una descomposición $\bigoplus_{g=0}^{\infty} A_g$ donde A_g es un grupo abeliano para todo g y se cumple que $A_g A_h \subseteq A_{g+h}$ para todo g y h.*

Sea ahora M un A-módulo. Se dice que es un A-módulo graduado si existe una descomposición $\bigoplus_{g\in\mathbb{Z}} M_g$ donde M_g es un grupo abeliano para todo g y se cumple que $A_h M_g \subseteq M_{g+h}$.

Los elementos de A_g y de M_g se denominan homogeneos de grado g.

El problema de estos grados es que no nos permiten ordenar los distintos monomios que nos aparecen de forma unívoca. Por ejemplo, en $xyz+x^2y+xy^2$ los tres monomios que aparecen son distintos el uno del otro aunque son del mismo grado. Para solucionar esto, debemos introducir el concepto de orden monomial.

3.2. 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,

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

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 3.3. *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 $\mathbb{N}^n$.

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:

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

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

Para poder generalizar este concepto 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 órdenes monomiales de módulos distintos: 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 $>_{(\texttt{POS},\texttt{LEX})}$ para el correspondiente a la definición (3.1) y $>_{(\texttt{LEX},\texttt{POS})}$ 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 respuesta de las preguntas con las que abríamos el capítulo.

Definición 3.9. *Sea $p := c_1x^{\mathbf{s_1}}\mathbf{e}_{i_1} + c_2x^{\mathbf{s_2}}\mathbf{e}_{i_2} + \cdots + c_mx^{\mathbf{s_m}}\mathbf{e}_{i_m}$ un polinomio de $K[\mathbf{x}]^r$ y $>$ un orden monomial de módulos. Sea $k \in \{1,\dots,m\}$ 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 $\mathrm{LT}(p) := \mathrm{LC}(p)\,\mathrm{LM}(p)$.*

Con este aparataje ya tenemos una noción de cuáles son los términos «importantes» dentro de un polinomio, lo cual nos hace empezar a vislumbrar cómo dividir uno por otro. Lo primero es entender cuándo pueden dividirse dos monomios de $K[\mathbf{x}]^r$. Según la definición 2.6, 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 $x^\alpha | x^\beta$. Ahora sí, podemos dar un algoritmo de la división en $K[\mathbf{x}]^r$. Este consiste en imitar el algoritmo usual para dividir un polinomio por otro en una variable; pero en este caso, en vez de guiarnos por el grado para construir el cociente, utilizamos los términos líderes.

Definición 3.10. *Supongamos que tenemos dos polinomios f y g en $K[\mathbf{x}]^n$ junto con un orden monomial sobre este.*

1: *Definimos $D \leftarrow f$, $d \leftarrow g$, $c \leftarrow 0$ y $r \leftarrow 0$ como las variables que representan el dividendo, divisor, cociente y resto, respectivamente.*
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*** $D = 0$

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:

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

La primera iteración ejecuta el bucle interno dos veces dejando $D = 2x^2y\mathbf{e}_2 - 6x^2y\mathbf{e}_3 + x^2\mathbf{e}_1 - 4xy\mathbf{e}_3$; después, se encuentra con el término líder $2x^2y\mathbf{e}_2$, que no es divisible por $\mathrm{LT}(g) = x^2\mathbf{e}_1$, así que lo elimina del dividendo, que pasa a ser $D = -6x^2y\mathbf{e}_3 + x^2\mathbf{e}_1 - 4xy\mathbf{e}_3$ y lo añade al resto, que pasa a ser $r = 2x^2y\mathbf{e}_2$. En la segunda iteración el término líder sigue sin ser divisible por $\mathrm{LT}(g)$; así que lo eliminamos del dividendo y lo añadimos al resto. En la tercera iteración, $\mathrm{LT}(D) = x^2\mathbf{e}_1$ sí es divisible por $\mathrm{LT}(g)$, por lo que procedemos como en la primera iteración primero reduciendo y después pasando el término líder que queda al resto. En la última iteración, volvemos a retirar el término líder y ya nos encontramos en la situación de salida del algoritmo.

El resultado puede leerse como

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

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

Cuando obtenemos el resto de f dividido por g lo que esencialmente buscamos es un representante r «canónico» de la clase de equivalencia de f en ${}^{K[\mathbf{x}]^r}\!/_{\langle g\rangle}$. En este caso, entendemos canónico como que no tenga ningún término divisible por $\mathrm{LT}(g)$, es decir, que sea «irreducible». Entendida así, la noción de «dividir» puede extenderse a submódulos de $K[\mathbf{x}]^r$ en general. Es decir, dado cualquier $K[\mathbf{x}]$-submódulo N de $K[\mathbf{x}]^r$, podemos «dividir» f por N encontrando el representante «canónico» de la clase de f en ${}^{K[\mathbf{x}]^r}\!/_N$. En este caso, nuestra idea de canónico será que no haya ningún elemento g en N de forma que $\mathrm{LT}(g)$ sea uno de los términos de este representante. Para formalizar esta idea de división más general, necesitamos de algunos resultados previos.

Definición 3.12. *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*

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

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

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 es de gran importancia, ya que nos asegura que es suficiente con tener un algoritmo de la división para N finitamente generado.

Definición 3.15. *Sean f un elemento y $N = \langle g_1,\ldots,g_k\rangle$ un $K[\mathbf{x}]$-submódulo de $K[\mathbf{x}]^r$. Definimos el algoritmo de la división 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* $\mathrm{LM}(d_i) \,|\mathrm{LM}(D)$ ***haz***
4: *Sea i de forma que* $\mathrm{LM}(d_i) \,|\mathrm{LM}(D)$.
5: *Sea* $m \in K[\mathbf{x}]$ *de forma que* $\mathrm{LM}(D) = m\mathrm{LM}(d_i)$.
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*** $D = 0$

En este caso, procedemos como en el algoritmo 3.10 pero, en vez de intentar reducir en cada paso por un solo divisor, buscamos si alguno de todos ellos nos sirve para anular $\mathrm{LM}(D)$ y, en caso de que sí, lo utilizamos para reducir. Nótese que puede haber varios, en cuyo caso, puede elegirse el que se prefiera.

Pudiera parecer que ya hemos solucionado el problema que planteábamos al principio del capítulo puesto que ya tenemos un algoritmo de la división y además sabemos que todos los submódulos de $K[\mathbf{x}]^n$ son finitamente generados. Sin embargo, todavía podemos encontrarnos con casos como el siguiente:

Ejemplo 3.16. 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 3.15 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 $f = -y(x\mathbf{e}_1 + y\mathbf{e}_2) + x(y\mathbf{e}_1 + x\mathbf{e}_2)$ y, por ende, sí que pertenece.

¿Qué es lo que ocurre aquí? Si nos fijamos, en la operación $f = -y(x\mathbf{e}_1 + y\mathbf{e}_2) + x(y\mathbf{e}_1 + x\mathbf{e}_2)$, 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 $\langle \mathrm{LM}(x\mathbf{e}_1 + y\mathbf{e}_2), \mathrm{LM}(y\mathbf{e}_1 + x\mathbf{e}_2) \rangle$. 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 $\mathrm{LM}(N) \neq \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_k) \rangle$, 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 algo mejor. Esta mejor representación se conoce como base de Gröbner.

3.3. 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 $\alpha_1, \alpha_2, \ldots, \alpha_k$ 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 $N := \langle x^\alpha \mathbf{e}_{i_\alpha} | \alpha \in J \rangle$ 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;

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

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 monomios.

Lema 3.19. *Sea N un $K[\mathbf{x}]$-submódulo monomial de $K[\mathbf{x}]^r$ de forma que $N = \langle x^{\alpha_1}\mathbf{e}_{i_1}, x^{\alpha_2}\mathbf{e}_{i_2}, \ldots, x^{\alpha_k}\mathbf{e}_{i_k} \rangle$. 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 3.15. 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 3.15 es* 0.

Demostración. Como ya mencionamos antes, si el resto es 0 ya sabemos que $f \in N$. Asumamos ahora que el resto no es cero. 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. 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, $f - g \notin N$ 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 3.16. 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:

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

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

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

[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. Ambos serían válidos, pero siempre nos referiremos a aquel que no está multiplicado por constante.

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 $G := \{g_1,\dots,g_k\}$ 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 $i \in \{1,\dots,k\}$ y $t \leftarrow k$.*
2: ***mientras** hayan i y j en $\{1,\dots,t\}$ de forma que el resto de $\mathrm{S}(g_i,g_i)$ entre $d_1,\dots,d_t$ 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 $d_1,\dots,d_t$.*
5: *$d_{t+1} \leftarrow r$*
6: *$t \leftarrow t+1$*

Al final del algoritmo, $\{d_1,\dots,d_t\}$ 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, tenemos que los $K[\mathbf{x}]$-submódulo $\langle \mathrm{LM}(d_1),\dots,\mathrm{LM}(d_t)\rangle$ 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 criterio que garantiza que nuestro conjunto generador sea una base de Gröbner.

Teorema 3.23 (criterio de Buchberger)**.** *Sea G un subconjunto de $K[\mathbf{x}]^r$ 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. contenidos... □

3.4. 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 $f_1,f_2,\dots,f_k$ elementos de M. Una sicigia de los elementos $f_1,f_2,\dots,f_k$ es una k-tupla $(g_1,g_2,\dots,g_k)$ de elementos de A de forma que $f_1g_1+f_2g_2+\cdots+f_kg_k=0$.*

Nótese que el conjunto de sicigias de $f_1,f_2,\dots,f_k$ forma un A-submódulo de A^k.

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

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

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

recordemos que podemos ver ∂_i como $\mathbf{e}_i$ a través del isomorfismo κ de (2.2);

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

Para poder calcular las sicigias necesitaremos dos resultados. El primero nos permite restringir una base de Gröbner a solamente unas coordenadas.

Lema 3.26. *contenidos...*

Con este resultado, ya podemos calcular sicigias.

Teorema 3.27. *contenidos...*

Capítulo 4

El Criterio de Saito

En 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.

Ejemplo de submódulo de $K[\mathbf{x}]^r$ que no admite base.

Definición 4.2. *Sea A un anillo, M un A-módulo y N un A-submódulo de M. Diremos que N es libre si admite una base.*

El criterio de Saito nos da una forma bastante rápida de determinar si $\mathrm{Der}(f)$ es o no libre.

Teorema 4.3 (Criterio de Saito)**.** *Sea f un polinomio 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* $\det(\delta_1, \delta_2, \ldots, \delta_n) = uf$ *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 [Faenzi]. 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 donde A es un anillo 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 4.4. *Sea A un anillo y M y N dos A-módulos. Tomemos 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 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 4.5. Quizás el ejemplo más natural sea el producto escalar. Así pues, tomemos la aplicación $\langle \bullet, \bullet \rangle : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$. 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—:

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

(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,

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

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 $b(m,m') = -b(m',m)$. En esta situación tendremos que imponer que $m \otimes n = -n \otimes m$.

Definición 4.6. *Sea A un anillo y M un A-módulo. Consideremos el A-submódulo T de* $M \otimes M$ *definido como*

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

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 4.7. 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).

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

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 $\{\mathbf{e}_1 \wedge \mathbf{e}_2, \mathbf{e}_1 \wedge \mathbf{e}_3, \mathbf{e}_2 \wedge \mathbf{e}_3\}$ y las imágenes de estos son

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

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 4.8. 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 $\mathbb{R}(\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3)$, 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 4.9. *Sea V un espacio vectorial de dimensión n. Entonces,* $\dim \bigwedge^k V = \binom{n}{k}$.

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

Definición 4.10. *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, $\wedge^n V$ y $\wedge^n W$ 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. Evaluémosla en $v_1 \wedge v_2 \wedge \cdots \wedge v_n$ para ver exactamente cuál es. Pero antes, démonos cuenta de que en (4.2) la forma de simplificar construía el determinate, lo cual es cierto en general; por ende,

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

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:

$$M \text{ módulo libre} \xrightarrow{\text{lema 2.23}} M \text{ módulo proyectivo} \Longrightarrow M \text{ módulo reflexivo}$$

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

¿Lo de que reflexivo implica proyectivo es si es un módulo de con como mucho dos variables o que es de rango 2? ¿Y la referencia dónde está?

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 $f \in K[x,y]$.

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 4.11. *Sea A un anillo 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

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

forma un cuerpo al cual llamaremos cuerpo de fracciones de A.

Definición 4.12. *Sea M un A-módulo finitamente generado. Diremos que M tiene rango r si $M \otimes \mathrm{Q}(A)$ es un $\mathrm{Q}(A)$-módulo libre de rango r.*

En general, la cadena de implicaciones que nos serán útiles a lo largo de la demostración del Criterio de Saito serán las siguientes:

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

Puede encontrarse en [Saito, corolario 1.7] una demostración de que $\mathrm{Der}(f)$ es un módulo reflexivo. 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.

Lema 4.13. *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. Recordemos que ya en 4.9 este resultado aparecía tras observar lo que ocurría con los elementos de las bases. Ahora consideremos $(\bigwedge^s M)\otimes \mathrm{Q}(A)$. Hay un isomorfismo de $\mathrm{Q}(A)$-módulos entre $\bigwedge^s \otimes \mathrm{Q}(A)$ y $\bigwedge^s (M\otimes \mathrm{Q}(A))$:

$$\begin{aligned}
\bigwedge^s M\otimes \mathrm{Q}(A) &\longleftrightarrow \bigwedge^s (M\otimes \mathrm{Q}(A)) \\
(m_1\wedge m_2\wedge\cdots\wedge m_s)\otimes \frac{a}{b} &\longrightarrow \left(m_1\otimes \frac{a}{b}\right)\wedge (m_2\otimes 1)\wedge\cdots\wedge (m_s\otimes 1) \\
(m_1\wedge m_2\wedge\cdots\wedge m_s)\otimes \frac{a_1a_2\ldots a_s}{b_1b_2\ldots b_s} &\longleftarrow \left(m_1\otimes \frac{a_1}{b_1}\right)\wedge \left(m_2\otimes \frac{a_2}{b_2}\right)\wedge\cdots\wedge \left(m_s\otimes \frac{a_s}{b_s}\right)
\end{aligned}$$

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

$$\begin{aligned}
\left(m_1\otimes \frac{a_1}{b_1}\right)\wedge \left(m_2\otimes \frac{a_2}{b_2}\right)\wedge\cdots\wedge \left(m_s\otimes \frac{a_s}{b_s}\right) &= \left[\frac{a_1}{b_1}(m_1\otimes 1)\right]\wedge \left[\frac{a_2}{b_2}(m_2\otimes 1)\right]\wedge\cdots\wedge \left[\frac{a_s}{b_s}(m_s\otimes 1)\right] \\
&= \frac{a_1a_2\ldots a_s}{b_1b_2\ldots b_s}(m_1\otimes 1)\wedge (m_2\otimes 1)\wedge\cdots\wedge (m_s\otimes 1) \\
&= \left(m_1\otimes \frac{a_1a_2\ldots a_s}{b_1b_2\ldots b_s}\right)\wedge (m_2\otimes 1)\wedge\cdots\wedge (m_s\otimes 1)\,.
\end{aligned}$$

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, $(\bigwedge^s M)\otimes \mathrm{Q}(A)$ es igualmente otro $\mathrm{Q}(A)$-espacio vectorial de rango $\binom{n}{s}$ lo cual quiere decir que M es de rango $\binom{n}{s}$. □

Este lema nos garantiza que $\bigwedge^n \mathrm{Der}(f)$ es un $K[\mathbf{x}]$-módulo reflexivo de rango 1. Por 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 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 dimensión 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 4.3. De forma similar,

Esto de antes lo teníamos ya que el módulo era libre. Habría que justificar que para módulos finitamente generados de rango n también ocurre.

aquí tendremos que $\bigwedge^n \Phi$ se corresponde con multiplicar por el determinante de Φ. Como además Φ jugaba el papel de inclusión, llegamos a que es este determinante el valor de p, es decir, $\bigwedge^n \mathrm{Der}(f) = \langle \det\Phi\partial_1\wedge\partial_2\wedge\cdots\wedge\partial_n\rangle$.

Aquí vendría la parte en la que demostramos que $\det\Phi = f$.

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 y consideremos la inclusión $N \xrightarrow{\iota} \mathrm{Der}(f)$. Volvamos a recordar la aplicación Φ de 2.2. Para aclararnos algo más, escribimos el siguiente esquema de los homomorfismos —¡ojo!, esto no es una secuencia exacta—:

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

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

$$(\delta_1,\delta_2,\ldots,\delta_n) = (\partial_1,\partial_2,\ldots,\partial_n)A$$

Por lo tanto, podemos pensar en que la aplicación $\Phi \circ \imath$ envía a cada δ_i a $(\partial_1, \partial_2, \ldots, \partial_n) A_i$ 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 $\{\partial_1, \partial_2, \ldots, \partial_n\}$. Pensemos ahora en la aplicación

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

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

Puede verse, gracias al mismo razonamiento de 4.3, como $\det(\Phi \circ \imath) = \det\Phi \det\imath = f \det\imath$. Vemos pues que si $N = \mathrm{Der}(f)$, es decir, si $\mathrm{Der}(f)$ es libre, entonces $N = \mathrm{Der}(f)$ y por lo tanto se cumple que $\det\imath$ es una unidad de $K[\mathbf{x}]$. Para ver exactamente esto último, recordemos la regla de Cramer: como $\imath$ es un isomorfismo, necesariamente tiene inversa y eso quiere decir que $\det\imath$ es inversible. Por otro lado, observemos que $\det(\Phi \circ \imath) = \det A$. Con esto concluimos que si $\mathrm{Der}(f)$ es libre, entonces $\det(\delta_1, \delta_2, \ldots, \delta_n) = \det A = \det\Phi \det\imath = f \det\imath$ donde $\det\imath$ es una unidad de $K[\mathbf{x}]$, como se pedía en el enunciado del teorema.

Ahora asumamos que existen $\delta_1, \delta_2, \ldots, \delta_n$ de forma que $\det(\delta_1, \delta_2, \ldots, \delta_n) = fu$ con u una unidad de $K[\mathbf{x}]$.

Terminar la otra implicación de Saito.

Apéndice A

Un ejemplo completo de cálculo

Bibliografía

[IdVaAl] David A. Cox, John Little y Donal O'Shea. Ideals, Varieties and Algorithms. 4.ª ed. Undergraduate Texts in Mathematics. Springer Cham, 2015. ISBN: 978-3-319-16720-6. DOI: https://doi.org/10.1007/978-3-319-16721-3.

[Singular] Wolfram Decker et al. SINGULAR 4-4-0 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de. 2024.

[Faenzi] Daniele Faenzi, Marcos Jardim y Jean Vallès. Saito criterion and its avatars. 2024. arXiv: 2402.08305 [math.AG]. URL: https://arxiv.org/abs/2402.08305.

[Singular] Gert-Martin Greuel y Gerhard Pfister. A Singular Introduction to Commutative Algebra. 2.ª ed. Springer, 2007. ISBN: 978-3-540-73541-0. DOI: https://doi.org/10.1007/978-3-540-73542-7.

[CoCoA1] Martin Kreuzer y Lorenzo Robbiano. Computational Commutative Algebra 1. 1.ª ed. Springer Berlin, Heidelberg, 2000. ISBN: 978-3-540-67733-8. DOI: https://doi.org/10.1007/978-3-540-70628-1.

[LectMoRi] T. Y. Lam. Lectures on Modules and Rings. 1.ª ed. Graduate Texts in Mathematics. Springer New York, 1998. ISBN: 978-0-387-98428-5. DOI: https://doi.org/10.1007/978-1-4612-0525-8.

[Lang] Serge Lang. Algebra. 3.ª ed. Graduate Texts in Mathematics. Springer New York, 2002. ISBN: 978-0-387-95385-4. DOI: https://doi.org/10.1007/978-1-4613-0041-0.

[Saito] Kyoji Saito. "Theory of logarithmic differential forms and logarithmic vector fields". En: Journal of the Faculty of Science (sección 1A) 27.2 (ene. de 1980), págs. 265-291. ISSN: 00408980. URL: https://repository.dl.itc.u-tokyo.ac.jp/records/39646 (visitado 28-05-2025).

[Stacks] The Stacks Project Authors. *Stacks Project*. 2025. URL: https://stacks.math.columbia.edu (visitado 28-05-2025).