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 7
3.1. Graduación de Módulos 8
3.2. Órdenes monomiales 8
3.3. Bases de Gröbner 12
3.4. Syzygias 13

4. El Criterio de Saito 15
4.1. Producto Exterior 15

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

Como hemos podido ver, 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.

¿Haría falta alguna introducción o hilo conductor para esta definición o es mejor yuxtaponerlas?

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,

¿Es necesario explicar cómo serían las combinaciones lineales de los módulos o con la analogía a espacios vectoriales hecha antes es suficiente?

$$\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{R}[x,y]} := \{ a\mathbf{u} + b\mathbf{v} \,|\, a, b \in \mathbb{R}[x,y] \}\,,$$

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. Diremos que N está generado por $G \subseteq N$ y lo denotaremos como $N = \langle G \rangle$ 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 $N = \langle G \rangle$ diremos que N está finitamente generado y lo escribiremos como $N = \langle g_1, g_2, \ldots, g_n \rangle$.

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 $M/N := M/\sim$. 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 $a \in A$.

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:

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

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

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

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 2.11. *Diremos que 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 $N = \langle n_1, n_2, \ldots, n_k \rangle_A$.

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. *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 2.15. *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 2.16. *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 2.17. 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 2.18.

Poner ejemplo de un módulo no reflexivo.

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

$$\ldots \xrightarrow{\phi_k} M_k \xrightarrow{\phi_{k+1}} M_{k+1} \xrightarrow{\phi_{k+2}} M_{k+2} \xrightarrow{\phi_{k+3}} \ldots$$

es una sucesión exacta si se cumple que $\operatorname{im}\phi_i = \ker\phi_{i+1}$ *para todo i.*

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:

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

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

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 siguiendo las claves del ejercicio (**??**) para que este pueda aplicarse a estos nuevos objetos y, asimismo, deberemos trabajar en una representación del ideal que también nos permita que esto funcione como es debido, para evitar las ambigüedades vistas en este mismo ejercicio.

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. Es decir, lo que hacemos puede expresarse como

$$x^3+2x^2-x+1 = 0q + x^3+2x^2-x+1$$
$$x^3+2x^2-x+1 = xq +$$

Completar.

Como puede apreciarse, el funcionamiento de este algoritmo depende muy fuertemente de la noción de grado de un polinomio. Sin embargo, en el caso de módulos el grado no siempre está claro. Por lo tanto, introducimos el concepto de que un anillo o un módulo esté «graduado».

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, podemos tratar

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 $2xy\mathbf{e}_1 + y^2\mathbf{e}_1 + x^3\mathbf{e}_2 + y\mathbf{e}_3$. Así que 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 3.6. *Sea $>$ un orden monomial en $K[\mathbf{x}]$. Un orden monomial de módulos $>_{mód}$ 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*

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

para todo α, β y γ en $\mathbb{N}^n$ e i y j en $\{1,\dots,r\}$.

Ejemplo 3.7. La extensión natural del 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. Ahora, podemos dar algunas respuestas a las preguntas que nos aparecían en los ejemplos (**??**) y (**??**).

Definición 3.8. *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 $k \in \{1,\ldots,m\}$ 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 $\mathrm{LT}(p) := \mathrm{LC}(p)\mathrm{LM}(p)$.*

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 encontrar los términos «principales» del cociente y el dividendo, utilizamos el término líder.

Definición 3.9. *Supongamos que tenemos dos polinomios f y g en $K[\mathbf{x}]^n$ junto con un orden monomial sobre este. Para dividir f entre g aplicaremos un algoritmo que consiste en replicar el algoritmo que ya conocemos para los polinomios en una variable. Sin embargo, ahora los términos que guían los coeficientes que vamos poniendo son $\mathrm{LT}(f)$ y $\mathrm{LT}(g)$:*

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 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 3.10. 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:

$$
\begin{array}{rllllll|l}
3x^4\mathbf{e}_1 & +2x^3\mathbf{e}_1 & +2x^2y\mathbf{e}_2 & & +x^2\mathbf{e}_1 & & & x^2\mathbf{e}_1+2y\mathbf{e}_3 \\
\cline{7-7}
-(3x^4\mathbf{e}_1 & & & +6x^2y\mathbf{e}_3) & & & & 3x^2+2x+1 \\
\cline{1-5}
 & +2x^3\mathbf{e}_1 & +2x^2y\mathbf{e}_2 & -6x^2y\mathbf{e}_3 & +x^2\mathbf{e}_1 & & & \\
 & -(2x^3\mathbf{e}_1 & & & & +4xy\mathbf{e}_3) & & \\
\cline{2-6}
 & \text{1ª iteración:} & \cancel{2x^2y\mathbf{e}_2} & \cancel{-6x^2y\mathbf{e}_3} & +x^2\mathbf{e}_1 & -4xy\mathbf{e}_3 & & \\
 & & \uparrow \text{1ª iteración} & \uparrow \text{2ª iteración} & -(x^2\mathbf{e}_1 & & +2y\mathbf{e}_3) & \\
\cline{4-7}
 & & & & \text{3ª iteración:} & \cancel{-4xy\mathbf{e}_3} & \cancel{-2y\mathbf{e}_3} & \\
 & & & & & \uparrow \text{3ª iteración} & \uparrow \text{4ª iteración} &
\end{array}
$$

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

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

Teorema 3.12 (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 3.13. *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 3.13, $K[\mathbf{x}]^r$ 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 3.14. *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 3.9 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: 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 3.14 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 3.15. *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 3.16 (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;

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

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 3.13; sino que además admiten conjuntos generadores finitos formados por monomios.

Lema 3.17. *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 3.14. Con todo esto, ya damos la respuesta final a la pregunta que abre el capítulo.

Teorema 3.18. *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 3.14 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.

3.4. Syzygias

Capítulo 4

El Criterio de Saito

4.1. Producto Exterior

De cara a la demostración del Criterio de Saito, utilizaremos una operación que nos