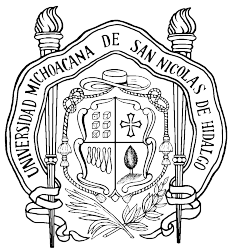
Bases de Gröbner en ideales tóricos simpliciales con un enfoque computacional



Uziel Silva Espino

Asesor: Dr. Luis Abel Castorena Martínez

Facultad de Ciencias Físico-Matemáticas
Universidad Michoacana de San Nicolás de Hidalgo

Tesis para obtener el grado de:
Licenciado en Ciencias Físico-Matemáticas

December 2017

Quiero dedicar esta tesis a todas las personas que me apoyaron, familia, amigos, y compañeros
...

Agradecimientos

Me gustaría agradecer a ...

Índice general

Capítulo 1

Prerequisitos

1.1. Variedades afines y proyectivas

Las variedades son estructuras muy importantes en la geometría algebraica, gracias a ellas y al teorema de los ceros de Hilbert tenemos equivalencias entre ideales del anillo de polinomios y conjuntos de puntos en un espacio.

1.1.1. Variedades afines

Sea $n \in N$, y sea K un campo algebraicamente cerrado. Sea $\mathbb{A}^n$ el espacio (K-)afín de n dimensiones, es decir:

$$\mathbb{A}^n = \{(a_1, \ldots, a_n) | i \in \{1, \ldots, n\}, a_i \in K\}$$

Denotaremos por $K[x_1, \ldots, x_n]$ al anillo de polinomios con coeficientes en K con n indeterminadas, y por $\mathscr{P}(S)$ al conjunto potencia del conjunto S.

Observemos que los elementos de $K[x_1, \ldots, x_n]$ se pueden interpretar como funciones $f : \mathbb{A}^n \to K$.

Definición 1.1.1. Sea $A = K[x_1, \ldots, x_n]$. Podemos definir la función $Z : \mathscr{P}(A) \to \mathscr{P}(\mathbb{A}^n)$ bajo la siguiente regla de correspondencia:

$$Z(\mathscr{F}) = \{P \in \mathbb{A}^n | (\forall f \in \mathscr{F})(f(P) = 0)\}$$

Si $k \in \mathbb{N}$ y $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, $Z(f_1, \ldots, f_k) := Z(\{f_1, \ldots, f_k\})$. Observemos que si $\mathfrak{a}$ es el ideal generado por $\mathscr{F}$, entonces, $Z(\mathscr{F}) = Z(\mathfrak{a})$.

Definición 1.1.2. Un subconjunto Y de $\mathbb{A}^n$ es un conjunto *algebraico* si existe un subconjunto $T \subseteq K[x_1,\ldots,x_n]$ tal que $Y = Z(T)$.

De la definición se desprende la siguiente proposición.

Proposición 1.1.3. (a) $\emptyset$ y $\mathbb{A}^n$ son conjuntos algebraicos.

(b) La intersección de cualquier familia de conjuntos algebraicos es un conjunto algebraico.

(c) La unión de dos conjuntos algebraicos es un conjunto algebraico.

Demostración. (a) Sea $c \in K$, y sea $\bar{c} \in K[x_1,\ldots,x_n]$ el polinomio constante correspondiente. Entonces, si $c \neq 0$, $Z(\bar{c}) = \emptyset$; y si $c = 0$, $Z(\bar{c}) = \mathbb{A}^n$.

(b) Sea $\mathscr{F}$ una familia de conjuntos algebraicos, y sea $Y \in \mathscr{F}$. Existe un subconjunto $I(Y) \subseteq K[x_1,\ldots,x_n]$ tal que $Y = Z(I(Y))$. Es de notar que se cumple lo siguiente:

$$(\forall Y \in \mathscr{F})\,(\forall f \in I(Y))\left(\forall x \in \bigcap \mathscr{F} \subseteq Y\right)(f(x) = 0)$$

Entonces, $\bigcap \mathscr{F} \subseteq Z\left(\bigcup_{Y\in\mathscr{F}} I(Y)\right)$.

Ahora, sea $x \in Z\left(\bigcup_{Y\in\mathscr{F}} I(Y)\right)$, entonces x cumple que para cualquier $f \in \bigcup_{Y\in\mathscr{F}} I(Y)$, $f(x) = 0$. Entonces:

$$(\forall Y \in \mathscr{F})(x \in Z(I(Y)) = Y)$$

y $x \in \bigcap \mathscr{F}$. Por lo tanto $\bigcap \mathscr{F} = Z\left(\bigcup_{Y\in\mathscr{F}} I(Y)\right)$.

(c) Sean $Y_1, Y_2 \subseteq \mathbb{A}^n$ conjuntos algebraicos, sea $Y_1 = Z(T_1), Y_2 = Z(T_2)$, y sea $T_1T_2 = \{f \cdot g | f \in T_1, g \in T_2\}$. Veamos que $Y_1 \cup Y_2 = Z(T_1T_2)$. Sea $x \in Y_1 \cup Y_2, h = f \cdot g \in T_1T_2$, supongamos que $x \in Y_1$, entonces, para cada $t \in T_1$ se cumple que $t(x) = 0$, en particular para $t = f$. Por lo tanto, $f(x) \cdot g(x) = 0$ y $h(x) = 0$, lo que prueba $Y_1 \cup Y_2 \subseteq Z(T_1T_2)$. Para probar la otra contención, sea $x \in Z(T_1T_2)$. Si $x \notin Y_1$, existe $f \in T_1$ tal que $f(x) \neq 0$, Sea $G = \{f \cdot g | g \in T_2\}$, y $h = f \cdot g \in G$. Como $G \subset T_1T_2$, $h(x) = 0$, y $g(x) = 0$. Por lo tanto, $x \in Y_2$.

□

Definición 1.1.4. Por la proposición anterior, podemos definir a la *Topología de Zariski* en $\mathbb{A}^n$ tomando como abiertos a los complementos de los conjuntos algebraicos.

Ejemplo 1.1.5. Consideremos la topología de Zariski en $\mathbb{A}^1$. Sea C conjunto algebraico, entonces existe $T \subset K[x]$ tal que $C = Z(T) = Z((T)_{K[x]})$. Como $K[x]$ es dominio de ideales principales, existe $f \in K[x]$ tal que $(T)_{K[x]} = (f)$, entonces $Z(f)$ sólo puede ser finito, o $\mathbb{A}^1$, en caso de que f sea el polinomio constante 0. Además, dado un subconjunto finito $A := a_1, \ldots, a_k \subset \mathbb{A}^1$, para cada $i \in \{1, \ldots, k\}$ existe $b_i \in K$ tal que $a_i = (b_i)$. Así que A determina un polinomio $f = (x - b_1) \cdots (x - b_k)$, tal que $A = Z(f)$. Por lo tanto, la topología de Zariski coincide en este caso con la topología cofinita.

Definición 1.1.6. Dado un espacio topológico, un subconjunto no vacío es *irreducible* si no puede expresarse como la unión de dos subconjuntos cerrados propios. El subconjunto vacío no se considera irreducible.

Ejemplo 1.1.7. Sea A conjunto con cardinalidad infinita, con la topología cofinita. Entonces A es irreducible, ya que los cerrados propios son los subconjuntos finitos, por lo tanto la unión de dos de ellos no puede ser A.

Ejemplo 1.1.8. En $\mathbb{A}^2$, $Z(x^3 + y^3 + xy^2 + x^2y - x - y)$ no es irreducible, ya que es unión de $Z(x^2 + y^2 - 1)$ y $Z(x - y)$, una circunferencia y una recta(véase la demostración de la unión de conjuntos algebraicos de la Proposición 1.1.3).

Definición 1.1.9. Una *variedad afín* es un subconjunto cerrado irreducible de $\mathbb{A}^n$ con la topología inducida. Un subconjunto abierto irreducible es una *variedad quasi-afín*.

Cabe preguntarse si podemos definir una función inverza para la función Z, y así poder establecer relaciones biunívocas entre variedades e ideales. La siguiente definición introduce este enfoque.

Definición 1.1.10. Sea $A = K[x_1, \ldots, x_n]$. Podemos definir la función ideal $I : \mathscr{P}(\mathbb{A}^n) \to \mathscr{P}(A)$ bajo la siguiente regla de correspondencia:

$$Z(Y) = \{f \in A | (\forall P \in Y)(f(P) = 0)\}$$

Ahora tenemos una función que relaciona a subconjuntos del espacio afín con ideales, es de notar que I no es función inversa de Z, sin embargo, ambas cumplen propiedades con las que podemos trabajar, como lo indica la siguiente proposición.

Proposición 1.1.11. (a) Si $T_1 \subseteq T_2$ son subcojuntos de $K[x_1, \ldots, x_n]$, entonces $Z(T_1) \supseteq Z(T_2)$.

(b) Si $Y_1 \subseteq Y_2$ son subcojuntos de $\mathbb{A}^n$, entonces $I(Y_1) \supseteq I(Y_2)$.

(c) Para cualesquiera dos subconjuntos $Y_1, Y_2 \subseteq \mathbb{A}^n$, se cumple que $I(Y_1 \cup Y_2) = I(Y_1) \cup I(Y_2)$.

(d) Para cualquier ideal $\mathfrak{a} \subseteq K[x_1, \ldots, x_2]$, $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$, el radical de $\mathfrak{a}$.

(e) Para cualquier subconjunto $Y \subseteq \mathbb{A}^n$, $Z(I(Y)) = \bar{Y}$, la cerradura de Y.

Demostración. (a) Si $x \in Z(T_2)$, entonces, para toda $f \in T_2$ se cumple $f(x) = 0$. Como $T_1 \subseteq T_2$, en particular para toda $f \in T_2$ se cumple $f(x) = 0$, entonces $x \in Z(T_1)$.

(b) Es análogo a (a).

(c) Sea $f \in I(Y_1 \cup Y_2)$, sea $x \in Y_1 \cup Y_2$, sin pérdida de generalidad $x \in Y_1$, entonces $f(x) = 0$, por lo tanto $f \in I(Y_1)$, y $f \in I(Y_1) \cap I(Y_2)$. Ahora, sea $f \in I(Y_1) \cap I(Y_2)$, entonces, $f \in I(Y_1)$, por lo tanto, para todo $x \in Y_1$, $f(x) = 0$, además, como $f \in I(Y_2)$, entonces para todo $x \in Y_2$, $f(x) = 0$, entonces $f \in I(Y_1 \cup Y_2)$.

(d) Este resultado es consecuencia del *Teorema de los ceros de Hilbert*, del cual hablaremos a continuación.

(e) Veamos que $Y \subseteq Z(I(Y))$, el cual es un conjunto cerrado, entonces basta con probar que es el cerrado más pequeno que contiene a Y. Sea W un conjunto cerrado que contiene a Y, entonces $W = Z(\mathfrak{a})$ para algún ideal $\mathfrak{a}$. Entonces $Z(\mathfrak{a}) \supseteq Y$, y por el inciso (b), $I(Z(\mathfrak{a})) \subseteq I(Y)$. Pero $\mathfrak{a} \subseteq I(Z(\mathfrak{a}))$, entonces, por (a), tenemos que $W = Z(\mathfrak{a}) \supseteq Z(I(Y))$. Por lo tanto, $\bar{Y} = Z(I(Y))$.

□

Es de notar que el inciso (d) de la proposición anterior hace referencia al *Teorema de los ceros de Hilbert*, este es un teorema muy importante de la geometría algebraica que revisaremos más a fondo en una sección posterior.

La proposición anterior responde la pregunta acerca de la relación biunívoca entre ideales y variedades, como lo indica el siguiente corolario.

Corolario 1.1.12. Un conjunto algebraico es irreducible sí y sólo sí corresponde a un ideal primo bajo las funciones Z, I.

Demostración. Si $fg \in I(Y)$, entonces $Y \subseteq Z(fg) = Z(f) \cup Z(g)$. Entonces $Y = (Y \cap Z(f)) \cup (Y \cap Z(g))$, ambos subconjuntos cerrados de Y. Como Y es irreducible, $Y = Y \cap Z(f)$ ó $Y = Y \cap Z(f)$, por lo que $Y \subseteq Z(f)$ ó $Y \subseteq Z(g)$, y $f \in I(Y)$ ó $g \in I(Y)$

Por otro lado, sea $\mathfrak{p}$ un ideal primo, y supongamos que $Z(\mathfrak{p}) = Y_1 \cup Y_2$. Entonces $\mathfrak{p} = I(Y_1) \cap I(Y_2)$. entonces tenemos que $\mathfrak{p} = I(Y_1)$ ó $\mathfrak{p} = I(Y_2)$. Entonces $Z(\mathfrak{p}) = Y_1$ ó $Z(\mathfrak{p}) = Y_2$. Por lo tanto es irreducible. □

Usemos la estructura de ideal que obtenemos de evaluar conjuntos algebraicos bajo la función I.

Definición 1.1.13. Sea $Y \subseteq \mathbb{A}^n$ un conjunto algebraico, definimos al anillo de coordenadas $A(Y)$ de Y, como $A(Y) = K[x_1, \ldots, x_n]/I(Y)$.

Ejemplo 1.1.14. Sea Y la curva $y = x^2$ definida en el plano, es decir, $Y = Z(\{y - x^2\}) \subseteq \mathbb{A}^2$. Entonces $A(Y)$ es isomorfo a $K[x]$, ya que existe un homomorfismo de anillos $\phi : K[x,y] \to K[x]$ definido por la "sustitución", es decir, $\phi(f(x,y)) = f(x,x^2)$; que cumple que $\ker(f) = I(Y)$, y además es claramente suprayectivo, así que,, por el primer teorema de isomorfismo tenemos que $K[x,y]/I(Y) \approx K[x]$

1.1.2. Teorema de los ceros de Hilbert

El teorema fundamental del Álgebra es un teorema que sentó las bases de la geometría algebraica, ya que relaciona un objeto algebraico como lo es un polinomio con una variable, con un elemento geométrico, como el conjunto de sus raíces, bajo un campo algebraicamente cerrado.

En cierto modo, el teorema de los ceros de Hilbert es un teorema que generaliza al teorema fundamental del Álgebra, hablaremos un poco más de este resultado y daremos una demostración usando algunas estructuras y resultados de los que hablaremos a continuación. Para ello, diremos que si tenemos un anillo conmutativo R, un álgebra es un R-módulo con una operación binaria R-bilineal, que además tiene un elemento neutro. Decimos que un álgebra (K-)afín es un álgebra sobre K finitamente generada, y un dominio (K-)afín es un álgebra K-afín que además es un dominio entero.

Lema 1.1.15. Sea A un álgebra sobre un campo K:

(a) Si A es un dominio entero y un conjunto algebraico sobre K, entonces es un campo.

(b) Si A es un campo y está contenido en un dominio K-afín, entonces A es algebraico.

Demostración. (a) Basta con probar que $K[a]$ es campo para todo $a \in A$. Sea $a \in A$, podemos definir $\phi : K[x] \to K[a]$ tal que $\phi(f(x)) = f(a)$. Como a es algebraico, $\ker(\phi) \neq \emptyset$. Además,

como $K[x]$ es dominio de ideales principales, existe $f \in \ker(\phi)$ tal que $\ker(\phi) = (f)$. Y como $K[a] \subseteq A$ es dominio entero, $\ker(\phi)$ es ideal primo, y f es irreducible. Por lo tanto, $\ker(f)$ es un ideal maximal, y $K[a] \approx K[x]/\ker(f)$ es campo.

(b) Supongamos que existe $a_1 \in A$ elemento no algebraico, entonces podemos decir que $A \subseteq B = K[a_1, \ldots, a_n]$, siendo B el dominio K-afín. Ordenemos a $a_2, \ldots, a_n$ de tal manera que los primeros r elementos $a_1, \ldots, a_r$ formen un subconjunto maximal de $\{a_1, \ldots, a_n\}$ algebraicamente independiente. Sea $\mathbb{Q}(B)$ el campo de cocientes de B, veamos que $\mathbb{Q}(B)$ es una extensión finita de $L = K(a_1, \ldots, a_r)$, así que podemos escoger una L-base de $\mathbb{Q}(B)$ con m elementos finitos. Dado un elemento $b \in \mathbb{Q}(B)$, la multiplicación por este elemento define un endomorfismo L-lineal, entonces podemos construír la función $\phi : \mathbb{Q}(B) \to L^{m \times m}$ tomando la matriz de la transformación definida para cada $b \in \mathbb{Q}(B)$. Sea ahora $g \in K[a_1, \ldots, a_r]$ el común denominador de todas las entradas de todas las matrices devueltas para cada $a_1, \ldots, a_n$. Entonces $\phi(a_i) \in K[a_1, \ldots, a_r, g^{-1}]^{m \times m}$ para toda $i \in \{1, \ldots, r\}$. Gracias a las propiedades lineales de la adición y la multiplicación concluímos que:

$$\phi(B) \subseteq K[a_1, \ldots, a_r, g^{-1}]^{m \times m} \tag{1.1}$$

$K[a_1, \ldots, a_r]$ es isomorfo a un anillo de polinomios, y por lo tanto, es un dominio de factorización única. Tomemos una factorización de g, y sean $p_1, \ldots, p_k$ sus factores irreducibles elementos de $K[a_1]$. Sea $p \in K[a_1]$ un elemento irreducible arbitrario, tenemos que $p^{-1} \in A \subseteq B$ ya que $K[a_1] \subseteq A$ y A es campo. Al hacer $\phi(p^{-1})$ obtendremos la matriz diagonal con entradas igual a p^{-1}, puesto que $p^{-1} \in L$. Gracias a (1.1) existe $f \in K[a_1, \ldots, a_r]$, y s natural tal que $p^{-1} = g^{-s} \cdot f$, entonces $g^s = f \cdot p$. Como p es irreducible, p es un K-múltiplo de alguno de los p_i's. Como eso se cumple para todo irreducible en $K[a_1]$, entonces todos los elementos de $K[a_1]$ son múltiplos de alguno de los p_i's. Pero esto es una contradicción, ya que $(\prod_{i=1}^{k} p_i) + 1$ no es múltiplo de ninguno de los p_i.

□

Proposición 1.1.16. Sea $\phi : A \to B$ un homomorfismo de álgebras sobre un campo K, y sea $\mathfrak{m} \subset B$ un ideal maximal. Si B es finitamente generada, entonces la preimagen de $\mathfrak{m}$ también es un ideal maximal.

Demostración. Podemos definir un homomorfismo $\psi : A \to B/\mathfrak{m}$ componiendo a ϕ con la proyección natural. Entonces, $\ker(\psi) = \mathfrak{n} := \phi^{-1}(\mathfrak{m})$. Entonces $A/\mathfrak{n}$ es isomorfo a una subálgebra de $B/\mathfrak{m}$. Por el lema anterior inciso (b), $B/\mathfrak{m}$ es algebraico, ya que B es finitamente generado, y

la inclusión a B está dada por la propiedad universal del cociente. Además, si B no es dominio entero, hereda la propiedad de álgebra afín a $B/\mathfrak{m}$, el cual es campo. Gracias a ψ, $A/\mathfrak{n}$ también es algebraico, y dominio entero, entonces por el inciso (a) del lema anterior, $A/\mathfrak{n}$ es campo y $\mathfrak{n}$ es maximal. □

Lema 1.1.17. Sea K un campo, y $P = (\xi_1, \ldots, \xi_n)$ un punto en el espacio afín, entonces el ideal:

$$\mathfrak{m}_P := (x_1 - \xi_1, \ldots, x_n - \xi_n) \subseteq K[x_1, \ldots, x_n]$$

es un ideal maximal en $K[x_1, \ldots, x_n]$.

Demostración. Por la definición del ideal es claro que dado $f \in K[x_1, \ldots, x_n]$, es congruente con $f(P)$, por lo que $\mathfrak{m}_P$ es el kernel del homomorfismo "evaluación en P", de donde $K \approx K[x_1, \ldots, x_n]/\mathfrak{m}_P$. Por lo tanto $\mathfrak{m}_P$ es maximal. □

Proposición 1.1.18. Sea K un campo algebraicamente cerrado, y sea $\mathfrak{m}$ un ideal maximal en $K[x_1, \ldots, x_n]$, entonces existe un punto $P = (\xi_1, \ldots, \xi_n)$ en el espacio afín tal que:

$$\mathfrak{m} = (x_1 - \xi_1, \ldots, x_n - \xi_n)$$

Demostración. Sea $i \in \{1, \ldots, n\}$. Gracias a la Proposición (1.1.16), tenemos que $\mathfrak{m} \cap K[x_i]$ es un ideal maximal en x_i. Como $K[x_i]$ es un dominio de ideales principales, $\mathfrak{m} \cap K[x_i] = (f_i)$. Además, como (f_i) es maximal y estamos en un campo algebraicamente cerrado, existe $\xi_i \in K$ tal que $f_i = x - \xi_i$. Por lo tanto, $x_i - \xi_i \in \mathfrak{m}$ y $\mathfrak{m}_P \subseteq \mathfrak{m}$, de donde obtenemos la maximalidad. □

Teorema 1.1.19. *Sea K un campo algebraicamente cerrado, y $S \subseteq K[x_1, \ldots, x_n]$ un subconjunto de polinomios. Sea $\mathscr{M}_S$ el conjunto de todos los ideales maximales $\mathfrak{m} \subseteq K[x_1, \ldots, x_n]$ tales que $S \subseteq \mathfrak{m}$. Entonces la función*

$$\Phi_S : Z(S) \to \mathscr{M}_S, (\xi_1, \ldots, \xi_n) \to (x - \xi_1, \ldots, x - \xi_n)$$

es una biyección.

Demostración. Sea $P = (\xi_1, \ldots, \xi_n) \in Z(S)$. Por el Lema (1.1.17), $\Phi_S(P)$ es maximal, y para todo $f \in S$ se cumple $f(P) = 0$. Entonces, $f \in \Phi_S(P)$ y $\Phi_S(P) \in \mathscr{M}_S$. Así, Φ_S está bien definida. Por otro lado, sea $\mathfrak{m} \in \mathscr{M}_S$. Por la Proposición (1.1.18), Existe $P = (\xi_1, \ldots, \xi_n) \in \mathbb{A}^n$ tal que $\mathfrak{m} = (x_1 - \xi_1, \ldots, x_n - \xi_n)$. Como $S \subseteq \Phi_S(P)$, $P \in Z(S)$, lo que prueba la suprayectividad de Φ_S.

Para probar la inyectividad, sean $P = (\xi_1, \ldots, \xi_n), Q = (\eta_1, \ldots, \eta_n)$ elementos de $Z(S)$, tal que $\Phi_S(P) = \Phi_S(Q) = \mathfrak{m}$. Veamos que, para toda $i \in \{1, \ldots, n\}$, $x - \xi_i \in \mathfrak{m}$, y $x - \eta_i \in \mathfrak{m}$, entonces $\xi_i - \eta_i \in \mathfrak{m}$ y $\xi_i = \eta_i$ porque sino, la resta resultaría en una unidad, y $\mathfrak{m}$ sería igual a $K[x_1, \ldots, x_n]$. □

Corolario 1.1.20. (Teorema de los ceros de Hillbert, primera versión) Sea K un campo algebraicamente cerrado, y sea $I \subset K[x_1, \ldots, x_n]$ ideal propio, entonces:

$$Z(I) \neq \emptyset$$

Demostración. Sea $\mathscr{F}_I$ la familia de todos los ideales propios que contienen a I, y ordenemos por contención. Entonces $I \in \mathscr{F}$, por lo que no es familia vacía, entonces por el lema de Zorn, existe $\mathfrak{m} \in \mathscr{F}_I$ ideal maximal, que contiene a I, y por el Teorema (1.1.19), existe $P \in Z(I)$ preimagen bajo Φ_I de $\mathfrak{m}$, y $Z(I) \neq \emptyset$. □

Llegados a este punto podemos empezar a comprender la importancia del Teorema de los ceros de Hilbert. Si tenemos un sistema de polinomios y buscamos las soluciones, el Teorema de los ceros de Hilbert nos da una rápida respuesta acerca de la existencia de éstas, que consiste en observar que el ideal generado por nuestro sistema de polinomios sea propio. Condiciona la existencia de respuestas a sólo una verificación, y esta verificación es la obvia, ya que si nuestros polinomios generan a $K[x_1, \ldots, x_n]$, entonces existen $g_1, \ldots, g_n$ polinomios tales que:

$$\sum_{i=1}^{n} f_i g_i = 1$$

Y obviamente no existen soluciones que anulen a todas las f_i y que se mantenga la igualdad. La verificación de que un ideal sea propio se puede realizar a través de un algoritmo que analizaremos más adelante.

Anillos de Jacobson

La versión completa del Teorema de los ceros de Hilbert aún nos da más información, ya que incluso es capaz de decirnos qué polinomios se pueden incluir a nuestro sistema, conservando el mismo conjunto solución, y de esta manera, conseguir una biyección entre variedades e ideales de polinomios a través de las funciones Z e I. Probar la versión completa será nuestro siguiente objetivo.

Definición 1.1.21. Sea R anillo.

(a) El *espectro* de R es la familia de todos los ideales primos de R:

$$\mathrm{Spec}(R) = \{P \subset R | P \text{ es ideal primo } \}$$

(b) El *espectro maximal* de R es la familia de todos los ideales maximales de R:

$$\mathrm{Spec}_{\max}(R) = \{P \subset R | P \text{ es ideal maximal } \}$$

(c) El *espectro de Rabinowitsch* de R es el conjunto:

$$\mathrm{Spec}_{\mathrm{rab}}(R) = \{\mathfrak{m} \cap R | \mathfrak{m} \in \mathrm{Spec}_{\max}(R[x])\}$$

Nótese que:

$$\mathrm{Spec}_{\mathrm{rab}}(R) \subseteq \mathrm{Spec}(R)$$

Gracias a que si S es una extensión de R, y P es ideal primo en S, entonces $S \cap R$ es ideal primo en R.

Recordemos que el radical de un ideal I en un anillo de polinomios se define como:

$$\sqrt{I} = f \in K[x_1, \ldots, x_n] | (\exists n \in \mathbb{N})(f^n \in I)$$

Un ideal I se considera radical si $I = \sqrt{I}$. Es de notar que todo ideal primo es radical.

Lema 1.1.22. Sea R un anillo, $I \subseteq R$ un ideal, y $\mathscr{M} \subseteq \mathrm{Spec}(R)$ un subconjunto. Entonces:

$$\sqrt{I} \subseteq \bigcap_{P \in \mathscr{M}, I \subseteq P} P.$$

Si no existe $P \in \mathscr{M}$ tal que $I \subseteq P$, entonces la intersección se interpreta como R.

Demostración. Sea $a \in \sqrt{I}$, entonces $a^k \in I$ para alguna $k \in \mathbb{N}$. Sea $P \in \mathscr{M}$ con $I \subseteq P$, entonces $a^k \in P$. Como P es primo se sigue que $a \in P$. □

Proposición 1.1.23. Sea R un anillo, e $I \subseteq R$ un ideal. Entonces:

$$\sqrt{I} = \bigcap_{P \in \mathrm{Spec}_{\mathrm{rab}}(R), I \subseteq P} P.$$

Si no existe $P \in \mathrm{Spec}_{\mathrm{rab}}(R)$ tal que $I \subseteq P$, entonces la intersección se interpreta como R.

Demostración. La inclusión "$\subseteq$" se sigue del lema anterior, y del hecho que $\mathrm{Spec}_{\mathrm{rab}}(R) \subseteq \mathrm{Spec}(R)$. Para probar la otra contención, sea a en la intersección. Consideremos el ideal:

$$J := (I \cup \{ax-1\})_{R[x]} \subseteq R[x]$$

Generado por I y por $\{ax-1\}$. Supongamos que $J \subset R[x]$ es un ideal propio. Por el lema de Zorn, existe $\mathfrak{m} \in \mathrm{Spec}_{\mathrm{max}}(R[x])$ tal que $J \subseteq \mathfrak{m}$. Entonces tenemos que $I \subseteq R \cap J \subseteq R \cap \mathfrak{m} \in \mathrm{Spec}_{\mathrm{rab}}(R)$. Entonces, por hipótesis, $a \in R \cap \mathfrak{m}$ y $a \in \mathfrak{m}$. Pero, como $J \subseteq \mathfrak{m}$, $ax-1 \in \mathfrak{m}$, entonces $\mathfrak{m} = R[x]$, una contradicción. Por lo tanto, $J = R[x]$, así que existe $n \in \mathbb{N}$, $g, g_1, \ldots, g_n \in R[x]$ y $b_1, \ldots, b_n \in I$ tales que:

$$1 = \sum_{j=1}^{n} g_j b_j + g(ax-1)$$

Sea $R[x,x^{-1}]$ el anillo de polinomios de Laurent, y consideremos la función $\phi : R[x] \to R[x,x^{-1}]$ definida por $\phi(f) = f(x^{-1})$, entonces, para $k = \max\{\deg(g_1), \ldots, \deg(g_n), \deg(g)+1\}$, podemos definir para toda $i \in \{1, \ldots, n\}$, polinomios $h_i := x^k \phi(g_i) \in R[x]$, $h := x^{k-1}\phi(g) \in R[x]$, tal que, aplicando ϕ a ambos lados de la igualdad y multiplicando ambos lados por x^k obtenemos:

$$x^k = \sum_{j=1}^{n} h_j b_j + h(a-x)$$

Como todos los términos de la igualdad son elementos de $R[x]$, podemos evaluar $x = a$, y obtenemos:

$$a^k = \sum_{j=1}^{n} h_j(a) b_j \in I$$

Por lo tanto, $a \in \sqrt{I}$. □

Tenemos el siguiente Corolario.

Corolario 1.1.24. Sea R un anillo, e $I \subseteq R$ un ideal. Entonces:

$$\sqrt{I} = \bigcap_{P \in \mathrm{Spec}(R), I \subseteq P} P.$$

Si no existe $P \in \mathrm{Spec}(R)$ tal que $I \subseteq P$, entonces la intersección se interpreta como R.

Demostración. Se sigue del Lema (1.1.22) y de la Proposición (1.1.23). □

Teorema 1.1.25. *Sea A un álgebra afín, e $I \subseteq A$ un ideal. Entonces:*

$$\sqrt{I} = \bigcap_{\mathfrak{m} \in Spec_{max}(A), I \subseteq \mathfrak{m}} \mathfrak{m}.$$

Si no existe $\mathfrak{m} \in Spec(A)$ tal que $I \subseteq \mathfrak{m}$, entonces la intersección se interpreta como A.

Demostración. Sea $P \in \mathrm{Spec}_{\mathrm{rab}}(A)$, entonces $P = A \cap \mathfrak{m}$ con $\mathfrak{m} \in \mathrm{Spec}_{\mathrm{max}} A[x]$, pero $A[x]$ es un álgebra afín, entonces por la Proposición (1.1.16), $P \in \mathrm{Spec}_{\mathrm{max}}(A)$. Por lo tanto:

$$\mathrm{Spec}_{\mathrm{rab}}(A) \subseteq \mathrm{Spec}_{\mathrm{max}}(A)$$

Así, el Lema (1.1.22) y la Proposición (1.1.23) prueban la igualdad. □

Tratando de generalizar el resultado del teorema anterior, es como nace la definición de anillo de Jacobson.

Definición 1.1.26. Un anillo R es un *anillo de Jacobson*, si para cada $I \subset R$ ideal propio, se cumpla que:

$$\sqrt{I} = \bigcap_{\mathfrak{m} \in \mathrm{Spec}_{\mathrm{max}}(R), I \subseteq \mathfrak{m}} \mathfrak{m}.$$

Esta definición sirve, entre otras cosas, para generalizar aún más el Teorema de los ceros de Hilbert. En efecto, uno de los resultados conocidos de anillos de Jacobson dice que si un anillo es de Jacobson, entonces cualquier álgebra afín es de Jacobson, y que las intersecciones de ideales maximales de estas álgebras con el anillo conserva su maximalidad en el anillo. Por lo tanto, también nos ayuda a descartar sistemas polinomiales sin soluciones incluso en estos anillos.

Ahora podemos probar la versión completa del Teorema de los ceros de Hilbert.

Teorema 1.1.27. *(Teorema de los ceros de Hilbert, versión completa) Sea K un campo algebraicamente cerrado, y sea $J \subseteq K[x_1, \ldots, x_n]$ ideal. Entonces*

$$I(Z(J)) = \sqrt{J}$$

Demostración. Probemos primero "$\supseteq$". Sea $f \in \sqrt{J}$, entonces existe $k \in \mathbb{N}$ tal que $f^k \in J$, entonces, para todo $P \in Z(J)$ se tiene que $f^k(P) = 0$, y $f(P) = 0$. Por lo tanto $f \in I(Z(J))$.

Probemos la otra contención. Por el Teorema (1.1.25) basta con probar que, dados $f \in I(Z(J))$, y $\mathfrak{m} \in \mathrm{Spec}_{\max}(K[x_1,\ldots,x_n])$ tal que $I \subseteq \mathfrak{m}$, se cumpla que $f \in \mathfrak{m}$; pero por el Teorema (1.1.19), existe $(\xi_1,\ldots,\xi_n) \in Z(J)$ tal que $\mathfrak{m} = (x-\xi_1,\ldots,x-\xi_n)$, entonces $f(\xi_1,\ldots,\xi_n) = 0$ y $f \in \mathfrak{m}$. Por lo tanto, se cumple la segunda contención. □

1.1.3. Variedades Proyectivas

1.1.4. Funciones Racionales

1.2. Bases de Hilbert

Capítulo 2

Anillos Cohen-Macaulay

Dada la complejidad de las variedades que podemos encontrar, es complicado estudiarlas. Existen ejemplos de variedades que suelen ir en contra de la intuición. Para aterrizar conceptos y poder trabajar con relaciones interesantes hacia ciertas constantes de las que hablaremos más adelante, nos interesa estudiar los anillos Cohen-Macaulay; que son anillos R que cumplen que para todo ideal $I \subset R$ se cumple que su profundidad con respecto a R coincide con la codimensión de I (basta probar esto para sus ideales maximales). Estos anillos son importantes porque proporcionan un contexto natural, lo suficientemente amplio como para incluir los anillos asociados a muchas clases interesantes de variedades singulares y esquemas, a los que se pueden generalizar muchos resultados sobre anillos regulares. Para este capítulo asumiremos que los anillos considerados son Noetherianos. Es posible trabajar sin esta condición, pero algunas definiciones deberían cambiar un poco.

2.1. Sucesiones regulares y complejos de Koszul

Una definición muy importante para poder trabajar, es la de *sucesión regular*, ya que extiende la noción de un elemento que no es divisor de cero. A lo largo de esta sección a estos elementos les llamaremos *regulares*

Definición 2.1.1. Sea R anillo y M R-módulo. Una sucesión de elementos $x_1, \ldots, x_n \in R$ es una *sucesión regular* en M (o una M-sucesión) sí:

I) $(x_1, \ldots, x_n)M \neq M$

II) $(\forall i \in \{1, \ldots, n\})(x_i$ es regular en $M/(x_1, \ldots, x_{i-1}))$

Estudiaremos esta noción con una herramienta homológica llamada *complejo de Koszul*. Su definición es algo complicada, por lo que primero trataremos de entender los casos más simples para después generalizar.

2.1.1. Definiciones

Antes de continuar, necesitaremos definiciones tanto para entender la definición particular del complejo de Koszul de longitud 1 y 2, como para entender la definición general(no constructiva) para cualquier longitud.

Definición 2.1.2. Un *complejo de cadenas de R-módulos* (o simplemente *complejo*) $C^\bullet$ es una sucesión de módulos $\{C^i\}_{i\in\mathbb{Z}}$ y funciones $\{d^i : C^{i-1} \to C^i\}_{i\in\mathbb{Z}}$ tal que, para toda $i \in \mathbb{Z}$, $d^{i+1} \circ d^i = 0$. En ocasiones a estas funciones se les denomina como diferenciales.

Nos referimos al kernel de d^n como $Z^n(C^\bullet)$, y a su imagen como $B^n(C^\bullet)$.

La *homología* H^i de este complejo en C^i es el módulo:

$$\ker(d^{i+1})/\mathrm{im}(d^i)$$

Un complejo, en efecto, puede usar índices finitos, si lo completamos con módulos cero y morfismos cero.

Es de notar que la enumeración y el indexado en la literatura se manejan de derecha a izquierda y con subíndices en lugar de superíndices, pero por conveniencia nosotros usaremos esta notación, que se usa más frecuentemente para hablar de la cohomología.

Para hablar de la homología de los complejos de Koszul, la siguiente definición nos será de mucha utilidad.

Definición 2.1.3. Si M es un submódulo de un S-módulo libre, y J es un ideal de S, podemos definir a los siguientes submódulos:

$$(M : J) := \{f \in F | fJ \subset M\} \subset F$$

$$(M : J^\infty) := \bigcup_{d=1}^{\infty} (M : J^d) \subset F$$

Al submódulo $(M : J^\infty)$ se le conoce como la *saturación de M con respecto a J*. Podemos abusar de la notación y escribir $(x : y)$ en lugar de $((x) : (y))$.

Nótese que gracias a esta definición es muy sencillo representar a los divisores de cero de un ideal A, que de hecho son un R-módulo. Basta con representarlos como $(0:A)$.

También, cuando estudiamos relaciones entre complejos es inevitable encontrarnos en algún momento con diagramas conmutativos, lo que nos lleva a las siguientes definiciones.

Definición 2.1.4. Un *morfismo de cadenas* entre dos complejos $F^\bullet$ y $G^\bullet$ es una sucesión de homomorfismos de módulos $\{f^\bullet = f^i : F^i \to G^i\}_{i\in\mathbb{Z}}$ tal que, para cada $i \in \mathbb{Z}$, el siguiente diagrama conmuta:

$$\begin{array}{ccc} F^{i-1} & \xrightarrow{f^{i-1}} & G^{i-1} \\ \downarrow{\scriptstyle d^i} & & \downarrow{\scriptstyle d^i} \\ F^i & \xrightarrow{f^i} & G^i \end{array}$$

Utilizamos el mismo símbolo d^i para referirnos a los diferenciales correspondientes de cada complejo.

Definición 2.1.5. Una *sucesión exacta de complejos*

$$\cdots \to C^\bullet_{i-1} \xrightarrow{f^\bullet_i} C^\bullet_i \xrightarrow{f^\bullet_{i+1}} C^\bullet_{i+1} \to \cdots$$

Es una sucesión de morfismos de cadenas $\{f^\bullet_i : C^\bullet_{i-1} \to C^\bullet_i\}_{i\in\mathbb{Z}}$ tales que, para cada $j \in \mathbb{Z}$, la sucesión de homomorfismos de módulos

$$\cdots \to C^j_{i-1} \xrightarrow{f^j_i} C^j_i \xrightarrow{f^j_{i+1}} C^j_{i+1} \to \cdots$$

es exacta. También se le denomina *sucesión exacta corta* a una sucesión exacta que consta de sólamente dos morfismos $f^\bullet : C \to D$, $g^\bullet : D \to E$ consecutivos distintos de cero, representándose de la siguente manera:

$$0 \to C^\bullet \xrightarrow{f^\bullet} D^\bullet \xrightarrow{g^\bullet} E^\bullet \to 0$$

Para hablar de la definición general del complejo de Koszul necesitaremos unas cuantas definiciones de álgebra multilineal.

Definición 2.1.6. Sean M,N R-módulos, definimos al producto tensorial $M \otimes_R N$ como el R-módulo generado por el conjunto

$$\{m \otimes n | m \in M, n \in N\}$$

bajo la relación:

$$(am+a'm')\otimes(bn+b'n') = ab(m\otimes n)+a'b(m'\otimes n)+ab'(m\otimes n')+a'b'(m'\otimes n')$$

en donde

$$r(m\otimes n) = (rm)\otimes n = m\otimes(rn)$$

Cuando el anillo es inferido por el contexto, podemos denotarlo simplemente como $M\otimes N$.

Definición 2.1.7. Sea R anillo, N un R-módulo, y $k\in\mathbb{Z}^*$; definimos la k-ésima potencia tensorial como el producto tensorial de N consigo mismo k veces:

$$T^kN = N\otimes N\otimes\cdots\otimes N$$

Por convención decimos que $T^0N = R$. El álgebra tensorial de N es la suma directa de T^kN para $k = 0,1,2,\ldots$

$$T(N) = \bigoplus_{k=0}^{\infty} T^kN$$

Definición 2.1.8. Sea N un R-módulo, el álgebra exterior $\wedge N$ de N se define como el álgebra tensorial $T(N)$ módulo las relaciones $x\otimes y = -y\otimes x$ y $x\otimes x = 0$ para toda $x,y\in N$. El producto de dos elementos $a,b\in\wedge N$ se denotará como $a\wedge b$.

$\wedge N$ es un álgebra graduada, las componentes de grado k, que corresponden a $T^k(N)$ bajo la relación de equivalencia, se denotan como $\wedge^k N$. Además, es anticonmutativa en el sentido de que si a y b son elementos homogéneos, entonces

$$a\wedge b = (-1)^{(\deg a)(\deg b)} b\wedge a$$

y si a es de grado 1, entonces $a\wedge a = 0$. Abusaremos de la notación y escribiremos $(-1)^{ab}$ en lugar de $(-1)^{(\deg a)(\deg b)}$.

La construcción de $\wedge N$ es funtorial. Esto significa que si tomamos $f : N\to M$ un morfismo de módulos, podemos definir al morfismo de álgebras $\wedge f : \wedge N\to\wedge M$ mandando $a\wedge b\wedge\ldots$ a $fa\wedge fb\wedge\ldots$.

Por último, si N es un módulo libre de rango n, entonces $\wedge^n N \cong R$, y si $f : N \to N$ es un morfismo, entonces $\wedge^n f$ es la multiplicación por el determinante de alguna matríz de representación de f. Además, $\wedge^m N = 0$ para $m > n$.

2.1.2. Complejos de Koszul de longitud 1 y 2

Podemos decidir si un elemento $x \in R$ es regular a través de la homología del complejo

$$K(x) : 0 \to R \xrightarrow{x} R$$

la cual resulta ser $(0 : x)$. Esta sencilla observación es la base para nuestro estudio de las sucesiones regulares a través de la homología.

Dado un segundo elemento $y \in R$, la multiplicación por y define una función entre complejos $K(x) \to K(x)$, es decir, un diagrama conmutativo

$$\begin{array}{ccccc} K(x): 0 & \longrightarrow & R & \xrightarrow{x} & R \\ & & \downarrow{\scriptstyle y} & & \downarrow{\scriptstyle y} \\ K(x): 0 & \longrightarrow & R & \xrightarrow{x} & R \end{array}$$

Podemos usar la conmutatividad del cuadrado en el diagrama para construir un complejo más grande, el cual lo representamos esquemáticamente de la siguiente manera

$$\begin{array}{ccccccccc} & & 0 & \longrightarrow & R & \xrightarrow{x} & R & \longrightarrow & 0 \\ K(x,y): & & & \searrow^{y} & \oplus & \searrow^{y} & & & \\ & & 0 & \longrightarrow & R & \xrightarrow{-x} & R & \longrightarrow & 0 \end{array} \qquad (\star)$$

o en una notación más usual como

$$K(x,y): \quad 0 \longrightarrow R \xrightarrow{\binom{y}{x}} R \oplus R \xrightarrow{(-x\ y)} R \qquad (\star\star)$$

En la literatura se suele definir de otra forma al complejo de Koszul, usualmente se representa con los signos de la siguiente manera

$$K(x,y): \quad 0 \longrightarrow R \xrightarrow{\binom{y}{-x}} R \oplus R \xrightarrow{(x\ y)} R$$

Estas dos posibilidades de representarlo, sin embargo, son isomorfas como complejos, por lo que no representa un problema. Nosotros elegiremos la primera forma por conveniencia para cálculos que analizaremos más adelante.

Podemos ver de la definición que $H^0(K(x)) = (0 : x)$, el anulador de x, y $H^0(K(x,y))$ es $(0,(x,y))$, así que si x es regular entonces $H^0(K(x,y)) = 0$.

Ahora analizemos qué es $H^1(K(x,y))$. Primero analicemos el kernel de la función de la derecha. Un elemento $(a,b) \in R \oplus R$ está en el kernel sí y sólo si $-xa + yb = 0$, por lo que $b \in (x : y)$. De igual manera, si $b \in (x : y)$, entonces hay un elemento a tal que $-xa + yb = 0$, así que (a,b) estará en el kernel. Si asumimos que x es regular, entonces a está únicamente determinada por b, y la asociación $b \to a$ es un homomorfismo de módulos, así que el kernel es isomorfo a $(x : y)$. Por otro lado, un elemento está en la imagen de la función de la derecha sí y sólo si es de la forma (cy, cx), así que los elementos de $(x : y)$ que corresponden a los elementos de la imagen son los elementos de (x). Así, si x es regular, entonces

$$H^1(K(x,y)) \cong (x : y)/(x)$$

En particular, si x es regular entonces $H^1(K(x,y)) = 0$ sí y sólo si la sucesión x, y satisface la condición (II) en la definición de sucesión regular.

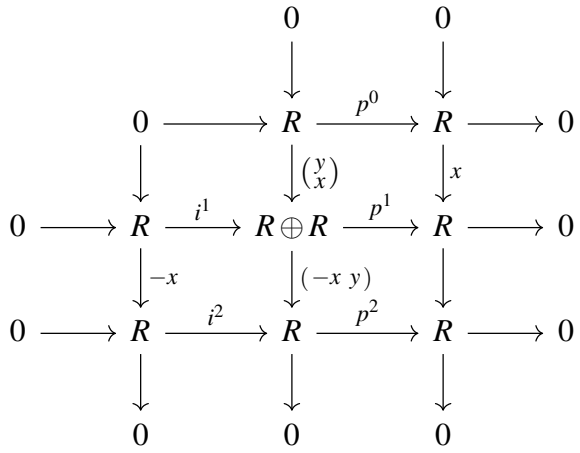
Aún podemos extraer más información si dirigimos nuestra atención al diagrama ($\star$): La fila de abajo es un subcomplejo(es decir, sus diferenciales no se salen de él) isomorfo a $K(x)$, mientras que la fila de arriba, también isomorfa a $K(x)$, es el cociente de $K(x,y)$ por la fila de abajo. En efecto, el $i-1$-ésimo termino del subcomplejo $K(x)$ está incluído en el i-ésimo término de $K(x,y)$, el cual proyecta hacia el i-ésimo término del cociente $K(x)$, por lo que tenemos la siguiente sucesión exacta corta:

$$0 \to K_1(x) \xrightarrow{i^\bullet} K(x,y) \xrightarrow{p^\bullet} K_2(x) \to 0$$

Además, un famoso lema llamado el *"lema de la serpiente"* establece que es posible obtener una sucesión exacta larga de homologías a partir de una sucesión exacta corta de complejos, redefiniendo a los morfismos $f^i : C^i \to D^i$ como $H(f^i) : H^i(C^\bullet) \to H^i(D^\bullet), H(f^i)(x + B^i(C^\bullet)) = f^i(x) + B^i(D^\bullet)$ (el lema también garantiza que estos nuevos morfismos están bien definidos), así que esta sucesión exacta larga obtenida tiene la forma:

$$\cdots \to H^0(K_2(x)) \xrightarrow{\delta} H^0(K_1(x)) \to H^1(K(x,y)) \to H^1(K_2(x)) \to \cdots$$

donde la función δ es el "homomorfismo que conecta". Para explicar este homomorfismo nos apoyaremos en el siguiente diagrama, cuyas columnas representan a $K_1(x), K(x,y)$ y $K_2(x)$, respectivamente:



Donde $i^1(z) = \binom{z}{0}$, p_1 es la proyección de la segunda coordenada, y p^0, i^2, p^2 son id_R. Ahora, sea $z \in H^0(K_2(x))$. Para obtener su imagen a través de δ, debemos tomar su preimagen a través de $H(p^0)$, que es el mismo z, y luego aplicar a un representante de la clase el diferencial. En este caso la imagen es trivial y sólo tenemos un representante, así que obtendremos $\binom{yz}{xz}$. Pero recordemos que $z \in Z^0(K_2(x))$, así que $z \in (0:x)$ y $\binom{yz}{xz} = \binom{yz}{0}$, que pertenece al kernel de p^1, así que, como $H(i^1)$ y $H(p^1)$ forman una sucesión exacta, tomemos la preimagen de $\binom{yz}{0} + B^1(K(x,y))$ a través de $H(i^0)$, que es yz, siendo finalmente la imagen de δ, por lo tanto, $\delta(z) = yz$.

Ahora supongamos solamente que $H^1(K(x,y)) = 0$. Se sigue de la sucesión exacta de homologías que:

$$H^0(K(x))/yH^0(K(x)) = 0$$

En general, esto no nos dice mucho, pero si suponemos además que R es un anillo noetheriano local y y está en el ideal maximal, entonces, por el lema de Nakayama(falta hablar de esto) tenemos que $H^0(K(x)) = 0$. Por ende, x es regular, y x, y forman una sucesión regular por lo visto anteriormente. Enunciaremos lo discutido anteriormente en el siguiente teorema.

Teorema 2.1.9. *Si R es un anillo noetheriano local, y x, y están en el ideal maximal, entonces x, y forman una sucesión regular sí y sólo si $H^1(K(x,y)) = 0$.*

Por la manera en la que definimos al complejo de Koszul en ($\star\star$), es claro que los complejos $K(x,y)$ y $K(y,x)$ son isomorfos. Así que, bajo la hipótesis del teorema anterior, x,y es una sucesión regular sí y sólo si y,x lo es. Esto es suficiente para mostrar que las sucesiones regulares permiten permutaciones.

Corolario 2.1.10. Si R es un anillo noetheriano local, y $x_1,\ldots,x_r$ es una sucesión regular de elementos en el ideal maximal de R, entonces cualquier permutación de $x_1,\ldots,x_r$ es sucesión regular.

Demostración. Como toda permutación es producto de transposiciones de elementos vecinos, basta con probar que el corolario se cumple cuando transponemos dos elementos vecinos; es decir, si $x_1,\ldots,x_i,x_{i+1},\ldots,x_r$ es una sucesión regular, entonces $x_1,\ldots,x_{i+1},x_i,\ldots,x_r$ también lo es. Para esto basta con probar que x_{i+1},x_i es sucesión regular módulo $(x_1,\ldots,x_{i-1})$, pero gracias a la propiedad (II) de la definición de sucesión regular, x_i,x_{i+1} es una sucesión regular módulo $(x_1,\ldots,x_{i-1})$, y gracias al teorema 2.1.9 la sucesión permutada es regular. □

A primera impresión podemos pensar que la hipótesis de anillo local en estos dos resultados está de más, pero no es el caso.

Ejemplo 2.1.11. Consideremos el anillo

$$R = K[x,y,z]/(x-1)z$$

y la sucesión de elementos

$$x,(x-1)y.$$

El ideal que generan es $(x,(x-1)y) = (x,y) \neq R$. Más aún, es fácil de ver que x es regular en R, y $R/(x) = K[x,y]/(z)$. Así, $x,(x-1)y$ forman una sucesión regular, y

$$H^1(K(x,(x-1)y)) = 0$$

Sin embargo, $(x-1)y$ es un divisor de cero(se anula al multiplicarse con z), así que la sucesión en orden inverso no es regular.

Algo importante de destacar es lo siguiente: Si $x \in R$ es arbitrario, entonces $H^0(K(x,0)) = H^0(K(x))$(ya que ambos son isomorfos a $(0:(x))$) incluso si el complejo $K(x,0)$ no es isomorfo a $K(x)$.

2.1.3. Complejos de Koszul en general

Podemos construír al complejo de Koszul paso a paso, iterando el proceso antes mencionado, pero la siguiente construcción es más directa, simple, e invariante, por lo que tiene más ventajas. Después veremos que tanto esta deficinión como la definición iterativa son equivalentes.

Definición 2.1.12. Dado un módulo N y un elemento $x \in N$, definimos al *Complejo de Kozsul* como el complejo

$$K(x) : 0 \to R \to N \to \wedge^2 N \to \cdots \to \wedge^i N \xrightarrow{d_x} \wedge^{i+1} N \to \cdots$$

donde d_x manda un elemento a al elemento $x \wedge a$; en particular, $1 \in R$ es mandado a $d_x(1) = x \in N$. Si N es libre de rango n y

$$x = (x_1, \ldots, x_n) \in R^n \cong N$$

entonces en ocasiones escribiremos $K(x_1, \ldots, x_n)$ en lugar de $K(x)$.

Una de las ventajas de esta definición es que hace obvias las propiedades funtoriales del complejo de Koszul. En efecto, si $f : N \to M$ es un morfismo de módulos que manda $x \in N$ a $y \in M$, entonces el morfismo $\wedge f : \wedge N \to \wedge M$ preserva diferenciales, e induce un morfismo de complejos, por ser un morfismo de álgebras.

Para familiarizarnos más con el complejo de Koszul, y dado que será importante después, mostremos que $H^n(K(x_1, \ldots, x_n)) = R/(x_1, \ldots, x_n)$. Sea $N = R^n$, y consideremos el lado derecho del complejo de Koszul:

$$\cdots \to \wedge^{n-1} N \to \wedge^n N \to \wedge^{n+1} N = 0$$

Sea $e_1, \ldots, e_n$ una base para $N = R^n$. Tenemos que $\wedge^n N \cong R$ por el isomorfismo que manda $e_1 \wedge \cdots \wedge e_n$ a 1, además que $Z^n(K(x_1, \ldots, x_n)) = \wedge^n N$, por lo tanto basta con probar que $B^n(K(x_1, \ldots, x_n))$ es isomorfo a $(x_1, \ldots, x_n)$. De igual manera, $\wedge^{n-1} N \cong R^n$, con base $e_1 \wedge \cdots \wedge e_{i-1} \wedge \hat{e}_i \wedge e_{i+1} \wedge \cdots \wedge e_n$, para $i = 1, \ldots, n$, en donde el símbolo $\hat{e}_i$ indica que e_i fue omitida. Esto debido a que la imagen de $e_1 \wedge \cdots \wedge e_{i-1} \wedge \hat{e}_i \wedge e_{i+1} \wedge \cdots \wedge e_n$ bajo el diferencial del complejo de Kozsul es

$$\left(\sum x_i e_i\right) \wedge e_1 \wedge \cdots \wedge e_{i-1} \wedge \hat{e}_i \wedge e_{i+1} \wedge \cdots \wedge e_n = (-1)^{i+1} x_i e_1 \wedge \cdots \wedge e_n$$

así que el cokernel de $\wedge^{n-1} \to \wedge^n$ es isomorfo a $R/(x_1, \ldots, x_n)$.

En general, como lo sugiere el caso de longitud 2, la homología del complejo de Koszul guarda relación con las sucesiones regulares. No detectamos siempre si $x_1,\dots,x_n$ es una sucesión regular, pero detectamos algo más interesante: las longitudes de las sucesiones regulares maximales en el ideal $(x_1,\dots,x_n)$. El resultado siguiente también nos dice que todas estas longitudes son la misma.

Teorema 2.1.13. *Sea M un R-módulo finitamente generado, y $r \in \mathbb{Z}^*$. Si*

$$H^j(M \otimes K(x_1,\dots,x_n)) = 0 \text{ para } j < r$$

mientras que

$$H^r(M \otimes K(x_1,\dots,x_n)) \neq 0$$

entonces toda M-sucesión en $I = (x_1,\dots,x_n) \subset R$ tiene longitud r.

La demostración de este teorema implica definir herramientas que no necesitaremos, pero se puede encontrar a detalle en (Eisenbud referencia).

Corolario 2.1.14. Si $x_1,\dots,x_n$ es una M-sucesión, entonces la sucesión $M \otimes K(x_1,\dots,x_n)$ es exacta excepto en el extremo derecho; es decir, $H^j(M \otimes K(x_1,\dots,x_n)) = 0$ para $j < n$. Más aún, $H^n(M \otimes K(x_1,\dots,x_n)) = M/(x_1,\dots,x_n)$

Demostración. La longitud de una M-sucesión maximal en $(x_1,\dots,x_n)$ es $l > n$, así que el teorema anterior nos confirma la primera afirmación. Ahora, el producto tensorial como funtor es exacto por la derecha, por lo que preserva cokernels, así que

$$\begin{aligned} \operatorname{coker}(M \otimes \wedge^{n-1}N \to M \otimes \wedge^n N) &= M \otimes \operatorname{coker}(\wedge^{n-1}N \to \wedge^n N) \\ &= M \otimes H^n(K(x_1,\dots,x_n)) \end{aligned}$$

Usando los cálculos que hicimos de $H^n(K(x_1,\dots,x_n))$, concluímos que

$$\begin{aligned} H^n(M \otimes K(x_1,\dots,x_n)) &= M \otimes R/(x_1,\dots,x_n) \\ &= M/(x_1,\dots,x_n)M \end{aligned}$$

□

Se puede apreciar que el recíproco es falso con el Ejemplo 2.1.11, ya que en ningún momento usamos el orden de $x_1,\ldots,x_n$, así que podríamos permutar para obtener una sucesión que no es regular; pero veremos más adelante que bajo la hipótesis de anillo local es válido el resultado.

Veamos ahora que si $IM \neq M$, entonces, al menos

$$H^n(M \otimes K(x_1,\ldots,x_n)) = M/(x_1,\ldots,x_n)M \neq 0$$

mientras, por supuesto,

$$H^{-1}(M \otimes K(x_1,\ldots,x_n)) = 0,$$

así que existe una r para la cual el Teorema 2.1.13 se puede aplicar. Por otro lado, veremos que si $IM = M$, entonces, para toda $j \in Z$, $H^j(M \otimes K(x_1,\ldots,x_n)) = 0$.

Si $IM \neq M$, entonces por el Teorema 2.1.13 las longitudes de toda M-sucesión maximal en I es la misma. Definimos a la *profundidad* de I en M, denotada como $\text{depth}(I,M)$, como la longitud de cualquier M-sucesión maximal en I. Si $M = R$, simplemente decimos profundidad de I. Si $IM = M$, por convención diremos que $\text{depth}(I,M) = \infty$.

La profundidad de I es una especie de medida aritmética del "tamaño"de I, mientras que la codimensión de I es una medida geométrica. Veremos que, tal como la codimensión, la profundidad depende únicamente del radical de I, y tiene un significado geométrico en el sentido de que, en el caso de los anillos afines, está determinada por las intersecciones de la variedad generada por I. Siguiendo esta idea, el teorema 2.1.13 implica un análogo del teorema del ideal principal(que menciona que la altura de cada ideal propio I generado por n elementos es a lo más n): Un ideal con r generadores puede tener profundidad a lo más n. Más adelante veremos que, en general, $\text{depth}I \leq \text{codim}I$.

Bajo la hipótesis de anillo local podemos dar un resultado más fuerte, y así, tener un criterio para saber si una sucesión en particular es una M-sucesión.

Teorema 2.1.15. *Sea R anillo local con ideal maximal $\mathfrak{m}$, y sea M un R-módulo finitamente generado. Sean $x_1,\ldots,x_n \in \mathfrak{m}$. Si para alguna K*

$$H^k(M \otimes K(x_1,\ldots,x_n)) = 0,$$

entonces

$$(\forall j \leq k)(H^j(M \otimes K(x_1,\ldots,x_n))).$$

En particular, si $H^{n-1}(H \otimes K(x_1,\ldots,x_n)) = 0$, entonces $x_1,\ldots,x_n$ es una M-sucesión.

La demostración de este teorema implica definir herramientas que no necesitaremos, pero se puede encontrar a detalle en (Eisenbud referencia).

Una consecuencia inmediata de este teorema refuerza al corolario 2.1.10.

Corolario 2.1.16. Sea R anillo local, M un R-módulo finitamente generado, y $(x_1,\ldots,x_n) \subset R$ un ideal propio que contiene a una M-sucesión de longitud n, entonces $x_1,\ldots,x_n$ es una M-sucesión.

Demostración. Como M es finitamente generado, el lema de Nakayama muestra que

$$H^n(M \otimes K(x_1,\ldots,x_n)) = M/(x_1,\ldots,x_n)M \neq 0.$$

Si r es el entero más pequeño tal que $H^r(M \otimes K(x_1,\ldots,x_n)) \neq 0$, entonces, por el teorema 2.1.13, toda M-sucesión maximal en $(x_1,\ldots,x_n)$ tiene longitud r, y por nuestra hipótesis, $r = n$. Así, $x_1,\ldots,x_n$ es una sucesión regular por el teorema 2.1.15. □

Este resultado se puede usar frecuentemente para demostrar que una sucesión dada es regular. Para ejemplificarlo, demostraremos el siguiente corolario.

Corolario 2.1.17 (Naturaleza geométrica de la profundidad)**.** Sea R anillo, y M un R-módulo finitamente generado.

a. Si $x_1,\ldots,x_n$ es una M-sucesión, y $t_1,\ldots,t_n \in \mathbb{Z}^+$, entonces $x_1^{t_1},\ldots,x_n^{t_n}$ es una M-sucesión.

b. Si I es un ideal de R y J es su radical, tenemos que $\operatorname{depth}(I,M) = \operatorname{depth}(J,M)$.

Demostración. a. Haremos inducción sobre r para reducir el problema al caso de anillo local.

Para $r = 1$ observemos que la potencia de un elemento regular es regular.

Ahora, supongamos que la sucesión $x_1^{t_1},\ldots,x_{n-1}^{t_{n-1}}$ es regular. Basta con probar que x_n es regular en $M/(x_1^{t_1},\ldots,x_{n-1}^{t_{n-1}})M$, lo que equivale a probar que el automorfismo $\bar{x_n}$ definido por la multiplicación por x_n tiene kernel 0.

Veamos que, si $y \in \ker \bar{x_n}$ entonces existe algún ideal primo P tal que $(0:y) \subset P$. Al localizar a $M/(x_1^{t_1},\ldots,x_{n-1}^{t_{n-1}})M$ en P, tenemos que $\frac{y}{1} \neq \frac{0}{1}$, ya que de lo contrario habría $t \in R \setminus P$ tal que $ty = 0$, una contradicción. Entonces, $x_n \cdot \frac{y}{1} = 0$ y el kernel del automorfismo inducido es distinto de 0. Por lo anterior, probemos que para todo ideal primo, el automorfismo inducido tiene kernel 0, pero eso reduce el problema al caso de anillo local, ya que si P no contiene a

algún $x_1,\ldots,x_n$, entonces $M/(x_1^{t_1},\ldots,x_{n-1}^{t_{n-1}})M = 0$ ó x_n es unidad. Por lo tanto asumiremos que R es un anillo local y $x_1,\ldots,x_n$ está contenida en el ideal maximal.

Si $x_1,\ldots,x_n$ es una sucesión regular, entonces claramente $x_1,\ldots,x_{n-1},x_n^{t_n}$ es regular. Por el corolario 2.1.16, $x_n^{t_n},x_1,\ldots,x_{n-1}$ es regular. Iterando este proceso, obtenemos que $x_{n-1}^{t_{n-1}}$, $x_n^{t_n}$, x_1, …, x_{n-2} también es regular. Después de n iteraciones concluímos que $x_1^{t_1},\ldots,x_n^{t_n}$ es sucesión regular.

b. Como $I \subset J$, es claro que $\operatorname{depth}(I,M) \leq \operatorname{depth}(J,M)$. La otra desigualdad se da gracias al inciso a, ya que si $x_1,\ldots,x_n$ es una M-sucesión en J, entonces existen $t_1,\ldots,t_n \in Z^+$ tal que $x_1^{t_1},\ldots,x_n^{t_n}$ es M-sucesión en I.

□

2.2. Profundidad

Retomando las observaciones de la sección anterior, si tenemos I ideal de un anillo R, y M un R-módulo, entonces la profundidad de I en M(denotado como $\operatorname{depth}(I,M)$) es la longitud de cualquier M-sucesión maximal contenida en I.

Frecuentemente nos veremos en el caso de localizar un anillo, así que algunas observaciones sobre el comportamiento de la profundidad bajo localizaciones serán de utilidad.

Lema 2.2.1. Si R es un anillo, y P es un ideal primo en el soporte de un R-módulo finítamente generado M. Entonces toda M-sucesión en P localiza a una M_P sucesión. De esta manera, para cualquier ideal $I \subset P$ tenemos que $\operatorname{depth}(I,M) \leq \operatorname{depth}(I_P,M_P)$, este último tomado en el anillo R_P. En general, la inecuación puede ser estricta, pero para cualquier ideal I, existen ideales maximales P en el soporte de M tales que $\operatorname{depth}(I,M) = \operatorname{depth}(I_P,M_P)$. En particular, si P es un ideal maximal, entonces $\operatorname{depth}(I,M) = \operatorname{depth}(I_P,M_P)$.

Demostración. Para la primera afirmación, el lema de Nakayama nos garantiza que $I_P M_P \neq M_P$, que es la única parte de la demostración que no es tan evidente. La profundidad puede crecer dado a que la localización $M \to M_P$ puede anular elementos que anulaban en M a elementos de I, por lo tanto, estos elementos de I se volverían regulares.

Para la segunda afirmación, sea $I = (x_1,\ldots,x_n)$ y $r = \operatorname{depth}(I,M)$. Por □

Capítulo 3

Bases de Gröbner

Muchas de las estructuras algebraicas no son constructivas, es decir, no tienen un proceso definido para obtenerse. Son muy comunes y populares los teoremas de existencia, y a través de estos podemos trabajar. Sin embargo, las computadoras necesitan pasos definidos para construir y trabajar con estructuras.

Las bases de Gröbner son muy útiles por esta razón, ya que a través de ellas podemos obtener información de una estructura algebraica a través de pasos bien definidos. Entre las aplicaciones de las bases de Gröbner figuran: una forma de evaluar si un polinomio pertenece a un ideal de un anillo de polinomios, métodos constructivos para encontrar el kernel de un morfismo de anillos, la obtención de la dimensión de un álgebra afín, intersecciones de ideales, resolución de sistemas de ecuaciones polinomiales, entre otras.

Hablaremos un poco sobre bases de Gröbner para entender mejor el proceso que realizan programas como Macaulay2, mismo en el que nos enfocaremos para estudiar las intersecciones completas.

3.0.1. Definición

Para entender las bases de Gröbner debemos definir primero unas cuantas cosas. En este capítulo, K es un campo, y $K[x_1,\ldots,x_n]$ es el anillo de polinomios con coeficientes en K, y con n indeterminadas.

Definición 3.0.1. Decimos que un polinomio $f \in K[x_1,\ldots,x_n], f \neq 0$ es un *monomio* si se cumple que:

$$(\forall i \in \{1,\ldots,n\})(\exists k_i \in \mathbb{N}_0)(f = x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n})$$

Además, si un polinomio f es de la forma $c \cdot t$ con $c \in K \setminus \{0\}$ y t monomio, entonces decimos que f es un *término*.

Denotaremos como $T(f)$ como el conjunto de todos los términos de f, de esta manera, $f = \sum_{ct \in T(f)} ct$. Más aún, diremos que $\text{Mon}(f)$ denota al conjunto de todos los monomios en f.

Definición 3.0.2. a) Sea M el conjunto de todos los monomios en $K[x_1, \ldots, x_n]$. Decimos que un buen orden $(\leq)$ sobre M es un orden monomial si se respeta bajo la multiplicación. Es decir:

$$(\forall t_1, t_2, s \in M)(t_1 \leq t_2 \Rightarrow s \cdot t_1 \leq s \cdot t_2)$$

b) Supongamos que $(\leq)$ es un orden monomial. Si $f \in K[x_1, \ldots, x_n]$ es un polinomio distinto de cero, denotamos como $\text{LM}(f)$ al elemento mayor de $\text{Mon}(f)$. Más aún, denotamos como $\text{LC}(f)$ al coeficiente de $\text{LM}(f)$ en f, y $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$. Se les conoce como *monomio principal*, *coeficiente principal* y *término principal* de f a $\text{LM}(f), \text{LC}(f)$ y $\text{LT}(f)$ respectivamente.

Recordemos que todo subconjunto en un conjunto bien ordenado tiene un primer elemento. Supongamos que $f \neq 1$ es el mínimo elemento de M, pero entonces $f \leq 1$ y $f^2 \leq f$, una contradicción. Por lo tanto, para todo elemento de $f \in M$ se cumple que $1 \leq f$.

Veamos algunos ejemplos de órdenes monomiales.

Ejemplo 3.0.3. Sean $t = x_1^{e_1} \cdots x_n^{e_n}$ y $t' = x_1^{e'_1} \cdots x_n^{e'_n}$ monomios.

(1) El *orden lexicográfico* es tal que $t \leq t'$ si $t = t'$ o $e_i < e'_i$ para la i más pequeña que cumpla que $e_i \neq e'_i$.

(2) El *orden lexicográfico de grado inverso(grevlex)* es tal que $t \leq t'$ si $t = t'$, ó $\deg(t) := \sum_{i=1}^{n} e_i < \deg(t')$, ó $\deg(t) = \deg(t')$ y $e_i > e'_i$ para el índice i más grande tal que $e_i \neq e'_i$

(3) Dados $(\leq_1)$ y $(\leq_2)$ órdenes monomiales en $K[x_1, \cdots, x_k]$ y $K[x_{k+1}, \cdots, x_n]$, el *orden de bloque* con $(\leq_1)$ dominante es tal que $t \leq t'$ si $x_1^{e_1} \cdots x_k^{e_k} <_1 x_1^{e'_1} \cdots x_k^{e'_k}$, ó $x_1^{e_1} \cdots x_k^{e_k} =_1 x_1^{e'_1} \cdots x_k^{e'_k}$ y $x_{k+1}^{e_{k+1}} \cdots x_n^{e_n} \leq_2 x_{k+1}^{e'_{k+1}} \cdots x_n^{e'_n}$

Definición 3.0.4. (a) Sea S un conjunto de polinomios en $K[x_1, \ldots, x_n]$. El ideal

$$L(S) = (\text{LM}(f) | f \in S)_{K[x_1, \cdots, x_n]}$$

es el *ideal de monomios principales* de S.

(b) Sea $I \subseteq K[x_1,\ldots,x_n]$ un ideal. Una *base de Gröbner* del ideal es un subconjunto finito $G \subseteq I$ tal que:

$$L(I) = L(G)$$

Observemos que todo ideal tiene una base de Gröbner por trabajar en anillos noetherianos. Es de resaltar que la base de Gröbner depende del orden monomial escogido.

Veamos unos ejemplos para entender mejor lo que es una base de Gröbner.

Ejemplo 3.0.5. Sea $A = k[x,y,z]$, y sea $I \subseteq A$ el ideal generado por $S = \{x^2-y^2, x^2-z^2, y^2-z^2\}$. Veamos que, tomando el orden lexicográfico, S no es una base de Gröbner, ya que $z^2 \notin L(S)$. Sin embargo, $S' = S \cup \{z^2\}$ sí lo es.

Ataquemos el objetivo principal de este capítulo, que es definir una construcción metódica para nuestras estructuras. El primer paso es hablar de formas normales.

Definición 3.0.6. Sea $S = \{g_1,\ldots,g_r\} \subseteq K[x_1,\ldots,x_r]$ un conjunto finito de polinomios, y $f \in K[x_1,\ldots,x_r]$.

(a) Decimos que f está en *forma normal* con respecto a S si ningún $t \in \mathrm{Mon}(f)$ es divisible por el monomio principal $\mathrm{LM}(g_i)$ de algún $g_i \in S$.

(b) Un polinomio f^* es la *forma normal* de f con respecto a S si cumple las siguientes condiciones:

- f^* está en forma normal con respecto a S.
- Existen $h_1,\ldots,h_r \in K[x_1,\ldots,x_n]$ tales que:

$$f^* - f = \sum_{i=1}^{r} h_i g_i, \text{ y } (\forall i \in \{1,\ldots,r\})(\mathrm{LM}(h_i g_i) \leq \mathrm{LM}(f))$$

Veamos que si f^* es forma normal de f con respecto a S, entonces ambos son congruentes módulo el ideal generado por S, pero no al contrario. Sea $S = \{x_1, x_1+1\}$, entonces 1 es congruente con 0, pero 0 no es una forma normal de 1, ya que no cumple con la desigualdad de la segunda condición de (b). Más aún, x_1 tiene dos formas normales, 0 y -1, así que, en general, las formas normales no son únicas.

Esta es la primera estructura que construiremos a través de pasos concretos. A continuación se describe un algoritmo para encontrar la forma normal de un polinomio con respecto a un conjunto S, es cual a la vez prueba la existencia de las formas normales para cada polinomio.

Algoritmo 3.0.7. Cálculo de forma normal.

Datos: Un conjunto finito $S = \{g_1, \ldots, g_r\} \subseteq K[x_1, \ldots, x_n]$, y un polinomio $f \in K[x_1, \ldots, x_n]$

Resultado: Una forma normal f^* de f con respecto a S, y, si se desea, los polinomios $h_1, \ldots, h_r$ que satisfacen 3.0.6(b)

$f^* := f$;

$h_i := 0$ para toda i;

$\mathscr{M} := \{(t,i) | t \in \text{Mon}(f^*)$ tal que $\text{LM}(g_i)$ divida a $t\}$;

mientras $\mathscr{M} \neq \emptyset$ **hacer**

  $p := (t,i) \in \mathscr{M}$ con t maximal;

  $c :=$ coeficiente de la primera entrada de p en f^*;

  $f^* := f^* - \frac{ct}{\text{LC}(g_i)} g_i$;

  $h_i := h_i + \frac{ct}{\text{LC}(g_i)}$;

fin

devolver $f^*, h_1, \ldots, h_r$;

Al redefinir a f^*, estamos eliminando de $\text{Mon}(f^*)$ a un término que rompe la normalidad, y agregamos elementos más pequeños. Por lo tanto, el algoritmo siempre va a terminar porque el orden monomial es un buen orden.

Hagamos un ejemplo para entender mejor cómo funciona nuestro algoritmo:

Ejemplo 3.0.8. Cálculo de forma normal.

Datos: $S = \{x^2 - y^2, x^2 - z^2, y^2 - z^2\} \subseteq K[x,y,z]$, $f = 2y^2z^2 - 2x^2z^2$

Resultado: 0, ya que f está generada por $L(S)$

$f^* := f$;

$h_i := 0$ para toda i;

$\mathscr{M} := \{(y^2z^2, 3), (x^2z^2, 1), (x^2z^2, 2)\}$;

`// comienzo del ciclo, continuamos porque` $\mathscr{M} \neq \emptyset$

$p := (x^2z^2, 1)$;`// podría ser cualquiera de` $(x^2z^2, 1), (x^2z^2, 2)$

$c :=$ -2;

$f^* := (2y^2z^2 - 2x^2z^2) - \frac{-2(x^2z^2)}{x^2}(x^2 - y^2) = 0$;

$h_3 := -2z^2$;

`// final del ciclo`

devolver $0, h_1 = 0, h_2 = 0, h_3 = -2z^2$;

La condición de que S sea una base de Gröbner de un ideal I es suficiente para que un polinomio tenga precisamente una forma normal con respecto a G, como lo indica el siguiente teorema.

Teorema 3.0.9. *Sea G una base de Gröbner de un ideal I. Las siguientes afirmaciones se cumplen:*

(a) Todo polinomio $f \in K[x_1,\ldots,x_n]$ tiene precísamente una forma normal con respecto a G. Entonces existe una función $NF_G : K[x_1,\ldots,x_n] \to K[x_1,\ldots,x_n]$ tal que manda a cada polinomio con la forma normal que le corresponde.

(b) La función NF_G es lineal, y $\ker(NF_G) = I$

(c) Si $\widetilde{G}$ es otra base de Gröbner de I bajo el mismo orden monomial, entonces $NF_G = NF_{\widetilde{G}}$

Demostración. Probaremos (a) y (c) juntos. Sean f^* y $\widetilde{f}$ formas normales de f con respecto a G y $\widetilde{G}$ respectivamente. Por ser formas normales se cumple que $(f^* - f) - (\widetilde{f} - f) = f^* - \widetilde{f} \in I$ así que:

$$\mathrm{LM}(f^* - \widetilde{f}) \in L(I) = L(G) = L(\widetilde{G})$$

Supongamos que $f^* \neq \widetilde{f}$. Entonces existen $g \in G$, $\widetilde{g} \in \widetilde{G}$ tales que generan, y, por ende, dividen a $\mathrm{LM}(f^* - \widetilde{f})$. Pero $\mathrm{LM}(f^* - \widetilde{f})$ es elemento de $\mathrm{Mon}(f^*)$ o de $\mathrm{Mon}(\widetilde{f})$. Por lo tanto alguna de las dos no es forma normal, una contradicción, entonces $f^* = \widetilde{f}$ y se cumplen (a) y (c).

Para la linealidad hay que observar que, por 3.0.6(b), $h := \mathrm{NF}_G(f + cg) - (\mathrm{NF}_G(f) + c\mathrm{NF}_G(g))$ es congruente con $f + cg - (f + cg) = 0$ módulo (G), entonces $h \in I$. Además, h está en forma normal con respecto a G ya que es suma de formas normales con respecto a G, y la suma no puede agregar monomios que rompan la propiedad de normalidad. Si $h \neq 0$, entonces $LM(h)$ debería ser generado por(o divide a, ya que son monomios) $LM(g)$ para algún $g \in G$, pero esto contradice el hecho de que h está en forma normal con respecto a G.

Finalmente, para $f \in \ker(\mathrm{NF}_G)$ tenemos que $f = f - \mathrm{NF}_G(f) \in I$. Por otro lado, si $f \in I$, entonces $f^* := \mathrm{NF}_G(f) \in I$. Si $f^* \neq 0$, nuevamente existe una $g \in G$ tal que $LM(g)$ divide a $LM(f^*)$, una contradicción. Entonces $f^* = 0$ □

El teorema anterior nos da una forma de probar si un polinomio está dentro de un ideal de manera metódica, por lo tanto programable. En el caso particular de probar con $f = 1$, obtenemos una prueba para saber si un ideal es propio, o contiene una constante no cero. También obtenemos el siguiente corolario:

Corolario 3.0.10. Sea G una base de Grobner de un ideal $I \in K[x_1,\ldots,x_n]$. Entonces $I = (G)_{K[x_1,\ldots,x_n]}$

Demostración. Por definición, $G \subseteq I$, entonces $(G) \subseteq I$. Por otro lado, si $f \in I$ tenemos que $\mathrm{NF}_G(f) = 0$ por el teorema 3.0.9, entonces $f \in (G)$. □

Como vemos, las bases de Gröbner son bases del ideal, pero no necesariamente pasa lo contrario, pero podemos construír una base de Gröbner partiendo de una base del ideal, y agregando los elementos que faltan para que también sea una base de Gröbner. Para esto necesitamos una forma de obtener polinomios del ideal que tengan como monomio principal a un monomio que no se pueda generar por los monomios principales de la base del ideal. En primer lugar, para lograr esto, este nuevo polinomio no debería de tener como monomio principal a uno de los monomios principales de la base del ideal. Una forma de obtener estos polinomios es a través de la siguiente definición.

Definición 3.0.11. Sean $f,g \in K[x_1,\ldots,x_n]$, y sea $t = \gcd\{\mathrm{LM}(f),\mathrm{LM}(g)\}$, entonces el polinomio:

$$\mathrm{spol}(f,g) = \frac{\mathrm{LT}(g)}{t} * f - \frac{\mathrm{LT}(f)}{t} * g$$

es llamado el *s-polinomio* de f y g.

Ahora cabe preguntarnos si sacando el s-polinomio de dos polinomios de la base de un ideal podemos hacer crecer la base hasta que sea una base de Gröbner. Este hecho lo prueba el siguiente teorema, conocido como el criterio de Buchberger:

Teorema 3.0.12. *Sea $G \subseteq K[x_1,\ldots,x_n]$ un conjunto finito de polinomios distintos de cero, entonces las siguientes afirmaciones son equivalentes:*

(a) G es una base de Gröbner del ideal $I \subseteq K[x_1,\ldots,x_n]$ generado por G.

(b) Para toda $g,h \in G$, 0 es una forma normal de $spol(g,h)$ con respecto a G.

Demostración. Claramente todos los s-polinomios de elementos de G son elementos de I, por lo tanto, si G es una base de Gröbner, todos los s-polinomios tendrán a 0 como forma normal con respecto a G. Entonces (a) implica (b).

Para probar que (b) implica (a) supongamos que no es así, entonces G no es una base de Gröbner, por lo tanto existe $f \in I$ tal que $\mathrm{LM}(f) \notin L(G)$. Sea $\mathscr{F}$ la familia de todos los conjuntos de polinomios $\{k_1,\ldots,k_r\}$ tales que cumplen que:

$$f = \sum_{i=1}^{r} k_i g_i \tag{3.1}$$

Ahora, ordenemos los elementos de $\mathscr{F}$ de la siguiente manera:

$$S \leq R \Leftrightarrow \text{máx}\{\text{LM}(h_i g_i) | g_i \in S\} \leq \text{máx}\{\text{LM}(h_i g_i) | g_i \in R\}$$

Escojamos $H \in \mathscr{F}$ minimal bajo este orden. Es posible porque el orden monomial es un buen orden, y sea $H = \{h_1, \ldots, h_k\}, t = \text{máx}\{\text{LM}(h_i g_i) | i = 1 \ldots r\}$

Gracias a (3.1) sabemos que existe una i para la que $\text{LM}(f) \in \text{Mon}(h_i g_i)$, y como $\text{LM}(f) \notin L(G)$, esto implica que $\text{LM}(h_i g_i) > \text{LM}(f)$, y a su vez, $t > \text{LM}(f)$, por lo tanto el coeficiente de t en el lado derecho de la suma es cero, entonces, si definimos:

$$c_i := \begin{cases} \text{LC}(h_i), & \text{si LM}(h_i g_i) = t \\ 0, & \text{en otro caso} \end{cases}$$

obtenemos que:

$$\sum_{i=1}^{r} c_i \text{LC}(g_i) = 0 \tag{3.2}$$

Podemos asumir que $c_1 \neq 0$. Sea $J = 2, \ldots, r$ el conjunto de los índices tales que $c_i \neq 0$, y sea $i \in J$. Entonces $\text{LM}(g_i)$ divide a t. Si t_i es el mínimo común múltiplo de $\text{LM}(g_i)$ y $\text{LM}(g_1)$, entonces t_i también divide a t, por lo tanto la definición del s-polinomio la podemos reescribir para estos polinomios en particular de la siguiente manera:

$$\text{spol}(g_i, g_1) = \frac{\text{LC}(g_1) t_i}{\text{LM}(g_i)} * g_i - \frac{\text{LC}(g_i) t_i}{\text{LM}(g_1)} * g_1$$

De lo que concluímos que $\text{LM}(\text{spol}(g_i, g_1)) < t_i$. Por hipótesis, tenemos que existen $h_{i,j}$ polinomios tales que:

$$\text{spol}(g_i, g_1) = \sum_{j=1}^{r} h_{i_j} g_j, \text{ y } (\forall j \in 1, \ldots, r)(\text{LM}(h_{i,j} g_j) < \text{LM}(\text{spol}(g_i, g_i))) < t_i)$$

Sea $s_i = t/t_i * \text{spol}(g_i, g_i)$. Como

$$\mathrm{LM}(h_i)\mathrm{LM}(g_i) = t = \mathrm{LM}(h_1)\mathrm{LM}(g_1)$$

tenemos de la reescritura de la definición del s-polinomio, que:

$$s_i = \mathrm{LC}(g_1)\mathrm{LM}(h_i)g_i - \mathrm{LC}(g_i)\mathrm{LM}(h_1)g_1 \tag{3.3}$$

y de la hipótesis, tenemos que:

$$s_i = \sum_{j=1}^{r} \frac{t}{t_1} h_{i_j} g_j, \text{ y } (\forall j \in 1,\ldots,r)(\mathrm{LM}(\frac{t_i}{t} h_{i,j} g_j) < (t/t_i)t_i = t) \tag{3.4}$$

Ahora sea $g = \sum_{i=1}^{r} c_i \mathrm{LM}(h_i)g_i$ y escribamos a $\mathrm{LC}(g_1)g$ como:

$$\mathrm{LC}(g_1)g = \sum_{j=2}^{r} c_i \left(\mathrm{LC}(g_1)\mathrm{LM}(h_i)g_i - \mathrm{LC}(g_i)\mathrm{LM}(h_1)g_i\right) +$$

$$\left(\sum_{i=2}^{r} c_i \mathrm{LC}(g_i) + c_1 \mathrm{LC}(g_1)\right) \mathrm{LM}(h_1)g_1$$

Sustituyendo gracias a (3.2), (3.3) y (3.4) tenemos que:

$$g = \sum {i_2}^{r} \frac{c_i}{\mathrm{LC}(g_1)} s_i = \sum_{j_1}^{r} \widetilde{h_j} g_j, \text{ y } (\forall j \in 1,\ldots,r)(\mathrm{LM}(\widetilde{h_j} g_j) < t)$$

Por (3.1) se sigue que:

$$f = (f-g) + g = \sum_{i_1}^{r} \left(h_j - c_j \mathrm{LM}(h_j) + \widetilde{h_j}\right) g_j$$

y esto sigue de la definición de t y c_j, que $\mathrm{LM}(((h_j - c_j\mathrm{LM}(h_j))g_j)) < t$, ya que si $\mathrm{LM}(h_j g_j) \neq t$, entonces $c_j = 0$ y $\mathrm{LM}(h_j g_j) < t$, y si $\mathrm{LM}(h_j g_j) = t$, entonces al hacer $((h_j - c_j\mathrm{LM}(h_j))g_j)$ se eliminará el monomio principal. Entonces:

$$\mathrm{LM}((h_j - c_j\mathrm{LM}(h_j) + \widetilde{h_j})g_j) < t$$

Lo que contradice la minimalidad de t. Esta contradicción muestra que G es una base de Gröbner. □

Este criterio senta las bases para un algoritmo muy importante en la geometría algebraica computacional, que da una construcción de la base de Gröbner de cualquier ideal de polinomios. El cual mostramos a continuación:

Algoritmo 3.0.13. Algoritmo de Buchberger

Datos: Un conjunto finito $S = \{g_1, \ldots, g_r\} \subseteq K[x_1, \ldots, x_n]$

Resultado: Una base de Gröbner del ideal generado por S, con respecto a algún orden monomial indicado

$G := S \setminus \{0\}$; $s^* := 0$;

hacer

  para cada $g, h \in G$ **hacer**

    $s^* := \text{spol}(g, h)$;

    si $s^* \neq 0$ **entonces**

      $G := G \cup \{s^*\}$;

      Salir del ciclo;

    fin

  fin

mientras $s^* \neq 0$;

devolver G;

Por el teorema de las bases de Hilbert el algoritmo termina, ya que cada que se agrega un nuevo polinomio, $L(G)$ crece estrictamente.

Este algoritmo es muy importante para diversos programas de cómputo enfocados a la geometría algebraica, tales como CoCoA, Macaulay 2, Magma, o Singular. En el transcurso del desarrollo de la tesis nos enfocamos en Macaulay 2. Podemos calcular la base de Gröbner de un ideal en este programa de la siguiente manera:

Ejemplo 3.0.14. Calculamos la base de Gröbner del ideal correspondiente a la gráfica de la función $f : \mathbb{A}^1_k \to \mathbb{A}^3_k$ definida por $f(t) = (t^3, t^2, t)$, usando el orden lexicográfico.

```
i1 : KK = QQ


o1 = QQ


o1 : Ring
```

```
i2 : R = KK[x,y,z]

o2 = R

o2 : PolynomialRing

i3 : S=KK[t]

o3 = S

o3 : PolynomialRing

i4 : SxR = KK[t,x,y,z,MonomialOrder=>Lex]

o4 = SxR

o4 : PolynomialRing

i5 : gamma = ideal(x-t^3,y-t^2, z-t)

                  3          2
o5 = ideal (- t  + x, - t  + y, - t + z)

o5 : Ideal of SxR

i6 : gens gb gamma

o6 = | y-z2 x-z3 t-z |

                1          3
o6 : Matrix SxR  <--- SxR
```

Gracias a usar la base de Gröbner con este orden dado, pudimos obtener una base en la cual tenemos parametrizado tanto a x como a y en términos de z, y por tanto, podemos observar que el kernel de la función es exactamente lo generado por $y-z^2, x-z^3$.

Capítulo 4

Bases de Gröbner en ideales tóricos simpliciales

Ya hemos visto la gran utilidad que representa obtener la base de Gröbner de nuestros ideales. Sin embargo, los métodos para obtenerla, aunque sabemos que terminan, no sabemos en cuánto tiempo. En un intento por simplificar el problema, tratamos de acotar el máximo grado de los polinomios que obtendremos en nuestra base de Gröbner(mínima). Sin embargo, no es fácil.

Una forma de estudiar esto es a través de un invariante que sea más fácil de usar, como la regularidad de Castelnuovo-Mumford. Este invariante se puede definir como el máximo de todas las restas entre el grado menos i de cualquier i-ésimo syzygy minimal(tomando a los generadores como 0-syzygy).

En las coordenadas genéricas y con respecto al orden lexicográfico inverso, el grado máximo en una base de Gröbner minimal de I está acotado por reg(I). Desafortunadamente, eso no es cierto para coordenadas arbitrarias (véase ejemplo). Por otra parte, una famosa conjetura por Eisenbud y Goto afirma que $reg(I) \leq deg(R/I) - codim(R/I) + 1$, tomando a I como un ideal primo conteniendo una forma no lineal. Aquí, $deg(R/I)$ y $codim(R/I)$ denotan la multiplicidad y la codimensión de R/I, respectivamente. No obstante, en las coordenadas genéricas, la cota de Eisenbud-Goto: $degR/I - codimR/1 + 1$ es una cota esperada para el máximo grado en una base de Gröbner minimal de I con respecto al orden lexicográfico inverso de un ideal primo que no contiene una forma lineal. Podemos confiar que se siga esperando esto para algunas otras coordenadas.

En este trabajo estamos interesados en la estimación de la complejidad de grados de bases de Gröbner de ideales tóricos simpliciales. Los ideales tóricos se portan bien, particularmente

porque son ideales primos, y en las coordenadas naturales, son generados por binomios. Con respecto a encontrar una base de Gröbner mínima de algún ideal, es por tanto natural intentar mantener las coordenadas originales, asi que estos elementos en una base de Gröbner se pueden tomar como binomios - los cuales son fáciles de calcular y restaurar - . Por otro lado, en referencia, los últimos dos autores muestran que para una gran clase de ideales tóricos simpliciales I, la regularidad de Castelnuovo-Mumford reg(I) está acotado por la cota de Eisenbud-Goto $deg(R/I) - codim(R/I) + 1$. Por este fenómeno creemos que la siguiente conjetura se cumple.

Teorema 4.0.1. *Asumamos que I es el ideal tórico asociado al semigrupo afín homogéneo simplicial S sobre un campo arbitrario K. El máximo grado en una base de Gröbner minimal de I en las coordenadas naturales y con respecto a el orden lexicográfico inverso, está acotado superiormente por* $degK[S] - codimK[S] + 1$

Note que esto no es cierto para un orden de términos arbitrario. Para el resto del trabajo, si no decimos lo contrario, consideraremos las coordenadas naturales y el orden lexicográfico inverso. Aunque todavía no somos capaces de resolver el problema de arriba, podemos establecer la cota superior $2(degK[S] - codimK[S])$. Para lograr esto, primero establecemos una cota superior en términos del número de reducción $r(S)$ de $K[S]$. Entonces, combinando con una cota de (Referencia) en $r(S)$, obtenemos el resultado principal, (Teorema 1.1). También podemos proveer otra cota en términos de la codimensión $c = codimK[S]$ y el grado total α de los monomios que definen a S. En muchos de los ejemplos de cotas en los teoremas 1.1 y 1.4 son incluso más pequeños que la cota de Eisenbud-Goto.

En la Sección 2 resolveremos la conjetura de arriba para ciertas clases de ideales tóricos simpliciales. Los ideales de la primera clase vienen de una simple observación de que el máximo grado en su mínima base de Gröbner está acotado por el número de regularidad de Castelnuovo-Mumford si los anillos correspondientes $K[S]$ son anillos Cohen-Macaulay generalizados. Los ideales del segundo tipo son caracterizados por ciertas propiedades del conjunto de parámetros $\mathscr{A}$(proposiciones 2.4 y 2.6). En esta situación, usando el (teorema 1.4) podemos restringirnos a pocos casos excepcionales cuando al codimensión es muy grande. Entonces, la técnica principal es refinar las cotas en base al número de reducción o calcular su valor exacto. Así que alguna puede aplicar (teorema 1.1). En particular, mostraremos que la conjetura se sostiene para todos los ideales tóricos simpliciales en (referencia), para los cuales la conjetura de Eisenbud-Goto se sabe que es cierta.

4.1. Cotas

Recordemos que un semigrupo afín es uno que se puede escribir como semigrupo de $\mathbb{N}^d$, Sea $S \subseteq \mathbb{N}^d$ un semigrupo homogéneo simplicial afín, generado por un conjunto de elementos de la siguiente forma:

$$\mathscr{A} \;=\; \{\mathbf{e}_1,\ldots,\mathbf{e}_d,\mathbf{a}_1,\ldots,\mathbf{a}_c\} \;\subseteq\; M_{\alpha,d} \;=\; \{(x_1,\ldots,x_d) \;\in\; \mathbb{N}^d \;\mid\; x_1 + \cdots + x_d\}$$

donde $c \geq 2$, $\alpha \geq 2$ son números naturales

4.2. Ideales tóricos simpliciales

Sea $S \subseteq \mathbb{N}^d$ semigrupo afín homogéneo simplicial generado por:

$$\mathscr{A} = \{\mathbf{e}_1,\ldots,\mathbf{e}_d,\mathbf{a}_1,\ldots,\mathbf{a}_c\} \subset \mathscr{M}_{\alpha,d} = \{(a_1,\ldots,a_d) \in \mathbb{N}^d | \sum_{i=1}^{d} a_i = \alpha\}$$

donde $x \geq 2$, $\alpha \geq 2$ son súmeros naturales, y $\mathbf{e}_1 = (\alpha,0,\ldots,0),\ldots,e_d = (0,\ldots,0,\alpha)$. Más aún, si $\mathbf{a}_i = (a_{i1},a_{id})$, podemos asumir que, para $i \in \{1,\ldots,c\}, j \in \{1,\ldots,d\}$, los enteros a_{ij} son primos relativos.

También veamos que $K[S] \equiv K[t_1^\alpha,\ldots,t_d^\alpha,\mathbf{t}^{\mathbf{a}_1},\ldots,\mathbf{t}^{\mathbf{a}_c}] \subseteq K[\mathbf{t}]$, y, de hecho, $\{t_1^\alpha,\ldots,t_d^\alpha\}$ es un conjunto maximal algebraicamente independiente de este anillo. Por lo tanto, $\dim K[S] = d$ y $\operatorname{codim} K[S] = c$, si vemos a $K[S]$ como cociente de una normalización de Noether.

Definición 4.2.1. Sea $I_{\mathscr{A}}$ el kernel del homomorfismo:

$$K[\mathbf{x},\mathbf{y}] := K[x_1,\ldots,x_c,y_1,\ldots,y_d] \to K[t_1^\alpha,\ldots,t_d^\alpha,\mathbf{t}^{\mathbf{a}_1},\ldots,\mathbf{t}^{\mathbf{a}_c}]$$

$$x_i \to \mathbf{t}^{\mathbf{a}_i}; y_i \to t_j^\alpha; i \in \{1,\ldots,c\}; j \in \{1,\ldots,d\}$$

Entonces, decimos que $I_{\mathscr{A}}$ es un *ideal tórico simplicial definido por* $\mathscr{A}$ (ó por S).

Consideraremos la graduación estándar en $K[\mathbf{x},\mathbf{y}]$ y $K[S]$. Es decir, $\deg(x_i) = \deg(y_i) = 1$ y si $\mathbf{b} \in S$, entonces $\deg(\mathbf{b}) = (\sum_{i=1}^{d} b_i)/\alpha$.

Gracias a (Referencia) sabemos que $I_{\mathscr{A}}$ tiene una base de Gröbner minimal que consiste de binomios. Nos interesa conoces su grado máximo.

Sea $A = A_0 \bigoplus A_1 \bigoplus \cdots$, donde $A_0 = K$