UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

¿Y SI LA CARACTERISTICA DEL CAMPO DIVIDE AL ORDEN DEL GRUPO?

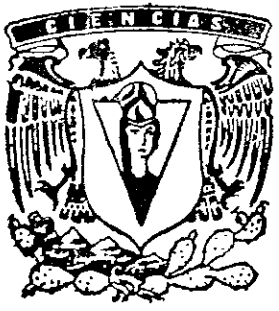
T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A

RAUL SIERRA ALCOCER



DIRECTOR DE TESIS: DR. RODOLFO SAN AGUSTIN CHI

2000

2624

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

MAT. MARGARITA ELVIRA CHÁVEZ CANO
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo de Tesis

"Si la característica del campo divide al orden del grupo"

realizado por Raúl Sierra Alcocer

con numero de cuenta 9550102-4 , pasante de la carrera de Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio

Atentamente

Director de Tesis Propietario	Dr. Rodolfo San Agustín Chi
Propietario	Dr. Alejandro Javier Díaz Barriga Casales
Propietario	Dra. Bertha María Tomé Arreola
Suplente	Dr. Hugo Alberto Rincón Mejía
Suplente	Dr. Herbert Kanarek Blando

Consejo Departamental de
Matemáticas

DR. HECTOR MENDEZ LANGO

MATEMATICAS

FACULTAD DE CIENCIAS
DIVISION DE ESTUDIOS PROFESIONALES

página

Introducción.

La relación entre el álgebra y la computación es un fenómeno natural debido al carácter algorítmico de la primera En las últimas dos décadas se han desarrollado herramientas computacionales muy poderosas y accesibles lo cual ha incrementado esta relación abriendo nuevas áreas de investigación en álgebra. A su vez esto ha permitido la aplicación de aspectos teóricos de esta área de las matemáticas a la solución de problemas en otras disciplinas como la física y la ingeniería.

Entre las principales tareas del álgebra computacional están el cálculo de cerraduras y descomposiciones de objetos en el anillo de polinomios. En este texto se dan ejemplos de ambas El cálculo del anillo de invariantes, tema central de esta tesis, es ejemplo del primer tipo, mientras que la descomposición primaria de ideales es ejemplo del segundo

Existen varios métodos efectivos para el cálculo del anillo de invariantes Sin embargo la mayor parte de estos funcionan sólo cuando estamos trabajando con un campo cuya característica es cero, esto es debido a que recaen fuertemente en el uso del operador de Reynolds y la fórmula de Molien, los cuales involucran división entre el orden del grupo, por lo que no resultan útiles cuando el orden del grupo es múltiplo de la característica del campo, a este caso se le llamará modular.

No fue sino hasta la publicación del artículo "Calculating Invariant Rings of Finite Groups over Arbitrary Fields"(Gregor Kemper, 1996) cuando se expuso un algoritmo que responde tanto al caso modular como al no modular, anteriormente la solución al caso modular se daba mediante técnicas específicas para el campo y el grupo con los que se estaba trabajando La presentación de los algoritmos presentados en dicho artículo conforma el principal objetivo de este trabajo

La primera sección trata sobre las bases de Groebner, tema al parecer inevitable cuando se habla de álgebra computacional. En esta sección se explica que son estos conjuntos y como calcularlos Al final se da una versión de bases de Groebner para módulos, la cual nos permite, como en el caso para ideales, resolver el problema de pertenencia. A lo largo del texto aparecerán en varias ocasiones estos conjuntos y creo que al final se habrá dado una buena idea del por qué de su importancia.

En la segunda sección de este trabajo se presentan los algoritmos para el cálculo de invariantes primarios y secundarios En esta sección se plantean los algoritmos en términos generales señalando los cálculos necesarios para su ejecución, pero sin entrar en detalles. Es en al apéndice A donde se explica más cuidadosamente como llevar a cabo los pasos más complejos de estos algoritmos.

Uno de los algoritmos que se presentan en el apéndice A es el de descomposición primaria Este es el que presenta mayores dificultades y no se expone en su totalidad La explicación que aquí se hace llega hasta el punto en que son necesarias técnicas factorización de polinomios, tema de no poco interés, pero que se aleja del objetivo de este trabajo.

El apéndice B reúne algunos de los resultados de álgebra conmutativa utilizados en las secciones anteriores, la mayor parte con sus respectivas demostraciones.

La tesis esta dirigida a lectores interesados en el álgebra conmutativa y cuyo contacto con el álgebra computacional ha sido poco. El lector encontrará que los capítulos 1, 2, 3, 4 y 7 del libro "Introduccion to Commutative Algebra"(Atiyah, 1969) contienen el material requerido para esta lectura.

Por último, cabe mencionar que en algunos casos se utilizan resultados que no se demuestran. esto es debido a que hacerlo habría implicado ahondar en temas que distan del enfoque que se ha buscado dar al texto. Cuando esto suceda se señalará dando la referencia que permita al lector revisar la teoría que justifica la afirmación.

1 Bases de Groebner.

Antes de definir que es una base de Groebner necesitamos definir algunos conceptos y fijar un poco de notación

1.1 Ordenes monomiales.

Sea M el conjunto de monomios x^{α}, $\alpha \in \mathbf{Z}^n_{\geq 0}$

1.1.1 Definición. *Un orden monomial en M es una relación $>$ tal que, para cualesquiera $m_1, m_2, m_3 \in M$ no constantes*

i) $>$ *es un orden total en* M.
ii) $m_1 > 1$.
iii) *si* $m_1 > m_2$ *entonces* $m_3 \cdot m_1 > m_3 \cdot m_2$.

Un ejemplo de orden monomial es el orden lexicográfico para el cual

$$x^{\alpha} >_{lex} x^{\beta}, \ \alpha, \beta \in \mathbf{Z}^n_{\geq 0},$$

si $\alpha \neq \beta$ y para $\alpha - \beta = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ tenemos que si $i = \min\{j \mid \alpha_j \neq \beta_j\}$ entonces $\alpha_i - \beta_i > 0$

Dado un orden monomial $>$ podemos definir los siguientes conceptos

1.1.2 Definición. *Sea $>$ un orden monomial en M y $f \in K[x_1, \ldots, x_n]$. Supongamos que $f = c x^{\alpha} + f'$, donde x^{α} es mayor que cualquier monomio en f' con respecto a $>$, entonces*

i) $LT(f) = c x^{\alpha}$ *es el término principal de* f.
ii) $LM(f) = x^{\alpha}$ *es el monomio principal de* f
iii) $LC(f) = c$ *es el coeficiente principal de* f.

Dado un ideal $I \subset K[x_1, \ldots, x_n]$ definimos LT(I) como el conjunto de todos los términos principales de elementos de I. Si consideramos el ideal $\langle LT(I) \rangle$ dado que por el lema de Dickson[1] todo ideal generado por un conjunto de monomios de

[1] Cox, D., Little, J., O'Shea, D. (1997) p 69

$K[x_1, \ldots x_n]$ es generado por un subconjunto finito del conjunto de generadores entonces existe un número finito de elementos de I tales que sus términos principales generan a $<LT(I)>$

1.2 Bases de Groebner(Definición y construcción)

1.2.1 Definición. *Sea $I \subset K[x_1, \ldots x_n]$ un ideal y $G=\{g_1, \ldots, g_s\} \subset I$ un conjunto tal que $<LT(I)> = <LT(g_1), \ldots LT(g_s)>$ con respecto a algún orden monomial $>$ entonces G es una Base de Groebner de I.*

1.2.2 Definición. *Sea $I \subset K[x_1, \ldots x_n]$ y G una Base de Groebner de I con respecto a algún orden $>$ entonces el conjunto $M \setminus <LT(I)>$ es el conjunto de monomios standard asociado a G.*

El conjunto de monomios standard resulta ser una base para $K[x_1, \ldots, x_n]/I$ como espacio vectorial sobre K

1.2.3 Definición. *Dado un polinomio $f \in K[x_1, \ldots x_n]$ el único polinomio*

$$res(f) = \Sigma a_\alpha x^\alpha, \text{ donde cada } x^\alpha \text{ es un monomio standard, tal que}$$

$$f - res(f) \in I,$$

es el residuo de f, o forma normal, módulo I con respecto al orden elegido.

Nótese que en la definición se afirma que dada $f \in K[x_1, \ldots, x_n]$ tenemos que res(f) es unico. El siguiente argumento nos permite hacer dicha aseveración. Sean $r=\Sigma a_\alpha x^\alpha$ y $r'=\Sigma b_\alpha x^\alpha$ tales que cumplen con las condiciones de la definición. Dado que f-r y f-r' $\in I$ entonces $r-r' \in I$ Sea $(a_\alpha - b_\alpha)x^\alpha$ el término principal de r-r' entonces $x^\alpha \in <LT(I)>$ o $(a_\alpha - b_\alpha)=0$ Por hipótesis debemos tener $a_\alpha - b_\alpha = 0$, por lo tanto $r-r'=0$.

Antes de comenzar a estudiar algunas de las propiedades de las bases de Groebner se requiere de un algoritmo para dividir en $K[x_1, \ldots, x_n]$. La idea es generalizar el algoritmo de la división en $K[x_1]$ de tal forma que dado un conjunto de polinomios $F=\{f_1, \ldots f_s\}$ podamos expresar cualquier polinomio en términos de $f_1, \ldots, f_s$ y un residuo r cuyos términos no son divisibles por ningún término en LT(F).

Sea T un orden monomial en $K[x_1, \ldots, x_n]$ y sean $f_1, \ldots, f_s$, $f \in K[x_1, \ldots x_n]$. Decimos que f es reducible módulo $F=\{f_1, \ldots, f_s\}$ si existe $f_i \in F$ tal que $LT(f_i)$ divide a algún termino de f

1.2.3 Algoritmo de la división en $K[x_1,\ldots,x_n]$.

Datos: $F=\{f_1,\ldots, f_s\}$, f.
Resultado: $a_1,\ldots, a_s$, $r\in K[x_1,\ldots,x_n]$ tales que $f=\Sigma a_i\cdot f_i + r$ y ningún término de r es divisible por alguno de los términos $LT(f_1), \ldots, LT(f_s)$.

Definimos $a_{1\,0}:=0,\ldots,a_{s\,0}:=0$, $r_0:=f$.

Dados $a_{1\,i},\ldots,a_{s\,i}$, p_i. Si p_i es reducible módulo F escogemos $f_j\in F$ tal que $LT(f_j)\cdot cm$ es igual a algún término de r_i, para algún $m\in M$ y $c\in K$. Entonces

$$r_{i+1}:= r_i - cm\cdot f_j,\ a_{j,i+1}:= a_{j,i} + cm \text{ y } a_{h,i+1}:=a_{h,i}, \text{ con } h\in\{1,\ldots,s\} \text{ y } h\neq j.$$

Si r_i es irreducible módulo F entonces
$r:=r_i$, $a_1:= a_{1\,i},\ldots, a_s:= a_{s,i}$.

Cuando un polinomio f se puede expresar como una suma $\Sigma a_i\cdot f_i + r$ por medio del algoritmo de la división decimos que f se reduce a r módulo $f_1, \ldots, f_s$

Uno esperaría que si tuviésemos un conjunto de generadores $f_1, \ldots, f_s$ para algún ideal I y un elemento $f\in I$ entonces dividir f entre $f_1, \ldots, f_s$ nos daría una expresión de f en términos de la base de tal forma que el residuo sería cero. Sin embargo esto no es cierto en general y es aquí donde se hace presente una propiedad básica de las bases de Groebner.

Supongamos que $G=\{g_1, \ldots, g_s\}$ es una base de Groebner para I y sea $f\in K[x_1,\ldots,x_n]$. Después de dividir f entre G obtenemos $a_1, \ldots, a_s$, r tales que $f=\Sigma a_i\cdot g_i + r$, y ningún término de r es múltiplo de algún término en LT(G). Así que ningún término de r está en $<LT(G)>$, que es $<LT(I)>$ por definición de G, por lo tanto $r=res(f)$. Esto en particular nos esta diciendo que si $f\in I$ entonces el residuo de dividir f entre G es cero. De la última afirmación se sigue que G es una base para I y es una base tal que nos permite saber cuando un polinomio pertenece al ideal. Sólo nos falta un método para calcular una base de Groebner a partir de un conjunto de generadores de I.

Dado $F=\{f_1, \ldots, f_s\}$ un conjunto de generadores de I, el objetivo es tener un criterio para saber si F es una base de Groebner y, si no lo es, poder decidir que elementos de I agregar a F para obtener dicha base. Una primera observación nos sugiere que si $f\in I$ es tal que al dividirlo entre F el residuo r es distinto de cero entonces hay que

añadir r a F. Es claro que $r \in I$, sin embargo LT(r) no está en $<LT(F)>$ y es por eso que hay que sumarlo a F En efecto ésta es la estrategia, pero debemos refinarla, pues de otro modo podríamos pasar el resto de nuestra vida tratando de encontrar dichos polinomios Es con este fin que se presentan los siguientes polinomios.

Definición 1.2.4. *Sean $f,g \in K[x_1, \ldots, x_n]$ polinomios distintos de cero. Sea $mcm(LM(f), LM(g)) = x^\gamma$ el mínimo común múltiplo de los monomios principales de f y g El polinomio*

$$S(f,g) = \left(x^\gamma / LT(f)\right) f - \left(x^\gamma / LT(g)\right) g$$

es el s-polinomio de f y g.

Proposición 1.2.5. *Sea I un ideal Entonces un conjunto generador $F=\{f_1, \ldots, f_s\}$ de I es una base de Groebner si y sólo si para cualquier par $f_i, f_j \in F$, $S(f_i, f_j)$ se reduce a cero módulo F.*

Demostración. Si F es una Base de Groebner ya mencionamos anteriormente que cualquier elemento de I se reduce a cero con respecto a F, en particular $S(f_i,f_j)$
Sea $f \in I$ entonces existen $h_1, \ldots, h_s$ tales que $f=\Sigma h_i f_i$ Sea $m_i = LM(h_i f_i)$ y $m=\max(m_1, \ldots, m_s)$ es claro que $LM(f) \leq m$. Consideremos todas las formas posibles en que se puede expresar f, para cada forma tenemos una m_i la cual puede diferir o no de otras, sea x^δ el mínimo de todas estas y $h_1, \ldots, h_s$ el conjunto de polinomios al que x^δ corresponde.
Si $LM(f) = x^\delta$ entonces $LT(f) \in <LT(f_1), \ldots, LT(f_s)>$ y podemos reducir f a algún polinomio f' tal que $LM(f') < LM(f)$
Supongamos que $LM(f) < x^\delta$ y sean $m_{i(1)}, \ldots, m_{i(d)}$ los monomios principales de los $h_i f_i$ tales que $m = m_{i(1)} = \ldots = m_{i(d)}$ entonces debemos tener $\Sigma LT(h_{i(j)} f_{i(j)}) = 0$ y por lo tanto $\Sigma LT(h_{i(j)}) f_{i(j)}$ es una combinación lineal de los polinomios

$$S(x^{\alpha(j)} f_{i(j)}, x^{\alpha(h)} f_{i(h)}), \text{ donde } x^{\alpha(g)} = LM(h_{i(j)}).^2$$

Sea $x^\gamma = mcm(LM(f_{i(j)}), LM(f_{i(h)}))$ entonces

$$S(x^{\alpha(j)} f_{i(j)}, x^{\alpha(h)} f_{i(h)}) = x^{\delta-\gamma} \cdot S(f_{i(j)}, f_{i(h)}) \text{ y tenemos que}$$

$$\Sigma LT(h_{i(j)}) f_{i(j)} = \Sigma c_{sh} x^{\delta-\gamma} \cdot S(f_{i(s)}, f_{i(h)}), \; c_{sh} \in K$$

---

[2] Cox, D , Little, J , O'Shea, D (1997) Lema 2.6 5

Por hipótesis los s-polinomios $S(f_{i(j)}, f_{i(h)})$ se reducen a cero módulo F Sea

$$S(f_{i(j)}, f_{i(h)}) = \sum a_{ijh} f_i,\ a_{ijh} \in K[x_1, \quad, x_n],$$

la expresión que obtenemos mediante el algoritmo de la división. Por la forma en que éste funciona se deduce que cada $LM(a_{ijh}f_i)$ es menor o igual que el monomio principal de $S(f_{i(j)}, f_{i(h)})$ Por lo tanto

$$x^{\delta-\gamma_i} LM(a_{ijh}f_i) \leq x^{\delta-\gamma} \cdot LM(\ S(f_{i(j)}, f_{i(h)})\ ) < x^{\delta-\gamma} \cdot mcm(LM(f_{i(j)}), LM(f_{i(h)})) = x^{\delta}$$

Pero esto implica que hemos encontrado una expresión $f=\sum p_i f_i$ donde $LM(p_i f_i) < x^{\delta}$ para toda i lo cual contradice la minimalidad de x^{δ} Por lo tanto debemos tener $LM(f)=x^{\delta}$

Esta proposición nos da el criterio que necesitábamos para extender una base de un ideal a una base de Groebner y para identificar cuando ya tenemos una base de Groebner.

Algoritmo de Buchberger 1.2.6. Sea F una base de I

Datos F
Resultado: $G:= \{g_1,\ldots,g_m\}$ una base de Groebner de I con respecto a >.

$G_0 = F$
$B_0:= \{ (g_i, g_j) \mid g_i, g_j \in G_0,\ g_i \neq g_j \}$

Dados B_i y G_i. Si $B_i \neq \emptyset$ entonces escogemos una pareja $(g_1, g_2) \in B_i$.
Sea g' la reducción de $S(g_1, g_2)$ con respecto a G_i y $C= B_i \setminus \{(g_1, g_2)\}$ entonces

$$G_{i+1}:=G_i \cup \{g'\} \text{ y } B_{i+1}:= C \cup \{ (g',h) \mid h \in G_i \}.$$

Este proceso lo repetimos recursivamente hasta que $B_i=\emptyset$. Una vez que esto sucede $G:=G_i$.

Dado un ideal I y F un conjunto de generadores ahora podemos calcular una base de Groebner partiendo de F y expresar cualquier $f \in I$ en términos de G utilizando el

algoritmo de la división, en particular los elementos de F Sin embargo habrá ocasiones en las que se necesite expresar los elementos de G en términos de los elementos de F Esto tiene solución.

Para expresar cada $g \in G$ en términos de los elementos de F necesitamos una familia de polinomios $\{\{q_{gf}\}_{f\in F}\}_{g\in G}$ tal que para cada $g\in G$

$$g = \Sigma q_{gf} \cdot f \quad (1)$$

En el algoritmo de Buchberger comenzamos con G_0 y B_0, ahora tendremos un nuevo conjunto $H_0 = \{q_{gf} \mid q_{gf}=\delta_{gf},\ f\in F,\ g\in G_0\}$ donde

$$\delta_{fg} = \begin{cases} 1 & \text{si } f=g \\ 0 & \text{si } f\neq g \end{cases}$$

es claro que los elementos de H_0 cumplen con (1) para F y G_0.

En el paso inductivo si la condición $B_i\neq\emptyset$ se cumple escogemos $(g_1,g_2)\in B_i$ y calculamos un elemento g' tal que

$$S(g_1,g_2)=m_1g_1-m_2g_2= \Sigma q_g g + g',\ g\in G_i,$$

y formamos $G_{i+1}=G_i\cup\{g'\}$

Supongamos que $H_i=\{q_{gf} \mid g\in G_i,\ f\in F\}$ es tal que las q_{gf} cumplen con (1) para F y G_i. Entonces

$$g' = m_1g_1-m_2g_2 - \Sigma q_g g,\ g\in G_i$$

$$= m_1\Big(\sum_{f\in F} q_{g1f}\cdot f\Big) - m_2\Big(\sum_{f\in F} q_{g2f} f\Big) - \sum_{g\in G_i} q_g \Big(\sum_{f\in F} q_{gf} f\Big)$$

$$= \sum_{f\in F}\Big(m_1q_{g1f} - m_2q_{g2f} - \sum_{g\in G_i} q_g\cdot q_{gf}\Big)\cdot f$$

definimos $q_{g'f}= m_1q_{g1f} - m_2q_{g2f} - \sum_{g\in G_i} q_g\cdot q_{gf}$ para cada $f\in F$ y $H_{i+1}= H_i \cup \{q_{g'f}\}_{f\in F}$

Dado que los conjuntos H_i mantienen la propiedad de que sus elementos q_{gf} nos permiten expresar los elementos de G_i en términos de los elementos de F entonces el

añadir este proceso al algoritmo de Buchberger nos permite obtener la familia de polinomios que buscábamos.

1.3 Teorema de eliminación.

Las bases de Groebner presentan otra importante propiedad cuando son calculadas con respecto a ciertos órdenes.

Teorema 1.3.1. *Sea $I \subset K[x_1, \ldots, x_n]$ un ideal. Dado un conjunto de indeterminadas $\{u_1, \ldots, u_r\} \subset \{x_1, \ldots, x_n\}$ y G una base de Groebner con respecto a algún orden $>$ tal que cualquier monomio en las u_i's es menor que cualquier monomio que involucre alguna $x_i \in \{x_1, \ldots, x_n\} \setminus \{u_1, \ldots, u_r\}$ Entonces $G \cap K[u_1, \ldots, u_r]$ es una base de Groebner del ideal de eliminación $I_U = I \cap K[u_1, \ldots, u_r]$*

Demostración. Sea $G' = G \cap K[u_1, \ldots, u_r]$. Por construcción $G' \subset I_U$ y por lo tanto $\langle LT(G') \rangle \subset \langle LT(I_U) \rangle$ Sea $f \in I_U$ entonces existe $g \in G$ tal que $LT(g)$ divide a $LT(f)$ lo cual implica que $LT(g)$ sólo involucra u_i's. Observemos que si el término principal de un polinomio p involucra únicamente a las u_i's entonces $p \in K[u_1, \ldots, u_r]$ por el orden que estamos utilizando De esta observación se sigue que $g \in K[u_1, \ldots, u_r]$, por lo tanto $LT(f) \in \langle LT(G') \rangle$ Con esto hemos demostrado que también tenemos $LT(I_U) \subset \langle LT(G') \rangle$

1.4 Bases de Groebner para módulos polinomiales.

Para terminar presentaremos una versión de bases de Groebner para módulos sobre anillos de polinomios Estos conjuntos nos permiten, como en el caso anterior, resolver al problema de pertenencia, es decir, dado el módulo $K[x_1, \ldots, x_n]^m$ y un submódulo $N \subset K[x_1, \ldots, x_n]^m$ permiten saber de manera efectiva cuando un elemento $m \in K[x_1, \ldots, x_n]^m$ está en N

Consideremos el anillo $K[x_1, \ldots, x_n, z_1, \ldots, z_m]$.

Definimos $H_1(K[x_1, \ldots, x_n, z_1, \ldots, z_m]) := \{ h_1 \cdot z_1 + \ldots + h_m \cdot z_m \mid h_i \in K[x_1, \ldots, x_n] \}$, observemos que este conjunto es un módulo sobre $K[x_1, \ldots, x_n]$, simplemente hay que considerar la suma y la multiplicación de $K[x_1, \ldots, x_n, z_1, \ldots, z_m]$ restringidas a este conjunto

Lema 1.4.1. *Sea $F \subset H_1(K[X,Z])$ entonces*

$$lin(F) = id(F) \cap H_1(K[X,Z]),$$

donde lin(F) es el submódulo de $H_1(K[X,Z])$ generado por F y id(F) es el ideal generado por F en K[X,Z]

Demostración Sea $g \in lin(F)$ entonces $g=g_1f_1+ \ldots +g_sf_s$, con $g_i \in K[X]$ y $f_i \in F$, esto quiere decir que $g \in id(F) \cap H_1(K[X,Z])$
Sea $g \in id(F) \cap H_1(K[X,Z])$ entonces $g=m_1f_1+ \ldots +m_sf_s$, donde $f_i \in F$(las f_i no tienen que ser distintas entre ellas) y las m_i's son monomios en K[X,Z], cada m_if_i debe tener grado 1 en las z_i's y por lo tanto cada $m_i \in K[X]$. Con esto concluimos que $h \in lin(F)$.

Este sencillo lema nos da una importante herramienta para tener en módulos un equivalente a las bases de Groebner, lo único que necesitamos es un conjunto de generadores del módulo en consideración El mapeo φ

$$\begin{aligned} \varphi \; K[x_1, \ldots, x_n]^m &\rightarrow H_1(K[X,Z]) \\ (h_1, \ldots, h_m) &\rightarrow z_1h_1+ \ldots +z_mh_m \end{aligned}$$

es un isomorfismo de $K[x_1, \ldots, x_n]$-módulos, eso nos permite mandar un submódulo M de $K[x_1, \ldots, x_n]^m$ en uno de $H_1(K[X,Z])$, en donde podemos calcular una base de Groebner para id(M), luego intersecar con $H_1(K[X,Z])$ y regresar a $K[x_1,\ldots,x_n]^m$, pero en realidad sólo nos tenemos que preocupar por calcular los elementos de la base con grado 1 en las z_i's
Sea M submódulo de $K[x_1, \ldots, x_n]^r$ con generadores $b_1, \ldots, b_s$ entonces consideremos el ideal generado por el conjunto de polinomios
$H = \{ h_i = z_1 \cdot b_{1i} + \ldots + z_r \cdot b_{ri} , i \in \{ 1, \ldots, s \} \} \subset K[x_1, \ldots, x_n, z_1, \ldots, z_r]$ Sea G un nuevo conjunto de generadores construido aplicando el algoritmo de Buchberger a H, pero con la modificación de que sólo consideramos los S-polinomios de pares h_i, h_j tales que $mcm(LT(h_i),LT(h_j))$ tiene grado total 1 en las z_i's Entonces G es una base que por medio del algoritmo de la división nos permite saber cuando un polinomio de $H_1(K[X,Z])$ está en $<H>$
El conjunto G que obtenemos es lo que llamaremos una base de Groebner para M, pues cumple con la propiedad de que $g \in M$ si y sólo si el residuo de $\varphi(g)$ módulo G es 0

2 Cálculo de invariantes primarios y secundarios

2.1 Anillo de invariantes.

Sea Γ un subgrupo de GL(n, K) el grupo de matrices invertibles de n×n con coeficientes en el campo K, definimos la acción Γ sobre $K[x_1, \ldots, x_n]$ de la siguiente manera Dados $f \in K[x_1, \ldots, x_n]$, $\pi \in \Gamma$ entonces $f \circ \pi(x_1, \ldots, x_n) = f(\pi \cdot (x_1, \ldots, x_n))$ En nuestro caso estaremos interesados en subgrupos finitos de GL(n, K).

Ejemplo:

Sea $\pi = \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}$, entonces $f \circ \pi(x_1, x_2) = f(4 \cdot x_1 + 3 \cdot x_2, x_1 + x_2)$

En el estudio de la teoría de invariantes estamos interesados en el conjunto

$$K[x_1, \ldots, x_n]^{\Gamma} = \{ f \in K[x_1, \ldots, x_n] \mid f \circ \pi = f, \text{ para toda } \pi \in \Gamma \}$$

este conjunto es cerrado bajo la suma y el producto y por lo tanto es un subanillo de $K[x_1, \ldots, x_n]$

El anillo $K[x_1, \ldots, x_n]$ es un anillo graduado y esta graduación induce de manera natural una en $K[x_1, \ldots, x_n]^{\Gamma}$ Recordemos que un anillo R es graduado si existe una *familia* $\{R_i\}_{i \in Z}$ de subgrupos de R tal que $R = \oplus_{i \in Z} R_i$ y $R_i \cdot R_j \subset R_{i+j}$ A un elemento $f \in R_i$ se le llama homogéneo de grado i

En lo que resta de esta sección Γ será un subgrupo finito de GL(n, K).

Teorema 2.1.1. *$K[x_1, \ldots, x_n]$ es una extensión entera de $K[x_1, \ldots, x_n]^{\Gamma}$.*

Demostración. Sea $P_t = \Pi_{\pi \in \Gamma} (x_i \circ \pi - t) \in K[x_1, \ldots, x_n][t]$ Observemos que cada P_t es invariante bajo la acción de Γ y dado que Γ sólo actúa en los coeficientes de P_t y su acción es lineal Si $P_t = \Sigma^{n!} a_j \cdot t^j$, $a_j \in K[x_1, \ldots, x_n]$ entonces tenemos que

$$\sum_{j=0}^{i} a_j \cdot t^j = \sum_{j=0}^{n} (a_j \circ \pi) \cdot t^j,$$

esto sucede si y sólo si $a_j = \pi \circ a_j$, por lo tanto $P_i \in K[x_1, \ldots, x_n]^\Gamma[t]$. Por otro lado P_i es distinto de cero pues $a_{|\Gamma|} = (-1)^{|\Gamma|}$ y la identidad está en Γ entonces $P_i(x_i)=0$. Por lo tanto para cada x_i tenemos un polinomio distinto de cero con coeficientes en $K[x_1, \ldots, x_n]^\Gamma$ tal que x_i es raíz de este. Lo cual quiere decir que cada x_i es entera sobre $K[x_1, \ldots, x_n]^\Gamma$ lo que implica que $K[x_1, \ldots, x_n]$ es una extensión entera de $K[x_1, \ldots, x_n]^\Gamma$

Esto es equivalente a decir que el grado de trascendencia de $K[x_1, \ldots, x_n]^\Gamma$ sobre K es el mismo que de $K[x_1, \ldots, x_n]$, es decir n. Este teorema también implica que $K[x_1, \ldots, x_n]$ es generado finitamente como módulo sobre $K[x_1, \ldots, x_n]^\Gamma$ (proposición B.1.2)

El anillo de invariantes es una K-álgebra graduada finitamente generada[3] y por el teorema de normalización de Noehter existen $f_1, \ldots, f_n$ invariantes homogéneos tales que $K[x_1, \ldots, x_n]^\Gamma$ es generado finitamente como módulo sobre $K[f_1, \ldots, f_n]$. A los invariantes $f_1, \ldots, f_n$ se les llama invariantes primarios mientras que los invariantes que generan a $K[x_1, \ldots, x_n]^\Gamma$ como módulo se les llama invariantes secundarios. El objetivo será presentar algoritmos que nos permitan calcularlos.

2.2 Cálculo de invariantes primarios.

La siguiente proposición es, en nuestro caso, fundamental para el cálculo de invariantes primarios

Proposición 2.2.1. *Un conjunto $\{f_1, \ldots, f_i\} \subseteq I$ de invariantes homogéneos puede ser extendido a un sistema de invariantes primarios si y sólo si $\dim(f_1, \ldots, f_i) = n-i$.*

Demostración. Un conjunto de invariantes homogéneos $f_1, \ldots, f_n$ es un sistema de invariantes primarios si $\dim(f_1, \ldots, f_n)=0$ [4]

---

[3] En 1926 Emmy Noether publicó el artículo *Der Endlichkeitssatz der Invarianten endlicher linearen Gruppen der Charakteristik p.* Dicho artículo "está dedicado a la prueba del siguiente teorema Sea G un grupo finito tal que actua sobre el anillo de polinomios $P[x_1, \ldots, x_n]$ por medio de automorfismos sobre P que estabilizan al espacio vectorial $\Sigma P x_i$ Sea Inv G el conjunto de puntos fijos bajo esta acción Entonces Inv G es un algebra finitamente generada sobre P " Noether, E. (1983) *Introducción de Jacobson*, N .p 25

[4] Smith, L (1995) Proposición 5 3 7

=>) Si demostramos que cada f_i puede bajar la dimensión en a lo más 1 entonces se debe tener que $\dim(f_1, \ldots, f_i)=n-i$
Supongamos que $\dim(f_1, \ldots, f_i)=d$. Sea $f_{i+1} \in K[x_1, \ldots x_n]$ y P un ideal primo minimal entre los que contienen a $<f_1, \ldots, f_{i+1}>$, consideremos el anillo
$R = K[x_1, \ldots x_n]/<f_1, \ldots, f_i>$ si γ: $K[x_1, \ldots, x_n] \rightarrow R$ es la proyección de $K[x_1, \ldots, x_n]$ en R entonces $\gamma(P)$ es un ideal primo minimal en R entre los que contienen a $\gamma(f_{i+1})$ y por el teorema del ideal principal de Krull(teorema B 2.5) tenemos que $\operatorname{codim}(\gamma(P)) \leq 1$ sobre R. Sea $P_0 \subset \ldots \subset P_j$ una cadena de longitud máxima en $K[x_1, \ldots, x_n]$ con $P_0=P$. Ahora consideremos una cadena $Q_0 \subset \ldots \subset Q_i$ maximal de primos contenidos propiamente en $<f_1, \ldots f_i>$, esta última tiene longitud n-d-1, ya que existe una cadena maximal de primos que contienen a $<f_1, \ldots, f_i>$, cuya longitud es d. Si pegamos ambas cadenas obtenemos una nueva cadena

$$Q_0 \subset \ldots \subset Q_i \subset P_0 \subset \ldots \subset P_j \text{ de longitud n-d+j, donde}$$

$$Q_i \subset <f_1, \ldots, f_i> \subset <f_1, \ldots, f_{i+1}> \subset P_0 = P \text{ con } Q_i \neq <f_1, \ldots, f_i>,$$

esta puede no ser maximal, pero entre Q_0 y $<f_1, \ldots, f_i>$ ya no se pueden insertar más primos, tampoco entre $<f_1, \ldots f_{i+1}>$ y P_j, por lo que sólo se pueden insertar primos entre $<f_1, \ldots, f_i>$ y $<f_1, \ldots, f_{i+1}>$ de manera que sigamos teniendo una cadena, pero la imagen de P en R tiene codimensión menor o igual a 1, entonces podemos añadir a lo mas un primo a la cadena. Dado que toda cadena maximal tiene longitud n (proposición B 2.6) entonces $n-1 \leq n-d+j$, por lo tanto $d-1 \leq j$, es decir
$d-1 \leq \dim(P)$, que es lo que queríamos, pues P es cualquier primo minimal entre los que contienen a $<f_1, \ldots f_{i+1}>$

<=)Ahora supongamos que $\dim(f_1, \ldots, f_i)= n-i$ entonces por el lema de normalización de Noether existen $f_{i+1}, \ldots, f_n \in K[x_1, \ldots, x_n]^I / <f_1, \ldots, f_i>$, tales que
$K[x_1, \ldots, x_n]^I / <f_1, \ldots, f_i>$ está generado finitamente como módulo sobre $K[\bar{f}_{i+1}, \ldots, \bar{f}_n]$. Sabemos que $K[x_1, \ldots, x_n]$ está generado finitamente como módulo sobre $K[x_1, \ldots, x_n]^I$ por lo cual $K[x_1, \ldots, x_n]/<f_1, \ldots, f_i>$ también lo está sobre $K[x_1, \ldots, x_n]^I / <f_1, \ldots, f_i>$. De esto se sigue que $R = K[x_1, \ldots, x_n]/<f_1, \ldots, f_i>$ es un $K[\bar{f}_{i+1}, \ldots \bar{f}_n]$-módulo generado finitamente, por lo tanto el cociente $R/<\bar{f}_{i+1}, \ldots, \bar{f}_n>$ es generado finitamente como espacio vectorial sobre K. Para ver esto observemos que cualquier $p \in K[\bar{f}_{i+1}, \ldots, \bar{f}_n]$ pertenece a la misma clase en $R/<\bar{f}_{i+1}, \ldots, \bar{f}_n>$ que su término constante, por ende si $g_1, \ldots, g_s$ generan a R como módulo sobre $K[\bar{f}_{i+1}, \ldots, \bar{f}_n]$ entonces todo elemento de $R/<\bar{f}_{i+1}, \ldots, \bar{f}_n>$ es una combinación lineal de las g_i's. $R/<\bar{f}_{i+1}, \ldots, \bar{f}_n>$ y $K[x_1, \ldots, x_n]/<f_1, \ldots, f_n>$ son isomorfos, por lo tanto este

último también tiene dimensión finita como espacio vectorial sobre K y por el teorema B 2 3 tenemos que $\dim(f_1,\ldots,f_n)=0$.

La proposición 2 2 1 nos da el paso inductivo para construir un conjunto de invariantes primarios Si tenemos i invariantes primarios hay que buscar un invariante que le baje la dimensión al ideal que generan los i invariantes y continuar así hasta obtener n invariantes tales que el ideal que generan tiene dimensión cero. Sin embargo todavía nos falta algo, no sabemos como encontrar tal invariante.

Proposición 2.2.2 *Sean $P_1,\ldots,P_s$ los primos asociados a $\langle f_1,\ldots,f_i\rangle$ y $f_{i+1}\in K[x_1,\ldots,x_n]$ tal que $f_{i+1}\notin P_j$, $j\in\{1,\ldots,s\}$ entonces $\dim(f_1,\ldots,f_{i+1}) < \dim(f_1,\ldots,f_i)$.*

Demostración. Supongamos que para toda j, $f_{i+1}\notin P_j$. Sea P un ideal primo tal que $\langle f_1,\ldots,f_{i+1}\rangle\subseteq P$ entonces P debe contener propiamente algún primo asociado a $\langle f_1,\ldots,f_i\rangle$, pues entre los primos que contienen a $\langle f_1,\ldots,f_i\rangle$ todos los minimales son primos asociados a este ideal y por tanto P no puede ser minimal, es decir, debe contener propiamente algún ideal primo que contenga a $\langle f_1,\ldots,f_i\rangle$. Esto implica que toda cadena maximal de ideales primos $Q_1\subset\ldots\subset Q_r$, $\langle f1,\ldots,f_{i+1}\rangle\subseteq Q_1$, se puede extender a una cadena $Q_0\subset Q_1\subset\ldots\subset Q_r$, $\langle f_1,\ldots,f_i\rangle\subseteq Q_0$ Por lo tanto $\dim(f_1,\ldots,f_i) > \dim(f_1,\ldots,f_{i-1})$.

Las proposiciones 2 2 1 y 2.2 2 nos dan las herramientas necesarias para comprobar la efectividad del siguiente algoritmo.

2.2.3 Algoritmo para construir invariantes primarios.

Datos: Γ un subgrupo finito de GL(n, K) y $\pi_1,\ldots,\pi_r$ un conjunto de generadores de Γ.
Resultado: $f_1,\ldots,f_n$ un conjunto de invariantes primarios de $K[x_1,\ldots,x_n]^\Gamma$

Dense valores iniciales i.= 1, r:= 1, $P_1:=\emptyset$.

Mientras $i\leq n$ {
  Calcular una K-base $\{b_1,\ldots,b_{md}\}$ del espacio de invariantes de grado d.
  Se define $I_d(t_1,\ldots,t_n) := \sum^{md} t_j\cdot b_j$.
  Para k=1, ..., r calcular el residuo $r_k(t_1,\ldots,t_{md})$ de I_d con respecto a la base de Groebner P_k.
  Si existen $\alpha_1,\ldots,\alpha_{md}$ en K tales que $r_k(\alpha_1,\ldots,\alpha_{md})\neq 0$ para toda k = 1, ...,r
  Entonces {

$f_i := I_d(\alpha_1, \ldots, \alpha_{md})$
Calcular los ideales primos asociados de $<f_1, \ldots, f_i>$
r := número de primos asociados
Sean $P_1, \ldots, P_r$ las bases de Groebner, con respecto a algún orden monomial, de los primos asociados de $<f_1, \ldots, f_i>$
i := i+1
}
Si no existen $\alpha_1, \ldots, \alpha_{md}$ en K tales que $r_k(\alpha_1, \ldots, \alpha_{md}) \neq 0$ para toda k = 1, ..., r
d:= d+1
}

El primer paso consiste en calcular una base del espacio de invariantes homogéneos de grado d, esto se puede hacer planteando un polinomio homogéneo general de grado d y aplicándole los generadores del grupo, es suficiente comprobar que un polinomio es invariante bajo la acción de los generadores del grupo ya que esto sucede si y sólo si el polinomio es un invariante bajo la acción del grupo, con esto obtenemos un sistema de ecuaciones lineales para los coeficientes del polinomio. Una base del espacio de soluciones del sistema nos da una base para el espacio de invariantes en consideración
Una vez que tenemos una base $\{b_1, \ldots, b_{md}\}$ para el espacio de invariantes homogéneos de grado d, construimos el polinomio I_d y consideramos sus residuos r_k con respecto a las bases de Groebner P_k de los primos asociados al ideal generado por los invariantes primarios encontrados hasta el momento. Si existe un elemento $(\alpha_1, \ldots, \alpha_{md}) \in K^{md}$ tal que para toda k, $r_k(\alpha_1, \ldots, \alpha_{md}) \neq 0$ entonces $I_d(\alpha_1, \ldots, \alpha_{md})$ no esta en ningún primo asociado de $<f_1, \ldots, f_i>$ y por lo tanto
$\dim(f_1, \ldots, I_d(\alpha_1, \ldots, \alpha_{md})) < \dim(f_1, \ldots, f_i)$
Para encontrar $(\alpha_1, \ldots, \alpha_{md})$ debemos considerar dos casos, pero antes observemos que si $r_k = 0$ para alguna k entonces tenemos que pasar al siguiente espacio de invariantes homogéneos En el caso en que $r_k \neq 0$, para todas las k y K es infinito entonces $r_k = 0$ define un subespacio propio de K^{md} para cada k y dado que la unión finita de subespacios propios no puede cubrir todo K^{md} entonces debe existir un elemento $\alpha \in K^{md}$ tal que $r_k(\alpha) \neq 0$ para toda K
Si K es finito entonces únicamente buscamos entre todos los elementos de K^{md}.

Dado que en el algoritmo el conjunto de invariantes $f_1, \ldots, f_i$ siempre cumple con que $\dim(f_1, \ldots, f_i) = n-i$ entonces la proposición 2.2.1 nos asegura que este puede ser extendido a un conjunto de invariantes primarios

2.3 Cálculo de invariantes secundarios

Para el cálculo de invariantes secundarios se sigue la siguiente estrategia Primero se considera un subgrupo H tal que la característica de K no divida al orden de H. Es posible hacer este cálculo utilizando la fórmula de Molien para saber la dimensión como espacio vectorial sobre K de cada componente homogéneo $K[x_1,\ldots,x_n]_d^H$.
Una vez encontrados los invariantes secundarios $p_1,\ldots,p_t$ para $K[x_1,\ldots,x_n]^H$ entonces cualquier elemento $g\in K[x_1,\ldots,x_n]^H$ es de la forma $\Sigma^t h_i\cdot p_i$, $h_i \in K[f_1,\ldots,f_n]$, en particular los generadores de $K[x_1,\ldots,x_n]^\Gamma$ *como módulo sobre* $K[f_1,\ldots,f_n]$ deben tener esa forma, así que nos falta encontrar las h_i's. Dado que los elementos que nos interesan son los que cumplen $g = g\circ\pi$, para toda $\pi\in\Gamma$, entonces estamos buscando generadores para el submódulo de $K[f_1,\ldots,f_n]^t$ dado por las sicigias $(h_1,\ldots,h_t)$ tales que

$$g\circ\pi - g = \sum_{i=1}^{t} (p_i\circ\pi - p_i)\cdot h_i = 0 \quad (1), \text{ para toda } \pi\in\Gamma$$

Sean $c_1,\ldots,c_r$ los generadores de este submódulo, la afirmación es que los polinomios $g_j = \Sigma c_{ji}\cdot p_i$ son invariantes secundarios de $K[x_1,\ldots,x_n]^\Gamma$. La primera observación es que por construcción los g_j están en $K[x_1,\ldots,x_n]^\Gamma$ Sea
$f = \Sigma a_i p_i \in K[x_1,\ldots,x_n]^\Gamma$, $a_i\in K[f_1,\ldots,f_n]$, las a_i's cumplen con (1), por lo tanto existen $q_1,\ldots,q_t\in K[f_1,\ldots,f_n]$ tales que $(a_1,\ldots,a_t) = \Sigma q_i\cdot c_i$, entonces

$$f = \sum_{i=1}^{t}\Big(\sum_{j=1}^{r} q_j\cdot c_{ji}\Big) p_i = \sum_{j=1}^{t}\sum_{i=1}^{r} q_j\cdot c_{ji}\cdot p_i = \sum_{j=1}^{r} q_j\cdot\Big(\sum_{i=1}^{t} c_{ji}\cdot p_i\Big) = \sum_{j=1}^{r} a'_j\cdot g_j$$

Así que $K[x_1,\ldots,x_n]^\Gamma = \Sigma A\cdot g_j$

Para encontrar los c_i's primero buscamos generadores para el módulo

$$M=\{ (h_1,\ldots,h_t)\in K[x_1,\ldots,x_n]^t \mid \sum_{i=1}^{t} (p_i\circ\pi - p_i)\cdot h_i = 0 \}$$

y después calculamos la intersección $M\cap A$.

Apéndice A

A.1 Descomposición primaria en $K[x_1,\ldots,x_n]$.

Definición A.1.1 *Sea R un anillo e I un ideal en R. Una familia de ideales primarios $\{Q_i\}$ es una descomposición primaria de I si $I=\cap_i Q_i$. Los ideales primos $P_i=\sqrt{Q_i}$ son los primos asociados de I.*

En general no todo ideal tiene una descomposición primaria, sin embargo en el caso en que el anillo es noetheriano todo ideal se puede descomponer en primarios. En particular, para todo ideal I de $K[x_1,\ldots,x_n]$, I tiene una descomposición primaria.

Lema A.1.2. *Sea R un anillo noetheriano. $M\subset R$ ideal maximal y $I\subset R$ ideal tal que $\sqrt{I}=M$ entonces existe $n\in N$ tal que $M^n\subset I$.*

Demostración. Sea $B=\{m_1,\ldots,m_s\}$ una base de M entonces existen $i_1,\ldots,i_s$ tales que $m_k^{i_k}\in I$. Definimos $n:= 1 + \Sigma(i_k - 1)$. Si tenemos un producto $m_1^{\alpha 1}\cdot\ldots\cdot m_s^{\alpha s}$, $\alpha_1+\ldots+\alpha_s = n$, entonces para alguna k, $\alpha_k>i_k-1$ por lo tanto $m_k^{\alpha k}\in I$. B^n está generado por productos que cumplen esta condición, así que, $B^n\subset I$

A lo largo de esta sección $R=K[y_1,\ldots,y_m]$, $0\le m$, y dados $<_1$ y $<_2$ cualesquiera ordenes monomiales en R y en $K[x_1,\ldots,x_n]$ respectivamente entonces en $R[x_1,\ldots,x_n]$ consideraremos el orden producto dado por

$$y^{\alpha 1}\cdot x^{\alpha 2} < y^{\beta 1}\cdot x^{\beta 2} \text{ si } x^{\alpha 2} <_2 x^{\beta 2} \text{ o}$$

$$x^{\alpha 2} = x^{\beta 2} \text{ y } y^{\alpha 1} <_1 y^{\beta 1}.$$

Lema A.1.3 *Sea I un ideal de $R[x_1,\ldots,x_n]$ y supongamos que $R\cap I$ tiene dimensión cero y es primario. Sea G una base de Groebner de I. Entonces I tiene dimensión cero si y solo si para cada i existe $g_i\in G$ tal que $LT(g_i)= c_i x_i^{mi}$, $c_i \in R$ unidad módulo $R\cap I$.*

Demostración. Sea $G_i = \{ g\in G \mid LT(g)= c\cdot x_i^m,\ c\in R\ \ 0\le m\}$ y L_i el ideal generado por los coeficientes principales de G_i. Nótese que en G_i el exponente de x_i puede ser cero, por lo tanto G_i contiene a $G\cap R$ y dado $p\in G\cap R$ tenemos $LC(p)=p$ por lo tanto L_i contiene a $I\cap R$, pues $G\cap R$ genera a $I\cap R$ Como $R\cap I$ tiene dimensión cero

entonces cualquier primo que lo contenga debe ser maximal y puesto que es primario entonces $\sqrt{R\cap I}$ es primo y por ende maximal.
I tiene dimensión cero si y sólo si $L_i=<1>$ para cada i.[1] Supongamos que $L_i=<1>$, dado que $\sqrt{I\cap R}\subset\sqrt{I}$, entonces $L_i=<1>$ *si y sólo si existe* $g\in G_i$ *tal que* $LC(g)\notin\sqrt{R\cap I}$, ya que $LC(G_i)$ genera a L_i. Si consideramos el ideal $<LC(g), R\cap I>$ el radical de este ideal contiene propiamente a $\sqrt{R\cap I}$ por lo tanto $\sqrt{<LC(g), R\cap I>}=<1>$ lo cual sucede si y sólo si $<LC(g), R\cap I>=<1>$, es decir, $1=h\cdot LC(g)+f$, $h\in R$ y $f\in R\cap I$. por lo tanto $LC(g)$ es unidad módulo $R\cap I$.

Teorema A.1.4 *Sea $I\subset R[x]$ un ideal de dimensión cero tal que $I\cap R$ tiene dimensión cero y es primario. Sea G una base de Groebner mínima de I y sea g de grado máximo en G entonces $LT(g)=c\,x^t$ con $c\in R$ unidad módulo $R\cap I$ y $\sqrt{I}=\sqrt{(g,I\cap R)}$.*

Demostración. Por el lema A.1.3 existe $g_1\in G$ tal que $LT(g_1)=c\cdot x^t$ con $c\in R$ unidad módulo $R\cap I$. Sea $b\in R$ tal que $c\cdot b=1+r$, $r\in R\cap I$.
Supongamos que $LT(g)=d\cdot x^{t+j}$ entonces $(c\cdot x^t)\cdot(bd\cdot x^j)=d\cdot x^{t+j}+rd\cdot x^{t+j}$ *por lo tanto* $d\cdot x^{t+j}\in<c\cdot x^t, r>$ y por la minimalidad de G debemos tener $g=g_1$.

Supongamos que $LT(g)=d\cdot x^{t+j}$ entonces $(c\cdot x^t)\cdot(bd\cdot x^j)=d\cdot x^{t+j}+rd\cdot x^{t+j}$ por lo tanto $d\cdot x^{t+j}\in<c\cdot x^t, r>$ y por la minimalidad de G debemos tener $g=g_1$.
Dado que $LC(g)=c$ es unidad módulo $R\cap I$ entonces $x^t\in LT(<g, R\cap I>)\subset LT(I)$. Por la minimalidad de G no existe ninguna potencia de x menor que t, pues si existiese, x^t sería reducible módulo G. Demostraremos que esto implica que cualquier $f\in I$ de grado menor que t es divisor de cero módulo $R\cap I$.

Sea $L\subset R$ el ideal generado por los coeficientes principales de los elementos de I cuyo grado es menor que t. Afirmamos que si $f\in I$ tiene grado menor que t entonces $f\equiv 0$ modulo L. Sea $f=a_1x^{t-1}+\ldots+a_t$ y sea $p=x^t+b_1x^{t-1}+\ldots+b_t\in I$. Definimos
$f'=a_1\cdot f-a_1\cdot p$ es claro que $f'\in I$. Supongamos que $f'=a_1'\cdot x^{t-1}+\ldots+a_t'$ entonces
$a_i'\equiv a_{i-1}$ mod L, pues $a_j'=a_{j+1}-a_1\cdot b_j$ y $a_1\in L$. Observemos que $a_1'\in L$ por lo que también tenemos $a_2\in L$ y siguiendo por inducción obtenemos que a_j está en L. Por lo tanto $f\equiv 0$ mod L. L es un ideal propio de R ya que si $1\in L$ entonces existe un polinomio monico en I de grado menor que t, lo cual es una contradicción.
Dado que $\dim(R\cap I)=0$ y $R\cap I\subset L$, L debe estar contenido en algún P primo asociado de $R\cap I$. Si probamos que existe $a\notin R\cap I$ tal que $a\cdot L\subset R\cap I$ entonces habremos terminado. Por el lema A.1.2 existe m tal que $P^m\subset R\cap I$. Sea $h=\min\{m\mid P^m\subset R\cap I\}$ entonces existen $p_1,\ \ldots p_{h-1}\in P$(las p_i's pueden repetirse) tales que $\Pi p_i\notin R\cap I$, pero para cualquier $q\in P$, $q\cdot\Pi p_i\in R\cap I$. Por lo tanto $\Pi p_i\cdot L\subset R\cap I$. Por lo tanto f es divisor de cero módulo $R\cap I$.

---

[1] Gianni et al (1988) p 159

Dado que $R\cap I$ es primario entonces el conjunto de divisores de cero en R módulo $R\cap I$ es precisamente el radical de este, que es primo Entonces si el grado de f es menor que r debemos tener que $f\equiv 0 \bmod \sqrt{R\cap I}$ Sea $f\in J$ tal que f se reduce a f' modulo $<g, R\cap I>$, dado que $x^r \in LT(g, R\cap I)$ entonces f' tiene grado menor que r y por lo tanto $f'\equiv 0 \bmod \sqrt{R\cap I}$, es decir, $f\in <g, R\cap I> + \sqrt{R\cap I} = <g, \sqrt{R\cap I}>$. Hemos demostrado que

$$I \subset <g, \sqrt{R\cap I}> \subset \sqrt{I}$$

y tomando radicales obtenemos que

$$\sqrt{I} = \sqrt{<g, R\cap I>}$$

Teorema A.1.5. *Sea M un ideal maximal de R e I un ideal de $R[x_1,\ldots,x_n]$ tal que $I\cap R$ es M-primario. Entonces existen ideales $I_i \subseteq R[x]$ y $M_i \subseteq R[x_n]$ tales que $I=\cap_i I_i$ y $I_i\cap R[x_n]$ es M_i-primario.*

Demostración. Sea $I^c = I\cap R[x_n]$ entonces existe $g\in I^c$ tal que $\sqrt{I^c}=\sqrt{(g, M)}$. Sea $g\equiv \Pi_i p_i^{s_i} \bmod M$ la factorización completa de g módulo M, es decir, las imágenes de las p_i en $(R/M)[x_n]$ son coprimos por pares, irreducibles y no son unidades. Dado que p_i y p_j son coprimos módulo M existen $h_1, h_2 \in R[x_n]$ tales que $h_1\cdot p_i + h_2\cdot p_j = 1 + m$, $m\in M[x_n]$, por lo tanto, sea t tal que $M^t \subseteq I$ entonces $(h_1\cdot p_i + h_2\cdot p_j - m)^t \in I$, es decir p_i y p_j son coprimos módulo I y esto implica que $\cap_i <p_i^{s_i s}, I> = <\Pi p_i^{s_i s}, I> = I$. Sea $I_i = <p_i^{s_i s}, I>$ ideal en $R[x_1,\ldots,x_n]$ y $M_i = <p_i, M>$ ideal en $R[x_n]$.

Es fácil ver que $M[x_n]=<M> \subset R[x_n]$ y que $(R/M)[x_n] \cong R[x_n]/M[x_n]$ Sea $g\in R[x_n]$ tal que $g\notin M_i$ entonces $g+M[x_n] \notin <p_i+M[x_n]> \subset R[x_n]/M[x_n]$ $R[x_n]/M[x_n]$ es un dominio de ideales principales y $p_i+M[x_n]$ es irreducible, por lo tanto $<p_i+M[x_n]>$ es maximal y $<g+M[x_n], p_i+M[x_n]> = <1+M[x_n]>$ i.e existen $h_1, h_2 \in R[x_n]$ y $m\in M[x_n]$ tales que $1=h_1\cdot g + h_2\cdot p_i + m$ Se sigue que $1\in <g, p_i, M>$, así que M_i es maximal.

Por otro lado tenemos que el radical de $I_i\cap R[x_n]$ contiene a M_i y por lo tanto $I_i\cap R[x_n]$ contiene una potencia de M_i. Dado que M_i es maximal entonces $\sqrt{I_i\cap R[x_n]}$ contiene propiamente a M_i y por lo tanto es todo $R[x_n]$ o $\sqrt{I_i\cap R[x_n]}=M_i$ y $I_i\cap R[x_n]$ es M_i-primario. Si $I_i\cap R[x_n]=<1>$ entonces dado que $\Pi_{i\neq j} p_j^{s_j s}\cdot I_i \subset I$, debemos tener $\Pi_{i\neq j} p_j^{s_j s} \in I^c$ y por lo tanto $\Pi_{i\neq j} p_j^{s_j} \in \sqrt{I_i} = \sqrt{<g, M>}$. Esto contradice el que p_i no sea unidad módulo M Por lo tanto $I_i\cap R[x_n]$ es M_i-primario.

Esta última proposición nos da un algoritmo para calcular la descomposición primaria de cualquier ideal con dimensión cero en $R[x_1,\ldots,x_n]$

Algoritmo A.1.6

Datos: R un anillo; $I \subset R[x_1,\ldots,x_n]$ un ideal cuya dimensión es cero; M un ideal maximal de R tal que $I \cap R$ es M-primario.

Resultado: Un conjunto F_I de parejas (Q_i,M_i), $1 \leq i \leq m$, donde Q_i y M_i son ideales de $R[x_1,\ldots,x_n]$; $\{Q_i\}_{i=1}^m$ es una descomposición primaria de I; $M_i \neq M_j$ si $i \neq j$; M_i es el primo asociado a Q_i.

Si n=0 entonces no hay más que hacer.

Calculamos G una base de Groebner *mínima para* $I \cap R[x_n]$.
Sea $g \in G$ de grado total máximo en G.(Lema 5.3)
Calculamos una factorización completa de g módulo M, $g \equiv \Pi p_i^{s_i} \in (R/M)[x_n]$.
Sea s tal que $(\Pi p_i^{s_i})^s \in I \cap R[x_n]$.
Definimos $I_i := \langle p_i^{s_i}, I \rangle \subset R[x_1,\ldots,x_n]$, $M_i := \langle p_i, M \rangle \subset R[x_n]$.
El resultado es $F_I = \cup F_i$, donde F_i es el resultado de aplicar el algoritmo A.1.6 a $R[x_n]$, I_i y M_i ideales de $R[x_n][x_1,\ldots,x_{n-1}]$.

Si I no tiene dimensión cero podemos calcular su descomposición reduciendo al caso anterior utilizando recursivamente un resultado que nos permite encontrar un elemento tal que $I=(I,r) \cap I^{sc}$ de tal forma que (I,r) tiene dimensión menor a la de I y I^{sc} es la contracción de la extensión de I a un anillo de dimensión menor.
El resultado que nos permite calcular una descomposición primaria de I es el siguiente.

Teorema A.1.7 *Sea $I \subset K[x_1,\ldots,x_n]$ un ideal entonces podemos calcular su descomposición primaria.*

Demostración. Si I tiene dimensión cero entonces hay que utilizar el algoritmo A.1.6.
Supongamos que $\dim(I) > 0$, entonces podemos encontrar por el lema B.2.2 una i tal que $\dim(I \cap K[x_i]) > 0$. Sea $R=K[x_i]$ entonces podemos encontrar $r_1 \in R$, $r_1 \neq 0$, tal que

$I=\langle I,r_1\rangle\cap I^{\infty}$.[6] Entonces para calcular una descomposición primaria de I es suficiente con calcular descomposiciones primarias para $\langle I, r_1\rangle$ y para I^{∞} por separado.
Dado que R es un dominio de ideales principales y $0\neq r_1\in R$ entonces $\langle I,r_1\rangle\cap R$ tiene dimensión cero o es R En el primer caso buscamos x_j tal que $\dim(\langle I,r_1\rangle\cap K[x_j]) > 0$ y aplicamos a $\langle I, r_1\rangle$ el proceso descrito en el parágrafo anterior En el segundo caso tenemos que $I=I^{\infty}$.
Para descomponer I^{∞} la idea es descomponer $I^e= K(x_i)[x_1, \ldots,x_{i-1},x_{i+1},\ldots,x_n]$ y después contraer la descomposición a $K[x_1,\ldots,x_n]$.

A.2 Módulos de sicigias.

Supongamos que $R=K[x_1, \ldots,x_n]$ y sea $F=\{f_1,\ldots,f_m\} \subset K[x_1, \ldots,x_n]$ Consideremos la ecuación

$$y_1\cdot f_1+ \ldots +y_m f_m=0,$$

una solución de esta ecuación es una m-tupla $(h_1, \ldots,h_m)$ tal que

$$h_1\cdot f_1+ \ldots +h_m\cdot f_m=0$$

Cada una de estas soluciones es una sicigia del conjunto $f_1, \ldots,f_m$ Es fácil ver que el conjunto de todas las sicigias de F $sis(f_1,\ldots,f_m)\subset R^m$ es un submódulo de R^m, visto como R-módulo

En esta sección veremos como calcular un conjunto de generadores para $sic(f_1, \ldots,f_m)$ El primer paso es calcular una base de Groebner $G=\{g_1, \ldots,g_s\}$ para el ideal generado por F G nos da una nueva ecuación

$$y_1\cdot g_1+ \ldots +y_s\cdot g_s= 0, \qquad (2)$$

podemos pedir que loa g_i's sean mónicos y distintos entre si. Ahora consideremos los s-polinomios

$$p_{ij}=spol(g_i,g_j)= s_{ij}g_i - s_{ji}g_j,$$

dado que los g_{ij}'s están en el ideal generado por G entonces existen $q_{ijh}\in K[x_1,\ldots,x_n]$ tales que

[6] Vease Proposición 8 2, Gianni et al (1988)

$p_{ij} = \sum q_{ijh} \cdot g_h$, entonces

$$(q_{iji} - s_{ij}) \cdot g_i + (q_{ijj} + s_{ji}) \cdot g_j + \sum_{h \neq i,j} q_{ijh} \cdot g_h = 0, \text{ y } LT(q_{ijk} \cdot g_k) \leq LT(p_{ij})$$

hemos encontrado un conjunto de soluciones para (2), a continuación veremos que este conjunto genera a $S_G = sic(g_1, \ldots, g_s)$ La siguiente notación nos facilitara esto,

$$r_{ijh} = \begin{cases} q_{iji} - s_{ij} & \text{si} \quad h=i \\ q_{ijj} + s_{ji} & \text{si} \quad h=j \\ q_{ijh} & \text{en caso contrario} \end{cases}$$

y $r_{ij} = (r_{ij1}, \ldots, r_{ijs})$.

Ahora podemos expresar la última afirmación de manera más clara.

Teorema A.2.1. *El conjunto $B=\{r_{ij},\ 1 \leq i < j \leq s\}$ genera a S_G como módulo sobre $K[x_1, \ldots x_n]$.*

Demostración. Se hará por reducción al absurdo. Así pues, supongamos que $M = S_G \backslash in(C) \neq \emptyset$. Sea $(h_1, \ldots, h_s) \in M$ tal que

$$t = \max\{LT(h_i \cdot g_i) |\ 1 \leq i \leq s\}$$

es el mínimo de

$$\{ \max\{LT(p_i \cdot g_i) |\ 1 \leq i \leq s \} |\ (p_1, \ldots, p_s) \in M \}$$

y además de entre todos los elementos de M que satisfacen esta condición el conjunto

$$J = \{ i |\ 1 \leq i \leq s, LT(h_i \cdot g_i) = t \}$$

es de cardinalidad mínima Dado que

$$\sum_{i=1}^{s} h_i \cdot g_i = 0, \text{ pues } (h_1, \ldots, h_s) \in S_G,$$

debemos tener que la suma de los términos principales que igualan a t es 0, para que esto último suceda J debe tener al menos cardinalidad 2. Supongamos que i<j están en J Entonces

$$LT(h_i)\cdot LT(g_i) = LT(h_j)\cdot LT(g_j) = t, \text{ es decir,}$$

t es común múltiplo de g_i y g_j. Por definición de p_{ij} sabemos que $s=s_{ij}\cdot g_i=s_{ji}\cdot g_j$ es el mínimo común múltiplo de g_i y g_j, por lo tanto $t= u\cdot s$, para algún monomio $u \in K[x_1, \ldots, x_n]$. Sea $a_k=LC(h_k)$ y consideremos la suma

$$\sum_{k=1}^{s} h_k\cdot g_k + a_k\cdot u\cdot[(q_{ijk} - s_{ij})\cdot g_i + (q_{ijj} + s_{ji})\cdot g_j + \sum_{k\neq i}^{s} q_{ijk}\cdot g_k]$$

$$\sum_{k=1}^{s} (h_k + a_k\cdot u\cdot r_{ijk})\cdot g_k = 0$$

Si $p_k = h_k + a_i\cdot u\cdot r_{ijk}$, $1\leq k \leq s$, entonces $(p_1, \ldots, p_s) \in S_G$. A continuación probaremos que $LT(p_kg_k) \leq t$, para cada k, y el número de ocasiones en que se da la igualdad es menor que la cardinalidad de J.
Primero observemos que $LT(q_{ijk}\cdot g_k) \leq LT(p_{ij}) < s$, la última desigualdad se da por propiedades de los s-polinomios. Para $k \neq j,i$

$$LT(a_k\cdot u\cdot r_{ijk}\cdot g_k) = u\cdot LT(q_{ijk}\cdot g_k) < u\cdot s = t,$$

por lo tanto $LT(p_k\cdot g_k) \leq t$ y si $LT(h_k\cdot g_k)<t$ entonces $LT(p_k\cdot g_k) < t$. Con esto hemos visto que para $k\neq i,j$ no aumenta el número de términos que igualan a t. Cuando k=j tenemos que

$$LT(a_j\cdot u\cdot r_{iji}\cdot g_i) = u\cdot LT(q_{iji}\cdot g_j + s_{ji}\cdot g_j) = u\cdot s = t,$$

así que $LT(p_j\, g_j)=t$. Para k=i,

$$LM(a_i\cdot u\cdot r_{iji}\cdot g_i) = a_i\cdot u\cdot LM(q_{iji}\cdot g_i - s_{ij}\cdot g_i) = -a_i\cdot u\cdot LT(s_{ij}\cdot g_i) = -a_i\cdot u\cdot s = -LM(h_i\cdot g_i),$$

por lo tanto $LT(p_i\cdot g_i) < t$. Dado que en los casos anteriores aumenta el número de veces que $LT(p_k\cdot g_k)=t$ y por otro lado tenemos que $LT(h_i\cdot g_i) = t$, pero $LT(p_i\cdot g_i) < t$ entonces

$$\#\{k|\ LT(p_k\cdot g_k) = t,\ 1 \leq k \leq s\} < \#J$$

Por la minimalidad de J $(p_1,\ldots,p_s) \in \text{lin}(B)$, pero $(p_1,\ldots,p_s)= (h_1,\ldots,h_s) + a_i\cdot u\cdot r_{ij}$ lo cual implica que $(h_1,\ldots,h_s) \in \text{lin}(B)$. Contradicción

El paso siguiente consiste en utilizar este conjunto de generadores de S_G para construir un grupo de generadores de S Primero observemos que dado que F y G generan el mismo ideal existen $c_{ij}, d_{ji} \in K[x_1,\ldots,x_n]$ tales que

$$f_j= \sum d_{ji}\cdot g_i \quad y \quad g_i= \sum c_{ij}\cdot f_j, \qquad \text{para } 1 \le j \le m \text{ y } 1\le i \le s, \quad (3)$$

sustituyendo obtenemos

$$f_j= \sum_{i=1}^{s} d_{ji}\cdot\Big(\sum_{k=1}^{m} c_{ik}\cdot f_k \Big) = \sum_{k=1}^{m}\Big(\sum_{i=1}^{s} d_{ji}\cdot c_{ik} \Big)\cdot f_k.$$

Sea δ_{ij} tal que $\delta_{ii}=1$ y $\delta_{ij}=0$ si $i\neq j$, entonces se da la siguiente igualdad

$$\sum_{k=1}^{m}\delta_{kj}\cdot f_k - \sum_{k=1}^{m}\Big(\sum_{i=1}^{s} d_{ji}\cdot c_{ik} \Big)\cdot f_k = \sum_{k=1}^{m}\Big(\delta_{kj} - \sum_{i=1}^{s} d_{ji}\cdot c_{ik} \Big)\cdot f_k = 0$$

por lo tanto si $a_{ik}= \delta_{kj} - \sum_{i=1}^{s} d_{ji}\cdot c_{ik}$ entonces $A=\{ a_j \mid a_j=(a_{j1},\ldots,a_{jm}),\ 1 \le j \le s \} \subset S_F$.

Sea $B=\{b_1,\ldots,b_r\}$ el conjunto de generadores de S_G con $b_i=(b_{i1},\ldots,b_{is})$, entonces

$$0 = \sum_{j=1}^{s} b_{ij}\cdot g_j \text{, utilizando (3) obtenemos}$$

$$0 = \sum_{i=1}^{s} b_{ij}\cdot\Big(\sum_{k=1}^{m} c_{kj}\, f_k\Big)= \sum_{k=1}^{m}\Big(\sum_{j=1}^{s} b_{ij}\cdot c_{kj}\Big)\cdot f_k$$

por lo tanto $b_i^*=(b_{i1}^*,\ldots,b_{im}^*)\in S_F$, con $b_{ik}^*= \sum_{j=1}^{s} b_{ij}\cdot c_{kj}$ Hemos visto que A y $B^*=\{b_i^* \mid 1\le i\le m\}$ están contenidos en S_F, la afirmación es que además lo generan. En resumen, para encontrar un conjunto de generadores para el módulo definido por

$$y_1\cdot f_1+ \quad +y_m f_m=0$$

primero calculamos una base de Groebner $G=\{g_1,\ldots,g_s\}$ para el ideal generado por $F=\{f_1,\ldots,f_m\}$ con los g_i's mónicos Luego calculamos un conjunto de generadores para S_G, expresamos cada g_i en términos de F, $g_i= \sum c_{ij}\cdot f_j$, y cada f_j en términos de G,

$f_j = \sum d_{ji} \cdot g_i$ Finalmente utilizamos los c_{ij}'s y d_{ji}'s para construir los conjuntos A y B^*, los cuales generan a S_F

A.3 Intersección entre un submódulo de $K[x_1,\ldots,x_n]^r$ y el módulo $K[f_1,\ldots,f_k]^r$

Teorema A.3.1 *Sea* $R = K[x_1, \ldots, x_n]$. $M = \sum_{i=1}^{s} R \cdot b_i \subseteq R^r$ *un submódulo y* $A = K[f_1, \ldots, f_k] \subseteq R$ *la subálgebra generada por elementos* $f_1, \ldots, f_k \in R$. *Considérese el anillo de polinomios* $S = K[x_1, \ldots, x_n, t_1, \ldots, t_k]$ *y* $T = K[t_1, \ldots, t_k]$ *y fórmense*

$$M' = \sum_{i=1}^{s} S \cdot b_i + \sum_{j=1}^{k} (t_j - f_j) \cdot S^r \subseteq S^r \quad y$$

$$M'_I = M' \cap T^r.$$

Entonces con $\Phi : T^r \to A^r$, $t_i \to f_i$ *tenemos*

$$\Phi(M'_I) = M \cap A^r.$$

En este lema las b_i's son elementos de R^r, es decir son r-adas de polinomios en R, así que M es el R-módulo generado por las b_i's

Demostración. Primero consideremos el homomorfismo Ψ: $S^r \to R^r/M$ dado por $t_i \to f_i$, entonces $\mathrm{Ker}(\Psi) = M'$

El que M' este en el kernel se sigue de su construcción, pues los coeficientes de las b_i's van a dar a R después de aplicar Ψ y los términos que provengan del otro sumando se anulan.

Ahora, con el objeto de demostrar la otra contención, se demostrara por inducción en el grado de P que $(P(t_1,\ldots,t_k) - P(f_1,\ldots,f_k)) \cdot e_i \in M'$, donde P es un monomio en las t's y $e_i \in S^r$ es un vector de la base canónica

Si P tiene grado 0, entonces la diferencia es 0 y el vector cero está en M'

Supongamos que el grado de P es mayor que cero, entonces $P(t_1,\ldots,t_k) = t_i P'(t_1,\ldots,t_k)$, para alguna i, $k \geq i \geq 1$, así entonces

$$(P(t_1,\ldots,t_k) - P(f_1,\ldots,f_k)) \cdot e_i =$$

$$((t_i - f_i) \cdot P'(t_1,\ldots,t_k) + f_i \cdot (P'(t_1,\ldots,t_k) - P'(f_1,\ldots,f_i))) \cdot e_i \in M'.$$

pues el primer sumando está en M', dado que es de la forma $\Sigma (t_j - f_j) \cdot S^r$, y el segundo está en M' por hipótesis de inducción Con esto es fácil ver que para cualquier $(g_1, \ldots, g_r) \in S^r$,

$$(g_1,\ldots, g_r) - \Psi(g_1,\ldots, g_k) \in M'.$$

$\Psi(g_1, \ldots, g_n) = 0$ implica que $\Psi(g_1,\ldots, g_k) \in M \subseteq M'$ y por lo tanto $(g_1,\ldots, g_k) \in M'$, que es lo que queríamos. Así que $\ker(\Psi) = M'$ y esto implica $\ker(\Psi|_{Tr}) = M'_{Tr}$.

Observemos ahora lo siguiente

$$\Psi(T^r) = (A^r + M) / M \cong A^r / (M \cap A^r)$$

la igualdad es fácil de ver si se piensa que $\Psi (f) = \Phi (f) + M$, para toda $f \in T^r$. Para la otra parte basta darse cuenta que el homomorfismo que manda $g + (M \cap A^r)$ en $g+M$, $g \in A^r$, es un isomorfismo. Esto último y el Teorema del isomorfismo nos dan como resultado

$$T^r/M'_T \cong A^r/(M \cap A^r)$$

Como $\Psi|_{Tr} (f) = \Phi (f) + M$, entonces Φ induce este isomorfismo lo cual nos da lo que necesitábamos. Explícitamente, sea γ: $(A^r + M)/M \rightarrow A^r/M \cap A^r$ un isomorfismo y sea Φ' : $T^r / M'_T \rightarrow (A^r + M) / M$ el isomorfismo dado por $\Phi'(f) = \Phi(f) + M$

Este lema realmente facilita el cálculo de $M \cap A^r$ pues podemos usar técnicas de eliminación para obtener M'_T .

Como calcular la intersección entre M y A^r.

Sean $b_1, \ldots, b_s$ generadores del módulo $M \subseteq R^r$ y $f_1,\ldots,f_k$ generadores de la subálgebra A Sea $S= K[x_1, \ldots, x_n, t_1,\ldots, t_k]$
Construimos el módulo M'
Ahora calculemos una base de Groebner B para este módulo con respecto a cualquier orden monomial que cumpla con que todo monomio en las x_i's sea mayor que los monomios en las t_i's
Una vez que tenemos B sólo hay que sustituir $t_i \rightarrow f_i$ en $B \cap K[t_1,\ldots,t_k]^r$ y el conjunto resultante genera a $M \cap A^r$. Esto último lo podemos afirmar gracias a las propiedades de eliminación de las bases de Groebner

Apéndice B.

B.1 Extensiones enteras.

Definición B.1.1. *Sea S un anillo y R un subanillo de S. Dado $s \in S$, s es entero sobre R si existe un polinomio mónico en $p \in R[x]$ tal que $p(s)=0$. Si todos los elementos de S son enteros sobre R entonces se dice que S es una extensión entera de B.*

Proposición B.1.2. *Sea R un subanillo de S. Si $x \in S$ es entero sobre R entonces R[x] es generado finitamente como módulo sobre R.*

Demostración. Sea $p \in R[y]$ tal que $p(x)=0$ Dada $g \in R[y]$ existen $r,h \in R[y]$, tales que $g=h \cdot p + r$, donde grado p > grado r Entonces $g(x) = r(x)$ esto quiere decir que si m=grado p entonces cualquier elemento de R[x] es de la forma $a_{m-1}x^{m-1}+\ldots+a_0$, $a_i \in R$, es decir, $\{x^{m-1}, \ldots, x, 1\}$ genera a R[x] como R-módulo

Con este resultado es fácil ver ahora que si $R[x_1, \ldots, x_n]$ es una extensión entera de R entonces $R[x_1, \ldots, x_n]$ es finitamente generado como R-módulo Sólo hay que observar que si $R[x_1, \ldots, x_i]$ es finitamente generado como R-módulo por elementos $p_1, \ldots, p_s$ y $R[x_1, \ldots, x_{i+1}]$ es generado por elementos $q_1, \ldots, q_d$ sobre $R[x_1, \ldots, x_i]$ entonces $R[x_1, \ldots, x_{i+1}]$ es generado por los productos $p_i \cdot q_j$ sobre R.

B.2 Teoría de la dimensión.

Definición B.2.1 *Sea R un anillo, la dimensión de Krull de R es el máximo de las longitudes de cadenas de primos $P_0 \subset \ldots \subset P_n$, donde la longitud es n. Sea I un ideal, la dimensión de Krull de I es la dimensión de Krull de R/I, es decir, el máximo de las longitudes de cadenas de primos que contienen a I.*

Lema B.2.2. *Sea I un ideal propio de $K[x_1, \ldots, x_n]$ tal que para cada i, $I \cap K[x_i] \neq \langle 0 \rangle$ entonces dim(I)=0.*

Demostración. Sea P un ideal primo tal que $I \subseteq P$ y sean $a_0, \ldots, a_m$ tales que $a_m x_i^m + \ldots + a_1 x_i^1 + a_0 \equiv 0$ en $R=K[x_1, \ldots, x_n]/P$, con $a_j \neq 0$ para alguna $j \in \{1, \ldots, m\}$.
Demostraremos que R es un campo, es decir, que P es maximal
Supongamos que $a_0 \neq 0$ entonces $x_i \cdot (a_m x_i^{m-1}+\ldots+a_1) \equiv -a_0$, por lo tanto x_i es unidad en R. Sea $s=\min\{ s \mid a_s \neq 0 \}$ entonces $x_i^s(a_m x_i^{m-s}+ \ldots + a_s) \equiv 0$, por lo tanto $x_i \equiv 0$ ó

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

$a_m x_i^{m-s} + \ldots + a_s \equiv 0$ el segundo caso implica que x_i es unidad por el primer argumento. Hemos visto entonces que cada x_i es 0 o es unidad en R, esto quiere decir que es campo
Dado que cualquier ideal primo que contenga a I es maximal entonces dim(I) = 0.

Teorema B.2.3. *Si $K[x_1, \ldots, x_n]$ / I es finitamente generado como espacio vectorial sobre K entonces dim(I)= 0.*

Demostración. Demostraremos que $I \cap K[x_i] \neq \{0\}$ para toda i.
Sea $C_i = \{ [x_i^n], n \in N \}$ si C_i es finito entonces existen h y j tales que $[x_i^h] = [x_i^j]$, por lo tanto $x_i^h - x_i^j \in I$ Si es infinito entonces es linealmente dependiente, es decir, existe

$$f = \sum_{i=1}^{\wedge} a_j [x_i^{nj}] = \left[\sum_{i=1}^{\wedge} a_j \cdot x_i^{nj} \right] = 0, \; a_i \neq 0 \text{ para alguna i}$$

Por lo tanto $\Sigma a_j \cdot x_i^{nj} \in I$

Definición B.2.4. *Sea I ideal primo, la codimensión de I, codim(I), es la dimensión del anillo local R_I. Si I no es primo entonces definimos codim(I) como el mínimo de las codimensiones de primos que lo contienen.*

También podemos ver codim(I) como el máximo de las longitudes de cadenas de primos $P_0 \subset \ldots \subset P_i$ con $P_j = I$

Teorema B.2.5 (Teorema del ideal principal de Krull). *Sea $f \in R$ y sea P un ideal primo, minimal entre los primos que contienen a f, entonces codim(P) ≤ 1.*

Proposición B.2.6 *Toda cadena maximal de ideales primos en $K[x_1, \ldots, x_n]$ tiene longitud n.*

Demostración. Se demostrara por inducción sobre el número n de indeterminadas. Sean $P \neq <0>$, $Q \neq <0>$ ideales primos en K[x] tales que $P \subseteq Q$, $P \neq Q$. K[x] es de ideales principales por lo que deben existir $p \neq 0$ y $q \neq 0 \in K[x]$ tales que $P = < p >$ y $Q = < q >$, $p \in Q$ implica que $p = h \cdot q$, $h \in K[x]$, pero P es primo así que $h \in P$ y por lo tanto $h = p \cdot h_1$, $h_1 \in K[x]$ y esto nos permite concluir que q es unidad, es decir, Q=K[x]. Con esto hemos demostrado que las cadenas maximales en K[x] tienen longitud 1

Sea $I_0 \subseteq \ldots \subseteq I_s$ una cadena maximal de primos en $K[x_1, \ldots, x_n]$ y sean $d_0 = dim(I_0), \ldots, d_s = dim(I_s)$ Es claro que $d_0 > \ldots > d_s$ y que $d_s = 0$ entonces $d_{s-1} > 0$ y por el lema1 existe x_i tal que $K[x_i] \cap I_{s-1} = \{0\}$, podemos suponer sin perdida de

generalidad i=n. Entonces $I_{s-1} \cap K[x_1, \ldots, x_{n-1}] = I_{s-1}$ de tal *modo que* $I_0 \subseteq \ldots \subseteq I_{s-1}$ es una cadena maximal en $K[x_1, \ldots, x_{n-1}]$ y por hipótesis de inducción s-1= n-1.

Se sigue directamente de esta proposición que para todo ideal primo $P \in K[x_1, \ldots, x_n]$, dim(P)+codim(P)= n

Bibliografía.

Atiyah, M F., MacDonald, I.G. (1969). *Introduction to Commutative Algebra.* Addison-Wesley.

Becker, T . Weispfenning, V (1993) *Groebner Bases: A computational Approach to Commutative Algebra* Springer, New York.

Cox, D , Little, J., O'Shea, D (1997). *Ideals, Varieties, and Algorithms: an introduction to computational algebraic geometry and commutative algebra* Springer, New York.

Decker, W , Heydtmann, A E , Schreyer, F (1998) *Generating a Noetherian Normalization of the Invariant Ring of a Finite Group* Journal of Symbolic Computation 25, 725-731.

Eisenbud, D (1995) *Commutative Algebra with a View Toward Algebraic Geometry.* Springer. New York.

Gianni, P , Trager, B , Zacharias, G. (1988). *Groebner Bases and Primary Decomposition of Polynomial Ideals* Journal of Symbolic Computation 6, 149-267.

Noether, E (1983). *Gesammelte Abhandlungen: Collected Papers Jacobson, N.* Springer, Berlin Heidelberg

Kemper, G (1996). *Calculating Invariant Rings of Finite Groups over Arbitrary Fields.* Journal of Symbolic Computation 21, 351-366.

Smith, L (1995). *Polynomial Invariants of Finite Groups* Wellesley, Mass.. A.K.Peters.

Sturmfels, B (1993). *Algorithms in Invariant Theory* Springer, Wien.

Vasconcelos, W V. (1998) *Computational Methods in Commutative Algebra and Algebraic Geometry* Springer, Berlin Heidelberg