Aspectos computacionales de la descomposición primaria

Ujué Etayo Rodríguez

Trabajo fin de Grado
dirigido por Philippe T. Giménez

Grado en Matemáticas
Facultad de Ciencias
Universidad de Valladolid
2010–2014

Universidad de Valladolid

A Javi

Índice general

Lista de algoritmos

Capítulo 1

Introducción

Estudiar las propiedades de los anillos de polinomios es una tarea común a varias ramas de las matemáticas. No solo resulta interesante en sí mismo, en el ámbito del álgebra conmutativa, sino que además es una herramienta imprescindible en el ámbito de la geometría algebraica.

A lo largo de este trabajo vamos a intentar conocer un poco más estos anillos, en concreto la descomposición primaria de sus ideales. Cuando queremos hallar la descomposición primaria de un ideal, hay veces que resulta sencillo; por ejemplo, si consideramos el ideal $(x^4 - 1) \in \mathbb{Q}[x]$, su descomposición primaria vendrá dada por los ideales engendrados por los factores irreducibles del polinomio $(x^4 - 1) = (x^2 + 1) \cap (x - 1) \cap (x + 1)$.

Sin embargo, no siempre ocurre así. Consideremos por ejemplo el ideal $(x_5^4 + x_2^2 x_1, x_2^7 x_7 - x_1^2 - x_6^5 + 1, x_2^5 x_8^3 + x_4 x_1 + x_4^2 x_5)$ en $\mathbb{R}[x_1, ..., x_{12}]$; en este caso, ponernos a calcular una descomposición primaria parece más complicado. Pero, ¿qué no sea fácil significa que no se pueda hacer? Como somos matemáticos sabemos que eso no es cierto, y este trabajo intenta presentar una manera sistemática, determinista, de encontrar la descomposición primaria de un ideal cualquiera de un anillo de polinomios.

Hemos decidido seguir los pasos de [GTZ] en cuanto al modo de realizar la descomposición, sin embargo, este método no es único, y la puerta está abierta para que se descubran métodos más efectivos para obtener una descomposición primaria.

El capítulo fundamental del trabajo es el 4, los anteriores sirven de introducción y recopilación de proposiciones necesarias para elaborar nuestro algoritmo. Los conceptos presentados a lo largo de los dos primeros capítulos son muy diversos, así que hemos intentado mantener el hilo conductor a través de los ejemplos, que se van repitiendo a lo largo de todo el trabajo.

En el capítulo 5 nos dedicamos a estudiar dos casos particulares de lo expuesto en el capítulo anterior. Veremos que cuando los ideales son monomiales o binomiales, podemos usar otros métodos mucho más eficientes para calcular una descomposición primaria.

Los ejemplos no siempre han sido fáciles de elaborar y hemos necesitado el programa SINGULAR para calcular las bases de Gröbner de todos los ideales presentes en este trabajo. La realización del mismo ha supuesto la iniciación en este programa por parte de la autora. Así mismo, los pequeños dibujos que acompañan a algunos de los ejemplos han sido elaborados con el programa SURFER.

Al comenzar a realizar este trabajo no tenía mayores conocimientos sobre la descomposición primaria que los que aporta el Grado en Matemáticas, es por eso que el trabajo está planteado de tal forma que cualquier graduado en matemáticas pueda leerlo sin problema. Los conceptos nuevos se introducen con definiciones y ejemplos detallados y se recuerdan la mayor parte de los vistos en la asignatura optativa de cuarto de grado *Álgebra Conmutativa y Computacional*.

Capítulo 2

Primeras nociones de Álgebra Conmutativa

Las matemáticas no solamente poseen la verdad,
sino la suprema belleza, una belleza fría y austera,
como la de la escultura, sin atractivo para la parte
más débil de nuestra naturaleza ...
Bertrand Russell

En este primer capítulo recordaremos ciertos resultados vistos en la asignatura optativa de cuarto de grado *Álgebra conmutativa y computacional*. Lo más importante ahora es establecer un fundamento sólido sobre el que podamos cimentar los siguientes capítulos. Es por esto que nos dedicaremos principalmente a definir conceptos y a enunciar resultados fundamentales, sin entrar en detalles de pruebas o demostraciones. Todo el capítulo irá ilustrado con diferentes ejemplos y contraejemplos. Para el desarrollo de este capítulo nos basaremos fundamentalmente en los textos [AtMc], [Eis] y [Nun].

A lo largo de todo este capítulo, $(\mathfrak{R}, +, \times)$ será un **anillo conmutativo unitario** al que denotaremos simplemente por $\mathfrak{R}$. Que $\mathfrak{R}$ sea *conmutativo* implica que el producto de dos elementos suyos cualesquiera conmuta y que sea *unitario* hace referencia a que $\mathfrak{R}$ está dotado de un elemento neutro 1 para el producto al que llamaremos *elemento unidad*.

2.1. Variedades algebraicas

Dado que no existe una materia en el grado en matemáticas que verse sobre este tema, vamos a introducir brevemente unos conceptos básicos de Geometría Algebraica.

La Geometría Algebraica, como su nombre indica, establece una relación entre estas dos ramas: el álgebra y la geometría. En sus orígenes, se dedicó al estudio de los conjuntos de soluciones de los sistemas de ecuaciones algebraicas, aunque hoy en día abarca gran diversidad de temas.

Comenzamos por el aspecto geométrico e introduciremos el concepto de *variedad*. Consideramos el espacio vectorial $\mathbb{k}^n$ y su espacio afín asociado, al que denotaremos por $\mathbb{A}^n_{\mathbb{k}}$.

2.1 Definición. Sea S un conjunto de polinomios en $\mathbb{k}[x_1, ..., x_n]$ entonces podemos definir una *variedad (algebraica)* en $\mathbb{A}^n_{\mathbb{k}}$ por el conjunto anulador de S, $V(S) = \{x \in \mathbb{A}^n_{\mathbb{k}} \text{ tales que } \forall p \in S \;\; p(x) = 0\}$.

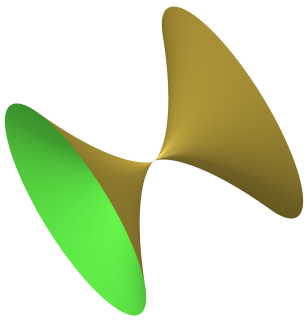
Es fácil ver que si tenemos dos conjuntos de polinomios $S, T \in \mathbb{k}[x_1, ..., x_n]$ entonces:

- Si $S \subset T \Rightarrow V(T) \subset V(S)$.
- Si $V(ST) = V(S) \cup V(T)$.

Decimos que una variedad V es *reducible* si es unión de dos subvariedades propias, en caso contrario, será *irreducible*.

2.2 Ejemplo. Consideremos por ejemplo la variedad de $\mathbb{R}^3$:

$$V = \{(x, y, z) \in \mathbb{R}^3 \text{ tales que } x^6 + (y^2 + z^2)^2 = 0\}$$



Variedad V

V es está formada por la unión de dos variedades propias

$$V_1 = V(x^3 - y^2 - z^2)$$

$$V_2 = V(-x^3 - y^2 - z^2)$$

Variedad V_1

Variedad V_2

Nota. En muchos libros también podemos encontrarnos con otra terminología: lo que nosotros hemos denominado *variedad* se conoce como *conjunto algebraico afín* y la palabra variedad está reservada para aquellos casos en los que dicho conjunto es irreducible.

Para estudiar el aspecto algebraico, realizamos la operación en sentido inverso. Denotamos por V a un subconjunto de $\mathbb{A}^n_{\Bbbk}$, y trabajamos en el anillo $\Bbbk[x] = \Bbbk[x_1, ..., x_n]$.

2.3 Definición. Definimos entonces el *ideal* $\mathfrak{I}(V)$ *de* $\Bbbk[x]$ *asociado a* V como el conjunto de los polinomios que se anula en V,

$$\mathfrak{I}(V) = \{p(x) \in \Bbbk[x] \text{ tales que } V \subset V(p)\}$$

Resulta sencillo comprobar que el conjunto $\mathfrak{I}(V)$ es un ideal, puesto que la suma de dos elementos que se anulan en x también se anulará en x y el producto de un polinomio que se anula en x por otro arbitrario sigue anulándose en x.

También es fácil ver que si tenemos dos subconjuntos $V, W \in \mathbb{A}^n_{\Bbbk}$, entonces $V \subset W \Rightarrow I(W) \subset I(V)$.

Llegados a este punto, hay dos cuestiones que se plantean automaticamente, ¿$V = V(\mathfrak{I}(V))$? ¿$S = \mathfrak{I}(V(S))$?

Zariski dió respuesta a la primera pregunta al definir una topología en $\mathbb{A}^n_{\Bbbk}$ compatible con la estructura algebraica de las ecuaciones. La respuesta a esta pregunta entonces, viene dada por esa topología.

2.4 Definición. La *topología de Zariski* en $\mathbb{A}^n_{\Bbbk}$ es la topología que tiene como conjuntos cerrados a las variedades de $\mathbb{A}^n_{\Bbbk}$.

2.5 Proposición. $V = V(\mathfrak{I}(V))$ *si y solo si* V *es una variedad.*

Demostración. Podemos ver directamente de las definiciones que:

1. $\forall V \subset \mathbb{A}^n_{\Bbbk}$, $V \subset V(I(V))$.

2. $\forall \mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$, $\mathfrak{I} \subset \mathfrak{I}(V(\mathfrak{I}))$.

Si tomamos $V = V(\mathfrak{I})$, por (1) tenemos que $V(\mathfrak{I}) \subset V(\mathfrak{I}(V(\mathfrak{I})))$, y por (2) $V(\mathfrak{I}(V(\mathfrak{I}))) \subset V(\mathfrak{I})$.

□

La segunda pregunta encuentra respuesta en una versión del *Nullstellensatz* de Hilbert, siempre que $\Bbbk$ sea un cuerpo **algebraicamente cerrado**.

2.6 Teorema (Hilbert Nullstellensatz)**.** *Supongamos que* $\Bbbk$ *es un cuerpo algebraicamente cerrado y sea* $\mathfrak{I}$ *un ideal de* $\Bbbk[x] = \Bbbk[x_1, ..., x_n]$*, entonces* $\mathfrak{I}(V(\mathfrak{I})) = \text{Rad}(\mathfrak{I})$.

Demostración. Podemos encontrar una prueba de este resultado en [Eis, Theorem 1.6].

□

El teorema implica entonces que $\mathfrak{I} = \mathfrak{I}(V(\mathfrak{I}))$ si y solo si $\mathfrak{I} =$Rad$(\mathfrak{I})$, es decir, si $\mathfrak{I}$ es un ideal radical. Puesto que todo ideal primo es radical, deducimos el siguiente corolario.

2.7 Corolario. *Todo ideal primo* $\mathfrak{P}$ *verifica* $\mathfrak{I}(V(\mathfrak{P})) = \text{Rad}(\mathfrak{P}) = \mathfrak{P}$.

Aprovechamos que hemos enunciado este teorema para fijarnos que tenemos una biyección entre la colección de variedades de $\mathbb{A}^n_{\Bbbk}$ y los ideales radicales de $\Bbbk[x_1, ..., x_n]$.

$$\begin{array}{rcl} \mathbb{A}^n_{\Bbbk} & \longrightarrow & \Bbbk[x_1, ..., x_n] \\ V & \longrightarrow & \mathfrak{I}(V) \\ V(\mathfrak{I}) & \longleftarrow & \mathfrak{I} \end{array}$$

Podemos caracterizar entonces una variedad irreducible de la siguiente manera:

2.8 Proposición. *Una variedad* $V \subset \mathbb{A}^n_{\Bbbk}$ *es irreducible si y solo si los polinomios que la definen generan un ideal primo* $\mathfrak{I}(V)$ *del anillo de polinomios* $\Bbbk[x_1, ..., x_n]$.

Demostración. Encontraremos una prueba en [CLO, Proposition 3, p.195].

□

Nota. Solo hemos utilizado la hipótesis de que $\Bbbk$ sea algebraicamente cerrado en el Nullstellensatz , el resto de resultados son ciertos en cualquier cuerpo $\Bbbk$.

2.2. Anillos noetherianos

A lo largo de esta sección, $\mathfrak{R}$ será un anillo **conmutativo y unitario**.

Consideramos el conjunto de ideales de $\mathfrak{R}$ con el orden parcial de inclusión de ideales. Dada una sucesión creciente de ideales $(\mathfrak{I}_n)_{n\in\mathbb{N}}$

$$\mathfrak{I}_1 \subseteq \mathfrak{I}_2 \subseteq \mathfrak{I}_3 \subseteq ... \subseteq \mathfrak{I}_k \subseteq \mathfrak{I}_{k+1} \subseteq ...$$

decimos que $(\mathfrak{I}_n)_{n\in\mathbb{N}}$ satisface la condición de cadena ascendente si a partir de un determinado $k \in \mathbb{N}$, $\mathfrak{I}_l = \mathfrak{I}_{l+1}$ $\forall l \geq k$.

Tenemos, de esta manera, la siguiente cadena:

$$\mathfrak{I}_1 \subseteq \mathfrak{I}_2 \subseteq \mathfrak{I}_3 \subseteq ... \subseteq \mathfrak{I}_k = \mathfrak{I}_{k+1} = \mathfrak{I}_{k+2} = ...$$

2.9 Definición. Decimos que un anillo $\mathfrak{R}$ es *noetheriano* si el conjunto de sus ideales con el orden de inclusión satisfacen la condición de la cadena ascendente.

También podemos caracterizar a estos anillos por la siguiente propiedad.

2.10 Proposición. *Un anillo $\mathfrak{R}$ es noetheriano si y sólo si dado un conjunto cualquiera de ideales de $\mathfrak{R}$ siempre podemos encontrar un elemento maximal en dicho conjunto.*

Demostración. Supongamos que $\mathfrak{R}$ es un anillo noetheriano, tomamos un conjunto de ideales de $\mathfrak{R}$, $\{\mathfrak{I}_i\}_{i\in I}$. Supongamos que no existe un elemento maximal en dicho conjunto, entonces $\forall i \in I$ $\exists j \in I$ tal que $\mathfrak{I}_i \subset \mathfrak{I}_j$ y la contención es estricta. De esta manera podemos construir una cadena de ideales de $\mathfrak{R}$ que no satisfacen la condición de la cadena ascendente, lo cual es absurdo, pues $\mathfrak{R}$ es noetheriano, y por lo tanto, verifica la condición de la cadena ascendente. Luego existe un elemento maximal.

Reciprocamente, si $\mathfrak{I}_k$ es un ideal maximal dentro de la sucesión de ideales $(\mathfrak{I}_n)_{n\in\mathbb{N}}$, formamos una cadena de inclusiones $\mathfrak{I}_1 \subseteq \mathfrak{I}_2 \subseteq \mathfrak{I}_3 \subseteq ...$ entonces el ideal $\mathfrak{I}_k$ ocupará una posición k-ésima, y por ser maximal, todos los que le contengan serán necesariamente iguales a él.

$$\mathfrak{I}_1 \subseteq \mathfrak{I}_2 \subseteq \mathfrak{I}_3 \subseteq ... \subseteq \mathfrak{I}_k = \mathfrak{I}_{k+1} = \mathfrak{I}_{k+2} = ...$$

Luego se verifica la condición de la cadena ascendente.

□

No resulta sencillo trabajar con esta definición de anillo noetheriano, así que normalmente utilizaremos la siguiente caracterización.

2.11 Proposición. *Un anillo $\mathfrak{R}$ es noetheriano si y solo si cada uno de sus ideales está generado por un sistema finito de generadores.*

Demostración. Consideramos un anillo noetheriano $\mathfrak{R}, \mathfrak{I}$ un ideal de $\mathfrak{R}, (f_i)_{i\in I}$ un conjunto de generadores de $\mathfrak{I}$, tomamos un elemento $f_1 \in (f_i)_{i\in I}$ y formamos la siguiente cadena:

$$(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset ...$$

Por ser $\mathfrak{R}$ noetheriano, verifica la condición de la cadena ascendente, y por lo tanto, $\exists k \in \mathbb{N}$ tal que $(f_1, ..., f_l) = (f_1, ..., f_l, f_{l+1})$ para todo $l \geq k$. Lo cual equivale a decir que $\mathfrak{I} = ((f_n)_{n\in\mathbb{N}}) = (f_1, ..., f_k)$ y por lo tanto, $\mathfrak{I}$ admite un sistema finito de generadores.

Veremos ahora la inclusión en el otro sentido. Sea $(\mathfrak{I}_n)_{n\in\mathbb{N}}$ una cadena ascendente de ideales de $\mathfrak{R}$, $\mathfrak{I}_1 \subseteq \mathfrak{I}_2 \subseteq \mathfrak{I}_3 \subseteq ...$, podemos considerar cada $\mathfrak{I}_n$ generado por el sistema finito de generadores del ideal anterior y un conjunto finito de generadores de él mismo. Es decir, si $\mathfrak{I}_n = (f_{n_1}, ..., f_{n_s})$ entonces $\mathfrak{I}_{n+1} = (f_{n_1}, ..., f_{n_s}, f_{n+1_1}, ..., f_{n+1_s})$. Sea $\mathfrak{I} = \bigcup_{n\in\mathbb{N}} \mathfrak{I}_n$, como $\mathfrak{I}$ es un ideal de $\mathfrak{R}$, estará finitamente generado. Pongamos $\mathfrak{I} = (f_1, ...f_m)$, tiene que existir un $k \in \mathbb{N}$ tal que $\mathfrak{I} = \mathfrak{I}_k = (f_1, ...f_m)$. Entonces, para todo $l \geq k$ tenemos $\mathfrak{I}_k \subset \mathfrak{I}_l \subset \mathfrak{I}$, luego $l \geq k$, $\mathfrak{I}_k = \mathfrak{I}_l$ y el anillo $\mathfrak{R}$ es noetheriano.

□

Podemos ver que varios anillos "conocidos" son anillos noetherianos; presentamos algunos en los siguientes ejemplos.

2.12 Ejemplo. Los cuerpos son anillos noetherianos: los únicos ideales que contiene un cuerpo son el ideal cero y el total, y ambos dos están generados por un único generador. En el caso del ideal cero, está generado obviamente por el cero, y en el caso del cuerpo, está generado por uno cualquiera de sus elementos no nulos.

2.13 Ejemplo. Los anillos de polinomios en una variable sobre un cuerpo son anillos noetherianos.

2.14 Ejemplo. Los anillos de polinomios en varias variables sobre un cuerpo son anillos noetherianos.

2.15 Ejemplo. Los dominios de ideales principales DIP son anillos noetherianos.

Hemos visto en el ejemplo (2.14) que los anillos de polinomios sobre cuerpos son anillos noetherianos. Sin embargo, el anillo de coeficientes no tiene que ser necesariamente un cuerpo, como veremos en el siguiente teorema.

2.16 Teorema (de la base de Hilbert)**.** *Sea $\mathfrak{R}$ un anillo noetheriano y $n \in \mathbb{N}$, entonces el anillo de polinomios $\mathfrak{R}[x_1, ..., x_n]$ es noetheriano.*

Demostración. Proponemos la prueba dada en [Eis, Theorem 1.2].

□

2.3. Descomposición primaria

A lo largo de esta sección, $\mathfrak{R}$ seguirá siendo un anillo **conmutativo y unitario**. Comenzamos repasando algunas nociones sobre los ideales radicales.

Decimos que un ideal $\mathfrak{I}$ es *radical* si coincide con su radical, $\mathrm{Rad}(\mathfrak{I}) = \mathfrak{I}$. Es fácil ver que todo ideal primo es radical: sea $x \in \mathrm{Rad}(\mathfrak{P}) \subset \mathfrak{R}$, con $\mathfrak{P}$ ideal primo, entonces $x^n \in \mathfrak{P}$, y como $\mathfrak{P}$ es primo y $x^n = xx^{n-1}$ tenemos que o bien $x \in \mathfrak{P}$ o bien $x^{n-1} \in \mathfrak{P}$. Si se da la primera opción, hemos terminado, y si se da la segunda, razonamos por inducción y llegamos también a la conclusión de que $x \in \mathfrak{P}$.

Sin embargo, no todo ideal radical es necesariamente primo, es más, podemos caracterizar al ideal $\mathrm{Rad}(\mathfrak{I})$ de la siguiente manera.

2.17 Proposición. *Sea $\mathfrak{I}$ un ideal de $\mathfrak{R}$, entonces el radical de $\mathfrak{I}$ está determinado por la intersección de los ideales primos de $\mathfrak{R}$ que contienen a $\mathfrak{I}$.*

$$\mathrm{Rad}(\mathfrak{I}) = \bigcap_{\mathfrak{I} \subset \mathfrak{P}} \mathfrak{P}, \text{ con } \mathfrak{P} \text{ ideal primo de } \mathfrak{R}.$$

Demostración. Podemos encontrar una demostración de esta proposición en [San, Corolario 1.5.7.].

□

Pasamos a dar la definición de un ideal primario.

2.18 Definición. Un ideal propio $\mathfrak{I}$ de un anillo $\mathfrak{R}$ es *primario* si todo elemento x de $\mathfrak{I}$ verifica que si $x = ab$ entonces, o bien $a \in \mathfrak{I}$, o bien $b \in \mathrm{Rad}(\mathfrak{I})$.

Llegados a este punto introduciremos algo de notación. De ahora en adelante, para referirnos a un ideal propio cualquiera de $\mathfrak{R}$ utilizaremos la letra $\mathfrak{I}$; cuando dicho ideal sea primario nos referiremos a él por $\mathfrak{Q}$. En el caso de un ideal primo, lo denotaremos por $\mathfrak{P}$ y si además de primo es maximal, será $\mathfrak{m}$.

2.19 Ejemplo. Consideramos el anillo $\mathbb{Z}$ de los números enteros y el ideal $4\mathbb{Z}$. El ideal $4\mathbb{Z}$ no es primo, pues

$$12 \in 4\mathbb{Z}, \text{ sin embargo } 12 = 2 \times 6 \text{ y } 2 \notin 4\mathbb{Z}, 6 \notin 4\mathbb{Z}$$

Sin embargo, $4\mathbb{Z}$ es *primario*: tenemos que $\text{Rad}(4\mathbb{Z}) = 2\mathbb{Z}$, sea $x \in 4\mathbb{Z}$, entonces $x = 4y$, con $y \in \mathbb{Z}$. Sea $x = ab = 4y$, entonces:

- Si a es múltiplo de 4, $a \in 4\mathbb{Z}$.
- Si b es múltiplo de 4, $b \in 4\mathbb{Z}$.
- Si a no es múltiplo de 4 y b no es múltiplo de 4, entonces $a \in 2\mathbb{Z} = \text{Rad}(4\mathbb{Z})$.

Luego el ideal $4\mathbb{Z}$ es primario.

También podemos caracterizar a un ideal primario $\mathfrak{Q}$ de $\mathfrak{R}$ por verificar que $\mathfrak{R}/\mathfrak{Q}$ es un anillo cociente no nulo y tal que todo elemento de $\mathfrak{R}/\mathfrak{Q}$ divisor de cero es nilpotente.

Podemos observar como el ideal del ejemplo (2.19) verifica que $\frac{\mathbb{Z}}{4\mathbb{Z}} \neq 0$; pues $1 \in \frac{\mathbb{Z}}{4\mathbb{Z}}$. Vamos a ver cuales son los elementos divisores de cero en dicho anillo.

- 0 no es divisor de cero por definición.
- 1 no es divisor de cero, pues $1 \times 1 = 1$, $1 \times 2 = 2$ y $1 \times 3 = 3$.
- 2 es divisor de cero, pues $2 \times 2 = 0$ y 2 es también nilpotente.
- 3 no es divisor de cero, pues $3 \times 1 = 3$, $3 \times 2 = 2$ y $3 \times 3 = 1$.

Luego en $\frac{\mathbb{Z}}{4\mathbb{Z}}$ todo divisor de cero es nilpotente.

Nota. Es evidente que todo elemento de $\mathfrak{R}/\mathfrak{Q}$ nilpotente es divisor de cero, si además tenemos la otra implicación, podemos deducir que $\mathfrak{Q}$ es un ideal primario.

Podemos sacar unas cuantas conclusiones inmediatas, como que cualquier ideal primo es primario, o que los ideales primarios se conservan en el paso al cociente.

Al principio de la sección hemos dicho que no todo ideal radical tiene que ser primo, sin embargo, si el ideal es radical de un ideal primario, entonces si es primo. Lo vemos en la siguiente proposición.

2.20 Proposición. *Sea $\mathfrak{Q}$ un ideal primario de $\mathfrak{R}$, entonces el radical de $\mathfrak{Q}, \mathrm{Rad}(\mathfrak{Q})$, es necesariamente el menor ideal primo que contiene a $\mathfrak{Q}$.*

Demostración. En primer lugar, veremos que $\mathrm{Rad}(\mathfrak{Q})$ es primo. Sea $x \in \mathrm{Rad}(\mathfrak{Q})$, $x = ab$. Entonces, por la definición de $\mathrm{Rad}(\mathfrak{Q})$, $\exists n \in \mathbb{N}$ tal que $x^n \in \mathfrak{Q}$. Tenemos entonces $x^n = a^n b^n$, y como $\mathfrak{Q}$ es un ideal primario, o bien $a^n \in \mathfrak{Q} \subset \mathrm{Rad}(\mathfrak{Q})$, o bien $b^n \in \mathrm{Rad}(\mathfrak{Q})$. En ambos casos, si $a^n \in \mathrm{Rad}(\mathfrak{Q})$ entonces $a \in \mathrm{Rad}(\mathfrak{Q})$, y si $b^n \in \mathrm{Rad}(\mathfrak{Q})$, entonces $b \in \mathrm{Rad}(\mathfrak{Q})$. Luego $\mathrm{Rad}(\mathfrak{Q})$ es un ideal primo.

Entonces, por la caracterización que nos ofrece la proposición (2.17) podemos concluir que $\mathrm{Rad}(\mathfrak{Q})$ es el menor ideal primo que contiene a $\mathfrak{I}$.

□

Este hecho nos sirve para introducir la siguiente terminología; si $\mathfrak{Q}$ es un ideal primario y $\mathfrak{P} = \mathrm{Rad}(\mathfrak{Q})$, entonces diremos que $\mathfrak{Q}$ es $\mathfrak{P}$-*primario*.

Podemos percatarnos de la existencia de cierta correspondencia entre los ideales primos y primarios de un anillo: es frecuente que la potencia de un ideal primo sea un ideal primario. Sin embargo, no existen implicaciones al respecto en ningún sentido. Lo ilustraremos con un par de ejemplos o, más bien, contraejemplos.

2.21 Ejemplo. Consideremos el anillo de polinomios $\mathbb{R}[x, y]$ y el ideal $\mathfrak{Q} = (x, y^2) \subset \mathbb{R}[x, y]$, veamos que:

- *El ideal $\mathfrak{Q}$ es primario:* utilizaremos la siguiente caracterización de ideal primario: $\mathfrak{Q}$ primario $\iff$ $\frac{\mathbb{R}[x,y]}{\mathfrak{Q}}$ es un anillo cociente no nulo y tal que todo elemento de $\frac{\mathbb{R}[x,y]}{\mathfrak{Q}}$ divisor de cero es nilpotente.

  Los elementos de $\frac{\mathbb{R}[x,y]}{(x,y^2)}$ son polinomios en la variable y con coeficientes en $\mathbb{R}$ y las potencias de y impares salvo para el término independiente, $p \in \frac{\mathbb{R}[x,y]}{(x,y^2)} \iff p = a_0 + a_1 y$.

Es evidente que $\frac{\mathbb{R}[x,y]}{(x,y^2)}$ es no nulo, pues $y \in \frac{\mathbb{R}[x,y]}{(x,y^2)}$. Podemos observar que los elementos divisores de cero en $\frac{\mathbb{R}[x,y]}{(x,y^2)}$ son precisamente los polinomios con término independiente nulo: $p(y) = a_1 y$, con $a_1 \in \mathbb{R}$, y que si elevamos $p(y)$ al cuadrado, obtenemos 0; por lo tanto, todo divisor de cero en $\frac{\mathbb{R}[x,y]}{(x,y^2)}$ es nilpotente y $\mathfrak{Q}$ es noetheriano.

- *El ideal $\mathfrak{Q}$ no es potencia de un ideal primo:* tenemos $\mathfrak{P} = \mathrm{Rad}(\mathfrak{Q}) = (x, y)$, luego si $\mathfrak{Q}$ fuera potencia de un primo, tendría que ser potencia de $\mathfrak{P}$. Sin embargo, $\mathfrak{P}^2 = (x, y)^2 = (x^2, y^2, xy) \subset \mathfrak{Q}$. La contención es estricta, pues $x \in \mathfrak{Q}$ pero $x \notin \mathfrak{P}^2$, y como tenemos $\mathfrak{P}^2 \supset \mathfrak{P}^3 \supset \mathfrak{P}^4 \supset ...$ podemos concluir que $\mathfrak{Q}$ no es potencia de un ideal primo.

Tenemos por tanto un ideal primario que no es potencia de un ideal primo.

2.22 Ejemplo. Consideremos ahora los anillos $\mathbb{Q}[x, y, z]$ y $\Bbbk[t]$ relacionados por el homomorfismo f:

$$\begin{array}{rccc} f : \mathbb{Q}[x,y,z] & \longrightarrow & \mathbb{Q}[t] \\ x & \mapsto & t^3 \\ y & \mapsto & t^4 \\ z & \mapsto & t^5 \end{array}$$

Calculamos el núcleo de f gracias a SINGULAR, usando *eliminación de variables*, un método que explicaremos más adelante. De esta manera obtenemos $\mathrm{Ker}(f) = \{p(x, y, z) \in \mathbb{Q}[x, y, z] : f(p) = 0\} = (x^3 - yz, y^2 - xz, z^2 - x^2y)$ y lo denotamos por $\mathfrak{P} = (x^3 - yz, y^2 - xz, z^2 - x^2y)$.

- *El ideal $\mathfrak{P}$ es primo:* $\mathfrak{P}$ es el nucleo de un homomorfismo de anillos, por lo que será primo si en el anillo de llegada no hay divisores de 0, pues $x \in \mathfrak{P} \iff f(x) = 0$. Sea $x = ab$, entonces $ab \in \mathfrak{P} \iff f(ab) = 0 \iff f(a)f(b) = 0$ y como $\mathbb{Q}[t]$ es un dominio de integridad no tiene divisores de 0 y necesariamente $f(a) = 0$ o $f(b) = 0$, luego $a \in \mathfrak{P}$ o $b \in \mathfrak{P}$.

- $\mathfrak{P}^2$ *no es $\mathfrak{P}$-primaria:* consideramos el ideal $\mathfrak{P}^2 = ((x^3 - yz)^2, (y^2 - xz)^2, (z^2 - x^2y)^2, (x^3 - yz)(y^2 - xz), (x^3 - yz)(z^2 - x^2y), (y^2 - xz)(z^2 - x^2y))$ y los siguientes elementos: $x \notin \mathfrak{P}$, $x^5 + xy^3 - 3x^2yz + z^3 \notin \mathfrak{P}^2$ pues el término xy^3 no puede obtenerse de ninguno de los polinomios que generan $\mathfrak{P}^2$ y sin embargo, $x(x^5 + xy^3 - 3x^2yz + z^3) = (x^3 - yz)^2 - (y^2 - xz)(z^2 - x^2y) \in \mathfrak{P}^2$.

Obtenemos de esta manera una potencia de un ideal primo que no es primaria.

Sin embargo, si establecemos otra condición más, si tomamos un ideal primo *maximal* $\mathfrak{m}$, entonces todas sus potencias son $\mathfrak{m}$-*primarias*.

2.23 Proposición. *Sea* $\mathfrak{m}$ *un ideal maximal de un anillo* $\mathfrak{R}$*, entonces,* $\mathfrak{m}^n$ *es un ideal primario* $\forall n \in \mathbb{N}$*.*

Demostración. Sea $x \in \mathfrak{m}^n$ con $\mathfrak{m}$ ideal maximal de $\mathfrak{R}$, obviamente, $\mathrm{Rad}(\mathfrak{m}^n) = \mathfrak{m}$, así que solo tenemos que demostrar que $\mathfrak{m}^n$ es primario . Pongamos $x = ab$ y supongamos que $b \notin \mathfrak{m}$, vamos a demostrar que entonces $a \in \mathfrak{m}^n$.

Consideremos el ideal $\mathfrak{m} + (b)$, es claro que $b \in \mathfrak{m} + (b)$ y además, como $\mathfrak{m}$ es un ideal maximal, $\mathfrak{m} + (b) = \mathfrak{R}$. Entonces, podemos escribir el elemento unidad de la siguiente forma:

$$1 = c + db, \qquad c \in \mathfrak{m},\ db \in (b)$$

Como $c \in \mathfrak{m}$, tendremos $c^n \in \mathfrak{m}^n$, así que, elevando la igualdad a la n-ésima potencia obtenemos:

$$1 = (c + db)^n = \sum_{k=0}^{n} \binom{n}{k} c^{n-k} (db)^k$$

Que podemos reescribir como

$$1 = c^n + bd' \text{ con } d' = \sum_{k=1}^{n} \binom{n}{k} c^{n-k} d^k b^{k-1} \in \mathfrak{R}$$

Si multiplicamos a ambos lados de la igualdad por a, obtenemos

$$a = ac^n + abd' \text{ con } c^n \in \mathfrak{m}^n, ab = x \in \mathfrak{m}^n$$

Luego podemos concluir que $a \in \mathfrak{m}^n$ y hemos terminado.

□

Recordamos al lector la noción de *cociente de dos ideales*; dado un anillo $\mathfrak{R}$, y dos ideales $\mathfrak{a}, \mathfrak{b} \subset \mathfrak{R}$, definimos el cociente del ideal $\mathfrak{a}$ por $\mathfrak{b}$ de la siguiente forma $(\mathfrak{a} : \mathfrak{b}) = \{x \in \mathfrak{R} \text{ tales que } x\mathfrak{b} \subset \mathfrak{a}\}$. Se puede comprobar mediante unos sencillos cálculos que $(\mathfrak{a} : \mathfrak{b})$ es un ideal.

De igual manera, si tenemos un ideal $\mathfrak{I}$ y un elemento $x \in \mathfrak{R}$, podemos definir el cociente del ideal $\mathfrak{I}$ por x considerando el cociente de $\mathfrak{I}$ por el ideal generado por x, (x); $(\mathfrak{I} : x) = \{y \in \mathfrak{R} : xy \in \mathfrak{I}\}$. Con vistas a preparar la siguiente sección, enunciaremos un par de resultados que no probaremos.

2.24 Lema ([AtMc, Lemma 4.3]). *La intersección finita de ideales $\mathfrak{P}$-primarios de $\mathfrak{R}$ es un ideal $\mathfrak{P}$-primario de $\mathfrak{R}$.*

2.25 Lema ([AtMc, Lemma 4.4]). *Sea $\mathfrak{Q}$ un ideal $\mathfrak{P}$-primario de $\mathfrak{R}$ y x un elemento de $\mathfrak{R}$, entonces:*

1. *Si $x \in \mathfrak{Q}$ entonces $(\mathfrak{Q} : x) = \mathfrak{R}$.*
2. *Si $x \notin \mathfrak{Q}$ entonces $(\mathfrak{Q} : x)$ es $\mathfrak{P}$-primario.*
3. *Si $x \notin \mathfrak{P}$ entonces $(\mathfrak{Q} : x) = \mathfrak{Q}$.*

Nota. Podemos afinar más en el apartado (2), si $x \in \mathfrak{P} - \mathfrak{Q}$, entonces $(\mathfrak{Q} : x)$ es un ideal $\mathfrak{P}$-*primario* que contiene estrictamente a $\mathfrak{Q}$.

2.26 Corolario. *Sea $\mathfrak{R}$ un anillo, $\mathfrak{Q}$ un ideal $\mathfrak{P}$-primario, entonces existe un $x \in \mathfrak{R}$ tal que $(\mathfrak{Q} : x) = \mathfrak{P}$.*

Demostración. Suponemos $\mathfrak{Q} \neq \mathfrak{P}$, sino nos bastaría con aplicar el punto 3 del lema (2.25). Sea $x \in \mathfrak{P} \backslash \mathfrak{Q}$, vamos a ver que $(\mathfrak{Q} : x) \subset \mathfrak{P}$.

Sea $y \in (\mathfrak{Q} : x)$, entonces por la definición $xy \in \mathfrak{Q}$ como $x \neq \mathfrak{Q}$ y $\mathfrak{Q}$ es primario, entonces necesariamente $y \in \mathfrak{P}$.

Veamos ahora que $\mathfrak{P} \subset (\mathfrak{Q} : x)$.

Sea $y \in \mathfrak{P}$, $x \in \mathfrak{P} \backslash \mathfrak{Q}$, entonces $xy \in \mathfrak{Q} \iff \forall a, b \in \mathfrak{R}$ tales que $xy = ab$ o bien $a \in \mathfrak{Q}$ o bien $b \in \mathfrak{P}$. Pero $xy \in \mathfrak{P}$, así que $ab \in \mathfrak{P}$, lo que implica que o bien $a \in \mathfrak{P}$ o bien $b \in \mathfrak{P}$ para cualquier $a, b \in \mathfrak{R}$ tales que $ab = xy$.

□

Una vez visto que es un ideal primario, podemos explicar que es una *descomposición primaria*.

2.27 Definición. Dado un anillo $\mathfrak{R}$, una *descomposición primaria* de un ideal $\mathfrak{I} \subset \mathfrak{R}$ es una expresión de $\mathfrak{I}$ como una intersección finita de ideales primarios:

$$\mathfrak{I} = \bigcap_{n=1}^{N} \mathfrak{Q}_n$$

donde cada $\mathfrak{Q}_n$ es un ideal $\mathfrak{P}_n$-*primario*.

En un anillo arbitrario, no todo ideal admite una tal descomposición, y es por eso que si $\mathfrak{I}$ admite una descomposición primaria diremos que es un ideal *descomponible*. Podemos encontrar varias descomposiciones primarias distintas de un mismo ideal $\mathfrak{I} \subset \mathfrak{R}$, como veremos en el ejemplo (2.29).

Antes de ver el ejemplo vamos a enunciar una proposición que nos resultará útil para construir una descomposición de un ideal.

2.28 Proposición. *Sean $\mathfrak{R}$ un anillo, $\mathfrak{I}$ un ideal de $\mathfrak{R}$, y un elemento de $\mathfrak{R}$ tal que $(\mathfrak{I} : y) = (\mathfrak{I} : y^2)$, entonces,*

$$\mathfrak{I} = (\mathfrak{I} : y) \cap (\mathfrak{I} + (y))$$

Demostración. Es obvio que $\mathfrak{I} \subset (\mathfrak{I} : y) \cap (\mathfrak{I} + (y))$, ya que:

- $\mathfrak{I} \subset (\mathfrak{I} : y)$ pues $\forall x \in \mathfrak{I}\ xy \in \mathfrak{I} \Rightarrow x \in (\mathfrak{I} : y)$.
- $\mathfrak{I} \subset (\mathfrak{I} + (y))$.

Vamos a demostrar entonces que $(\mathfrak{I} : y) \cap (\mathfrak{I} + (y)) \subset \mathfrak{I}$. Sea $x \in (\mathfrak{I} : y) \cap (\mathfrak{I} + (y))$, entonces:

1. $s \in (\mathfrak{I} : y) \iff xy \in \mathfrak{I}$.
2. $x \in (\mathfrak{I} + (y)) \iff x = i + yp$, con $i \in \mathfrak{I}$, $p \in \mathfrak{R}$.

De (1) y (2) tenemos que $(i + yp)y \in \mathfrak{I} \Rightarrow iy + y^2p \in \mathfrak{I}$. Como $i \in \mathfrak{I}$, $iy \in \mathfrak{I}$, así que tenemos que $y^2p \in \mathfrak{I}$.

$y^2p \in \mathfrak{I} \iff p \in (\mathfrak{I} : y^2)$, por hipótesis tenemos $(\mathfrak{I} : y) = (\mathfrak{I} : y^2)$, así que $p \in (\mathfrak{I} : y)$.

En (2) habíamos descrito x por $x = i + yp$ con $i \in \mathfrak{I}$, como $p \in (\mathfrak{I} : y)$, $yp \in \mathfrak{I}$, y podemos concluir que $x \in \mathfrak{I}$.

□

2.29 Ejemplo (*Falta de unicidad en la descomposición primaria*)**.** Consideremos el anillo $\mathbb{Q}[x, y, z]$ y el ideal $\mathfrak{I} = (x^2, xy, xz)$. Vamos a construir dos descomposiciones primarias distintas de $\mathfrak{I}$. Como todavía no hemos presentado una forma estándar de construirlas, lo haremos de "forma más artesanal".

Lo primero es ver que $\mathfrak{I}$ no es un ideal primario, para ello basta con considerar el elemento $xy \in \mathfrak{I}$, $x \notin \mathfrak{I}$ e $y \notin \mathrm{Rad}(\mathfrak{I})$. Tenemos además que $(\mathfrak{I} : y) = (x) = (\mathfrak{I} : y^2)$, luego podemos escribir $\mathfrak{I}$ como

$$\mathfrak{I} = (\mathfrak{I} : y) \cap (\mathfrak{I} + (y)) = (x) \cap (x^2, y, xz)$$

Sabemos que (x) es un ideal primario, sin embargo, (x^2, y, xz) no lo es, pues $xz \in (x^2, y, xz)$ con $x \notin (x^2, y, xz)$ y $z \notin \mathrm{Rad}((x^2, y, xz))$. Además, tenemos $((x^2, y, xz) : z) = (x, y) = ((x^2, y, xz) : z^2)$ luego

$$(x^2, y, xz) = ((x^2, y, xz) : z) \cap ((x^2, y, xz) + (z)) = (x, y) \cap (x^2, y, z)$$

Y podemos concluir que

$$\mathfrak{I} = (x) \cap (x, y) \cap (x^2, y, z) = (x) \cap (x^2, y, z) \tag{2.1}$$

Es una descomposición primaria de $\mathfrak{I}$.

Por otro lado, también podemos descomponer (x^2, y, xz) de la siguiente manera: $((x^2, y, xz) : z^2) = (x, y) = ((x^2, y, xz) : z^3)$ por lo tanto,

$$(x^2, y, xz) = ((x^2, y, xz) : z^2) \cap ((x^2, y, xz) + (z^2)) = (x, y) \cap (x^2, y, xz, z^2)$$

Luego también tenemos

$$\mathfrak{I} = (x) \cap (x, y) \cap (x^2, y, xz, z^2) = (x) \cap (x^2, y, xz, z^2) \tag{2.2}$$

Tanto (2.1) como (2.2) son descomposiciones primarias de $\mathfrak{I}$.

De entre todas las descomposiciones primarias que admite un ideal, algunas presentan unas características especiales, las llamamos *descomposiciones primarias minimales*. A continuación, enunciamos formalmente su definición.

2.30 Definición. Decimos que una descomposición primaria de un ideal $\mathfrak{I}$ en un anillo $\mathfrak{R}$ es *minimal* si verifica:

1. Los ideales $\mathfrak{P}_n$ son distintos dos a dos.
2. $\mathfrak{Q}_n \not\subset \bigcap_{m \neq n} \mathfrak{Q}_m$ para todo $n \in \{1, ..., N\}$

Dada una descomposición primaria de un ideal $\mathfrak{I}$ de un anillo $\mathfrak{R}$, siempre podemos obtener a partir de ella otra descomposición primaria minimal. Para comprobarlo basta con aplicar el Algoritmo 1 que aparece más adelante.

Llegados a este punto, una pregunta se plantea de forma inmediata: ¿existe algún componente invariante en la descomposición primaria de un ideal?, para dar respuesta esta pregunta, presentamos dos teoremas de unicidad de descomposición minimal. Las demostraciones de ambos resultados, que no forman parte de este trabajo, pueden encontrarse en la bibliografía citada.

2.31 Teorema (Primer teorema de unicidad [AtMc, Theorem 4.5])**.** *Sea* $\mathfrak{I}$ *un ideal descomponible de* $\mathfrak{R}$ *e* $\mathfrak{I} = \bigcap_{n=1}^{N} \mathfrak{Q}_n$ *una descomposición primaria minimal de* $\mathfrak{I}$. *Sea* $\mathfrak{P}_n = \mathrm{Rad}(\mathfrak{Q}_n)$ *para todo* n, $1 \leq n \leq N$.

Entonces, dichos $\mathfrak{P}_n$ *son independientes de la descomposición particular de* $\mathfrak{I}$.

Algorithm 1 Descomposición primaria minimal

procedure DPM($\{\mathfrak{Q}_1, ..., \mathfrak{Q}_n\}$ descomposición primaria de $\mathfrak{I}$)
  salida: $P = \{\mathfrak{Q}'_1, ..., \mathfrak{Q}'_m\}$ descomposición primaria minimal de $\mathfrak{I}$
  for $i = 0$ to n **do**
    $\mathfrak{Q}'_i \leftarrow \mathfrak{Q}_i$
  end for
  for $i = 0$ to n **do**
    for $j = i$ to n **do**
      if $\mathrm{Rad}(\mathfrak{Q}'_i) = \mathrm{Rad}(\mathfrak{Q}'_j)$ **then**
        $\mathfrak{Q}'_i \leftarrow \mathfrak{Q}_i \cap \mathfrak{Q}_j$
        $\mathfrak{Q}'_j \leftarrow \mathfrak{Q}_i \cap \mathfrak{Q}_j$
      end if
    end for
  end for
  for $i = 0$ to n **do**
    if $\mathfrak{Q}'_i \not\subset \bigcap_{j \neq i} \mathfrak{Q}_j$ **then**
      if $\mathfrak{Q}'_i \notin P$ **then**
        $P \leftarrow P \cup Q'_i$
      end if
    end if
  end for
  return: P
end procedure

Nota. Podemos observar que los $\mathfrak{P}_n$ son los ideales primos que aparecen en el conjunto de los ideales de la forma $\mathrm{Rad}((\mathfrak{I} : x))$ con $x \in \mathfrak{I}$, lo que los hace independientes de dicha descomposición.

Llamaremos *ideales primos asociados a* $\mathfrak{I}$ a los ideales primos $\mathfrak{P}_n$ que del teorema (2.31) y denotaremos por $\mathrm{Ass}_{\mathfrak{R}}(\mathfrak{I})$ al conjunto de los ideales primos asociados a $\mathfrak{I}$.

Dentro de $\mathrm{Ass}_{\mathfrak{R}}(\mathfrak{I})$ podemos encontrar dos tipos de ideales primos, decimos que un ideal primo es *aislado* cuando es un elemento minimal en $\mathrm{Ass}_{\mathfrak{R}}(\mathfrak{I})$ con respecto al orden de la contención; decimos que un primo es *inmerso* cuando no es aislado.

Vemos, por lo tanto, que dada una descomposición primaria minimal, podemos encontrar dos tipos de componentes, las *componentes aisladas*, formadas por los ideales primarios $\mathfrak{Q}_n$ cuyo radical $\mathfrak{P}_n$ sea un primo aislado; y las *componentes inmersas*, aquellas cuyo radical es un primo inmerso.

Volviendo al enfoque tomado en la introducción, y desde un punto de vista geométrico, podemos observar como si el ideal $\mathfrak{I}$ da origen a una variedad $V(\mathfrak{I})$, los primos aislados dan origen a las componentes irreducibles y los primos inmersos a las subvariedades de estas; es decir, a las variedades inmersas en las componentes irreducibles.

2.32 Ejemplo. Consideremos ahora el ideal $I = (y^2z^2 - x^2y^3 - xz^3 + x^3yz, y^2z - xz^2)$ en el anillo $\mathbb{Q}[x, y, z]$. Como todavía no hemos visto como calcular una descomposición primaria, utilizaremos un comando de SINGULAR para calcularla. A continuación reproducimos el código que hemos utilizado:

```
> LIB "primdec.lib";
```

Iniciamos el programa y descargamos la biblioteca de descomposición primaria de SINGULAR. A continuación, definimos nuestras variables.

```
> ring R=0,(x,y,z),dp;
> R;
//   characteristic : 0
//   number of vars : 3
//        block   1 : ordering dp
//                  : names    x y z
//        block   2 : ordering C
> ideal I=y^2*z^2-x^2*y^3-x*z^3+x^3*y*z,y^2*z-x*z^2;
> I;
I[1]=-x2y3+x3yz+y2z2-xz3
I[2]=y2z-xz2
```

Y le pedimos que calcule la descomposición primaria según el proceso "GTZ". Hemos elegido este proceso ya que será uno de los que expliquemos en el capítulo 4 del trabajo. Nosotros le llamaremos DPK.

```
> primdecGTZ(I);
[1]:
   [1]:
      _[1]=-y2+xz
   [2]:
      _[1]=-y2+xz
[2]:
   [1]:
      _[1]=z2
```

```
      _[2]=y
   [2]:
      _[1]=z
      _[2]=y
[3]:
   [1]:
      _[1]=z
      _[2]=x2
   [2]:
      _[1]=z
      _[2]=x
>
```

La salida del comando `primdecGTZ` es una lista de listas: la lista principal contiene tres elementos, lo cual nos indica que la descomposición primaria tiene tres componentes. Dentro de cada elemento encontramos una lista con dos elementos, en ella están en primer lugar los generadores del ideal y en segundo lugar los generadores de su radical. Así que la descomposición primaria buscada es

$$\mathfrak{I} = (y^2 - xz) \cap (y, z^2) \cap (x^2, z)$$

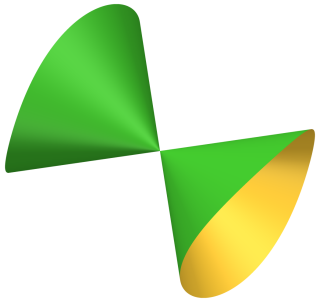
Tenemos entonces una única componente aislada de esta descomposición: el ideal $(y^2 - xz)$, y dos componentes inmersas, (y, z^2) y (x^2, z). Podemos observar la variedad que engendra cada uno de los componentes y comprobar como los ideales aislados dan origen a variedades irreducibles y los inmersos a variedades inmersas.

Las variedades engendradas por (y, z^2) y (x^2, z) dan lugar a las rectas x e y respectivamente, rectas que están contenidas en la variedad $V(y^2 - xz)$. Podemos observar el significado geométrico de la variedades inmersas: las rectas x e y están *inmersas* o incluidas en la variedad engendrada por $V(y^2 - xz)$.

El resultado que nos disponemos a enunciar a continuación nos simplificará a la hora de calcular los primos aislados asociados a un ideal $\mathfrak{I} \subset \mathfrak{R}$.

2.33 Proposición. *Sea $\mathfrak{I}$ un ideal descomponible de $\mathfrak{R}$ e $\mathfrak{I} = \bigcap_{n=1}^{N} \mathfrak{Q}_n$ una descomposición primaria minimal de $\mathfrak{I}$. Sea $\mathfrak{P}_n = \mathrm{Rad}(\mathfrak{Q}_n)$ para todo n, $1 \leq n \leq N$.*

Entonces, los ideales primos aislados asociados a $\mathfrak{I}$ son exactamente los ideales minimales entre los ideales primos que contienen a $\mathfrak{I}$.



Variedad $V(y^2 - xz)$

Demostración. Podemos encontrar una demostración en [AtMc, Proposition 4.6].

□

2.34 Teorema (Segundo teorema de unicidad [AtMc, Theorem 4.10])**.** *Sean* $\mathfrak{I}$ *un ideal descomponible de* $\mathfrak{R}$ *e* $\mathfrak{I} = \bigcap_{n=1}^{N} \mathfrak{Q}_n$ *una descomposición primaria minimal de* $\mathfrak{I}$*. Sea* $\mathfrak{P}_n = \mathrm{Rad}(\mathfrak{Q}_n)$ *para todo* $1 \leq n \leq N$*.*

Entonces, las componentes aisladas primarias están unívocamente determinadas por $\mathfrak{I}$*.*

Demostración. Tenemos un ideal descomponible $\mathfrak{I} \subset \mathfrak{R}$ e $\mathfrak{I} = \bigcap_{n=1}^{N} \mathfrak{Q}_n$ una descomposición primaria minimal. Sean $\mathfrak{Q}_{i_1}, ..., \mathfrak{Q}_{i_m}$ un conjunto de componentes aisladas primarias.

Entonces $\mathfrak{Q}_{i_1} \cap ... \cap \mathfrak{Q}_{i_m}$ es el ideal contraído de $\mathfrak{I}$ por la aplicación de paso al anillo de fracciones $\mathfrak{R} \longrightarrow S^{-1}\mathfrak{R}$ con $S = \mathfrak{R} \backslash (\mathfrak{P}_{i_1} \cap ... \cap \mathfrak{P}_{i_m})$, ya que $\mathfrak{P}_i$ sólo depende de $\mathfrak{I}$.

□

Descomposición primaria en anillos noetherianos

Acotando el conjunto de anillos en los que trabajamos, podemos obtener mejores resultados; vamos a ver que en un anillo noetheriano, todo ideal propio es descomponible. Previamente, recordamos la noción de ideal irreducible.

2.35 Definición. Decimos que un ideal $\mathfrak{I} \subset \mathfrak{R}$ es *irreducible* si no puede escribirse como intersección de otros dos ideales de $\mathfrak{R}$.

En un anillo noetheriano, tenemos el siguiente resultado.

2.36 Proposición. *En un anillo noetheriano, todo ideal propio irreducible es primario.*

Demostración. Podemos encontrar una demostración en [AtMc, Lemma 7.12]

□

Y enunciamos el resultado citado.

2.37 Teorema. *En un anillo noetheriano, todo ideal propio es descomponible.*

Demostración. Comenzaremos esta demostración probando que en un anillo noetheriano todo ideal propio se puede escribir como intersección finita de ideales irreducibles. Para ello, razonaremos por reducción al absurdo.

Sea A el conjunto de ideales de $\mathfrak{R}$ que no admiten una descomposición como intersección finita de ideales irreducibles. Como $\mathfrak{R}$ es un anillo noetheriano, todo subconjunto de ideales admite un elemento maximal, así que tomamos $\mathfrak{I}$ elemento maximal de A. Obviamente, $\mathfrak{I}$ es reducible, pues sino $\mathfrak{I}$ podría descomponerse como intersección finita de ideales irreducibles: el mismo.

Sea $\mathfrak{I} = \mathfrak{a} \cap \mathfrak{b}$ con $\mathfrak{a} \neq \mathfrak{b}$ ideales de $\mathfrak{R}$, una descomposición de $\mathfrak{I}$. Entonces tenderemos $\mathfrak{I} \subset \mathfrak{a}$ y como $\mathfrak{I}$ es maximal en A, entonces necesariamente $\mathfrak{a} \notin A$ luego $\mathfrak{a}$ se puede escribir como intersección finita de ideales irreducibles.

$$\mathfrak{a} = \bigcap_{i=1}^{N_\mathfrak{a}} \mathfrak{a}_i \text{ con } \mathfrak{a}_i \text{ irreducilble } \forall i.$$

Por el mismo razonamiento, tenemos que

$$\mathfrak{b} = \bigcap_{i=1}^{N_\mathfrak{b}} \mathfrak{b}_i \text{ con } \mathfrak{b}_i \text{ irreducilble } \forall i.$$

Podemos concluir que $\mathfrak{I}$ se puede escribir como intersección finita de ideales irreducibles.

$$\mathfrak{I} = \mathfrak{a} \cap \mathfrak{b} = \left(\bigcap_{i=1}^{N_\mathfrak{a}} \mathfrak{a}_i \right) \cap \left(\bigcap_{i=1}^{N_\mathfrak{b}} \mathfrak{b}_i \right) = \bigcap_{i=1}^{N_\mathfrak{b}+N_\mathfrak{b}} \mathfrak{I}_i$$

Lo cual es absurdo.

En la proposición 2.36 vimos que todo ideal irreducible es primario, con lo que ya tenemos la descomposición primaria buscada.

□

2.38 Corolario. *Todo ideal $\mathfrak{I}$ de un anillo noetheriano $\mathfrak{R}$ admite una descomposición primaria minimal.*

2.4. Localización en un anillo

Un concepto importante en Álgebra Conmutativa que guarda una gran relación con la Geometría Algebráica es el de *localización en un anillo con respecto a un ideal primo.*

A lo largo de esta sección solamente presentaremos definiciones y notaciones que serán necesarias en el capítulo cuatro. Para un estudio de la localización más detallado, podemos mirar, por ejemplo, [AtMc, Chapter 3].

En la asignatura de Álgebra Conmutativa y Computacional dedicamos un capítulo a hablar de anillos y módulos de fracciones, por lo que supondremos estos conceptos conocidos por el lector. Nos centraremos aquí en un único tipo de anillos de fracciones, el localizado respecto de un ideal primo.

2.39 Definición. Sean $\mathfrak{R}$ un anillo conmutativo y unitario, $\mathfrak{P}$ un ideal primo de $\mathfrak{R}$, el sistema multiplicativamente cerrado $S = \mathfrak{R}\backslash\mathfrak{P}$. El anillo de fracciones dado por $S^{-1}\mathfrak{R}$ es el *localizado* de $\mathfrak{R}$ con respecto a $\mathfrak{P}$ y lo denotamos por $\mathfrak{R}_{\mathfrak{P}}$.

Este proceso nos permite añadir ciertos inversos multiplicativos a elementos de nuestro anillo creando a su vez, un homomorfismo entre el anillo original y el nuevo anillo. Al transformar en unidades a los elementos de S, podemos realizar un estudio más detallado de estos elementos.

Por ejemplo, consideremos el anillo $\Bbbk[x_1, ..., x_n]$, V una variedad de $\mathbb{A}^n_{\Bbbk}$ y un punto $p \in V$. Si queremos estudiar las propiedades locales de V en p podemos considerar el ideal de todas los polinomios que se anulan en p, llamémosle $\mathfrak{I}$. Entonces el localizado de $\Bbbk[x_1, ..., x_n]$ con respecto a $\mathfrak{I}$ contiene la información sobre el comportamiento de V cerca de p.

Presentamos la notación que utilizaremos en el trabajo. Sea $\mathfrak{R}$ un anillo, $\mathfrak{I}$ un ideal de $\mathfrak{R}$, s un elemento de $\mathfrak{R}$ y $\mathfrak{P}$ un ideal primo de $\mathfrak{R}$. Entonces denotaremos por:

- $\mathfrak{R}_{\mathfrak{P}}$ al anillo localizado con respecto al ideal $\mathfrak{P}$; $\mathfrak{R}_{\mathfrak{P}} = S^{-1}\mathfrak{R}$ con $S = \mathfrak{R}\backslash\mathfrak{P}$.
- $\mathfrak{I}_{\mathfrak{P}}$ será la imagen de $\mathfrak{I}$ en el anillo $\mathfrak{R}_{\mathfrak{P}}$; $\mathfrak{I}_{\mathfrak{P}} = \mathfrak{I}\mathfrak{R}_{\mathfrak{P}}$.
- $\mathfrak{R}_s$ es el anillo localizado con respecto al elemento s; $\mathfrak{R}_s = S^{-1}\mathfrak{R}$ con $S = \{s^n\}_{n\in\mathbb{N}}$.
- $\mathfrak{I}_s$ la imagen de $\mathfrak{I}$ en el anillo $\mathfrak{R}_s$; $\mathfrak{I}_s = \mathfrak{I}\mathfrak{R}_s$.

Capítulo 3

Bases de Gröbner

Los símbolos algebraicos se usan cuando
no sabes de qué estás hablando.
Philippe Schnoebelen

Una base de Gröbner de un ideal $\mathfrak{I} \subset \mathfrak{R}$ es un sistema de generadores finito de $\mathfrak{I}$ con una característica muy importante: nos permite calcular la dimensión algebraica del ideal y, en caso de que esta sea finita, sus ceros de una manera mucho más sencilla. Así mismo, gracias a las bases de Gröbner podemos obtener fácilmente la imagen de una variedad bajo una proyección o ciertos tipos de aplicaciones.

Las bases de Gröbner vieron la luz simultaneamente en dos puntos muy alejados del globo: por un lado, Bruno Buchberger las presentó en su tesis, dirigida por Wolfgang Gröbner, que defendió en 1965. Un año antes, el profesor Heisuke Hironaka definía lo que el llamo *standard basis*, un sistema de generadores que permitía trabajar en anillos locales.

A lo largo de este capítulo $\Bbbk$ será un **cuerpo**, por lo que hemos visto en el capítulo anterior, sabemos que $\Bbbk$ es noetheriano. Trabajaremos esta vez en el anillo de polinomios en varias variables con coeficientes en $\Bbbk$, es decir, $\Bbbk[x_1, ..., x_n]$. Además, podremos generalizar varios resultados de este capítulo a un anillo de polinomios $\mathfrak{R}[x_1, ..., x_n]$ donde los coeficientes están en $\mathfrak{R}$, un anillo **conmutativo, unitario y noetheriano**; resultados que indicaremos oportunamente. Por el teorema de la base de Hilbert (2.16), tanto $\Bbbk[x_1, ..., x_n]$ como $\mathfrak{R}[x_1, ..., x_n]$ son anillos noetherianos.

Para redactar este capítulo nos hemos basado principalmente en [CLO], [Swa1] y [Gim].

3.1. Orden monomial

Comenzamos este capítulo introduciendo la noción de *orden monomial*, dicho orden dotará al conjunto de monomios de nuestro anillo $\Bbbk[x_1, ..., x_n]$ de la propiedad de ser un conjunto totalmente ordenado.

3.1 Definición. Dado un anillo $\Bbbk[x_1, ..., x_n]$, un *orden monomial* $<$ sobre $\Bbbk[x_1, ..., x_n]$ es un orden total en los monomios de $\Bbbk[x_1, ..., x_n]$ que verifica:

1. Es un buen orden: todo subconjunto no vacío de monomios de $\Bbbk[x_1, ..., x_n]$ admite un más pequeño elemento.

2. Es compatible con el producto: si $f_1 < f_2$ entonces $gf_1 < gf_2$ para todo g monomio de $\Bbbk[x_1, ..., x_n]$.

Vamos a presentar algunos de los órdenes monomiales que utilizaremos posteriormente en el trabajo.

- El *orden lexicográfico*, que denotaremos por $<_{lex}$, establece que $x_1^{\alpha_1}...x_n^{\alpha_n} \geq_{lex} x_1^{\beta_n}...x_n^{\beta_n}$ si la primera coordenada no nula de $(\alpha_1 - \beta_1, ..., \alpha_n - \beta_n)$ es positiva.

- El *orden lexicográfico graduado*, que denotaremos por $<_{glex}$, establece que $x_1^{\alpha_1}...x_n^{\alpha_n} \geq_{glex} x_1^{\beta_n}...x_n^{\beta_n}$ si se verifica una de estas dos propiedades: $\alpha_1 + ... + \alpha_n > \beta_1 + ... + \beta_n$ ó $\alpha_1 + ... + \alpha_n = \beta_1 + ... + \beta_n$ y $x_1^{\alpha_1}...x_n^{\alpha_n} \geq_{lex} x_1^{\beta_1}...x_n^{\beta_n}$.

- El *orden lexicográfico inverso graduado*, que denotaremos por $<_{grevlex}$, establece que $x_1^{\alpha_1}...x_n^{\alpha_n} \geq_{grevlex} x_1^{\beta_1}...x_n^{\beta_n}$ si la última coordenada no nula de $(\alpha_1 - \beta_1, ..., \alpha_n - \beta_n)$ es positiva.

Nota. Llamamos la atención al lector sobre el hecho de que $x_1^{\alpha_1}...x_n^{\alpha_n} \geq_{lex} x_1^{\beta_1}...x_n^{\beta_n}$ no implica necesariamente que $x_1^{\alpha_1}...x_n^{\alpha_n} \leq_{grevlex} x_1^{\beta_1}...x_n^{\beta_n}$. Los ordenes monomiales no son inversos.

3.2 Definición. Dados dos ordenes monomiales $<$ en $\Bbbk[x_1, ..., x_d]$ y $<'$ en $\Bbbk[x_{d+1}, ..., x_n]$, el *orden producto* de $<$ y $<'$ en $\Bbbk[x_1, ..., x_n]$ es un orden monomial $<_*$ que establece que $x_1^{\alpha_1}...x_n^{\alpha_n} \geq_* x_1^{\beta_1}...x_n^{\beta_n}$ si $x_1^{\alpha_1}...x_d^{\alpha_d} \geq x_1^{\beta_1}...x_d^{\beta_d}$ o $x_1^{\alpha_1}...x_d^{\alpha_d} = x_1^{\beta_1}...x_d^{\beta_d}$ y $x_{d+1}^{\alpha_{d+1}}...x_n^{\alpha_n} \geq' x_{d+1}^{\beta_{d+1}}...x_n^{\beta_n}$.

Resulta sencillo comprobar que el orden producto es un orden monomial. Además, si tenemos un anillo $\Bbbk[x_1, ..., x_n]$ dotado del orden lexicográfico $(x_1 > ... > x_n)$, entonces ese orden es un orden producto de los órdenes lexicográficos $(x_1 > ... > x_t)$ en $\Bbbk[x_1, ..., x_t]$ y $(x_{t+1} > ... > x_n)$ en $\Bbbk[x_{t+1}, ..., x_n]$, con t variando entre1 y $n - 1$.

3.2. Algoritmo de división

Consideramos ahora nuestro anillo $\Bbbk[x_1, ..., x_n]$ dotado de un orden monomial $<$, sea $p \in \Bbbk[x_1, ..., x_n]$, entonces:

- Llamamos *monomio inicial* de p al mayor de los monomios de p para el orden establecido $<$, lo denotaremos por $\text{in}_<(p)$.
- El *coeficiente dominante* de p será el coeficiente de $\text{in}(p)$ en p, y lo denotaremos por $\text{lc}_<(p)$
- Consiguientemente, el *término dominante* de p será el producto del monomio inicial de p por el coeficiente dominante de p; lo denotaremos por $\text{lt}_<(p)$.
- Definimos el *soporte de* p como el conjunto de monomios que forman el polinomio p, lo denotaremos por $\text{supp}(p)$.

Podemos definir una operación de *división* en nuestro anillo $\Bbbk[x_1, ..., x_n]$ con un orden monomial dado $<$. Vamos a enunciar el resultado teórico y a continuación haremos una prueba constructiva de como realizar la división.

3.3 Teorema. *Sea* $\Bbbk[x_1, ..., x_n]$ *un anillo dotado de un orden monomial* $<$*, sean* $f, f_1, ..., f_n \in \Bbbk[x_1, ..., x_n]$ *elementos no nulos.*

Entonces, existen polinomios $r, q_1, ..., q_n \in \Bbbk[x_1, ..., x_n]$ *tales que*

1. $f = q_1 f_1 + ... + q_n f_n + r$
2. $\forall x_1^{\alpha_1} ... x_n^{\alpha_n} \in \text{supp}(r), x_1^{\alpha_1} ... x_n^{\alpha_n} \notin (\text{in}_<(f_1), ..., \text{in}_<(f_n))$
3. *Si* $q_i \neq 0$ *entonces* $\text{in}_<(f) \geq \text{in}_<(q_i f_i)$

Demostración. Como hemos anunciando antes, vamos a dar una demostración constructiva del teorema. Para ello definimos el Algoritmo 2, que veremos a continuación.

Como el orden monomial es un bueno orden, el algoritmo termina y tanto r como los q_i verifican las condiciones 2 y 3.

□

Gracias al algoritmo de división podemos hablar de reducción de un polinomio o de *polinomio reducido.*

3.4 Definición. Sea $F = \{f_1, ..., f_n\}$ con $f, f_1, ..., f_n \in \Bbbk[x_1, ..., x_n]$ dotado de un orden monomial $<$ y sean $r, q_1, ..., q_n \in \Bbbk[x_1, ..., x_n]$ verificando las condiciones del teorema (3.3). Entonces decimos que r *es una reducción de* f *módulo* F y lo denotamos por $f \to_F r$.

Algorithm 2 División de polinomios

procedure DIV($f, f_1, ..., f_n \in (\Bbbk[x_1, ..., x_n], <)$)
  salida: $r, q_1, ..., q_n \in \Bbbk[x_1, ..., x_n]$
  for $i = 1$ TO n **do**
    $q_i \leftarrow 0$
  end for
  $r \leftarrow 0$
  $p \leftarrow f$
  while $p \neq 0$ **do**
    $i \leftarrow 1$
    $d \leftarrow 0$
    while $i \leq m$ AND $d = 0$ **do**
      if $\text{in}_<(f_i) | \text{in}_<(p)$ **then**
        $q_i \leftarrow q_i + \frac{\text{lt}_<(p)}{\text{lt}_<(f_i)}$
        $p \leftarrow p - \frac{\text{lt}_<(p)}{\text{lt}_<(f_i)} f_i$
        $d \leftarrow 1$
      else
        $i \leftarrow i + 1$
      end if
    end while
    if d $= 0$ **then**
      $p \leftarrow p - \text{lt}_<(p)$
      $r \leftarrow r + \text{lt}_<(p)$
    end if
  end while
  return: $r, q_1, ..., q_n$
end procedure

3.3. Bases de Gröbner

Comenzamos esta sección con una nueva definición.

3.5 Definición. Sean $\Bbbk[x_1, ..., x_n]$ un anillo dotado de un orden monomial $<$ e $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ un ideal. Definimos entonces el *ideal inicial de* $\mathfrak{I}$ *respecto de* $<$, denotado por $\text{in}_<(\mathfrak{I})$ como el ideal monomial engendrado por los monomios iniciales de todos los elementos de $\mathfrak{I}$:

$$\text{in}_<(\mathfrak{I}) = (\{\text{in}_<(f) \text{ tales que } f \in \mathfrak{I}\}).$$

Lo que nos lleva a definir una base de Gröbner.

3.6 Definición. Sean $\mathfrak{I}$ un ideal de $\Bbbk[x_1, ..., x_n]$, $<$ un orden monomial en $\Bbbk[x_1, ..., x_n]$ y G un subconjunto finito de $\mathfrak{I}$. Decimos que G es una *base de Gröbner* de $\mathfrak{I}$ si para todo $f \in \mathfrak{I}$ existe un $g \in G$ tal que $\text{in}(f) = \alpha\ \text{in}(g)$, con α un monomio de $\Bbbk[x_1, ..., x_n]$. Es decir,

$$\text{in}_<(\mathfrak{I}) = (\text{in}_<(g_1), ..., \text{in}_<(g_n))$$

con $G = \{g_1, ..., g_n\}$.

No sólo podemos afirmar que todo ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ admite una base de Gröbner, sino que además, vamos a dar un algoritmo para construir dicha base, el *algoritmo de Buchberger*. Antes definiremos un elemento necesario para el algoritmo: el S-polinomio.

3.7 Definición. Sean $f, g \in \Bbbk[x_1, ..., x_n]$ entonces definimos el *S-polinomio* de f y g por:

$$S(f, g) = \frac{\text{mcm}(\text{in}_<(f), \text{in}_<(g))}{\text{lt}_<(f)} f - \frac{\text{mcm}(\text{in}_<(f), \text{in}_<(g))}{\text{lt}_<(g)} g$$

Conocer el S- polinomio nos permite enunciar el Criterio de Buchberger.

3.8 Teorema. *Sean $\Bbbk[x_1, ..., x_n]$ un anillo de polinomios dotado de un orden monomial $<$ e $\mathfrak{I}$ un ideal de $\Bbbk[x_1, ..., x_n]$. Entonces las siguientes afirmaciones son equivalentes:*

1. *$G = \{g_1, ..., g_m\}$ es una base de Gröbner respecto del orden $<$.*
2. *El resto de la división de $S(f_i, f_j)$ por los elementos de G es 0, $\forall i, j$.*
3. *$S(f_i, f_j) \longrightarrow_G 0, \quad \forall i, j$.*

A continuación, vamos a dar una versión del algoritmo de Burchberger. Para ello, supongamos $\mathfrak{I}$ un ideal de $\Bbbk[x_1, ..., x_n]$ dado por un conjunto finito de generadores $F = (f_1, ..., f_m)$.

Nota. Una duda que se nos plantea al aplicar el algoritmo es si verdaderamente hay un momento en el que $S(f, g)$ sea igual a 0 para todo $f, g \in F$ o si al ir añadiendo polinomios a F podemos entrar en un bucle infinito.

La respuesta viene dada por el hecho de que $\Bbbk[x_1, ..., x_n]$ es noetheriano. Supongamos que siempre podemos añadir un f_{m+1} al conjunto $F = (f_1, ..., f_m)$ de tal manera que el monomio inicial de f_{m+1} no sea múltiplo de ninguno de los monomios iniciales de $(f_1, ..., f_m)$. Entonces, podemos crear la siguiente cadena ascendente:

$$\text{in}_<(f_1) \subset (\text{in}_<(f_1), \text{in}_<(f_2)) \subset (\text{in}_<(f_1), \text{in}_<(f_2), \text{in}_<(f_3)) \subset ...$$

Algorithm 3 Algoritmo de Buchberger

procedure DP0($f_1, ..., f_m \in (\Bbbk[x_1, ..., x_n], <)$)
  salida: $G = g_1, ..., g_t$
  $G \longleftarrow f_1, ..., f_m$
  while $G \neq G'$ **do**
    $G' \longleftarrow G$
    for $(p, q) \in G$ **do**
      $S \longleftarrow$ resto DIV($S(p, q), \{g_1, ..., g_t\}$)
      if $S \neq 0$ **then**
        $G \longleftarrow G \cup \{S\}$
      end if
    end for
  end while
  return: $G = g_1, ..., g_t$
end procedure

En algún paso del algoritmo, este ideal no podrás crecer más lo que significa que el Algoritmo 3 termina en un número finito de pasos.

3.9 Teorema. *Toda base de Gröbner de $\mathfrak{I}$ es un sistema de generadores de $\mathfrak{I}$.*

Demostración. Sea G una base de Gröbner de $\mathfrak{I}$, entonces $(G) \subset \mathfrak{I}$. Para ver que $\mathfrak{I} \subset (G)$ tomamos un elemento $f \in \mathfrak{I}$ y lo dividimos por los elementos de G. Obtenemos de esta manera una expresión del tipo

$$f = q_1 g_1 + ... + q_m g_m + r \tag{3.1}$$

con $q_1, ..., q_m, r$ polinomios de $\Bbbk[x_1, ..., x_n]$ verificando además, por la segunda tesis del teorema (3.3), que todo monomio $x_1^{\alpha_1} ... x_n^{\alpha_n}$ que pertenezca a $\text{supp}(r)$ no pertenece a $(\text{in}_<(g_1), ..., \text{in}_<(g_m)) = \text{in}_<(\mathfrak{I})$.

Luego si $r \neq 0$, entonces $\text{in}_<(r) \notin \text{in}_<(\mathfrak{I})$; absurdo, pues $r = f - (q_1 g_1 + ... + q_m g_m) \in \mathfrak{I}$. Así que $r = 0$ y $f \in (G)$.

□

Para que resulte más sencillo operar con una base de Gröbner introduciremos la siguiente proposición.

3.10 Proposición. *Sea $G = \{g_1, ..., g_m\}$ una base de Gröbner de un ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ y $f \in \Bbbk[x_1, ..., x_n]$. Entonces,*

$f \in \mathfrak{I} \iff$ *el resto de la división de f por los elementos de G es nulo.*

Demostración. Si el resto de la división de f por los elementos de G es nulo, entonces $f = q_1g_1 + ... + q_mg_m$, y por lo tanto $f \in (G)$. Por el teorema (3.9) $(G) = \mathfrak{I}$, así que $f \in \mathfrak{I}$ y hemos terminado.

Vamos a ver ahora cual es el resto de la división de f por $g_1, ..., g_m$ si $f \in \mathfrak{I}$. Supongamos que $f = q_1g_1+...+q_mg_m+r$ con $\forall x_1^{\alpha_1}...x_n^{\alpha_n} \in \text{supp}(r), x_1^{\alpha_1}...x_n^{\alpha_n} \notin (\text{in}_<(g_1), ..., \text{in}_<(g_n))$. Entonces $r \in \mathfrak{I}$, pues $r = f-q_1g_1+...+q_mg_m$ donde cada uno de los sumandos pertenece a $\mathfrak{I}$, pero $\text{in}_<(r) \notin (\text{in}_<(g_1), ..., \text{in}_<(g_n)) = \text{in}_<(\mathfrak{I})$ por definición de bases de Gróbner. Luego $\text{in}_<(r) \notin \text{in}_<(\mathfrak{I})$ pero $r \in \mathfrak{I}$, luego necesariamente $r = 0$.

□

El problema que nos planteamos a continuación es el siguiente: dada una base de Gröbner G de un ideal $\mathfrak{I}$, podemos añadir todos los elementos de $\mathfrak{I}$ que queramos a G y seguirá siendo una base de Gröbner. Por esta razón introducimos el concepto de *base de Gröbner minimal*.

3.11 Definición. Decimos que una base de Gröbner $G = \{g_1, ..., g_t\}$ de un ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x–n]$ es *minimal* si:

1. Todo polinomio de G tiene por coeficiente dominante el 1.
2. $(\text{in}_<(g_1), ..., \text{in}_<(g_{m-1}), \text{in}_<(g_{m+1}), ..., \text{in}_<(g_t)) \neq (\text{in}_<(g_1), ..., \text{in}_<(g_t))\forall 1 \leq m \leq t$.

Con esta definición resulta evidente que de toda base de Gröbner G de un ideal $\mathfrak{I}$ podemos extraer una base minimal. El algoritmo para realizar esta operación es muy similar al de obtención de una descomposición primaria minimal Algoritmo 1.

Sin embargo, la condición de que una base de Gröbner sea minimal no nos asegura su unicidad, para lo cual definiremos una *base de Gröbner reducida*.

3.12 Definición. Una base de Gröbner $G = \{g_1, ..., g_t\}$ de un ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ es *reducida* si verifica:

1. G es minimal.
2. Para todo $i \in (1, ..., t)$ se verifica que todo monomio de g_i no pertenece al ideal $(\text{in}_<(g_1), ..., \text{in}_<(g_{i-1}), \text{in}_<(g_{i+1}), ..., \text{in}_<(g_t))$

Ahora sí, podemos afirmar que:

3.13 Teorema. *Todo ideal no nulo de $\mathfrak{I}$ admite una única base de Gröbner reducida respecto de un orden monomial dado de $\Bbbk[x_1, ..., x_n]$.*

Demostración. Para ver la existencia daremos un algoritmo para obtener una base de Gröbner reducida respecto de una base minimal dada. Sea $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$, G una base de Gröbner reducida de $\mathfrak{I}$. Entonces construimos una base de Gröbner reducida de $\mathfrak{I}$ gracias a las propiedades que tiene el resto de la división de cada uno de los g_i entre $\{g_1, ..., \hat{g}_i, ..., g_t\}$. En particular, tenemos que cada uno de los monomios de r_i no pertenece a $\{g_1, ..., \hat{g}_i, ..., g_t\}$, luego si cambiamos cada g_i por el r_i correspondiente habremos logrado una base de Gröbner reducida para $\mathfrak{I}$.

A continuación presentamos el algoritmo.

Algorithm 4 Base de Gröbner reducida

1: **procedure** BGR($G = \{g_1, ..., g_t\}$ base de Gröbner minimal de $\mathfrak{I}$)
2: **salida:** $G = r_1, ..., r_t$ base de Gröbner reducida de $\mathfrak{I}$
3: **for** $i = 1$ TO t **do**
4: $r_i \longleftarrow$ resto DIV$(g_i, \{g_1, ..., \hat{g}_i, ..., g_t\})$
5: **end for**
6: **return:** $G = r_1, ..., r_t$
7: **end procedure**

Vamos a demostrar ahora la unicidad de la base. Para ello, supongamos que tenemos dos bases reducidas G, G' de $\mathfrak{I}$ respecto del mismo orden monomial $<$.

Tanto G como G' son minimales, por lo que el número de elementos de ambas bases coincide, y sus términos dominantes son iguales dos a dos. Tenemos entonces $G = \{g_1, ..., g_t\}$, $G' = \{g'_1, ..., g'_t\}$ con $\mathrm{lt}_<(g_i) = \mathrm{lt}_<(g'_i)$.

Si consideramos el polinomio $g_i - g'_i$, como $\mathrm{lt}_<(g_i) = \mathrm{lt}_<(g'_i)$, los términos dominantes se cancelan y tenemos que todo monomio x^α de $g_i - g'_i$ no se divide por g_i ni g'_i pero como ambas bases son reducidas tampoco se puede dividir por los demás generadores del ideal $\mathrm{in}_<(\mathfrak{I})$. Luego $x^\alpha \notin \mathrm{in}_<(\mathfrak{I})$, lo cual es absurdo, pues $g_i - g'_i \in \mathfrak{I}$, así que podemos concluir que $g_i - g'_i = 0$, lo que implica que $g_i = g'_i \ \ \forall i$.

□

Nota. La unicidad de la base de Gröbner reducida nos permite, entre otras cosas, determinar cuando dos ideales, $\mathfrak{I}, \mathfrak{G}$ de $\Bbbk[x_1, ..., x_n]$ son iguales.

3.4. Operaciones en ideales a través de las bases de Gröbner

A continuación presentaremos unas operaciones en ideales en las que las bases de Gröbner "se portan bien". Comenzamos con una proposición que nos ayudará a caracterizar las bases de Gröbner de distintos ideales.

3.14 Proposición ([GTZ, Proposition 3.1]). *Sea el anillo de polinomios* $\Bbbk[y_1, ..., y_n, x_1, ..., x_m]$ *dotado del orden monomial producto* $>$ *de* $>_1$ *en* $\Bbbk[x_1, ..., x_m]$ *y* $>_2$ *en* $\Bbbk[y_1, ..., y_n]$. *Sea* $\mathfrak{I}$ *un ideal de* $\Bbbk[y_1, ..., y_m, x_1, ..., x_n]$ *y* G *una base de Gröbner de* $\mathfrak{I}$ *respecto al orden* $>$. *Entonces:*

1. G *es una base de Gröbner de* $\mathfrak{I}$ *respecto al orden* $>_1$ *en el anillo de polinomios con coeficientes en* $\Bbbk[y_1, ..., y_n]$, $(\Bbbk[y_1, ..., y_n])[x_1, ..., x_m]$.

2. $G \cap \Bbbk[y_1, ..., y_n]$ *es una base de Gröbner para el ideal* $\mathfrak{I} \cap \Bbbk[y_1, ..., y_n]$ *con respecto al orden* $>_2$.

Demostración. 1. Por la definición de orden monomial producto tenemos que

$$\text{in}_>(\text{in}_{>_1}(f)) = \text{in}_>(f) \quad \forall f \in \Bbbk[y_1, ..., y_n, x_1, ..., x_m]$$

En particular, se verifica para todo $g \in G$.

$$\text{in}_>(\text{in}_{>_1}(G)) = \text{in}_>(G) = \text{in}_>(\mathfrak{I}) = \text{in}_>(\text{in}_{>_1}(\mathfrak{I}))$$

Como $\text{in}_>(\text{in}_{>_1}(G)) = \text{in}_>(\text{in}_{>_1}(\mathfrak{I}))$, entonces $\text{in}_{>_1}(G) = \text{in}_{>_1}(\mathfrak{I})$. Por la definición de base de Gröbner, tenemos que G es una base de Gröbner de $\mathfrak{I}$ en $(\Bbbk[y_1, ..., y_n])[x_1, ..., x_m]$.

2. Por la construcción del orden monomial producto, tenemos que $\text{in}_>(g) \in \Bbbk[y_1, ..., y_n] \iff g \in \Bbbk[y_1, ..., y_n]$. Luego,

$$\text{in}_>(G \cap \Bbbk[y_1, ..., y_n]) = \text{in}_>(G) \cap \Bbbk[y_1, ..., y_n]$$

$$= \text{in}_>(\mathfrak{I}) \cap \Bbbk[y_1, ..., y_n] = \text{in}_>(\mathfrak{I} \cap \Bbbk[y_1, ..., y_n])$$

y $G \cap \Bbbk[y_1, ..., y_n]$ es una base de Gröbner de $\mathfrak{I} \cap \Bbbk[y_1, ..., y_n]$ respecto a $>$. Como $>$ coincide con $>_2$ en $\Bbbk[y_1, ..., y_n]$, hemos terminado.

□

En el capítulo 3 vimos que el orden lexicográfico era un orden producto en las condiciones que especifica la proposición (3.14) para los órdenes $lex(x_1 > ... > x_t)$ y $lex(x_{t+1} > ... > x_n)$. Si consideramos la segunda parte de la

proposición en un anillo $\Bbbk[x_1, ..., x_n]$ con el orden lexicográfico obtenemos un resultado que se conoce como el **teorema de la eliminación de variables** o simplemente teorema de la eliminación.

3.15 Teorema (The Elimination Theorem [CLO, Theorem 2]). *Sea* $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ *un ideal y* G *una base de Gröbner de* $\mathfrak{I}$ *respecto al orden lexicográfico. Entonces, para todo* $0 \geq j \geq n$ *el conjunto*

$$G_j = G \cap \Bbbk[x_{j+1}, ..., x_n]$$

es una base de Gröbner del ideal de eliminación $\mathfrak{I} \cap \Bbbk[x_{j+1}, ..., x_n]$.

Antes de adentrarnos en las implicaciones que conlleva la proposición (3.14), recordamos brevemente la operación de *contraer un ideal*.

3.16 Definición. Dados dos anillos, $\mathfrak{R}$, $\mathfrak{S}$, un homomorfismo de anillos $f : \mathfrak{R} \longrightarrow \mathfrak{S}$, $\mathfrak{I}$ un ideal de $\mathfrak{S}$, entonces el *ideal contraído* de $\mathfrak{I}$ respecto de f es un ideal de $\mathfrak{R}$ que viene dado por $f^{-1}(\mathfrak{I}) = \mathfrak{I}^c$.

La segunda parte de la proposición (3.14) nos muestra como calcular la base de Gröbner de un ideal contraído por la aplicación inclusión:

$$\begin{array}{rccc} i: & \Bbbk[x_1, ..., x_d] & \hookrightarrow & \Bbbk[x_1, ..., x_d, x_{d+1}, ..., x_n] \\ & \mathfrak{I}^c = \mathfrak{I} \cap \Bbbk[x_1, ..., x_d] & \leftarrow & \mathfrak{I} \end{array}$$

Este proceso nos permite a su vez realizar unas cuantas operaciones que podemos expresar en términos de contracciones, veamos las más relevantes para el trabajo:

1. La intersección de dos ideales $\mathfrak{I} \cap \mathfrak{G}$ de $\Bbbk[x_1, ..., x_n]$.

   Este resultado viene del hecho de que podemos expresar una intersección de dos ideales como sigue: sea t una variable adicional a nuestro anillo $\Bbbk[x_1, ..., x_n]$, entonces:

   $$\mathfrak{I} \cap \mathfrak{G} = (\mathfrak{I}t + \mathfrak{G}(t-1)) \cap \Bbbk[x_1, ..., x_n]$$

   Aplicando la proposición (3.14), no tenemos más que calcular una base de Gröbner del ideal $(\mathfrak{I}t + \mathfrak{G}(t-1))$ en el anillo $\Bbbk[x_1, ..., x_n, t]$ e intersecarla con $\Bbbk[x_1, ..., x_n]$.

2. El cociente de dos ideales $(\mathfrak{I} : \mathfrak{G})$, con $\mathfrak{I}, \mathfrak{G}$ ideales de $\Bbbk[x_1, ..., x_n]$.

   Sea $\mathfrak{G} = (g_1, ..., g_n)$, entonces $(\mathfrak{I} : \mathfrak{G}) = \bigcap_{i=1}^{n} (\mathfrak{I} : g_i)$.

   Vamos a demostrar que $(\mathfrak{I} : g)g = \mathfrak{I} \cap (g)$:

- $(\mathfrak{I} : g)g \subseteq \mathfrak{I} \cap (g)$: sea $ag \in (\mathfrak{I} : g)g$, tenemos $a \in (\mathfrak{I} : g) \iff ag \in \mathfrak{I}$; luego $ag \in \mathfrak{I}$.

  Por otra parte, $ag \in (g)$ para todo $a \in \Bbbk[x_1, ..., x_n]$, en particular, para $a \in (\mathfrak{I} : g)$, así que $ag \in (g)$.

  Concluimos con $ag \in \mathfrak{I} \cap (g)$.
- $(\mathfrak{I} : g)g \supseteq \mathfrak{I} \cap (g)$: sea $a \in \mathfrak{I} \cap (g)$, como $a \in (g)$, podemos escribir $a = bg$. Para que se de la inclusión, solo necesitamos comprobar que $b \in (\mathfrak{I} : g)$, pero $b \in (\mathfrak{I} : g) \iff bg \in \mathfrak{I}$, y como $a = bg \in \mathfrak{I}$, hemos terminado.

Tenemos entonces que $(\mathfrak{I} : g)g = \mathfrak{I} \cap (g)$:, como $\Bbbk[x_1, ..., x_n]$ es un dominio de integridad, un sistema de generadores de $(\mathfrak{I} : g)$ vendrá dado al dividir cada generador de $\mathfrak{I} \cap (g)$ por g. Podemos calcular cada sistema de generadores de $(\mathfrak{I} : g)$ por el apartado anterior. Solo nos queda calcular $\bigcap_{i=1}^{n}(\mathfrak{I} : g_i)$, lo cual es posible también por el apartado anterior y obtendremos $(\mathfrak{I} : \mathfrak{G})$.

3. Dado un ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ y un elemento $f \in \Bbbk[x_1, ..., x_n]$, podemos construir la contracción de la localización de $\Bbbk[x_1, ..., x_n]$ con respecto a el elemento f. Si llamamos $\mathfrak{I}_f = \mathfrak{I}\Bbbk_f$, entonces podemos construir $\mathfrak{I}_f \cap \Bbbk$.

   Podemos expresar $\mathfrak{I}_f = (\mathfrak{I}t\Bbbk[x_1, ..., x_n, t] + (ft - 1)\Bbbk[x_1, ..., x_n, t])$ como ya hicimos en el apartado (1). Lo único que tenemos que hacer entonces es $(\mathfrak{I}t\Bbbk[x_1, ..., x_n, t] + (ft - 1)\Bbbk[x_1, ..., x_n, t]) \cap \Bbbk[x_1, ..., x_n]$, lo cual es posible.

3.5. Bases de Gröbner en ideales 0-dimensionales

En esta sección queremos presentar la noción de ideal 0-dimensional. Nuestro propósito, por consiguiente, no consiste en profundizar en la noción algebraica de dimensión, para lo cual proponemos la siguiente referencia [Eis, Chapter 8], sino presentar las primeras definiciones y notaciones relacionadas con los ideales 0-dimensionales y sus caracterización a través de las bases de Gröbner.

A lo largo de esta sección $\Bbbk$ será un cuerpo. Comenzamos definiendo un ideal $\mathfrak{I}$ 0-dimensional.

3.17 Definición. Decimos que un ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ es *0-dimensional* si $V(\mathfrak{I})$ tiene un número finito de puntos.

Podemos caracterizar los ideales 0-dimensionales por la siguiente proposición.

3.18 Proposición. *Sea $\mathfrak{I}$ un ideal de $\subset \Bbbk[x_1, ..., x_n]$, entonces $\mathfrak{I}$ es 0-dimensional si y sólo si la dimensión de $\frac{\Bbbk[x_1,...,x_n]}{\mathfrak{I}}$ como $\Bbbk$-espacio vectorial es finita.*

Demostración. Podemos ver una demostración en [CLO, Theorem 6].

□

Los ideales 0-dimensionales de $\Bbbk[x_1, ..., x_n]$ tienen las siguientes propiedades.

3.19 Proposición. *Todos los primos asociados de un ideal 0-dimensional son maximales.*

Demostración. Encontramos una demostración en [Eis, Theorem 2.14.].

□

Aprovechamos esta proposición para dar la definición de *dimensión de Krull*.

3.20 Definición. La *dimensión de Krull* o simplemente dimensión de un anillo $\mathfrak{R}$ es la máxima longitud de una cadena de ideales primos en $\mathfrak{R}$ sin contar con el ideal (0) ni con el anillo total.

Una vez definida la dimensión en un anillo, vamos a definir la dimensión de sus ideales.

3.21 Definición. Sea $\mathfrak{R}$ una anillo e $\mathfrak{I}$ un ideal propio de $\mathfrak{R}$, la dimensión de $\mathfrak{I}$ es la dimensión del anillo cociente $\frac{\mathfrak{R}}{\mathfrak{I}}$.

$$\dim(\mathfrak{I}) = \dim(\frac{\mathfrak{R}}{\mathfrak{I}})$$

Gracias a la proposición (3.19) podemos ver de donde proviene el nombre de ideales 0-dimensionales, son precisamente aquellos ideales cuya dimensión de Krull es igual a cero. Continuamos con las propiedades de los ideales 0-dimensionales.

3.22 Proposición. *Sea $\mathfrak{I}$ un ideal 0-dimensional de $\Bbbk[x_1, ..., x_n]$, entonces:*

$$\mathfrak{I} \textit{ es primario} \iff \mathrm{Rad}(\mathfrak{I}) \textit{ es primo}$$

Demostración. Sabemos que si $\mathfrak{I}$ es primario, entonces $\text{Rad}(\mathfrak{I})$ es primo; para ver la otra contención, consideremos el ideal primo $\text{Rad}(\mathfrak{I})$, que es un primo asociado del ideal 0-dimensional $\mathfrak{I}$. Por la proposición (3.19), $\text{Rad}(\mathfrak{I})$ es maximal, y entonces necesariamente $\mathfrak{I}$ es primario.

□

3.23 Proposición. *Sean $\mathfrak{I}$ un ideal de $\Bbbk[x_1, ..., x_n]$ dotado del orden monomial lexicográfico $>$ y G una base de Gröbner $\mathfrak{I}$.*

Entonces $\mathfrak{I}$ es 0-dimensional si y solo si para cada $1 \leq i \leq n$ existe un elemento g de G cuyo término principal es una potencia de x_i.

$$\text{lt}_>(g) = x_i^{m_i}$$

Antes de demostrar la proposición (3.23) vamos a enunciar un pequeño lema.

3.24 Lema. *Sean $\mathfrak{I}$ un ideal 0-dimensional de $\Bbbk[x_1, ..., x_n]$ dotado del orden monomial lexicográfico $>$; entonces $\forall i \in (2, ..., n)$ $\mathfrak{I} \cap \Bbbk[x_i, ..., x_n]$ es un ideal 0-dimensional en $\Bbbk[x_i, ..., x_n]$.*

Demostración (de la proposición (3.23)). Comenzamos suponiendo que $\mathfrak{I}$ es 0-dimensional y razonaremos por reducción al absurdo.

Supongamos que no existe ningún $g \in G$ tal que $\text{lt}_<(g) = x_1^{m_1}$. Como estamos considerando el orden lexicográfico, esto implica que en G no hay términos en x_1, luego $G \subset \Bbbk[x_2, ..., x_n]$. Entonces, nuestro ideal $\mathfrak{I}$ está contenido en el ideal primo $(x_2, ..., x_n)$, que a su vez está contenido en $(x_1, ..., x_n)$. Luego $\mathfrak{I}$ no puede ser 0-dimensional por la definición de la dimensión de Krull.

Supongamos entonces que no existe ningún $g \in G$ tal que $\text{lt}_<(g) = x_2^{m_2}$. Lo que hacemos en este caso es considerar el ideal $\mathfrak{I} \cap \Bbbk[x_2, ..., x_n]$, que por la proposición (3.14) sabemos que viene dado por $G \cap \Bbbk[x_2, ..., x_n]$ y razonar de manera idéntica a como hemos hecho con x_1. Utilizando el lema (3.24) volvemos a llegar a un absurdo.

Podemos iterar este proceso para $i \in (1, ..., n)$. Cuando llegamos al caso $\mathfrak{I} \cap \Bbbk[x_n] = (0)$ aplicamos directamente el lema (3.24) y llegamos de nuevo a un absurdo.

Luego si $\mathfrak{I}$ es un ideal 0-dimensional, entonces para cada $1 \leq i \leq s$ existe un elemento g de G cuyo término principal es una potencia de x_i.

Sea ahora $\mathfrak{I}$ un ideal de $\Bbbk[x_1, ..., x_n]$ tal que para cada $1 \leq i \leq n$ existe un elemento g de G cuyo término principal es una potencia de x_i. Entonces, como $x_i^{m_i} \in \text{in}_<(\mathfrak{I})$, $x_i \in \text{Rad}(\mathfrak{I})$ para cada $1 \leq i \leq n$, luego $(x_1, ..., x_n) \subset \text{Rad}(\mathfrak{I})$ y por tanto, el ideal es 0-dimensional.

□

Gracias a esta proposición podemos caracterizar completamente a los ideales primos y primarios de $\Bbbk[x_1, ..., x_n]$ a través de una de sus bases de Gröbner.

3.25 Proposición. *Sea $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ un ideal 0-dimensional., sea G una base de Gröbner reducida para $\mathfrak{I}$ con respecto al orden lexicográfico, y sean $\{g_1, ..., g_n\} \in G$ verificando la propiedad en (3.23). Entonces,*

$\mathfrak{I}$ es primo $\iff$ $\forall i$, g_i es irreducible módulo $\mathfrak{I} \cap \Bbbk[x_{i+1}, ..., x_n]$.

Demostración. Proponemos la demostración de [GTZ, Proposition 5.9].

□

Esta proposición nos indica que, dado un ideal primo $\mathfrak{P}$ con el orden monomial $\text{lex}(x_1 > ... > x_n)$, podemos caracterizarlo por una base de Gröbner de la forma :

$$G = \{x_1 + p_1(x_2, ..., x_n), x_2 + p_2(x_3, ..., x_n), ..., x_{n-1} + p_{n-1}(x_n), p_n(x_n)\} \tag{3.2}$$

Más adelante veremos que si $\mathfrak{P}$ viene dado de una forma particular que denotaremos por **estar en posición general**, entonces podemos dar una base de Gröbner de $\mathfrak{P}$ de la forma:

$$G' = \{x_1 + p_1(x_n), x_2 + p_2(x_n), ..., x_{n-1} + p_{n-1}(x_n), p_n(x_n)\} \tag{3.3}$$

3.26 Proposición. *Sea $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ un ideal 0-dimensional. Sea G una base de Gröbner reducida para $\mathfrak{I}$ con respecto al orden lexicográfico, y sean $\{g_1, ..., g_n\} \in G$ verificando la propiedad (3.23). Entonces,*

$\mathfrak{I}$ es primario $\iff$ $\forall i$, g_i es una potencia de un polinomio irreducible módulo $\text{Rad}(\mathfrak{I} \cap \Bbbk[x_{i+1}, ..., x_n])$.

Demostración. Vamos a razonar por inducción en el las variables. Comenzamos definiendo $\mathfrak{R}' = \Bbbk[x_2, ..., x_n]$ e $\mathfrak{I}' = \mathfrak{I} \cap \Bbbk[x_2, ..., x_n]$ y planteamos nuestra hipótesis de inducción.

Hipótesis: $\mathfrak{I}$ es primario $\iff$ $\mathfrak{I}'$ es primario y g_1 es potencia de un polinomio irreducible módulo $\text{Rad}(\mathfrak{I}')$.

Si conseguimos demostrar nuestra hipótesis, tendremos que (3.26) es cierta para $i = 1$ y además, como $\mathfrak{I}'$ también es primario, podemos volver a aplicar la hipótesis para $i = 2$.

Como $\mathfrak{I}$ es primario, entonces $\mathfrak{I}'$ también es primario. Consideremos entonces una base de Gröbner G de $\mathfrak{I}'$, por la proposición (3.26) $\exists g_1 \in G$ tal que $\mathrm{lt}_<(g_1) = x_1^{m_1}$. Sea $h \in G$, $h \neq g_1$, entonces h tiene grado menor que m_1 en x_1. Por un resultado que podemos encontrar en [GTZ, Lemma 5.6] podemos afirmar que $h = 0$ módulo $\mathrm{Rad}(\mathfrak{I}')$, con lo que g_i es irreducible módulo $\mathrm{Rad}(\mathfrak{I}')$.

Además, $\mathrm{Rad}(\mathfrak{I}) = \mathrm{Rad}(\mathfrak{I}', g_1) = \mathrm{Rad}(g_1, \mathrm{Rad}(\mathfrak{I}'))$. Por la proposición (3.22), como $\mathfrak{I}$ es primario, $\mathrm{Rad}(()\mathfrak{I})$ es primo, luego $\mathrm{Rad}(g_1, \mathrm{Rad}(\mathfrak{I}'))$ es primo, lo que implica que $(g_1, \mathrm{Rad}(\mathfrak{I}'))$ es primario, así que $\mathrm{Rad}(\mathfrak{I}')$ es primo y podemos concluir que $\mathfrak{I}'$ es primario.

□

3.27 Corolario. *Si estamos en la situación anterior e* $\mathfrak{I}$ *es primo, entonces todo* $h \in G \cap \Bbbk[x_i, ..., x_n]$ *es congruente con* 0 *módulo* $\mathrm{Rad}(\mathfrak{I} \cap \Bbbk[x_{i+1}, ..., x_n])$.

Al igual que sucedía con los ideales primos, también podemos caracterizar a un ideal primario $\mathfrak{Q}$ dotado del orden monomial lexicográfico por una base de Gröbner de la forma :

(3.4)

$$G = \{x_1^{m_1} + p_1(x_2, ..., x_n), x_2^{m_2} + p_2(x_3, ..., x_n), ..., x_{n-1}^{m_{n-1}} + p_{n-1}(x_n), p_n(x_n)\}$$

Capítulo 4

Construcción de una descomposición primaria

La belleza es la primera prueba; no hay lugar permanente en el mundo para unas matemáticas feas.
G.H.Hardy

El capítulo que comenzamos ahora constituye el núcleo fundamental del trabajo. Una vez presentados los conceptos de descomposición primaria y bases de Gröbner, nuestra meta es dar un algoritmo que nos permita calcular una descomposición primaria de un ideal propio $\mathfrak{I}$ del anillo de polinomios con coeficientes en un cuerpo $\Bbbk[x_1, ..., x_n]$.

Como acabamos de comentar, a lo largo de este capítulo trabajaremos en el anillo $\Bbbk[x_1, ..., x_n]$, donde $\Bbbk$ será un cuerpo cualquiera, y por lo tanto $\Bbbk[x_1, ..., x_n]$ será un **anillo notheriano**. Además, todo anillo de polinomios con coeficientes en un cuerpo es un **dominio de integridad**, lo que quiere decir que $\Bbbk[x_1, ..., x_n]$ no tiene elementos divisores de cero.

En ocasiones, también trabajaremos con los polinomios de $\mathfrak{R}[x_1, ..., x_n]$ donde $\mathfrak{R}$ será un anillo conmutativo, unitario y noetheriano.

[GTZ] ofrece una solución a nuestro problema para el caso en el que el ideal $\mathfrak{I}$ sea 0-dimensional; de hecho, nos propone dos soluciones, una cuando el anillo de coeficientes es un cuerpo de característica cero y otra cuando el anillo de coeficientes es un anillo noetheriano. Para el caso no 0-dimensional, nos propone pasar de un ideal no 0-dimensional hasta uno 0-dimensional a través de una inducción por la localización en los primos principales.

Todos los métodos aquí presentados se encuentran recogidos en otros textos de los que también hemos hecho uso para la elaboración de este capítulo.

Cabe destacar el texto [Swa1], que ofrece una visión esquemática del algoritmo para descomponer un ideal propio cualquiera de $\Bbbk[x_1, ..., x_n]$, así como [DGP] que recopila varios algoritmos de descomposición primaria y ofrece una versión implementada en el programa SINGULAR.

A lo largo de todo el capítulo, suponemos que podemos descomponer todo elemento $f \in \Bbbk[x_1, ..., x_n]$ como producto de factores irreducibles. Así mismo, nos limitaremos a un único orden monomial, el lexicográfico.

La estructura del capítulo será la siguiente: dedicaremos una sección a cada uno de los tres métodos principales; en cada una de las secciones desarrollaremos la teoría que fundamenta el método, representaremos de modo esquemático cada uno de los algoritmos y finalmente daremos un ejemplo de su implementación utilizando el programa SINGULAR.

4.1. Descomposición primaria de ideales 0-dimensionales

En esta sección presentaremos un método para calcular una descomposición primaria de un ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ 0-dimensional.

El método que presentamos no es exclusivo de $\Bbbk[x_1, ..., x_n]$, sino que en su versión original en [GTZ] está descrito para $\mathfrak{R}[x_1, ..., x_n]$, con $\mathfrak{R}$ un anillo noetheriano.

Sin embargo, nosotros lo implementaremos sólo para el caso de ideales en $\Bbbk[x_1, ..., x_n]$, ya que a lo largo de esta sección haremos uso de muchos de los resultados vistos en el capítulo tres que tienen sentido solo en el caso del anillo de polinomios con coeficientes en un cuerpo.

Bien es cierto, que la forma del algoritmo (recursivo en la dimensión) a veces nos obligará a trabajar en un anillo de polinomios con coeficientes en otro anillo de polinomios. Cuando llegue el caso, utilizaremos diferentes tácticas para remediarlo: a veces pasaremos a trabajar en el cuerpo residual del anillo cuando necesitemos calcular una base de Gröbner de un ideal del anillo; otras veces podremos extender resultados vistos en $\Bbbk[x_1, ..., x_n]$ a $\mathfrak{R}[x_1, ..., x_n]$, en el caso en que $\mathfrak{R}$ sea un dominio de ideales principales, etc.

Argumentos y *modus operandi*

Consideramos nuestro cuerpo $\Bbbk$; un conjunto de variables $x = (x_1, ..., x_n)$ y un ideal $\mathfrak{I}$ de $\Bbbk[x]$ 0-dimensional.

A través de este método, podremos calcular una familia de ideales primarios en $\Bbbk[x]$ cuya intersección será $\mathfrak{I}$.

Vamos a proceder de forma recursiva, disminuyendo el número de variables hasta llegar al cuerpo $\Bbbk$, en ese caso, tendremos o bien $\mathfrak{I} = (0)$ o bien $\mathfrak{I} = \Bbbk$, con lo que habremos acabado.

Comenzamos considerando el ideal $\mathfrak{I}' = \mathfrak{I} \cap \Bbbk[x_n]$ y calculamos una base de Gröbner minimal de $\mathfrak{I}'$ a la que llamaremos G. Podemos hacerlo en virtud de la proposición (3.14). Como $\Bbbk[x_n]$ es un dominio de ideales principales, entonces tendremos $G = \{g\}$.

Descomponemos el elemento g como producto de factores irreducibles,

$$g = p_1^{s_1} ... p_n^{s_n}$$

y para cada $i \in (1, ..., n)$ consideramos los ideales

$$\mathfrak{I}_i = (p_i^{s_i}, \mathfrak{I})$$

Tenemos entonces $\mathfrak{I} = \bigcap_{i=1}^{n} \mathfrak{I}_i$. Si iteramos este proceso, esta vez con los siguientes datos, obtendremos la deseada descomposición primaria:

- $\Bbbk[x_n]$ como anillo de coeficientes.
- $x = (x_1, ..., x_{n-1})$ son las nuevas variables. Podemos observar claramente como el algoritmo utiliza una inducción en la dimensión o número de variables.
- $\mathfrak{I}_i$ ideal 0-dimensional de $(\Bbbk[x_n])[x_1, ..., x_{n-1}]$.

  Demostración. $\mathfrak{I}$ es un ideal 0-dimensional en $\Bbbk[x_1, ..., x_n]$, luego $\mathfrak{I}_i \supset \mathfrak{I}$ también es un ideal 0-dimensional en $\Bbbk[x_1, ..., x_n]$. En particular, $\mathfrak{I}_i$ es 0-dimensional en $(\Bbbk[x_n])[x_1, ..., x_{n-1}]$.

Algorithm 5 Descomposición de un ideal 0-dimensional

procedure DP0($\Bbbk$: cuerpo; $x = (x_1, ..., x_n)$: variables; $\mathfrak{I}$: ideal 0 dimensional de $\Bbbk[x]$)
  salida: $\{(\mathfrak{Q}_1, ..., \mathfrak{Q}_m\}$ ideales de $\Bbbk[x]$ tales que $\forall i$ $\mathfrak{Q}_i$ es $\mathfrak{m}_i$-primario y $\bigcap_{i=1}^{m} \mathfrak{Q}_i = \mathfrak{I}$
  if $n = 0$ **then**
    return $\{\mathfrak{I}\}$
  end if
  calcular G: base de Gröbner reducida para $\mathfrak{I} \cap \Bbbk[x_n]$
  - Calcular base de Gröbner de $\mathfrak{I}$. *Algoritmo Buchberger* (3)
  - Por (3.14) podemos calcular $\mathfrak{I} \cap \Bbbk[x_n]$
  - $G = \{g\}$.

  descomponer: $g = p_1^{s_1} ... p_n^{s_n}$ en $\Bbbk[x_n]$
  $\mathfrak{I}_i \leftarrow (p_i^{s_i}, \mathfrak{I})$
  return: $\bigcup_{i=1}^{n}$ DP0($\Bbbk[x_n]; x = (x_1, ..., x_{n-1}); \mathfrak{I}_i$)
end procedure

Algoritmo

Nota. Podemos encontrar una versión mejorada de este algoritmo en [DGP], que nos ofrece un programa listo para ser ejecutado en SINGULAR. Las mejoras más notables de este algoritmo consisten en una reducción del número de operaciones al comprobar la primarialidad de cada $\mathfrak{I}_i$ y en caso afirmativo, unirlo directamente a la lista de salida.

Nota. Al actuar de forma recusiva, podemos encontrarnos con un problema al querer descomponer el elemento g como producto de factores irreducibles, ya que como estamos en un anillo no tenemos asegurada la posibilidad de descomponer un elemento, así que llegado el caso, trabajaremos en el cuerpo de fracciones del anillo.

Nota. También puede suponer un problema el calcular una base de Gröbner de un ideal si el anillo de coeficientes no es un cuerpo, de nuevo solucionamos dicho problema pasando al cuerpo de fracciones del anillo correspondiente. Veremos todo esto en la implementación del algoritmo.

Podemos simplificar este algoritmo si nuestro cuerpo de coeficientes $\Bbbk$ es un cuerpo de característica 0. A este caso dedicamos la siguiente sección.

Ejemplo

Consideramos el cuerpo de los números racionales $\mathbb{Q}$ y el anillo en tres variables $\mathbb{Q}[x, y, z]$, sea $\mathfrak{I} = (y^2z^2 - x^2y^3 - xz^3 + x^3yz, y^2z - xz^2, z + y, x + y^3) \subset \mathbb{Q}[x, y, z]$. Vamos a implementar el algoritmo DP0 paso a paso en el programa SINGULAR.

Ante todo, vamos a pedir que la base de Gröbner sea reducida, y a cargar la librería `primdec.lib`.

```
> option(redSB);
> LIB "primdec.lib";
```

A continuación, definimos nuestro anillo $\mathbb{Q}[x, y, z]$ y el ideal $\mathfrak{I}$.

```
> ring R=0,(x,y,z),lp;
> R;
//   characteristic : 0
//   number of vars : 3
//        block   1 : ordering lp
//                  : names    x y z
//        block   2 : ordering C
> ideal I = (y2z2-x2y3-xz3+x3yz , y2z-xz2,z+y,x+y3);
> I;
I[1]=x3yz-x2y3-xz3+y2z2
I[2]=-xz2+y2z
I[3]=y+z
I[4]=x+y3
```

Volvemos a definir nuestro ideal esta vez a través de su base de Gröbner reducida.

```
> I = std(I);
> I;
I[1]=z5-z3
I[2]=y+z
I[3]=x-z3
```

Y comprobamos que $\mathfrak{I}$ es un ideal 0-dimensional.

```
> dim(I);
0
```

Como $n \neq 0$,si seguimos el orden establecido en el algoritmo tenemos que calcular una base de Gröbner para $\mathfrak{I} \cap \mathbb{Q}[z] = (z^5 - z^3)$. A continuación descomponemos $g = z^5 - z^3 = z^3(z-1)(z+1)$, y definimos los nuevos ideales $\mathfrak{I}_1 = (\mathfrak{I}, z^3)$, $\mathfrak{I}_2 = (\mathfrak{I}, z-1)$ e $\mathfrak{I}_3 = (\mathfrak{I}, z+1)$.

```
> ideal I1 = (y2z2-x2y3-xz3+x3yz , y2z-xz2,z+y,x+y3,z^3);
> I1=std(I1);
> I1;
I1[1]=z3
I1[2]=y+z
I1[3]=x

> ideal I2 = (y2z2-x2y3-xz3+x3yz , y2z-xz2,z+y,x+y3,z-1);
> I2=std(I2);
> I2;
I2[1]=z-1
I2[2]=y+z
I2[3]=x-z

> ideal I3 = (y2z2-x2y3-xz3+x3yz , y2z-xz2,z+y,x+y3,z+1);
> I3=std(I3);
> I3;
I3[1]=z+1
I3[2]=y+z
I3[3]=x-z
```

Y volvemos a comenzar el procedimiento. Consideraremos esta vez los ideales $\mathfrak{I}_1$, $\mathfrak{I}_2$ e $\mathfrak{I}_3$ en el anillo $\mathbb{Q}(z)[x, y]$. Comenzamos definiendo el ideal $\mathfrak{I}_1$.

```
> ring R=(0,z),(x,y),lp;
> R;
//   characteristic : 0
//   1 parameter    : z
//   minpoly        : 0
//   number of vars : 2
//        block   1 : ordering lp
//                  : names    x y
//        block   2 : ordering C

> ideal I1 = (z2*y2-x2y3-x*z^3+x3y*z , y2*z-x*z^2,z+y,x+y3,z^3);
> I1;
```

```
I1[1]=(z)*x3y-x2y3+(-z3)*x+(z2)*y2
I1[2]=(-z2)*x+(z)*y2
I1[3]=y+(z)
I1[4]=x+y3
I1[5]=(z3)
> I1= std(I1);
> I1;
I1[1]=1
```

Tenemos que $\mathfrak{I}_1$ es el ideal total en $\mathbb{Q}(z)[x,y]$, así que no vamos a poder descomponerlo más y ya tenemos el primer elemento de nuestra descomposición primaria: $\mathfrak{I}_1$.

Continuamos trabajando ahora con $\mathfrak{I}_2$.

```
> ideal I2 = (z2*y2-x2y3-x*z^3+x3y*z , y2*z-x*z^2,z+y,x+y3,z-1);
> I2;
I2[1]=(z)*x3y-x2y3+(-z3)*x+(z2)*y2
I2[2]=(-z2)*x+(z)*y2
I2[3]=y+(z)
I2[4]=x+y3
I2[5]=(z-1)
> I2 = std(I2);
> I2;
I2[1]=1
```

Vemos que el ideal $\mathfrak{I}_2$ en $\mathbb{Q}(z)[x,y]$ también es el anillo total, así que comprobamos lo que sucede con $\mathfrak{I}_3$.

```
> ideal I3 = (z2*y2-x2y3-x*z^3+x3y*z , y2*z-x*z^2,z+y,x+y3,z+1);
> I3;
I3[1]=(z)*x3y-x2y3+(-z3)*x+(z2)*y2
I3[2]=(-z2)*x+(z)*y2
I3[3]=y+(z)
I3[4]=x+y3
I3[5]=(z+1)
> I3 = std(I3);
> I3;
I3[1]=1
```

Obtenemos de nuevo el mismo resultado, así que podemos concluir que hemos finalizado nuestra descomposición primaria, que está formada precisamente por los ideales $\mathfrak{I}_1$, $\mathfrak{I}_2$ e $\mathfrak{I}_3$.

(4.1) $\mathfrak{I} = \mathfrak{I}_1 \cap \mathfrak{I}_2 \cap \mathfrak{I}_3 = (z^3, y+z, x) \cap (z-1, y+z, x-z) \cap (z+1, y+z, x-z)$

Vamos a comprobar que interesección de $\mathfrak{I}_1$, $\mathfrak{I}_2$ e $\mathfrak{I}_3$ es el ideal $\mathfrak{I}$.

```
> ideal J = intersect(I1,I2,I3);
> J;
J[1]=y+z
J[2]=x2-xz
J[3]=-x+z3
J[4]=xz2-x
> J = std(J);
> J;
J[1]=z5-z3
J[2]=y+z
J[3]=x-z3
```

Luego efectivamente, $\mathfrak{I} = J$ y hemos obtenido una descomposición primaria de $\mathfrak{I}$.

Para terminar el ejemplo, podemos ver que si aplicamos directamente el comando `primdecGTZ`, obtenemos la misma descomposición primaria, aunque los generadores de cada ideal $\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3$ son distintos a los que hemos obtenido.

```
> primdecGTZ(I);
[1]:
   [1]:
      _[1]=z3
      _[2]=y+z
      _[3]=x-z3
   [2]:
      _[1]=z
      _[2]=y+z
      _[3]=x-z3
[2]:
   [1]:
      _[1]=z-1
      _[2]=y+z
      _[3]=x-z3
   [2]:
      _[1]=z-1
      _[2]=y+z
      _[3]=x-z3
[3]:
   [1]:
```

```
   _[1]=z+1
   _[2]=y+z
   _[3]=x-z3
[2]:
   _[1]=z+1
   _[2]=y+z
   _[3]=x-z3
```

$$\mathfrak{I} = (z^3, y+z, x-z^3) \cap (z-1, y+z, x-z^3) \cap (z+1, y+z, x-z^3) \tag{4.2}$$

Para ver que las descomposiciones primarias (4.1) y (4.2) son iguales, llamemos $\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3$ a los ideales que forman (4.1) e $\mathfrak{I}'_1, \mathfrak{I}'_2, \mathfrak{I}'_3$ a aquellos de (4.2). Entonces:

1. $\mathfrak{I}'_1 = \mathfrak{I}_1$, solo hace falta obtener su base de Gröbner reducida.

```
> ideal I'1 = z3,y+z,x-z3;
> I'1 = std(I'1);
> I'1;
I'1[1]=z3
I'1[2]=y+z
I'1[3]=x
```

2. $\mathfrak{I}'_2 = \mathfrak{I}_2$, en este caso nos hará falta calcularla las bases reducidas de ambos ideales.

```
> ideal I'2 = z-1,y+z,x-z3;
> I'2 = std(I'2);
> I'2;
I'2[1]=z-1
I'2[2]=y+1
I'2[3]=x-1
```

```
> ideal I2 = z-1,y+z,x-z;
> I2 = std(I22);
> I22;
I2[1]=z-1
I2[2]=y+1
I2[3]=x-1
```

3. $\mathfrak{I}'_3 = \mathfrak{I}_3$, actuamos de la misma forma que en el caso anterior.

```
> ideal I'3 = z+1,y+z,x-z3;
> I'3 = std(I'3);
> I'3;
I'3[1]=z+1
I'3[2]=y-1
I'3[3]=x+1

> ideal I3 = z+1,y+z,x-z;
> I3 = std(I3);
> I3;
I3[1]=z+1
I3[2]=y-1
I3[3]=x+1
```

Podemos concluir que tenemos la misma descomposición primaria.

4.2. Descomposición primaria de ideales 0-dimensionales sobre un cuerpo de característica 0

Tenemos un caso particular de descomposición primaria de un ideal 0-dimensional cuando el anillo de coeficientes es un cuerpo $\Bbbk$ de **característica 0**. En ese caso, el algoritmo anterior se simplifica, tal y como veremos a continuación.

Comenzamos la sección introduciendo una noción nueva: **estar en posición general**.

Consideremos un ideal $\mathfrak{I}$ primo, 0-dimensional de $\Bbbk[x_1, ..., x_n]$. Entonces, por la proposición (3.25), $\mathfrak{I}$ tiene una base de Gröbner minimal de la forma:

$$G = \{g_1, ..., g_n\} = \{x_1 + p_1(x_2, ..., x_n), x_2 + p_2(x_3, ..., x_n), ..., x_{n-1}+$$

$$+p_{n-1}(x_n), p_n(x_n)\}$$

Un cambio de coordenadas en $\Bbbk[x_1, ..., x_n]$ es un automorfismo lineal y biyectivo. Se verifica que para *casi todos* los cambios de coordenadas de $\Bbbk[x_1, ..., x_n]$, g_i es de la forma:

$$g_i = x_i - p_i(x_n) \text{ para } 1 \leq i < n$$

Nota. Esto solo ocurre cuando la característica del cuerpo es 0, sino, el término *casi todo* carece de sentido.

4.1 Definición. Sea $\mathfrak{I}$ un ideal primo, 0-dimensional de $\Bbbk[x_1, ..., x_n]$ y $G = \{g_1(x_1, ..., x_n), g_2(x_2, ..., x_n), ..., g_n(x_n)\}$ una base de Gröbner minimal de $\mathfrak{I}$ decimos que $\mathfrak{I}$ *está en posición general* si se verifica

$$g_i = x_i - p_i(x_n) \text{ para } 1 \leq i < n$$

En el caso de un ideal general (no necesariamente primo) en cambio tenemos lo siguiente.

4.2 Definición. Sea $\mathfrak{I}$ un ideal propio, 0-dimensional de $\Bbbk[x_1, ..., x_n]$, decimos que $\mathfrak{I}$ *está en posición general* si todos sus primos asociados están en posición general y las contracciones de los primos asociados a $\Bbbk[x_n]$ son dos a dos comaximales.

Si tenemos un ideal 0-dimensional primario $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ que no esté en posición general, podemos transformarlo en uno que esté en posición general mediante un cambio de coordenadas.

4.3 Proposición ([GP, Proposition 4.2.2.])**.** *Sea $\Bbbk$ un cuerpo de característica o, y sea $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ un ideal 0-dimensional. Entonces existe un conjunto abierto de Zariski no vacío $U \subset \Bbbk^{n-1}$ tal que para todo $a = (a_1, ..., a_{n-1}) \in U$ el cambio de coordenadas $\phi_a : \Bbbk[x_1, ..., x_n] \longrightarrow \Bbbk[x_1, ..., x_n]$ definido por $\phi_a(x_i) = x_i$ si $i < n$ y*

$$\phi_a(x_n) = x_n + \sum_{i=1}^{n-1} a_i x_i$$

tiene la propiedad de que $\phi_a(\mathfrak{I})$ está en posición general con respecto al orden lexicográfico.

Argumentos y *modus operandi*

Trabajaremos en el anillo $\Bbbk[x_1, ..., x_n]$ dotado del orden monomial lexicográfico y las bases de Gröbner de los ideales $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ serán reducidas, salvo que indiquemos lo contrario.

Sea $\mathfrak{I}$ un ideal no primario, si $\mathfrak{I}$ está en posición general consideramos $\mathfrak{I} \cap \Bbbk[x_n]$ y calculamos una base de Gröbner minimal de $\mathfrak{I} \cap \Bbbk[x_n]$, siempre en virtud de (3.14). La base obtenida será de la forma $G = g(x_n)$, calculamos

la descomposición en factores irreducibles de g, $g = p_1^{s_1}...p_n^{s_n}$ y consideramos los ideales $\mathfrak{I}_i = (\mathfrak{I}, p_i^{s_i})$.

Entonces $\{(\mathfrak{I}_i)_{i=1}^n\}$ es una descomposición de $\mathfrak{I}$, pues $\bigcap_{i=1}^n \mathfrak{I}_i = \bigcap_{i=1}^n (\mathfrak{I}, p_i^{s_i}) = \mathfrak{I}$. Vamos a ver que además que cada $\mathfrak{I}_i$ es un ideal primario:

- $\mathfrak{I}_i$ ideal 0-dimensional, pues $\mathfrak{I}_i$ contiene a $\mathfrak{I}$, ideal 0-dimensional.
- $\mathfrak{I}_i$ está contenido en exactamente un ideal primo, pues si $\mathfrak{I}$ está en posición general, entonces $\mathfrak{I}_i$ también está en posición general, ya que el factor $p_i^{s_i}$ solo afecta a los términos en x_n.

  Sean $\mathfrak{P}_1, ..., \mathfrak{P}_n$ los primos asociados de $\mathfrak{I}$, y sea $\mathfrak{P}_i \cap \Bbbk[x_n] = (g_i)$. Entonces, los polinomios $g_1, ..., g_n$ son dos a dos coprimos y tenemos:

$$\bigcap_{i=1}^n (\mathfrak{P}_i \cap \Bbbk[x_n]) = \bigcap_{i=1}^n (g_i) = (\prod_{i=1}^n g_i)$$

  Por otro lado tenemos:

$$\bigcap_{i=1}^n (\mathfrak{P}_i \cap \Bbbk[x_n]) = \bigcap_{i=1}^n (\mathfrak{P}_i) \cap \Bbbk[x_n] = \mathrm{Rad}(\mathfrak{I}) \cap \Bbbk[x_n]$$

  Como tenemos $\mathfrak{I} \cap \Bbbk[x_n] = (g)$, entonces $\prod_{i=1}^n g_i$ divide a g y g divide a una potencia de $\prod_{i=1}^n g_i$, lo que implica que $g_i = p_i$ para todo $1 \geq i \geq n$ y que $\mathfrak{P}_i$ es el único ideal primo asociado a $\mathfrak{I}$ que contiene a $p_i^{s_i}$ y por lo tanto, $\mathrm{Ass}(\mathfrak{I}_i) = \mathfrak{P}_i$.

  Como $\mathrm{Rad}(\mathfrak{I}_i)$ es la intersección de todos los ideales primos de $\Bbbk[x_1, ..., x_n]$ que contienen a $\mathfrak{I}_i$ entonces tenemos que $\mathrm{Rad}(\mathfrak{I}_i)$ es primo y por la proposición (3.23) tenemos que $\mathfrak{I}_i$ es primario.

Así que $\bigcap_{i=1}^n \mathfrak{I}_i = \mathfrak{I}$ es la descomposición primaria que buscábamos.

En el caso en el que $\mathfrak{I}$ o alguno de los $\mathfrak{I}_i$ no esté en posición general, por la proposición (4.3) sabemos que mediante un cambio de coordenadas del tipo $x_n = x_n + \sum_{i=1}^{n-1} c_i x_i$ podemos transformalo en un ideal en posición general.

A continuación mostramos el algoritmo.

Algorithm 6 Descomposición de un ideal 0-dimensional con coeficientes en un cuerpo de característica 0

procedure DP0C($\Bbbk$: cuerpo de característica 0; $x = (x_1, ..., x_n)$: variables; $\mathfrak{I}$: ideal 0-dimensional de $\Bbbk[x]$)
  salida: $\{\mathfrak{Q}_1, ..., \mathfrak{Q}_m\}$ ideales de $\Bbbk[x]$ tales que $\forall i$: $\mathfrak{P}_i \neq \mathfrak{P}_j$ si $i \neq j$; $\mathfrak{Q}_i$ es $\mathfrak{P}_i$-primario; $\bigcap_{i=1}^{m} \mathfrak{Q}_i = \mathfrak{I}$
  C será una colección de ideales, con $C = \{\mathfrak{I}\}$
  while todo $\mathfrak{J} \in C$ no es un ideal primario en posición general **do**
    seleccionamos aleatoriamente $c_1, ..., c_n \in \Bbbk$.
    $x_n \leftarrow x_n + \sum_{i=1}^{n-1} c_i x_i$
    calcular: $(g) = \mathfrak{I} \cap \Bbbk[x_n]$
    descomponer: $g = p_1^{s_1} ... p_n^{s_n}$ en $\Bbbk[x_n]$
    $\mathfrak{I}_i \leftarrow (p_i^{s_i}, \mathfrak{I})$
    $C = \{\mathfrak{I}_1, ..., \mathfrak{I}_n\}$
  end while
  $x_n \leftarrow x_n - \sum_{i=1}^{n-1} c_i x_i$
  return: $\{(\mathfrak{I}_i)_{i=1}^{n}\}$
end procedure

Nota. Comprobar que un ideal está en posición general tiene un gran coste operacional, es por eso que en vez de comprobar que $\mathfrak{I}$ está en posición general tras ese cambio de coordenadas, lo que hacemos es trabajar como si lo estuviera y a continuación comprobamos que cada $\mathfrak{I}_i$ es un ideal primario en posición general.

En realidad, lo único que necesitamos para tener una descomposición primaria es que cada $\mathfrak{I}_i$ sea primario. Sin embargo, si $\mathfrak{I}$ está en posición general, entonces $\mathfrak{I}_i = (\mathfrak{I}, p_i^{s_i})$ también lo estará y además, de esta manera podemos utilizar un test más sencillo para ver que $\mathfrak{I}_i$ es primario. El test que se utiliza en la práctica está recogido en el siguiente criterio.

4.4 Teorema ([GP, Criterion 4.2.4.]). *Sea $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ un ideal propio, entonces las siguientes condiciones son equivalentes:*

1. *$\mathfrak{I}$ es 0-dimensional, primario y en posición general.*
2. *Existen $g_1, ..., g_n \in \Bbbk[x_1, ..., x_n]$ y enteros positivos $s_1, ..., s_n$ tales que*

a) $\mathfrak{I} \cap \Bbbk[x_n] = (g_i^{s_i})$, g_i *es irreducible;*

b) *para cada* $i < n$, $\mathfrak{I}$ *contiene el elemento* $(x_i + g_i)^{s_i}$.

3. *Sea* S *una base de Gröbner reducida de* $\mathfrak{I}$ *respecto al orden lexicográfico* $lex(x_1 > ... > x_n)$. *Entonces existen* $g_1, ..., g_n \in \Bbbk[x_n]$ *y enteros positivos* $s_1, ..., s_n$ *tales que*

   a) $g_i^{s_i} \in S$ *y* g_i *es irreducible;*

   b) $(x_i + g_i)^{s_i}$ *es congruente con un elemento de* $S \cap \Bbbk[x_i, ..., x_n]$ *módulo* $(g_n, x_{n-1} + g_{n-1}, ..., x_{i+1} + g_{i+1})$ *para* $i = 1, ..., i = n - 1$.

Es relativamente sencillo programar un test de primalidad que compruebe las condiciones del apartado 3 y con él, damos por finalizado nuestro algoritmo.

Ejemplo

Consideraremos el mismo ejemplo que en (4.1) y compararemos la complejidad de cada algoritmo.

Comenzamos definiendo las nuestras variables:

```
> option(redSB);
> ring R=0,(x,y,z),lp;
> R;
//   characteristic : 0
//   number of vars : 3
//        block   1 : ordering lp
//                  : names    x y z
//        block   2 : ordering C
```

El ideal $\mathfrak{I} = (y^2z^2 - x^2y^3 - xz^3 + x^3yz, y^2z - xz^2, z + y, x + y^3)$ definido por una base de Gröbner reducida.

```
> ideal I = (y2z2-x2y3-xz3+x3yz , y2z-xz2,z+y,x+y3);
> I;
I[1]=x3yz-x2y3-xz3+y2z2
I[2]=-xz2+y2z
I[3]=y+z
I[4]=x+y3
> I = std(I);
> I;
```

```
I[1]=z5-z3
I[2]=y+z
I[3]=x-z3
```

Vemos que $\mathfrak{I}$ está en posición general, pues $G = \{x - z^3, y + z, z^5 - z^3\}$, vamos a ver si $\mathfrak{I}$ es primario en posición general, para ello utilizaremos un test de primalidad basado en el teorema (4.4), que encontramos implementado para SINGULAR en [GP, Algorithm 4.2.5.].

```
> LIB "primdec.lib";
> I;
I[1]=z5-z3
I[2]=y+z
I[3]=x-z3
> factorize(I[1]);
[1]:
   _[1]=1
   _[2]=z
   _[3]=z-1
   _[4]=z+1
[2]:
   1,3,1,1
```

Luego $\mathfrak{I}$ no es primario en posición general. Vamos a continuar con el algoritmo, tendríamos que realizar un cambio de coordenadas aleatorio para conseguir que $\mathfrak{I}$ esté en posición general, pero como ya hemos visto que lo está, vamos a pasar a la siguiente fase y, tras factorizar el elemento de G contenido en $\mathbb{Q}[z]$, definimos los siguientes ideales.

```
> ideal I1 = (I,z3);
> I1 = std(I1);
> I1;
I1[1]=z3
I1[2]=y+z
I1[3]=x

> ideal I2 = (I,z-1);
> I2 = std(I2);
> I2;
I2[1]=z-1
I2[2]=y+1
I2[3]=x-1
```

```
> ideal I3 = (I,z+1);
> I3 = std(I3);
> I3;
I3[1]=z+1
I3[2]=y-1
I3[3]=x+1
```

Volvemos a comprobar que los ideales $\mathfrak{I}_1$, $\mathfrak{I}_2$ e $\mathfrak{I}_3$ son primarios y están en posición general a través del algoritmo [GP, Algorithm 4.2.5.] y hemos terminado. Tenemos una tercera versión de la misma descomposición primaria de nuestro ideal:

$$\mathfrak{I} = \mathfrak{I}_1 \cap \mathfrak{I}_2 \cap \mathfrak{I}_3 = (z^3, z+y, x) \cap (z-1, y+1, x-1) \cap (z+1, y-1, x+1) \tag{4.3}$$

que se corresponde precisamente con la que obteníamos en (4.1) al hallar la base reducida de Gröbner de sus ideales primarios.

4.3. Descomposición primaria de un ideal en $\mathbb{k}[x_1, ..., x_n]$

La versión original de éste algoritmo corresponde a Gianni, Trager y Zacharias en su famoso artículo [GTZ], sin embargo, como ocurría en la sección uno, el algoritmo está descrito para el caso de que el ideal esté en un anillo de polinomios con coeficientes en un anillo. Nosotros nos limitaremos al caso de anillos de polinomios con coeficientes en un cuerpo $\mathbb{k}$, al igual que hace Irena Swanson en su artículo [Swa1].

Lo primero de todo, vamos a enunciar una propiedad que necesitaremos para construir el algoritmo.

4.5 Proposición ([Swa1, Proposition])**.** *Sea* $\mathbb{k}[x_1, ..., x_d]$ *un subanillo propio de* $\mathbb{k}[x_1, ..., x_n]$*, entonces para todo ideal* $\mathfrak{I} \subset \mathbb{k}[x_1, ..., x_n]$ *podemos calcular* $\mathfrak{I}_{\mathbb{k}[x_1,...,x_d]\setminus(x_1)} \cap \mathbb{k}[x_1, ..., x_n]$,

Demostración. Proponemos la demostración que aparece en dicho artículo.

□

Argumentos y *modus operandi*

Comenzamos trabajando con un ideal propio $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$. Si $\mathfrak{I}$ fuera 0-dimensional, entonces aplicaríamos directamente DP0c o DP0 (dependiendo de la característica del cuerpo) y habríamos terminado. Precisamente, la función de nuestro algoritmo consiste en escribir $\mathfrak{I}$ como un una intersección finita de ideales que, y esta vez sí, sean 0-dimensionales. Una vez llegados a este punto, podremos emplear tanto DP0 comoDP0c para lograr escribir cada uno de esos ideales como una intersección finita de ideales primarios. Al hacer una intersección finita de intersecciones finitas obtendremos la deseada descomposición primaria de $\mathfrak{I}$.

Como hemos dicho, obviamos el caso en el que $\mathfrak{I}$ sea 0-dimensional.

Estamos entonces en el caso $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ ideal no 0-dimensional. **Podemos encontrar un $i \in (1, ..., n)$ tal que $\mathfrak{I} \cap \Bbbk[x_i]$ no sea 0-dimensional**.

Demostración. Lo demostramos aplicando la caracterización (3.23): si G es una base de Gröbner de $\mathfrak{I}$, entonces tenemos que $\exists i$ tal que $\forall g \in G \ \text{in}_{>_{lex}}(g) \neq x_i^{m_i}$.

Tras una reordenación de variables si fuera necesario, consideramos el ideal $\mathfrak{I} \cap \Bbbk[x_i]$; por la proposición (3.14), la base de Gröbner de $\mathfrak{I} \cap \Bbbk[x_i]$ viene dada por $G \cap \Bbbk[x_i]$. Pero si $\forall g \in G \ \ \text{in}_{>_{lex}}(g) \neq x_i^{m_i}$, en particular $\forall g \in G \cap \Bbbk[x_i] \ \ \text{in}_{>_{lex}}(g) \neq x_i^{m_i}$. Luego de nuevo por la caracterización (3.23) $\mathfrak{I} \cap \Bbbk[x_i]$ no es un ideal 0-dimensional.

□

Que $\mathfrak{I} \cap \Bbbk[x_i]$ no sea 0-dimensional quiere decir (de nuevo por la caracterización (3.14)) que $\mathfrak{I} \cap \Bbbk[x_i] = (0)$.

Supongamos $\mathfrak{I} \cap \Bbbk[x_1] = (0)$, entonces es un ideal primo principal, por la proposición (4.5) tenemos que existe un $b \in \Bbbk[x_1]$ tal que

$$\mathfrak{I}\Bbbk(x_1)[x_2, ..., x_n] \cap \Bbbk[x_1, ..., x_n] = \mathfrak{I} : b^\infty$$

Sea $l \in \mathbb{N}$ tal que $(\mathfrak{I} : b^\infty) = (\mathfrak{I} : b^l)$.

Aplicando la proposición (2.28) tenemos que $\mathfrak{I} = (\mathfrak{I} : b^l) \cap (\mathfrak{I} + b^l)$. Como $\Bbbk[x_1] \cap (\mathfrak{I} + (b^l)) \neq 0$, nos basta con encontrar una descomposición primaria de $(\mathfrak{I} : b^l)$ para calcular una de $\mathfrak{I}$.

$(\mathfrak{I} : b^l) = (\mathfrak{I} : b^\infty)$ y está contenido en el anillo de polinomios con coeficientes en un cuerpo $\Bbbk(x_1)[x_2, ..., x_n]$, así que podemos aplicar a $(\mathfrak{I} : b^l)$ el mismo proceso que hemos aplicado a $\mathfrak{I}$. Si iteramos este proceso, en un nñumero finito de pasos llegaremos bien al anillo $\Bbbk(x_1, x_2, ..., x_n)$ que es cuerpo y por lo tanto, su descomposición primaria es única; bien a un ideal 0-dimensional, del cual podemos obtener una descomposición primaria.

Podemos hacer lo mismo con cualquiera de las variables x_i que verifiquen que $\mathfrak{I} \cap \Bbbk[x_i]$. Como a lo sumo son $n-2$ variables, en $n-2$ pasos habremos terminado el algoritmo.

Damos a continuación el algoritmo.

Algoritmo

Algorithm 7 Descomposición de un ideal propio de $\Bbbk[x_1, ..., x_n]$

procedure DPK($\Bbbk$: cuerpo. ; $x = (x_1, ..., x_n)$: variables; $\mathfrak{I}$: ideal de $\Bbbk[x]$)
  salida: $\{\mathfrak{Q}_1, ..., \mathfrak{Q}_m\}$ ideales de $\Bbbk[x]$ tales que $\mathfrak{Q}_i$ es primario; $\bigcap_{i=1}^{m} \mathfrak{Q}_i = \mathfrak{I}$
  if $\mathfrak{I}$ es 0-dimensional **then**
    if char($\Bbbk$) = 0 **then**
      return DP0C($\Bbbk$, x, $\mathfrak{I}$)
    else
      return DP0($\Bbbk$, x, $\mathfrak{I}$)
    end if
  end if
  encontrar: i tal que $\mathfrak{I} \cap \Bbbk[x_i]$ no sea 0-dim
  encontrar: $b \in \Bbbk[x_i]$ tal que $\mathfrak{I}\Bbbk(x_1)[x_2, ..., x_n] \cap \Bbbk[x_1, ..., x_n] = \mathfrak{I} : b^\infty$
  encontrar: $l \in \mathbb{N}$ tal que $(\mathfrak{I} : b^\infty) = (\mathfrak{I} : b^l)$
  $\{\mathfrak{Q}_1, ..., \mathfrak{Q}_m\} \leftarrow$ DPK($\Bbbk(x_1)$; $(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n)$, $(\mathfrak{I} : b^l)$)
  $\{\mathfrak{Q}_1, ..., \mathfrak{Q}_t\} \leftarrow$ DPK($\Bbbk$; $(x_1, ..., x_n)$, $(\mathfrak{I} + b^l)$)
  return: $\{(\mathfrak{Q}_i)_{i=1}^m \cup (\mathfrak{Q}_i)_{i=1}^t\}$
end procedure

Ejemplo

Retomamos esta vez el ejemplo (2.32) y vamos a calcular esta vez nosotros mismos su descomposición primaria.

Definimos el ideal $I = (y^2z^2 - x^2y^3 - xz^3 + x^3yz, y^2z - xz^2)$ en el anillo $\mathbb{Q}[x, y, z]$. Vamos a calcular una descomposición primaria de $\mathfrak{I}$, utilizando SINGULAR y el Algoritmo (7). A continuación, compararemos nuestra descomposición con la obtenida en (2.32).

Comenzamos nuestro programa en SINGULAR.

```
> LIB "primdec.lib";
> option(redSB);

> ring R=0,(x,y,z),dp;
> R;
//   characteristic : 0
//   number of vars : 3
//        block   1 : ordering dp
//                  : names    x y z
//        block   2 : ordering C
> ideal I=y^2*z^2-x^2*y^3-x*z^3+x^3*y*z,y^2*z-x*z^2;
> I = std(I);
> I;
I[1]=y2z-xz2
I[2]=x2y3-x3yz
```

Comprobamos si $\mathfrak{I}$ es 0-dimensional.

```
> dim(I);
2
```

Como no lo es, buscamos la variable x, y o z tal que $\mathfrak{I} \cap \mathbb{k}[x] = 0$, $\mathfrak{I} \cap \mathbb{k}[y] = 0$ o $\mathfrak{I} \cap \mathbb{k}[z] = 0$. Tomamos la variable z, que verifica $\mathfrak{I} \cap \mathbb{k}[z] = 0$. Definimos el anillo $\mathbb{Q}(z)[x, y]$, y el ideal $\mathfrak{I}' = \mathfrak{I}\mathbb{Q}(z)[x, y]$ vamos a calcular la componente $\mathfrak{I}' \cap \mathbb{Q}[x, y, z] = (\mathfrak{I} : b^\infty)$.

```
> ring S=(0,z),(x,y),dp;
> setring S;
> ideal I'=y^2*z^2-x^2*y^3-x*z^3+x^3*y*z,y^2*z-x*z^2;
> I' = std(I);
> I';
I'[1]=y2+(-z)*x
```

Como el ideal $(y^2 - zx)$ es primo, hemos encontrado entonces la primera componente de nuestra descomposición primaria: $\mathfrak{I}' = \mathfrak{I}_1 = y^2 - zx$, y el elemento b será z. Tenemos que calcular ahora la descomposición de $\mathfrak{I}'' = (\mathfrak{I} + (z))$ en $\mathbb{Q}[x, y, z]$.

```
> setring R;
> ideal I'' = y^2*z^2-x^2*y^3-x*z^3+x^3*y*z,y^2*z-x*z^2,z;
> I'' = std(I'');
> I'';
I''[1]=z
I''[2]=x2y3
```

Comprobamos si es 0-dimensional.

```
> dim(I'');
1
```

Como no lo es, buscamos una variable x, y o z tal que $\mathfrak{I} \cap \Bbbk[x] = 0$, $\mathfrak{I} \cap \Bbbk[y] = 0$ o $\mathfrak{I} \cap \Bbbk[z] = 0$. Tomamos por ejemplo la variable y, y repetimos el proceso anterior: definimos el anillo $\mathbb{Q}(y)[x, z]$, y el ideal $\mathfrak{I}''' = \mathfrak{I}''\mathbb{Q}(z)[x, y]$ vamos a calcular la componente $\mathfrak{I}''' \cap \mathbb{Q}[x, y, z] = (\mathfrak{I} : b^\infty)$.

```
> ring T = (0,y),(x,z),dp;
> setring T;
> ideal I''' = y^2*z^2-x^2*y^3-x*z^3+x^3*y*z,y^2*z-x*z^2,z;
> I''' = std(I2);
> I''';
I'''[1]=z
I'''[2]=x2
```

Como $(\mathfrak{I} : b^\infty) = (z, x^2)$ es un ideal primario, así que ya tenemos la segunda componente de nuestra descomposición primaria, $\mathfrak{I}_2 = \mathfrak{I}''' = (z, x^2)$. Además, resulta fácil deducir que $b = y^3$, y lo único que nos queda es hallar una descomposición primaria de $\mathfrak{I}'''' = (\mathfrak{I}'' + y) = (y^2z^2 - x^2y^3 - xz^3 + x^3yz, y^2z - xz^2, z, y)$ en $\mathbb{Q}[x, y, z]$.

```
> setring R;
> ideal I'''' = y^2*z^2-x^2*y^3-x*z^3+x^3*y*z,y^2*z-x*z^2,z,y3;
> I'''' = std(I'''');
> I'''';
I''''[1]=z
I''''[2]=y3
```

Obtenemos $\mathfrak{I}'''' = (\mathfrak{I}'' + y) = (z, y^3)$ ideal primario, así que $\mathfrak{I}_3 = (z, y^3)$ es nuestro último elemento de la descomposición primaria.

$$\mathfrak{I} = (xz - y^2) \cap (z, x^2) \cap (z, y^3) \tag{4.4}$$

Mientras que la descomposición primaria que obteníamos en (2.32) era:

$$\mathfrak{I} = (y^2 - xz) \cap (y, z^2) \cap (x^2, z) \tag{4.5}$$

Podemos observar como la componente aislada $(y^2 - xz)$ es igual en ambas descomposiciones mientras que las componentes inmersas varían.

4.4. Otros algoritmos de descomposición primaria

El algoritmo aquí presentado no es el único que se utiliza para computar la descomposición primaria en $\mathbb{k}[x_1, ..., x_n]$. Podemos encontrar una lista de algoritmos ya implementados para el programa SINGULAR en [DGP].

No podemos hacer un trabajo sobre los aspectos computacionales de la descomposición primaria sin nombrar a Eisenbud, Huneke y Vasconcelos, que en su artículo [EHV] presentan un algoritmo que no tiene nada que ver con el aquí descrito; en particular, no utiliza las bases de Gröbner. Es un algoritmo importante aunque de momento menos efectivo que sus competidores.

Y si hablamos de efectividad, debemos citar el artículo [ShiYo] de Shimoyama y Yokoyama quienes presentan un método de descomposición primaria parecido al de [GTZ] pero mejorando notablemente la parte de la localización en ideales primos mediante lo que llaman la *localización efectiva*.

Capítulo 5

Descomposición primaria en ideales particulares

Un matemático que no es también algo de poeta
nunca será un matemático completo.
Karl Weierstrass

Vamos a estudiar ahora la descomposición primaria en dos tipos particulares de ideales: los ideales monomiales y los ideales binomiales. Veremos como en el caso de un ideal monomial no es necesario utilizar los algoritmos descritos anteriormente ya que podemos conseguir una descomposición primaria a través de un proceso mucho más sencillo, utilizando la *dualidad de Alexander*. Además, demostraremos que toda descomposición primaria de un ideal binomial está formada por ideales binomiales.

A lo largo de todo el capítulo, trabajaremos en el anillo $\Bbbk[x_1, ..., x_n]$, donde $\Bbbk$ es un cuerpo **algebraicamente cerrado**. Para la realización de la sección de ideales monomiales nos hemos basado fundamentalmente en [MiSt]; mientras que para la realización de la sección de binomiales hemos utilizado las notas de Irena Swanson [Swa1] en la escuela doctoral EACA del 2013.

5.1. Ideales monomiales

Comenzamos definiendo qué es un *ideal monomial*.

5.1 Definición. Sea $\mathfrak{I}$ un ideal de $\Bbbk[x_1, ..., x_n]$, $\mathfrak{I}$ es monomial si está generado por un conjunto finito de monomios.

Veremos también algunas propiedades elementales de los ideales monomiales que ya hemos utilizado varias veces en esta memoria.

5.2 Proposición. *Sea $\mathfrak{I}$ un ideal monomial de $\Bbbk[x_1, ..., x_n]$. Entonces:*

- *[CLO, Lemma 2] Dado un conjunto M de monomios generadores de $\mathfrak{I}$, un monomio $x_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$ pertenece a $\mathfrak{I}$ si y sólo si es múltiplo de un elemento de M.*
- *[CLO, Exercise 8] $\mathfrak{I}$ admite un único sistema minimal de generadores formado por monomios, y éste es finito.*
- *La intersección de dos ideales monomiales es un ideal monomial. Además, la intersección de dos ideales monomiales $\mathfrak{I}_1$ e $\mathfrak{I}_2$ está engendrada por el conjunto de los mínimos comunes múltiplos de las parejas de elementos de $\mathfrak{I}_1$ e $\mathfrak{I}_2$.*

Necesitamos conocer también la noción de ideal monomial *irreducible*.

5.3 Definición. Decimos que un ideal monomial $\mathfrak{I}$ de $\Bbbk[x_1, ..., x_n]$ es *irreducible* si está generado por potencias puras de algunas variables. Denotaremos a un ideal irreducible por

$$\mathfrak{m}^{\mathbf{b}} = (x_i^{b_i} : b_i \geq 1).$$

Se puede demostrar que un ideal monomial irreducible lo es en el sentido usual de que no puede descomponerse como intersección de dos ideales distintos de él.

Veremos como dado un ideal monomial $\mathfrak{I}$, podemos descomponerlo como una intersección finita de ideales irreducibles,

$$\mathfrak{I} = \mathfrak{m}_1^{\mathbf{b}_1} \cap \mathfrak{m}_2^{\mathbf{b}_2} \cap ... \cap \mathfrak{m}_n^{\mathbf{b}_n}$$

Si no podemos omitir ninguno de los factores de nuestra descomposición irreducible, entonces diremos que la descomposición es *irredundante*. En ese caso, llamaremos *componentes irreducibles* de $\mathfrak{I}$ a $\mathfrak{m}_1^{\mathbf{b}_1}, \mathfrak{m}_2^{\mathbf{b}_2}, ..., \mathfrak{m}_n^{\mathbf{b}_n}$.

Vamos a poner un ejemplo para familiarizarnos con la nueva terminología.

5.4 Ejemplo. Consideramos el anillo de polinomios $\Bbbk[x, y, z]$ y los ideales $\mathfrak{I}_1 = (x, z)$, $\mathfrak{I}_2 = (y^2, z)$. Podemos observar que ambos ideales son irreducibles, pues están engendrados por potencias puras. Si utilizamos la notación de antes entonces tendríamos $\mathfrak{I}_1 = \mathfrak{m}^{[1,0,1]}$ y $\mathfrak{I}_2 = \mathfrak{m}^{[0,2,1]}$.

5.5 Proposición. *Todo ideal monomial admite una descomposición en ideales monomiales irreducibles irredundante y finita.*

Demostración. La demostración de esta proposición es constructiva; basta con considerar un conjunto finito de generadores de $\mathfrak{I}$, $(m_1, ..., m_n)$, si todos los m_i son potencias puras, entonces $\mathfrak{I}$ es irreducible y hemos terminado.

Supongamos entonces que existe un m_i que no es una potencia pura, entonces podemos descomponerlo como un producto de monomios relativamente primos $m_i = m_i' m_i''$. En ese caso tenemos $\mathfrak{I} = (\mathfrak{I} + (m_i')) \cap (\mathfrak{I} + (m_i''))$. Podemos iterar este proceso hasta que tanto m_i' como m_i'' sean potencias puras, a lo cual llegaremos en un proceso con un número de pasos finito.

Si seguimos razonando de esta manera con el resto de m_i que no sean potencias puras, llegaremos a la descomposición irreducible deseada.

□

5.6 Ejemplo. Consideremos por ejemplo el ideal monomial $\mathfrak{m} = (xy^2, z)$, $\mathfrak{m}$ no es un ideal monomial irreducible, pues xy^2 no es una potencia pura. Aplicamos el algoritmo utilizado en la demostración de la proposición anterior y tenemos $xy^2 = x \times y^2$, luego $\mathfrak{m} = (\mathfrak{m} + (x)) \cap (\mathfrak{m} + (y^2)) = (xy^2, z, x) \cap (xy^2, z, y^2)$. Si eliminamos ahora los monomios redundantes en los sistemas de generadores obtenemos $\mathfrak{m} = (x, z) \cap (y^2, z) = \mathfrak{I}_1 \cap \mathfrak{I}_2$.

Más adelante demostraremos como además dicha descomposición irreducible irredundante es única.

En la demostración de la proposición (5.5) hemos visto un posible algoritmo para obtener la descomposición irreducible de un ideal monomial. Como vimos en el capítulo 1, proposición (2.36) , toda descomposición irreducible es primaria; así que dicho algoritmo nos proporciona una forma de obtener una descomposición primaria. Sin embargo, el proceso es muy costoso, ya que obtenemos gran cantidad de componentes redundantes a cada paso.

Existe un método mucho más sencillo para calcular la descomposición primaria de un ideal monomial, que consiste en utilizar la **dualidad de Alexander**.

5.7 Definición. Dados dos vectores $\mathbf{a}, \mathbf{b} \in \mathbb{N}^n$ con $b_i \leq a_i$ para todo $i \in (1, ..., n)$, denotamos por $\mathbf{a} \backslash \mathbf{b}$ al vector de $\mathbb{N}^n$ que tiene por i-ésima coordenada:

$$a_i \backslash b_i = \begin{cases} a_i + 1 - b_i & \text{si } b_i \geq 1 \\ 0 & \text{si } b_i = 0 \end{cases}$$

Sea $\mathfrak{I}$ un ideal monomial dado por un conjunto minimal de generadores $(g_1, ..., g_n)$ y un monomio $\mathbf{x^a}$ tal que todos los generadores de $\mathfrak{I}$ dividen a $\mathbf{x^a}$. Entonces, el *dual de Alexander* de $\mathfrak{I}$ respecto de $\mathbf{a}$ es el ideal

$$\mathfrak{I}^{[\mathbf{a}]} = \cap\{\mathfrak{m}^{\mathbf{a}\setminus\mathbf{b}} : \mathbf{x^b} \text{ es un generador de } \mathfrak{I}\}.$$

Como siempre que hablamos de dualidad, se verifica la condición $(\mathfrak{I}^{[\mathbf{a}]})^{[\mathbf{a}]} = \mathfrak{I}$. Podemos encontrar una prueba de esta propiedad en [MiSt, Theorem 5.24]. El dual de Alexander nos permite hallar una descomposición irreducible irredundante de $\mathfrak{I}$ gracias al siguiente resultado.

5.8 Teorema ([MiSt, Theorem 5.27])**.** *Sean $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ un ideal monomial y $\boldsymbol{x^a}$ un monomio de $\Bbbk[x_1, ..., x_n]$ tal que todos los generadores minimales de $\mathfrak{I}$ dividen a $\boldsymbol{x^a}$.*

Entonces $\mathfrak{I}$ tiene una descomposición irreducible irredundante y única dada por

$$\mathfrak{I} = \cap\{\mathfrak{m}^{a\setminus b} : \boldsymbol{x^b} \text{ es un generador de } \mathfrak{I}^{[a]}\}.$$

De forma equivalente, podemos afirmar que el dual de Alexander de $\mathfrak{I}$ viene dado por el sistema minimal de generadores

$$\mathfrak{I}^{[a]} = (\boldsymbol{x}^{a\setminus b} : \mathfrak{m}^b \text{ es una componente irreducible de } \mathfrak{I}).$$

Tenemos así, una correspondencia biunívoca entre un ideal $\mathfrak{I}$ y su dual de Alexander $\mathfrak{I}^{[\mathbf{a}]}$ que asocia a cada generador minimal de $\mathfrak{I}$ las componentes irreducibles de $\mathfrak{I}^{[\mathbf{a}]}$ y viceversa.

$\mathfrak{I}$	$\longleftrightarrow$	$\mathfrak{I}^{[\mathbf{a}]}$
generadores minimales	$\longleftrightarrow$	componentes irreducibles
componentes irreducibles	$\longleftrightarrow$	generadores minimales

A la vista de este resultado, un buen método para obtener una descomposición primaria de $\mathfrak{I}$ consistirá en tomar los generadores minimales de $\mathfrak{I}$, que se corresponden con las componentes irreducibles de $\mathfrak{I}^{[\mathbf{a}]}$ y a partir de ellas obtener unos generadores minimales de $\mathfrak{I}^{[\mathbf{a}]}$ que a su vez se corresponderán con las componentes irreducibles de $\mathfrak{I}$ que queríamos obtener.

Presentamos un ejemplo para entender mejor el resultado.

5.9 Ejemplo. Retomamos el ejemplo (2.29), en él tenemos el ideal monomial $\mathfrak{I} = (x^2, xy, xz) \subset \mathbb{Q}[x, y, z]$ y dos descomposiciones primarias diferentes de $\mathfrak{I}$:

1. $\mathfrak{I} = (x) \cap (x^2, y, z)$

2. $\mathfrak{I} = (x) \cap (x^2, y, xz, z^2)$

Vamos a ver si alguna de las dos, y en su caso, cual de ellas, se corresponde con la descomposición irreducible irredundante de $\mathfrak{I}$.

Tenemos $\mathfrak{I} = (x^2, xy, xz)$ y tomamos, por ejemplo, $\mathbf{x^a} = x^2yz$.
Calculamos los $\mathfrak{m}^{\mathbf{a}\setminus\mathbf{b}}$ para $\mathbf{x^b} = x^2$, xy y xz.

- $x^2 \Rightarrow \mathfrak{m}^{\mathbf{a}\setminus\mathbf{b}} = (x)$.
- $xy \Rightarrow \mathfrak{m}^{\mathbf{a}\setminus\mathbf{b}} = (x^2, y)$.
- $xz \Rightarrow \mathfrak{m}^{\mathbf{a}\setminus\mathbf{b}} = (x^2, z)$

Así que el dual de Alexander de $\mathfrak{I}$ respecto de $\mathbf{a}$ es el ideal

$$\mathfrak{I}^{[\mathbf{a}]} = (x) \cap (x^2, y) \cap (x^2, z).$$

Por la proposición (5.2), podemos calcular fácilmente esas intersecciones y obtenemos:

$$\mathfrak{I}^{[\mathbf{a}]} = (x^2, xy) \cap (x^2, z) = (x^2, x^2z, x^2y, xyz) = (x^2, xyz).$$

Ahora tenemos que calcular los $\mathfrak{m}^{\mathbf{a}\setminus\mathbf{b}}$ con $\mathbf{x^b} = x^2$ y xyz.

- $x^2 \Rightarrow \mathfrak{m}^{\mathbf{a}\setminus\mathbf{b}} = (x)$.
- $xyz \Rightarrow \mathfrak{m}^{\mathbf{a}\setminus\mathbf{b}} = (x^2, y, z)$.

A la vista del teorema (5.8) podemos afirmar que (x) y (x^2, y, z) son las componentes irreducibles de $\mathfrak{I}$.

$$\mathfrak{I} = (x) \cap (x^2, y, z)$$

es la descomposición irreducible irredundante de $\mathfrak{I}$ y coincide con la descomposición primaria (2.1).

En general, juntando los ideales monomiales de mismo radical en la descomposición irreducible irredundante, obtendremos una descomposición primaria minimal.

Resulta evidente que este método es mucho más efectivo para el caso de ideales monomiales que los descritos en el apartado 4.

5.2. Ideales binomiales

Desarrollaremos en este último apartado los resultados expuestos por [Swa1] durante la II escuela doctoral EACA de álgebra computacional en Valladolid. No vamos a dar un nuevo algoritmo para realizar una descomposición primaria de un ideal binomial, sino que nos centraremos en demostrar que todo ideal binomial admite una descomposición primaria formada por ideales binomiales.

Definimos por *término* a un monomio de $\Bbbk[x_1, ..., x_n]$ con un coefiente en $\Bbbk$, por ejemplo x^2y^4 es un monomio y un término de $\mathbb{C}[x, y]$, sin embargo, $5x^2y^4$ es un término, pero no es un monomio. Un *binomio* es un elemento del anillo $\Bbbk[x_1, ..., x_n]$ que podemos escribir como la diferencia de dos términos.

5.10 Definición. Decimos que un ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ es *binomial* si está generado por un conjunto de binomios.

Enunciaremos a continuación una serie de propiedades de los ideales binomiales.

5.11 Proposición. *Sean $\mathfrak{I}$, $\mathfrak{G}$ ideales binomiales de $\Bbbk[x_1, ..., x_n]$, $t \in \Bbbk[x_1, ..., x_n]$, entonces:*

1. *$\mathfrak{I} + \mathfrak{G}$ es un ideal binomial.*
2. *$(\mathfrak{I} : t)$ es un ideal binomial.*
3. *$\mathfrak{I} \cap \mathfrak{G}$ no tiene porqué ser binomial.*
4. *La descomposición primaria de $\mathfrak{I}$ no tiene porque estar formada por ideales binomiales.*
5. *El radical de $\mathfrak{I}$ no es necesariamente binomial.*
6. *La base de Gröbner reducida de un ideal binomial respecto de cualquier orden monomial está formada por binomios.*

A lo largo de todo este capítulo consideraremos que los ideales monomiales son también binomiales, pues basta con que consideremos los binomios obtenidos a partir de la sustracción de un monomio y el elemento nulo.

Los resultados más importantes de esta sección nos muestran que si nuestro cuerpo de coeficientes $\Bbbk$ es **algebraicamente cerrado** (además de poseer

todas las demás propiedades de las que le hemos dotado hasta ahora), entonces los primos asociados, los ideales que forman la descomposición primaria y el radical de un ideal binomial de $\Bbbk[x_1, ..., x_n]$ son también binomiales.

Consideremos el anillo $\Bbbk[x_1, ..., x_n]_{x_1...x_n}$; que podemos escribir también como $\Bbbk[x_1, ..., x_n, x_1^{-1}, ..., x_n^{-1}]$ y denotémosle de ahora en adelante por S. Entonces tenemos el siguiente gran resultado.

5.12 Teorema ([Swa1, Theorem 2.1.2.]). *Un ideal propio binomial $\mathfrak{I}$ de S verifica:*

1. *Todos sus primos asociados son binomiales y minimales.*
2. *Su descomposición primaria está formada por ideales primarios binomiales.*
3. *Si el cuerpo $\Bbbk$ tiene **característica 0**, entonces todos los componentes de su descomposición primaria son ideales primos.*
4. *Si el cuerpo $\Bbbk$ tiene **característica 0**, $\mathfrak{I}$ es un ideal radical.*

No nos interesa estudiar todos los resultados contenidos en el teorema en este trabajo, así que nos contentaremos con estudiar lo concerniente a la descomposición primaria de un ideal binomial. Para ello, comenzaremos con una definición.

5.13 Definición. Decimos que un ideal $\mathfrak{I} \subset \Bbbk[x_1, ..., x_n]$ es *celular* si para todo $1 \geq i \geq n$, tenemos que x_n o bien no es zero divisor o bien es nilpotente módulo $\mathfrak{I}$.

Es fácil ver que tanto los ideales monomiales como los binomiales son celulares.

5.14 Definición. Sea $g = x^\alpha - cx^\beta$ un binomio y $d \in \mathbb{N}$, entonces definimos el elemento:

$$g^{[d]} = x^{d\alpha} - c^d x^{d\beta}$$

Y podemos enunciar la siguiente proposición, que será fundamental para construir la descomposición primaria.

5.15 Proposición. *Sea $\mathfrak{I}$ un ideal binomioal y $g = x^\alpha - cx^\beta$ un binomio (no monomio) en $\Bbbk[x_1, ..., x_n]$ tal que tanto x^α como x^β no son divisores de cero módulo $\mathfrak{I}$. Entonces, existe un ideal monomial $\mathfrak{I}_0$ tal que para un d suficientemente grande,*

$$(\mathfrak{I} : g^{[d!]}) = (\mathfrak{I} : (g^{[d!]})^2) = \mathfrak{I} + \mathfrak{I}_0$$

Demostración. Proponemos la demostración dada en [Swa1, Lemma 2.3.3.].

□

Construiremos ahora nuestra descomposición primaria.

Demostración (apartado (2) del teorema (5.12)). Sea $\mathfrak{I}$ un ideal binomial de $\Bbbk[x_1, ..., x_n]$, entonces para cada variable x_j, $1 \geq j \geq n$ existe un $l \in \mathbb{N}$ tal que

$$\mathfrak{I} = (\mathfrak{I} : x_j^l) \cap (\mathfrak{I} + x_j^l) \tag{5.1}$$

así que solo necesitamos encontrar la descomposición primaria de los ideales $\mathfrak{I}_1 = (\mathfrak{I} : x_j^l)$ e $\mathfrak{I}_2 = (\mathfrak{I} + x_j^l)$.

Como el ideal $\mathfrak{I}$ es binomial, por las propiedades de (5.11), tanto $\mathfrak{I}_1$ como $\mathfrak{I}_2$ son binomiales.

Si repetimos este proceso, esta vez con otra variable x_k y un natural $m \in \mathbb{N}$, $1 \geq k \geq n$, podemos encontrar otros cuatro ideales $\mathfrak{I}_{1,1}, \mathfrak{I}_{1,2}, \mathfrak{I}_{2,1}, \mathfrak{I}_{2,2}$ tales que $\mathfrak{I}_{1,1} = (\mathfrak{I}_1 : x_k^m)$, $\mathfrak{I}_{1,2} = (\mathfrak{I}_1 + x_k^m)$, $\mathfrak{I}_{2,1} = (\mathfrak{I}_2 : x_k^m)$, $\mathfrak{I}_{2,2} = (\mathfrak{I}_2 + x_k^m)$ con

$$\mathfrak{I} = (\mathfrak{I}_1 : x_k^m) \cap (\mathfrak{I}_1 + x_k^m) \cap (\mathfrak{I}_2 : x_k^m) \cap (\mathfrak{I}_2 + x_k^m) \tag{5.2}$$

Iterando este proceso un número finito de veces podemos asumir que llegamos a una descomposición de $\mathfrak{I}$ es ideales celulares. Luego lo único que necesitamos es **calcular una descomposición primaria de un ideal binomial celular** de $\Bbbk[x_1, ..., x_n]$.

Consideramos entonces un ideal binomial celular al que denotaremos de nuevo $\mathfrak{I}$. Y dividiremos las variables en los siguientes conjuntos: $x_1, ..., x_d$ son elementos no divisores de cero módulo $\mathfrak{I}$ y $x_{d+1}, ..., x_n$ son nilpotentes módulo $\mathfrak{I}$. Sea $\mathfrak{P} \in \mathrm{Ass}_{\Bbbk[x_1,...,x_n]}(\mathfrak{I})$. Un resultado del teorema (5.12) nos dice que entonces $\mathfrak{P}$ es un ideal binomial.

Como $\mathfrak{I}$ está contenido en $\mathfrak{P}$, entonces $\mathfrak{P}$ continen a las variables $x_{d+1}, ..., x_n$, y como las otras variables $x_1, ..., x_d$ son elementos no divisores de cero módulo $\mathfrak{I}$, no pertenecen a $\mathfrak{P}$. Así que podemos escribir $\mathfrak{P}$ de la forma $\mathfrak{P} = \mathfrak{P}_0 + (x_{d+1}, ..., x_n)$ con $\mathfrak{P}_0$ un ideal binomial primo con generadores binomiales en $\Bbbk[x_1, ..., x_n]$ y las variables $x_1, ..., x_d$ no son divisores de cero módulo $\mathfrak{I}$.

Sea g un binomio no nulo de $\mathfrak{P}_0$, por la proposición (5.15), tenemos que existe un $d \in \mathbb{N}$ tal que $(\mathfrak{I} : g^{[d]}) = (\mathfrak{I} : (g^{[d]})^2) = \mathfrak{I} + \mathfrak{I}_0$, con $\mathfrak{I}_0$ un ideal

monomial. Esto implica que en particular, $\mathfrak{P} \notin \mathrm{Ass}_{\Bbbk[x_1,...,x_n]}(\mathfrak{I} : (g^{[d]})$, por lo que $\mathfrak{P} \in \mathrm{Ass}(\mathfrak{I} + (g^{[d]}))$, aún más, el componente $\mathfrak{P}$-primario de $\mathfrak{I}$ es el componente $\mathfrak{P}$- primario del ideal binomial $\mathfrak{I} + (g^{[d]})$.

Podemos entonces reemplazar $\mathfrak{I}$ por $\mathfrak{I}+(g^{[d]})$ y la descomposición primaria se mantendrá. Repetimos este proceso con cada binomio g generador de $\mathfrak{P}_0$ hasta lograr que $\mathfrak{P}$ sea minimal sobre $\mathfrak{I}$. Las variables $(x_{d+1}, ..., x_n)$ siguen siendo nilpotentes módulo $\mathfrak{I}$ y el componente $\mathfrak{P}$-primario del ideal $\mathfrak{I}$ es el mismo que el de $(\mathfrak{I} : (x_1, ..., x_d)^\infty)$; así que si ahora **reemplazamos $\mathfrak{I}$ por** $(\mathfrak{I} : (x_1, ..., x_d)^\infty)$, el ideal $\mathfrak{I}$ seguirá siendo celular.

Si tenemos $\mathrm{Ass}_{\Bbbk[x_1,...,x_n]}(\mathfrak{I}) = \{\mathfrak{P}\}$, entonces $\mathfrak{I}$ es $\mathfrak{P}$-primario y hemos terminado. Si no estamos en este caso, es que existe un ideal $\mathfrak{Q} \in \mathrm{Ass}_{\Bbbk[x_1,...,x_n]}(\mathfrak{I})$ distinto de $\mathfrak{P}$. Como $\mathfrak{P}$ es minimal en $\mathrm{Ass}_{\Bbbk[x_1,...,x_n]}(\mathfrak{I})$ y $\mathfrak{P} \neq \mathfrak{Q}$, entonces existe un binomio irreducible $g = x^\alpha - cx^\beta$ tal que $g \in \mathfrak{Q}\backslash\mathfrak{P}$ y evidentemente, $g \notin (x_{d+1}, ..., x_n)$.

Volvemos a aplicar la proposición (5.15) y sabemos que existe un $d \in \mathbb{N}$ tal que $(\mathfrak{I} : g^{[d]}) = (\mathfrak{I} : (g^{[d]})^2) = \mathfrak{I} + \mathfrak{I}_0$, con $\mathfrak{I}_0$ un ideal monomial. Nos fijamos en que $\mathfrak{Q} \notin \mathrm{Ass}_{\Bbbk[x_1,...,x_n]}((\mathfrak{I} : g^{[d]}))$, y sin embargo $\mathfrak{Q} \in \mathrm{Ass}_{\Bbbk[x_1,...,x_n]}(\mathfrak{I})$, luego $(\mathfrak{I} : g^{[d]})$ es estrictamente mayor que $\mathfrak{I}$.

Si $g^{[d]} \notin \mathfrak{P}$, entonces el componente $\mathfrak{P}$-primario de $\mathfrak{I}$ es el componente $\mathfrak{P}$-primario de $(\mathfrak{I} : g^{[d]})$,y tenemos que el componente $\mathfrak{P}$-primario de $\mathfrak{I}$ es binomial. **Suponemos entonces que** $g^{[d]} \in \mathfrak{P}$. Entonces, $g^{[d]}$ contiene un factor de la forma $g_0 = x^\alpha - c'x^\beta$, con $c' \in \Bbbk$.

Por el automorfismo de Frobenius, tenemos que si la característica de $\Bbbk$ es p, entonces $g_0^{p^m}$ es binomial $\forall m \in \mathbb{N}$. Tomamos entonces el mayor $m \in \mathbb{N}$ tal que p^m divide a d y definimos los elementos $h = \frac{g^{[d]}}{g_0}$ y $b = g_0^{p^m}$. En característica 0, definimos $h = \frac{g^{[d]}}{g_0}$ y $b = g_0$.

En ambos casos, b es un binomio, $b \in (\mathfrak{I} : h)$ y $h \notin \mathfrak{P}$, así que el componente $\mathfrak{P}$-primario de $\mathfrak{I}$ es el mismo componente $\mathfrak{P}$-primario de $(\mathfrak{I} : h)$. Como además $\mathfrak{I} \subset \mathfrak{I} + (b) \subset (\mathfrak{I} : h)$ podemos concluir que el componente $\mathfrak{P}$-primario de $\mathfrak{I}$ es el mismo componente $\mathfrak{P}$-primario de $\mathfrak{I} + (b)$.

Si $b \in \mathfrak{Q}$, entonces $g_0 = x^\alpha - c'x^\beta$ y $g \notin (x_{d+1}, ..., x_n)$ pertenecen a $\mathfrak{Q}$. Como $c \neq c'$, $x^\alpha, x^\beta \in \mathfrak{Q}$, y como $g \notin (x_{d+1}, ..., x_n)$ entonces $\mathfrak{Q}$ contiene una de las variables $(x_1, ..., x_d)$. Pero esas variables no son divisores de cero módulo $\mathfrak{I}$, así que $\mathfrak{Q} \notin \mathrm{Ass}_{\Bbbk[x_1,...,x_n]}(\mathfrak{I})$ y por lo tanto $b \notin \mathfrak{Q}$.

Como $\mathfrak{I}$ está contenido estrictamente en $\mathfrak{I} + (b)$, entonces el componente $\mathfrak{P}$-primario de $\mathfrak{I}$ es binomial.

□

Existen algoritmos específicos para la obtención de una descomposición primaria de un ideal binomial. Si el lector está interesado puede consultar el artículo [OjPe] donde encontrará una versión mejorada de un algoritmo propuesto por Eisenbud y Sturmfels en 1996.

Bibliografía

[AtMc] M. F. Atiyah, I. G. Macdonald *Introduction to Commutative Algebra*, Addison-Wesley 1969.

[CCT] M. Caboara, P. Conti, C. Traverso Yet Another Ideal Decompositions Algorithm, in: *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997)*, 39-54, Lecture Notes in Computer Science **1255**, Springer, 1997.

[CLO] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, 2nd. Edition, Springer,1997.

[DGP] W. Decker, G.-M. Greuel, G. Pfister Primary Decomposition: Algorithms and Comparisons, in: *Algorithmic algebra and number theory (Heidelberg, 1997)*, 187-220, Springer, 1999.

[DGPS] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann Singular 3-1-6 — A computer algebra system for polynomial computations., http://www.singular.uni-kl.de (2012).

[Eis] D. Eisenbud *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer, 1994.

[EHV] D. Eisenbud, C. Huneke, W. Vasconcelos Direct methods for primary decomposition, Inventiones mathematicae **110**, 207-235, 1992.

[Gim] P. Gimenez, Notas de la VI Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2013, Francisco Ugarte Guerra Ed., aparecerá, 2014.

[GP] G.-M. Greuel, G. Pfister *A Singular Introduction to Commutative Algebra*, Springer, 2008.

[GTZ] P. Gianni, B. Trager, G. Zacharias *Gröbner Bases and Primary Descomposition of Polynomial Ideals*, J. Symbolic Computation **6**, 149-167, 1988.

[Harr] J. Harris *Algebraic Geometry: A First Course*, Graduate Texts in Mathematics **133**, Springer, 1995.

[MiSt] E. Miller, B. Sturmfels *Combinatorial Commutative Algebra*, Graduate Texts in Mathematics **227**, Springer, 2005.

[Nun] A. Núñez Jiménez Guión de la asignatura de *Álgebra conmutativa y computacional* de Grado en Matemáticas de la UVa, 2011.

[OjPe] I. Ojeda Martínez de Castilla, R. Peidra Sánchez *Cellular Binomial Ideals. Primary Decomposition of Binomial Ideals*, J. Symbolic Computation **30**, 383-400, 2000.

[San] P. Sancho de Salas Guión de la asignatura de *Álgebra conmutativa* de Grado en Matemáticas de la Unex, 2001. http://matematicas.unex.es/ sancho/AlgebraConmutativa/alco0.pdf

[Sau] A. Sausse *A New Approach to Primary Decomposition*, J. Symbolic Computation **31**, 243-257, 2001.

[ShiYo] T. Shimoyama, K. Yokoyama *Localization and Primary Decomposition of Polynomial Ideals*, J. Symbolic Computation **22**, 247-277, 1996.

[Swa1] I. Swanson, Lectures in Valladolid, EACA's Second International School on Computer Algebra and Applications, http://people.reed.edu/∼iswanson/EACA.pdf (2012).

[Swa2] I. Swanson, *Primary decompositions*, International Conference on Commutative Algebra and Combinatorics, Allahabad (India), http://people.reed.edu/∼iswanson/primdec.pdf (2003).