La Columna de Matemática Computacional

Sección a cargo de

Tomás Recio

Aspectos computacionales de la Descomposición Primaria

por

Ujué Etayo Rodríguez

Preliminares

El cometido principal de esta nota es recoger parte del curso impartido por Irena Swanson en la segunda escuela doctoral EACA, que tuvo lugar en junio de 2013 en Valladolid. El curso completo puede encontrarse en [16] y consta de tres partes: la primera está dedicada al estudio del algoritmo de descomposición primaria desarrollado por Gianni, Trager y Zacharias en su artículo [8], la segunda profundiza ese primer estudio para el caso de ideales binomiales y la tercera versa sobre algunos aspectos relacionados con la estadística algebraica.

En esta nota nos dedicaremos a estudiar el algoritmo de descomposición primaria de Gianni, Trager y Zacharias con las novedades que aporta el punto de vista de Swanson. Podemos encontrar el desarrollo, la implementación y varios ejemplos de todo lo aquí demostrado en [7].

A lo largo de esta nota trabajaremos en un anillo de polinomios $\Bbbk[x_1, \ldots, x_n]$ con coeficientes en un cuerpo $\Bbbk$ que será, bien un cuerpo finito, bien una extensión finita de $\mathbb{Q}$. En la primera sección recordaremos algunos conceptos básicos como los de ideal de un anillo, ideal primo o ideal primario, y daremos una definición de descomposición primaria de un ideal junto con sus principales características. Dedicaremos la segunda sección a presentar las bases de Gröbner y algunas operaciones que podemos realizar en ideales caracterizados por dichas bases. La tercera sección es la principal de la nota, ya que en ella presentamos el algoritmo de descomposición primaria de Gianni, Trager y Zacharias con las simplificaciones introducidas por Swanson. En la última sección daremos unas breves referencias sobre la descomposición primaria en ideales particulares.

Queremos dejar constancia de nuestro agradecimiento a la profesora I. Swanson, a la profesora P. Gianni y al profesor Ph. Giménez por la atenta lectura de versiones

preliminares de este artículo y por las muchas sugerencias y correcciones remitidas y que hemos tratado de incorporar.

1. Descomposición primaria

Consideremos un subconjunto $\mathfrak{I}$ no vacío del anillo de polinomios $\Bbbk[x_1,\ldots,x_n]$. Decimos que $\mathfrak{I}$ es un *ideal* de $\Bbbk[x_1,\ldots,x_n]$ si la diferencia de dos elementos de $\mathfrak{I}$ pertenece a $\mathfrak{I}$ y el producto de un elemento de $\mathfrak{I}$ por un elemento de $\Bbbk[x_1,\ldots,x_n]$ también pertenece a $\mathfrak{I}$. Un ideal $\mathfrak{I}\subset\Bbbk[x_1,\ldots,x_n]$ es *primo* si para todo $f\in\mathfrak{I}$ tal que $f=ab$ entonces, o bien $a\in\mathfrak{I}$, o bien $b\in\mathfrak{I}$; un ideal $\mathfrak{Q}$ es *primario* si para todo $f\in\mathfrak{Q}$ de la forma $f=ab$ entonces, o bien $a\in\mathfrak{Q}$, o bien $b\in\mathrm{Rad}(\mathfrak{Q})$. Recordamos que el *radical* de un ideal $\mathrm{Rad}(\mathfrak{I})$ está formado por los elementos $f\in\Bbbk[x_1,\ldots,x_n]$ para los cuales existe un $m\in\mathbb{Z}_+$ con $f^m\in\mathfrak{I}$. Por último, dados un homomorfismo de anillos $f:\Bbbk[x_1,\ldots,x_n]\longrightarrow\Bbbk[x_1,\ldots,x_m]$, un ideal $\mathfrak{a}$ de $\Bbbk[x_1,\ldots,x_n]$ y un ideal $\mathfrak{b}$ de $\Bbbk[x_1,\ldots,x_m]$, el *ideal contraído* de $\mathfrak{b}$ respecto de f, $\mathfrak{b}^c$, es un ideal de $\Bbbk[x_1,\ldots,x_n]$ que viene dado por $f^{-1}(\mathfrak{b})=\mathfrak{b}^c$ y el *ideal extendido* de $\mathfrak{a}$ respecto de f, $\mathfrak{a}^e$, es un ideal de $\Bbbk[x_1,\ldots,x_m]$ que viene dado por $(f(\mathfrak{a}))=\mathfrak{a}^e$. La imagen inversa por un homomorfismo de anillos de un ideal siempre será un ideal, pero la imagen directa de un ideal no tiene por qué serlo; por eso, el ideal extendido se define como el ideal generado por $f(\mathfrak{a})$.

Resulta inmediato comprobar que todo ideal primo es primario, que el radical de un ideal primario es un ideal primo y que la contracción de un ideal primario es un ideal primario. A partir de ahora, si tenemos un ideal primario $\mathfrak{Q}$ y su radical $\mathfrak{P}=\mathrm{Rad}(\mathfrak{Q})$, diremos que $\mathfrak{Q}$ es $\mathfrak{P}$-*primario*.

Tomemos un ideal cualquiera de $\Bbbk[x_1,\ldots,x_n]$, llamémosle $\mathfrak{I}$. Una *descomposición primaria* de $\mathfrak{I}$ es una expresión de $\mathfrak{I}$ como 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 y se denomina *componente* de la descomposición. Decimos que una descomposición primaria de un ideal $\mathfrak{I}=\bigcap_{n=1}^{N}\mathfrak{Q}_n$ de $\Bbbk[x_1,\ldots,x_n]$ es *minimal* si verifica:

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

Dada una descomposición primaria de un ideal $\mathfrak{I}$ de un anillo $\Bbbk[x_1,\ldots,x_n]$, siempre podemos obtener a partir de ella otra descomposición primaria minimal (encontramos una prueba en [1]). A partir de ahora, todas las descomposiciones primarias que utilizaremos serán minimales.

Los conceptos de ideal primario y descomposición primaria pueden generalizarse a todo tipo de anillos conmutativos y unitarios; sin embargo, en estos anillos no todo ideal tiene por qué admitir una descomposición primaria. Gracias a Emmy

Noether sabemos que en un anillo noetheriano, en particular en $\Bbbk[x_1,\dots,x_n]$, todo ideal admite una descomposición primaria. Podemos ver una demostración de este resultado en [3, Theorem 4, § 4.7].

Una vez confirmada la existencia de una descomposición primaria para cada ideal de $\Bbbk[x_1,\dots,x_n]$ nos preguntamos por su unicidad. Basta con comprobar que el ideal $\mathfrak{I}=(x^2,xy,xz)\subset\mathbb{Q}[x,y,z]$ admite las descomposiciones

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

para confirmar que la descomposición primaria de un ideal no es única en general. Sin embargo, sí que hay algunas componentes únicas en toda descomposición primaria de un ideal, como veremos a continuación. Dada una descomposición primaria de $\mathfrak{I}=\bigcap_{n=1}^{N}\mathfrak{Q}_n$, con $\mathfrak{Q}_n$ ideal $\mathfrak{P}_n$-primario para $1\leq n\leq N$, consideremos el conjunto de ideales primos $\{\mathfrak{P}_n\}_{n=1}^N$ a los que llamaremos *primos asociados* a $\mathfrak{I}$ y denotaremos por $\mathrm{Ass}(\mathfrak{I})$. Los $\mathfrak{P}_n$ son independientes de la descomposición particular de $\mathfrak{I}$ (para más detalles, ver [1, Theorem 4.5]).

Dentro del conjunto $\mathrm{Ass}(\mathfrak{I})$ existen elementos minimales respecto a la relación de contenido que reciben el nombre de *primos asociados aislados* de $\mathfrak{I}$; los ideales que no sean minimales recibirán el nombre de *primos asociados inmersos*. De esta forma, podemos definir las *componentes aisladas* de $\mathfrak{I}$ como aquellas formadas por los ideales primarios $\mathfrak{Q}_n$ cuyo radical $\mathfrak{P}_n$ sea un primo aislado y las *componentes inmersas* como aquellas cuyo radical sea un primo inmerso.

En el ejemplo anterior (1) podemos ver cómo la componente aislada, el ideal (x), aparece en las dos descomposiciones, mientras el otro ideal, la componente inmersa, es distinto en cada descomposición. Esto es totalmente general: las componentes aisladas son idénticas en todas las descomposiciones primarias de un ideal $\mathfrak{I}\subset\Bbbk[x_1,\dots,x_n]$ [1, Theorem 4.5].

Tomaremos ahora un punto de vista más geométrico. A todo ideal $\mathfrak{I}\subset\Bbbk[x_1,\dots,x_n]$ se le puede asociar una variedad algebraica $V(\mathfrak{I})$ en el espacio afín asociado a $\Bbbk^n$. Dicha variedad estará formada por los puntos que anulen todos los polinomios del ideal, $V(\mathfrak{I})=\{x\in\mathbb{A}^n_{\Bbbk}:\forall p\in\mathfrak{I},\ p(x)=0\}$, donde $\mathbb{A}^n_{\Bbbk}$ es el espacio afín asociado a $\Bbbk^n$. Para dar un ejemplo, hemos utilizado el programa Surfer [15] para representar la variedad asociada al ideal $\mathfrak{I}=(y^2-xz)\subset\mathbb{R}[x,y,z]$ (véase la figura 1).

Si el ideal $\mathfrak{I}$ da origen a una variedad $V(\mathfrak{I})$, los primos aislados dan origen a las componentes irreducibles de la variedad $V(\mathfrak{I})=V(\mathrm{Rad}(\mathfrak{I}))$ y los primos inmersos a subvariedades de estas; es decir, a variedades inmersas en las componentes irreducibles.

Consideremos, por ejemplo, una descomposición primaria del ideal $\mathfrak{I}=(y^2-xz)\cap(y,z^2)\cap(x^2,z)$ (véase la figura 2). La descomposición tiene una única componente aislada: el ideal (y^2-xz), y dos componentes inmersas, (y,z^2) y (x^2,z). Podemos observar la variedad que engendra cada una de las componentes y comprobar cómo 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 $V(y^2-xz)$; de ahí que digamos que las componentes son inmersas.

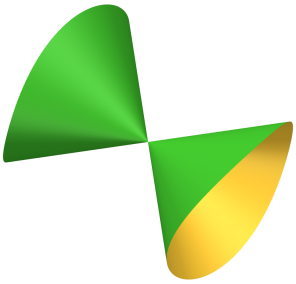

Figura 1: Vista de la variedad $V(y^2 - xz)$ en el interior de la esfera unidad.

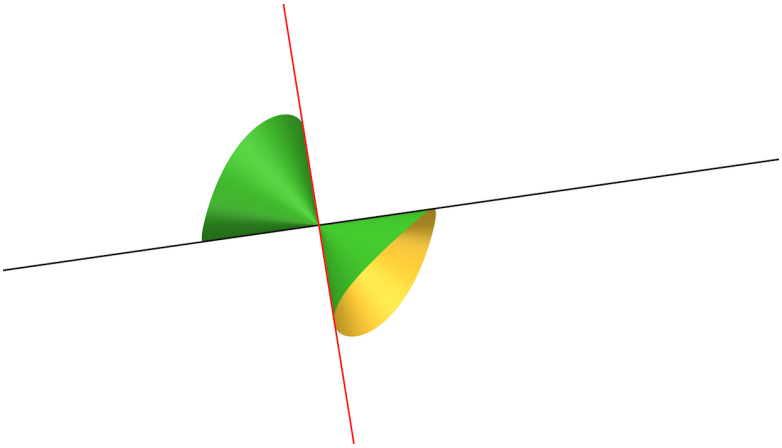

Figura 2: Vista parcial de la variedad $V((y^2 - xz) \cap (y, z^2) \cap (x^2, z)) = V(y^2 - xz) \cup V(y, z^2) \cup V(x^2, z) = V(y^2 - xz)$.

Dependiendo del tipo de anillo y del tipo de ideal, encontrar una descomposición primaria resultará más o menos sencillo. Si el ideal que queremos descomponer es principal, es decir, está generado por un solo elemento del anillo, $\mathfrak{I} = (f)$, entonces la obtención de una descomposición primaria es inmediata: basta con descomponer en factores irreducibles el polinomio que genera el ideal y considerar los ideales generados por cada uno de esos factores. Veámoslo con un ejemplo: dado el ideal $(x^4 - 1) \in \mathbb{Q}[x]$, una descomposición primaria vendrá dada por los ideales generados por los factores irreducibles del polinomio:

$$(x^4 - 1) = (x^2 + 1) \cap (x - 1) \cap (x + 1).$$

Asumimos, a lo largo de esta nota, que podemos calcular la descomposición en factores irreducibles de todo polinomio de $\Bbbk[x_1, \ldots, x_n]$. Consideremos ahora el ideal $\mathfrak{I} = (y^2z^2 - x^2y^3 - xz^3 + x^3yz, y^2z - xz^2)$ en el anillo $\mathbb{Q}[x, y, z]$; a primera vista, ya no parece tan sencillo calcular una de sus descomposiciones primarias, y lo que está claro

es que no podemos utilizar el mismo método que en el caso anterior (la diferencia entre los dos ejemplos está en que $\mathbb{Q}[x]$ es un *dominio de ideales principales*, mientras que $\mathbb{Q}[x, y, z]$ no lo es). De ahí la importancia de desarrollar un método efectivo de descomposición primaria.

2. Bases de Gröbner

Una de las primeras necesidades al trabajar con polinomios en varias variables es cómo ordenar sus términos; para ello, introducimos la noción de orden monomial. Un *orden monomial* $<$ en un anillo $\Bbbk[x_1, \ldots, x_n]$ es un orden total en los monomios de $\Bbbk[x_1, \ldots, x_n]$ que verifica lo siguiente:

1. Es un *buen orden*: todo subconjunto no vacío de monomios de $\Bbbk[x_1, \ldots, x_n]$ tiene un elemento mínimo.
2. Es compatible con el producto: si $f_1 < f_2$ entonces $gf_1 < gf_2$ para cualesquiera f_1, f_2, g monomios de $\Bbbk[x_1, \ldots, x_n]$.

Entre los distintos órdenes monomiales encontramos, por ejemplo, el *orden lexicográfico* $<_{\text{lex}}$, que establece que $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \geq_{\text{lex}} x_1^{\beta_n} \cdots x_n^{\beta_n}$ si la primera coordenada no nula de $(\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ es positiva; el *lexicográfico graduado*, que establece que $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \geq_{\text{glex}} x_1^{\beta_n} \cdots x_n^{\beta_n}$ si se verifica que $\alpha_1 + \cdots + \alpha_n > \beta_1 + \cdots + \beta_n$ o $(\alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n$ y $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \geq_{\text{lex}} x_1^{\beta_1} \cdots x_n^{\beta_n})$; y muchos otros.

Si tenemos un anillo de polinomios dotado de un orden monomial, para cada elemento no nulo del anillo podemos considerar un *monomio inicial* que será el mayor de los monomios que forman el polinomio con respecto al orden monomial elegido. Consideremos nuestro anillo $\Bbbk[x_1, \ldots, x_n]$ dotado de un orden monomial $<$ y un ideal $\mathfrak{I} \subset \Bbbk[x_1, \ldots, x_n]$. Definimos el *ideal inicial de* $\mathfrak{I}$ *respecto de* $<$, denotado por $\text{in}_<(\mathfrak{I})$, como el ideal monomial generado por los monomios iniciales de todos los elementos de $\mathfrak{I}$:

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

En este contexto, decimos que G, un subconjunto finito de $\mathfrak{I}$, es una *base de Gröbner* de $\mathfrak{I}$ respecto del orden monomial $<$ 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 $\Bbbk[x_1, \ldots, x_n]$. Dicho de otra forma, $G = \{g_1, \ldots, g_n\}$ es una base de Gröbner de $\mathfrak{I}$ si $\text{in}_<(\mathfrak{I}) = (\text{in}_<(g_1), \ldots, \text{in}_<(g_n))$.

No solo podemos afirmar que todo ideal $\mathfrak{I} \subset \Bbbk[x_1, \ldots, x_n]$ admite una base de Gröbner (utilizando el teorema de la base de Hilbert o simplemente el lema de Dickson, [5, Theorem 1.2]), sino que, además, conocemos un proceso para construir dicha base, el *algoritmo de Buchberger*. Podemos encontrar este algoritmo explicado detalladamente en [3]. La característica más importante de una base de Gröbner G de $\mathfrak{I}$ es que no solo los monomios iniciales de sus elementos generan $\text{in}_<(\mathfrak{I})$, sino que, tras una breve demostración basada en el algoritmo de la división polinomial[1],

[1]Con *división polinomial* nos referimos aquí a la división de un polinomio en varias variables entre varios polinomios en varias variables, donde el orden monomial juega un papel primordial. Podemos encontrar una explicación de esta división polinomial en [3].

podemos llegar a la conclusión de que G genera $\mathfrak{I}$ entero, así que una base de Gröbner de $\mathfrak{I}$ es un sistema de generadores de $\mathfrak{I}$.

Sin embargo, no tenemos unicidad de la base de Gröbner de un ideal, ya que basta con añadir un elemento cualquiera de $\mathfrak{I}$ a una base de Gröbner de $\mathfrak{I}$ y obtendremos otra base de Gröbner de $\mathfrak{I}$. En busca de la unicidad vamos a definir una nueva base de Gröbner asociada a un ideal, la *base de Gröbner reducida*, que tiene, además de ser base de Gröbner, las siguientes características:

1. El coeficiente dominante de todos los elementos de la base es 1 (el *coeficiente dominante* es el coeficiente del monomio inicial).
2. Dado un polinomio de la base, cualquiera de los monomios que lo forman no está contenido en el ideal generado por los términos iniciales del resto de los polinomios de la base. Es decir, si $G = \{g_1, \ldots, g_t\}$, entonces para todo $i \in \{1, \ldots, t\}$ se verifica que todo monomio de g_i no pertenece al ideal $(\mathrm{in}_<(g_1), \ldots, \widehat{\mathrm{in}_<(g_i)}, \ldots, \mathrm{in}_<(g_t))$.

Ahora sí, podemos afirmar que todo ideal no nulo de $\Bbbk[x_1, \ldots, x_n]$ admite una única base de Gröbner reducida respecto de un orden monomial dado. Además, podemos obtener la base de Gröbner reducida de un ideal $\mathfrak{I}$ a partir de cualquier base de Gröbner de $\mathfrak{I}$ (ver [3, Proposition 6, § 2.7]).

Definir ideales por sus bases de Gröbner nos permite realizar explícitamente varias operaciones en ideales. Quizás uno de los resultados más llamativos de las bases de Gröbner sea el que recoge el Teorema de Eliminación, que afirma que dado un ideal $\mathfrak{I} \subset \Bbbk[x_1, \ldots, x_n]$ y una base de Gröbner G de $\mathfrak{I}$ respecto al orden lexicográfico (o cualquier orden de eliminación respecto de las j primeras variables, véase [3]), una base de Gröbner del ideal $\mathfrak{I} \cap \Bbbk[x_{j+1}, \ldots, x_n]$ vendrá dada por $G_j = G \cap \Bbbk[x_{j+1}, \ldots, x_n]$. Gracias a este resultado, podemos obtener bases de Gröbner, y por tanto sistemas de generadores, de los siguientes ideales:

1. La intersección de dos ideales $\mathfrak{I} \cap \mathfrak{G}$ de $\Bbbk[x_1, \ldots, x_n]$ (ver [8, Corollary 3.2]).
2. El cociente de dos ideales $(\mathfrak{I} : \mathfrak{G})$, con $\mathfrak{I}, \mathfrak{G}$ ideales de $\Bbbk[x_1, \ldots, x_n]$ (ver [8, Corollary 3.2]).
3. Dado un ideal $\mathfrak{I} \subset \Bbbk[x_1, \ldots, x_n]$ y un elemento $f \in \Bbbk[x_1, \ldots, x_n]$, podemos construir la contracción de la localización de $\mathfrak{I}$ en $\Bbbk[x_1, \ldots, x_n]$: si llamamos $\mathfrak{I}_f = \mathfrak{I}\Bbbk[x_1, \ldots, x_n]_f$, entonces podemos construir $\mathfrak{I}_f \cap \Bbbk[x_1, \ldots, x_n]$ (ver [8, Proposition 3.7]).

Existen dos caracterizaciones muy precisas de las bases de Gröbner de los ideales 0-dimensionales[2]. Por un lado, sea $\mathfrak{I}$ un ideal de $\Bbbk[x_1, \ldots, x_n]$ dotado de un orden monomial $>$ y sea G una base de Gröbner de $\mathfrak{I}$. Entonces $\mathfrak{I}$ es 0-dimensional si, y solo si, para cada $1 \leq i \leq n$ existe un elemento g de G cuyo monomio inicial es una potencia de x_i, esto es, $\mathrm{in}_>(g) = x_i^{m_i}$, $m_i \in \mathbb{Z}_+$. Podemos encontrar una prueba de este resultado en [8, Proposition 5.5].

[2]Cuando hablamos de dimensión en este contexto nos referiremos siempre a la dimensión de Krull. Para profundizar en esta noción, se recomienda [5].

Por otro lado, los ideales 0-dimensionales también se caracterizan como aquellos ideales $\mathfrak{I}$ tales que el anillo $\Bbbk[x_1,\ldots,x_n]/\mathfrak{I}$ es un $\Bbbk$-espacio vectorial de dimensión finita (véase [3, Theorem 6, § 5.3]). Se tiene por tanto que un ideal es 0-dimensional si, y solo si, para cada variable x_i el ideal contiene un polinomio en x_i.

Utilizaremos ambas caracterizaciones para construir nuestro algoritmo de descomposición primaria.

3. El algoritmo de descomposición primaria de Gianni-Trager-Zacharias

En su artículo [8], Gianni, Trager y Zacharias presentan un algoritmo de descomposición primaria de ideales de un anillo de polinomios con coeficientes en un dominio de ideales principales. De ahora en adelante, denotaremos por **GTZ** dicho algoritmo. **GTZ** es un algoritmo iterativo en el número de variables del ideal, en cada iteración descompone el ideal como la intersección de dos ideales: uno de ellos tiene dimensión menor que el original o, al menos, contiene a un polinomio mónico en una de las variables que no estaba en el ideal original; el otro es la contracción de un ideal de dimensión menor (de hecho, es la contracción de la extensión del ideal en un anillo de polinomios donde una de las variables pasa a ser considerada, junto con su inversa, parte del anillo de coeficientes). Si en nuestro proceso damos con un ideal 0-dimensional, llamaremos a otra rutina encargada específicamente de descomponer ideales 0-dimensionales.

En [16] Swanson particulariza el algoritmo **GTZ** para el caso en el que el anillo de coeficientes sea un cuerpo finito o una extensión finita de $\mathbb{Q}$.

Primeramente, vamos a enunciar dos propiedades que necesitaremos para describir el algoritmo.

(P1) Sean $\Bbbk[x_1,\ldots,x_n]$ un anillo, $\mathfrak{I}$ un ideal de $\Bbbk[x_1,\ldots,x_n]$ e y un elemento de $\Bbbk[x_1,\ldots,x_n]$ tal que $(\mathfrak{I}:y)=(\mathfrak{I}:y^2)$. Entonces,

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

siendo $(\mathfrak{I}:y)=\{x\in\Bbbk[x_1,\ldots,x_n] : xy\in\mathfrak{I}\}$; podemos encontrar una demostración en [8, Lemma 8.1].

(P2) Sea $\Bbbk[x_1,\ldots,x_d]$ un subanillo propio de $\Bbbk[x_1,\ldots,x_n]$. Entonces, para todo ideal $\mathfrak{I}\subset\Bbbk[x_1,\ldots,x_n]$ dado por una base de Gröbner reducida G podemos calcular una base de Gröbner reducida de $\mathfrak{I}\Bbbk(x_1)[x_2,\ldots,x_d]\cap\Bbbk[x_1,\ldots,x_n]$. Además, existe $b\in\Bbbk[x_1]$ tal que $\mathfrak{I}\Bbbk(x_1)[x_2,\ldots,x_d]\cap\Bbbk[x_1,\ldots,x_n]=(\mathfrak{I}:b^\infty)$, donde $(\mathfrak{I}:b^\infty)=\{g\in\Bbbk[x_1,\ldots,x_n] : b^m g\in\mathfrak{I}\text{ para algún } m>0\}$. Esta propiedad está demostrada en [8, Proposition 8.2].

A continuación, mostraremos los pasos a seguir para realizar la deseada descomposición. Primero presentaremos el algoritmo principal que reduce al caso 0-dimensional y después daremos un esquema de la subrutina de descomposición de ideales 0-dimensionales.

3.1. Algoritmo principal

Como hemos dicho antes, lo que queremos conseguir a través de este algoritmo es expresar nuestro ideal $\mathfrak{I}$ como una intersección de ideales primarios o, en su defecto, como una intersección de ideales 0-dimensionales. Para lograrlo, comenzamos utilizando la propiedad (P1), que nos permite escribir un ideal $\mathfrak{I}$ como intersección de dos ideales mayores para el orden de contención. Iteraremos este proceso tomando cada vez ideales más grandes hasta llegar al anillo total o a un ideal 0-dimensional. Enumeramos a continuación los pasos del algoritmo.

1. Si $\mathfrak{I} \subset \Bbbk[x_1, \ldots, x_n]$ es un ideal no 0-dimensional, podemos encontrar un $i \in \{1, \ldots, n\}$ tal que $\mathfrak{I} \cap \Bbbk[x_i] = (0)$. Tras una reordenación de variables, si fuera necesario, consideramos $i = 1$. Si $\mathfrak{I} \cap \Bbbk[x_1] = (0)$, por la propiedad (P2) existe $b \in \Bbbk[x_1]$ tal que $\mathfrak{I}\Bbbk(x_1)[x_2, \ldots, x_n] \cap \Bbbk[x_1, \ldots, x_n] = (\mathfrak{I} : b^\infty)$.
2. Sea $l \in \mathbb{Z}_+$ tal que $(\mathfrak{I} : b^\infty) = (\mathfrak{I} : b^l)$; por la propiedad (P1) sabemos que

$$\mathfrak{I} = (\mathfrak{I} : b^l) \cap (\mathfrak{I} + (b^l)).$$

   De la igualdad anterior podemos deducir que si encontramos una descomposición primaria de $(\mathfrak{I} : b^l)$ y otra de $(\mathfrak{I} + (b^l))$, tendremos una descomposición primaria de $\mathfrak{I}$.

   Observemos que $\Bbbk[x_1] \cap (\mathfrak{I} + (b^l)) \neq 0$. Si todavía existe otro $j \in \{1, \ldots, n\}$ tal que $\mathfrak{I} \cap \Bbbk[x_j] = (0)$ y, por lo tanto, $(\mathfrak{I} + (b^l)) \cap \Bbbk[x_j] = (0)$, podemos repetir el paso 1 para descomponer $(\mathfrak{I}+(b^l))$ en otros dos ideales. Si no existiera, entonces $(\mathfrak{I} + (b^l))$ es un ideal 0-dimensional. Si se diera el primer caso, entonces, en un número finito de pasos, llegaremos a la conclusión de que $((\mathfrak{I}+(b_1^{l_1}))+(b_2^{l_2})+\cdots)$ es 0-dimensional.

   Nos basta entonces con encontrar una descomposición primaria de $(\mathfrak{I} : b^l)$ para calcular una de $\mathfrak{I}$.
3. $(\mathfrak{I} : b^l) = \mathfrak{I}^{ec}$ es la contracción del ideal $\mathfrak{I}^e \subset \Bbbk(x_1)[x_2, \ldots, x_n]$ y su dimensión es estrictamente menor que la de $\mathfrak{I}$. Podemos aplicar a $\mathfrak{I}^e$ el mismo proceso que hemos aplicado a $\mathfrak{I}$, es decir, comprobar si $\mathfrak{I}^e$ es 0-dimensional y, en caso negativo, descomponerlo en dos ideales, uno de ellos en $\Bbbk(x_1, x_j)[x_2, \ldots, \widehat{x_j}, \ldots, x_n]$ y otro en $\Bbbk(x_1)[x_2, \ldots, x_n]$. Después de cada iteración, debemos contraer los ideales obtenidos de nuevo a nuestro anillo original $\Bbbk[x_1, \ldots, x_n]$.

   Si iteramos este proceso, en un número finito de pasos llegaremos a un ideal contenido en el anillo $\Bbbk(x_1, x_2, \ldots, x_n)$ que es cuerpo y, por lo tanto, el ideal será el total o el ideal nulo, o llegaremos a un ideal 0-dimensional, del cual obtendremos una descomposición primaria en la sección 3.2.

En **Algoritmo 1** presentamos este algoritmo de modo esquemático.

DP0C y DP0 son dos algoritmos de descomposición primaria de ideales 0-dimensionales. Como veremos en la siguiente sección, además de un algoritmo general DP0, hay un algoritmo específico DP0C para cuando el cuerpo tiene característica 0.

Algoritmo 1. Descomposición de un ideal propio de $\Bbbk[x_1, \ldots, x_n]$

procedure DPκ($\Bbbk$: cuerpo; $x = (x_1, \ldots, x_n)$: variables; $\mathfrak{I}$: ideal de $\Bbbk[x]$)
  salida: $\{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m\}$ ideales de $\Bbbk[x]$ tales que $\mathfrak{Q}_i$ es primario y $\bigcap_{i=1}^{m} \mathfrak{Q}_i = \mathfrak{I}$
  if $\mathfrak{I}$ es 0-dimensional **then**
    if $\mathrm{char}(\Bbbk) = 0$ **then**
      return DP0C($\Bbbk$, x, $\mathfrak{I}$)
    else
      return DP0($\Bbbk$, x, $\mathfrak{I}$)
    end if
  end if
  encontrar: i tal que $\mathfrak{I} \cap \Bbbk[x_i] = (0)$
  encontrar: $b \in \Bbbk[x_i]$ tal que $\mathfrak{I}\Bbbk(x_i)[x_1, \ldots, \widehat{x_i}, \ldots, x_n] \cap \Bbbk[x_1, \ldots, x_n] = (\mathfrak{I} : b^\infty)$
  encontrar: $l \in \mathbb{Z}_+$ tal que $(\mathfrak{I} : b^\infty) = (\mathfrak{I} : b^l)$
  $\{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s\} \leftarrow$ DPκ($\Bbbk(x_i)$; $(x_1, \ldots, \widehat{x_i}, \ldots, x_n)$; $(\mathfrak{I} : b^l)^e$)
  $\{\mathfrak{Q}_{s+1}, \ldots, \mathfrak{Q}_m\} \leftarrow$ DPκ($\Bbbk$; $(x_1, \ldots, x_n)$; $(\mathfrak{I} + b^l)$)
  return: $\{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m\}$ (con los ideales contraídos en el anillo original)
end procedure

3.2. Subrutina de descomposición de ideales 0-dimensionales

Para realizar la descomposición de un ideal 0-dimensional de $\Bbbk[x_1, \ldots, x_n]$, $\mathfrak{I}$, comenzamos considerando el ideal $\mathrm{Rad}(\mathfrak{I})$. Utilizaremos, para calcular una base de $\mathrm{Rad}(\mathfrak{I})$, un método descrito en [8, § 9] que utiliza una construcción de radicales tomada de [12, Lemma 92]. En ella se demuestra que podemos calcular una base de $\mathrm{Rad}(\mathfrak{I})$ tomando una base de Gröbner reducida del ideal $\mathfrak{I}$ y añadiéndole ciertos términos $f \in \mathrm{Rad}(\mathfrak{I})$. Gracias a la segunda caracterización de ideales 0-dimensionales sabemos que, para cada variable x_i, el ideal $\mathfrak{I}$ contiene un polinomio en x_i; para generar $\mathrm{Rad}(\mathfrak{I})$ tomaremos precisamente los polinomios univariados de $\mathfrak{I}$ con sus factores libres de cuadrados y se los añadiremos a una base de $\mathfrak{I}$. Es decir, si $(f(x_i)) = \mathfrak{I} \cap \Bbbk[x_i]$ y $f(x_i) = p_1^{s_1} \cdots p_t^{s_t}$ es la descomposición en factores irreducibles de f en $\Bbbk[x_i]$, entonces añadimos a la base de $\mathfrak{I}$ el polinomio $p_1 \cdots p_t \in \mathrm{Rad}(\mathfrak{I})$. Repetimos la operación para cada $1 \leq i \leq n$ y obtenemos una base de $\mathrm{Rad}(\mathfrak{I})$ a través de la cual podemos obtener una base de Gröbner de $\mathrm{Rad}(\mathfrak{I})$.

A continuación, vamos a buscar una descomposición primaria de $\mathrm{Rad}(\mathfrak{I})$. Para ello, calculamos una base de Gröbner reducida del ideal $\mathrm{Rad}(\mathfrak{I}) \cap \Bbbk[x_n]$. Dicha base constará de un solo polinomio que podremos descomponer en factores irreducibles, $g = p_1 \cdots p_s$, con $p_i \neq p_j$ si $i \neq j$. Definimos entonces los ideales generados por el propio $\mathrm{Rad}(\mathfrak{I})$ y cada uno de los factores irreducibles del polinomio anterior, $\mathfrak{I}_i = (p_i, \mathrm{Rad}(\mathfrak{I}))$ para todo $1 \leq i \leq s$ y tenemos que $\mathrm{Rad}(\mathfrak{I}) = \bigcap_{i=1}^{s} \mathfrak{I}_i$. Realizamos la misma operación considerando cada ideal $\mathfrak{I}_i \cap [\Bbbk[x_n]/p_i(x_n)]\,[x_{n-1}]$. Si iteramos el proceso n veces, tendremos un conjunto de ideales primarios $(\mathfrak{R}_i)_{i=1}^m$ cuya inter-

sección será $\mathrm{Rad}(\mathfrak{I})$. En **Algoritmo 2** mostramos de forma esquemática el método para calcular la descomposición de un ideal radical.

Algoritmo 2. Descomposición de un ideal radical, 0-dimensional

procedure DP0R($\Bbbk$: cuerpo; $x = (x_1, \ldots, x_n)$: variables; $\mathfrak{I}$: ideal radical, 0-dimensional de $\Bbbk[x]$)
  salida: $\{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m\}$ ideales de $\Bbbk[x]$ tales que $\forall i\ \mathfrak{Q}_i$ es 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 de $\mathfrak{I} \cap \Bbbk[x_n]$
  descomponer: $g = p_1 \cdots p_s$ en $\Bbbk[x_n]$
  $\mathfrak{I}_i \leftarrow (p_i, \mathfrak{I}), \quad 1 \le i \le s$
  return: $\bigcup_{i=1}^{s} \mathrm{DP0R}(\Bbbk[x_n]/p_i(x_n); x = (x_1, \ldots, x_{n-1}); \mathfrak{I}_i)$ (con los ideales contraídos en el anillo original)
end procedure

Lo único que nos falta es obtener una descomposición primaria de $\mathfrak{I}$ a partir de la descomposición primaria de $\mathrm{Rad}(\mathfrak{I}) = \bigcap_{i=1}^{m} \mathfrak{R}_i$, con $\mathfrak{R}_i$ ideal $\mathfrak{P}_i$-primario. Podemos calcular el mínimo $k \in \mathbb{Z}_+$ tal que $(\mathrm{Rad}(\mathfrak{I}))^k \subset \mathfrak{I}$ comprobando que cada uno de los generadores de $(\mathrm{Rad}(\mathfrak{I}))^k$ (que podemos obtener a partir de los generadores de $\mathrm{Rad}(\mathfrak{I})$) está en $\mathfrak{I}$. Entonces, las componentes irreducibles de nuestra descomposición primaria vendrán dadas por

$$\mathfrak{Q}_i = (\mathfrak{I}, (\mathfrak{P}_i)^k), \quad 1 \le i \le m,$$

donde los $\mathfrak{P}_i$ son los primos asociados de $\mathrm{Rad}(\mathfrak{I})$. Con lo cual, el algoritmo de descomposición primaria de un ideal 0-dimensional queda como lo presentamos en **Algoritmo 3**.

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

Comenzamos introduciendo una noción nueva: *estar en posición general*. Consideremos un ideal $\mathfrak{I}$ primo, 0-dimensional de $\Bbbk[x_1, \ldots, x_n]$. Entonces, $\mathfrak{I}$ tiene una base de Gröbner minimal de la forma

$$\begin{aligned} G &= \{g_1, \ldots, g_n\} \\ &= \{x_1 + p_1(x_2, \ldots, x_n), x_2 + p_2(x_3, \ldots, x_n), \ldots, x_{n-1} + p_{n-1}(x_n), p_n(x_n)\}. \end{aligned}$$

Podemos ver la prueba de lo que aquí afirmamos en [8]. Un cambio de coordenadas en $\Bbbk[x_1, \ldots, x_n]$ es un automorfismo lineal y biyectivo; se verifica que, para *casi todos*

Algoritmo 3. Descomposición de un ideal 0-dimensional

procedure DP0($\Bbbk$: cuerpo; $x = (x_1, \ldots, x_n)$: variables; $\mathfrak{I}$: ideal 0-dimensional de $\Bbbk[x]$)
  salida: $\{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m\}$ ideales de $\Bbbk[x]$ tales que $\forall i\ \mathfrak{Q}_i$ es primario y $\bigcap_{i=1}^{m} \mathfrak{Q}_i = \mathfrak{I}$
  for $1 \leq i \leq n$ **do**
    $p_i = \mathfrak{I} \cap \Bbbk[x_i]$
    descomponer: $p_i = q_1^{s_1} \cdots q_{j_i}^{s_{j_i}}$
    $B = B \cup (q_1 \cdots q_{j_i})$
  end for
  $\mathrm{Rad}(\mathfrak{I}) = (\mathfrak{I}, B)$
  $\mathbf{D} = \mathrm{DP0R}(\Bbbk;\ x = (x_1, \ldots, x_n);\ \mathrm{Rad}(\mathfrak{I}))$
  calcular $\min k \in \mathbb{Z}_+$ tal que $(\mathrm{Rad}(\mathfrak{I}))^k \subset \mathfrak{I}$
  return: $\bigcup_{i=1}^{m} (\mathfrak{Q}_i = (\mathfrak{I}, (\mathfrak{P}_i)^k))$ donde los $\mathfrak{P}_i$ son los primos asociados a $\mathrm{Rad}(\mathfrak{I})$ obtenidos a partir de $\mathbf{D}$
end procedure

los cambios de coordenadas de $\Bbbk[x_1, \ldots, x_n]$, $G = \{g_1, \ldots, g_n\}$ es de la forma

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

Cuando la base de Gröbner de $\mathfrak{I}$ esté definida de esa forma, diremos que $\mathfrak{I}$ se encuentra en *posición general*. Esto solo ocurre cuando la característica del cuerpo es 0; si no, el término *casi todo* carece de sentido.

En el caso de un ideal $\mathfrak{I}$ general (no necesariamente primo) 0-dimensional de $\Bbbk[x_1, \ldots, x_n]$, diremos 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 $\mathfrak{I} \subset \Bbbk[x_1, \ldots, x_n]$ que no esté en posición general, podemos transformarlo en uno que esté en posición general mediante un cambio de coordenadas. En [8, Proposition 7.1] podemos encontrar el siguiente resultado:

(P3) Sea $\Bbbk$ un cuerpo de característica 0 y sea $\mathfrak{I} \subset \Bbbk[x_1, \ldots, x_n]$ un ideal 0-dimensional. Entonces existe un conjunto abierto de Zariski no vacío $U \subset \Bbbk^{n-1}$ tal que, para todo $a = (a_1, \ldots, a_{n-1}) \in U$, el cambio de coordenadas $\phi_a : \Bbbk[x_1, \ldots, x_n] \longrightarrow \Bbbk[x_1, \ldots, x_n]$ 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.

Sea entonces $\mathfrak{I}$ un ideal 0-dimensional no primario. Si $\mathfrak{I}$ está en posición general consideramos $\mathfrak{I} \cap \Bbbk[x_n]$ y calculamos una base de Gröbner minimal de $\mathfrak{I} \cap \Bbbk[x_n]$. La base obtenida será de la forma $G = g(x_n)$. Calculamos la descomposición en factores irreducibles de g, $g = p_1^{s_1} \cdots p_m^{s_m}$ y consideramos los ideales $\mathfrak{I}_i = (\mathfrak{I}, p_i^{s_i})$, $1 \leq i \leq m$. Entonces $\{(\mathfrak{I}_i)_{i=1}^m\}$ es una descomposición de $\mathfrak{I}$, pues $\bigcap_{i=1}^m \mathfrak{I}_i = \bigcap_{i=1}^m (\mathfrak{I}, p_i^{s_i}) = \mathfrak{I}$. Vamos a ver que, además, cada $\mathfrak{I}_i$ es un ideal primario:

- $\mathfrak{I}_i$ es un ideal 0-dimensional, pues $\mathfrak{I}_i$ contiene a $\mathfrak{I}$, ideal 0-dimensional.
- $\mathfrak{I}_i$ está contenido en exactamente un ideal primo: 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 $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ los primos asociados de $\mathfrak{I}$, y sea $\mathfrak{P}_i \cap \Bbbk[x_n] = (g_i)$. Entonces, los polinomios $g_1, \ldots, g_t$ son dos a dos primos entre sí y por tanto
$$\bigcap_{i=1}^t (\mathfrak{P}_i \cap \Bbbk[x_n]) = \bigcap_{i=1}^t (g_i) = \Big(\prod_{i=1}^t g_i\Big).$$
Por otro lado, tenemos
$$\bigcap_{i=1}^t (\mathfrak{P}_i \cap \Bbbk[x_n]) = \bigcap_{i=1}^t (\mathfrak{P}_i) \cap \Bbbk[x_n] = \mathrm{Rad}(\mathfrak{I}) \cap \Bbbk[x_n].$$
Como $\mathfrak{I} \cap \Bbbk[x_n] = (g)$, entonces $\prod_{i=1}^t g_i$ divide a g y g divide a una potencia de $\prod_{i=1}^t g_i$, lo que implica que $g_i = p_i$ para todo $1 \leq i \leq t$ 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 $\Bbbk[x_1, \ldots, x_n]$ que contienen a $\mathfrak{I}_i$ entonces tenemos que $\mathrm{Rad}(\mathfrak{I}_i)$ es primo. Como además $\mathfrak{I}_i$ es 0-dimensional, podemos concluir que $\mathfrak{I}_i$ es primario.

Así que $\bigcap_{i=1}^m \mathfrak{I}_i = \mathfrak{I}$ 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 propiedad (P3) sabemos que mediante un cambio de coordenadas del tipo $x_n = x_n + \sum_{i=1}^{n-1} c_i x_i$ podemos transformarlo en un ideal en posición general.

En **Algoritmo 4** mostramos el algoritmo de forma esquemática.

Comprobar que un ideal está en posición general tiene un gran coste operacional. Por esta razón, en vez de comprobar que $\mathfrak{I}$ está en posición general tras realizar el 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

Algoritmo 4. Descomposición de un ideal 0-dimensional con coeficientes en un cuerpo de característica 0

1: **procedure** DP0C($\Bbbk$: cuerpo de característica 0; $x = (x_1, \ldots, x_n)$: variables; $\mathfrak{I}$: ideal 0-dimensional de $\Bbbk[x]$)
2: **salida:** $\{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m\}$ 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; $\bigcap_{i=1}^{m} \mathfrak{Q}_i = \mathfrak{I}$
3: C será una colección de ideales, con $C = \{\mathfrak{I}\}$
4: **while** todo $\mathfrak{J} \in C$ no es un ideal primario en posición general **do**
5: seleccionamos aleatoriamente $c_1, \ldots, c_n \in \Bbbk$
6: $x_n \leftarrow x_n + \sum_{i=1}^{n-1} c_i x_i$
7: **calcular:** $(g) = \mathfrak{I} \cap \Bbbk[x_n]$
8: **descomponer:** $g = p_1^{s_1} \cdots p_n^{s_n}$ en $\Bbbk[x_n]$
9: $\mathfrak{I}_i \leftarrow (p_i^{s_i}, \mathfrak{I})$
10: $C = \{\mathfrak{I}_1, \ldots, \mathfrak{I}_n\}$
11: **end while**
12: $x_n \leftarrow x_n - \sum_{i=1}^{n-1} c_i x_i$. Deshacemos TODOS los cambios de coordenadas que hemos hecho.
13: **return:** $\{(\mathfrak{I}_i)_{i=1}^n\}$
14: **end procedure**

test más sencillo para ver que $\mathfrak{I}_i$ es primario. El test que se utiliza en la práctica fue propuesto por [8, Proposition 5.8, Corollary 7.3] y está recogido en el siguiente criterio [9, Criterion 4.2.4].

Sea $\mathfrak{I} \subset \Bbbk[x_1, \ldots, x_n]$ un ideal propio, entonces las siguientes condiciones son equivalentes:

1. $\mathfrak{I}$ es 0-dimensional, primario y está en posición general.
2. Existen $g_1, \ldots, g_n \in \Bbbk[x_1, \ldots, x_n]$ y enteros positivos $s_1, \ldots, s_n$ tales que
   a) $\mathfrak{I} \cap \Bbbk[x_n] = (g_n^{s_n})$, g_n es irreducible;
   b) para cada $i < n$, $\mathfrak{I}$ contiene el elemento $(x_i + g_i)^{s_i}$.
3. Sea G una base de Gröbner reducida de $\mathfrak{I}$ respecto al orden lexicográfico $\mathrm{lex}(x_1 > \cdots > x_n)$. Entonces existen $g_1, \ldots, g_n \in \Bbbk[x_n]$ y enteros positivos $s_1, \ldots, s_n$ tales que
   a) $g_i^{s_i} \in G$ y g_i es irreducible;
   b) $(x_i + g_i)^{s_i}$ es congruente con un elemento de $G \cap \Bbbk[x_i, \ldots, x_n]$ módulo $(g_n, x_{n-1} + g_{n-1}, \ldots, x_{i+1} + g_{i+1})$ para $i = 1, \ldots, n-1$.

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

4. Descomposición primaria en ideales particulares

Además del algoritmo aquí descrito, existen otros algoritmos que no utilizan las bases de Gröbner, como el de Eisenbud, Huneke y Vasconcelos [6], o versiones mejoradas de **GTZ**, como la que presentan Shimoyama y Yokoyama en su artículo [13]. Podemos encontrar varios de los algoritmos aquí mencionados implementados en el programa Singular en [4].

Existen también varios casos en los que podemos obtener una descomposición primaria de una forma más sencilla o, simplemente, de una forma diferente a la aquí expuesta. Si el ideal presenta alguna característica particular, por ejemplo, si es monomial, entonces existe un método que utiliza la *dualidad de Alexander* (podemos encontrar una definición de la dualidad de Alexander, así como un método de descomposición de ideales monomiales, en [10]). Además, existe una librería en Singular que recoge varios métodos para descomponer ideales monomiales [2]. Si el ideal es binomial, existen algoritmos específicos para la obtención de una descomposición primaria (el lector interesado puede consultar el artículo [11] donde encontrará una versión mejorada de un algoritmo propuesto por Eisenbud y Sturmfels en 1996).

Referencias

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

[2] I. Bermejo, E. García-Llorente y Ph. Giménez, monomialideal.lib: A Singular 3-1-16 library for computing primary and irreducible decompositions of monomial ideals, 2012.

[3] D. Cox, J. Little y D. O'Shea, *Ideals, Varieties, and Algorithms*, 3th edition, Undergraduate Texts in Mathematics, Springer, 2007.

[4] W. Decker, G.-M. Greuel y G. Pfister, Primary decomposition: algorithms and comparisons, *Algorithmic algebra and number theory (Heidelberg, 1997)*, 187–220, Springer, 1999.

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

[6] D. Eisenbud, C. Huneke y W. Vasconcelos, Direct methods for primary decomposition, *Invent. Math.* **110** (1992), 207–235.

[7] U. Etayo Rodríguez, Aspectos computacionales de la descomposicion primaria, Trabajo fin de grado, Facultad de Ciencias, Universidad de Valladolid, 2014, `http://uvadoc.uva.es/handle/10324/6261`

[8] P. Gianni, B. Trager y G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals. Computational aspects of commutative algebra, *J. Symbolic Comput.* **6** (1988), 149–167.

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

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

[11] I. Ojeda Martínez de Castilla y R. Piedra Sánchez, Cellular binomial ideals. Primary decomposition of binomial ideals, *J. Symbolic Comput.* **30** (2000), 383–400.

[12] A. Seidenberg, Constructions in algebra, *Trans. Amer. Math. Soc.* **197** (1974), 273–313.

[13] T. Shimoyama y K. Yokoyama, Localization and primary decomposition of polynomial Ideals, *J. Symbolic Comput.* **22** (1996), 247–277,

[14] Singular 3-1-6, A computer algebra system for polynomial computations, 2012. Disponible en `http://www.singular.uni-kl.de`

[15] Surfer A program by the Mathematisches Forschungsinstitut Oberwolfach (MFO) in collaboration with the Martin Luther University Halle-Wittenberg. Disponible en `http://imaginary.org/es/program/surfer`

[16] I. Swanson, Lectures in Valladolid, EACA's Second International School on Computer Algebra and Applications, 2013. Disponible en `http://people.reed.edu/~iswanson/EACA.pdf`

Ujué Etayo Rodríguez, Universidad de Cantabria
Correo electrónico: `ujue.etayo@gmail.com`