Universidad de Valladolid

Facultad de Ciencias

Resolución de sistemas de ecuaciones algebraicas mediante el método de cadenas regulares y otros algoritmos de triangularización

TRABAJO DE FIN DE GRADO

GRADO EN MATEMÁTICAS

Autor: David Andrés Gutiérrez

Tutor: José M. Cano Torres

Índice general

Capítulo 1

Introducción

La resolución de sistemas de ecuaciones polinomiales es un problema que está presente en prácticamente todas las ramas de la ciencia e incluso en muchas situaciones de la vida cotidiana. Por ello se hace necesario el estudio de algoritmos que nos permitan saber si un sistema tiene o no soluciones, en el caso de tenerlas saber si son un número finito, o bien existe un número infinito de ellas y ver si somos capaces de describir estas soluciones de una forma explícita Por lo tanto necesitamos desarrollar algoritmos que nos ayuden a responder estas preguntas.

La computación mediante bases de Gröbner es una de las principales herramientas para resolver sistemas de ecuaciones polinomiales e incluso responder a otra serie de problemas relacionados con la teoría de ideales polinomiales como la pertenencia de un polinomio a un cierto ideal o a su radical. Las bases de Gröbner se estudian en las asignaturas de Ecuaciones Algebraicas y de Álgebra Conmutativa y Computacional, sin embargo existen otros métodos que se ocupan de estos problemas y que no se estudian en el Grado de Matemáticas.

Por tanto el objetivo principal del trabajo es desarrollar uno de estos algoritmos alternativos. En particular, nos centraremos en la resolución de sistemas de ecuaciones polinomiales, pero veremos que seremos capaces de dar respuesta también a otras cuestiones.

Al igual que con los algoritmos que utilizan las bases de Gröbner, los algoritmos que se desarrollarán estarán basados en unos conjuntos de polinomios especiales a los que llamaremos cadenas regulares. La fuente bibliográfica que se ha seguido para el desarrollo de las propiedades de las cadenas regulares ha sido el artículo de Kalkbrenner [1]. En él se sientan las bases del concepto de cadena regular y se desarrollan los primeros algoritmos que utilizan este concepto. Posteriormente a este artículo, se han publicado gran cantidad de trabajos, entre ellos por ejemplo [7], [8] y [9], que desarrollan el concepto de cadena regular desde puntos de vista más algebraicos e implementando algoritmos muy eficientes. Existe un paquete en MAPLE llamado *RegularChains* que está dedicado exclusivamente a este método. Éste paquete lleva muchos años desarrollandose y ha llevado mucho trabajo, toda la información se encuentra en el página web [10]. Sin embargo, el objetivo de nuestro trabajo es sentar las bases de las cadenas regulares y de los primeros algoritmos siguiendo el artículo de Kalkbrenner.

Vamos a hacer ahora un pequeño resumen del trabajo viendo la estructura del mismo y los contenidos de cada capítulo. Comenzaremos el trabajo dando unas primeras nociones y conceptos

que serán necesarios para el desarrollo del algoritmo. En la primera parte se desarrollarán los conceptos de dependencia algebraica y de grado de trascendencia, claves en todo el trabajo. Después se recordarán los conceptos de variedad algebraica afín y de ideal asociado a una variedad, además de desarrollar una serie de propiedades de estos. Se continúa definiendo los conceptos de cero genérico y punto genérico con el objetivo final de demostrar que toda variedad es irreducible si y solo si tiene un punto genérico. En la siguiente sección se tratará de definir el concepto de dimensión de una variedad mediante el grado de trascendencia de los puntos genéricos de sus variedades irreducibles. Para terminar con el primer capítulo se desarrollarán algoritmos para calcular el máximo común divisor de un conjunto de polinomios en una variable y también desarrollaremos un algoritmo de pseudodivisión entre dos polinomios en $K[x_1, \ldots, x_n]$ los cuales serán claves en los algoritmos que desarrollaremos posteriormente.

El tercer capítulo se centrará en demostrar uno de los teoremas más importantes de la geometría algebraica el Hilbert's Nullstellensatz. En este trabajo se demostrará utilizando el Teorema de la Extensión el cual posee varias demostraciones una de ellas empleando bases de Gröbner. Dado que estamos desarrollando un algoritmo alternativo a ellas usaremos una demostración basada en resultantes.

A partir de aquí comenzará la parte principal del trabajo. Empezaremos definiendo el concepto de cadena regular y de cero regular, se relacionará estos ceros regulares con los puntos genéricos y se dará la definición de variedad representada por una cadena regular. A partir de este concepto se planteará el problema de describir la variedad como unión de estas variedades representadas por cadenas regulares. Problema para el cual se necesitarán desarrollar una serie de algoritmos en los siguientes capítulos.

En el quinto capítulo desarrollaremos algoritmos que nos permitirán trabajar en cuerpos de extensión dados por cadenas regulares. Se desarrollarán tres algoritmos $\mathbf{common}_n$, $\mathbf{separate}_n$ y $\mathbf{ggcd}_n$. El algoritmo $\mathbf{common}_n$ se utilizará para encontrar los ceros regulares de una cadena regular que también son ceros de otro polinomio que pasamos en la entrada. El algoritmo $\mathbf{separate}_n$ se utilizará para encontrar los ceros regulares de una cadena regular que no son ceros de otro polinomio que pasamos en la entrada. Finalmente el algoritmo $\mathbf{ggcd}_n$ es un algoritmo para calcular el máximo común divisor generalizado de un conjunto de polinomios en $K[x_1, \ldots, x_n]$ teniendo en cuenta también los ceros regulares de una cadena regular. Todos los algoritmos se definen de forma recursiva a partir de $\mathbf{ggcd}_1$ el cual se basa solamente en el algoritmo **gcd** que se define en el capítulo 2. La mayor parte del capítulo se basa en la justificación de la terminación y la corrección de estos algoritmos. Las demostraciones son muy técnicas y están escritas de manera completa en esta memoria. Es importante destacar que utilizan todas una inducción sobre $\mathbf{ggcd}_n$.

En el sexto capítulo se desarrollará el algoritmo $\mathbf{solve}_n$ capaz de resolver el problema de describir una variedad como unión de representantes de cadenas regulares. Este algoritmo se basa en el algoritmo $\mathbf{ggcd}_n$ del capítulo 5. También el algoritmo $\mathbf{solve}_n$ se construirá de forma recursiva a partir de $\mathbf{solve}_1$ el cual se basa solamente en el algoritmo **gcd** definido en el capítulo 2. Al igual que en el capítulo anterior la mayor parte del capítulo se centra en la demostración de la terminación y la corrección, la cual también es bastante técnica y se basa en una inducción sobre $\mathbf{solve}_n$.

Para finalizar el trabajo se mostrarán las distintas aplicaciones que se le pueden dar al problema resuelto y a los algoritmos desarrollados. Entre ellas encuentra calcular la dimensión de un ideal, resolver sistemas de ecuaciones y determinar la pertenencia al radical de un ideal.

Capítulo 2

Definiciones y conceptos previos

En este capítulo se desarrollarán todos los conceptos teóricos necesarios para poder definir los conceptos de cadena regular y cero regular, y luego poder desarrollar los algoritmos. Se comenzará desarrollando la teoría necesaria para dar una definición rigurosa del grado de trascendencia concepto muy importante durante todo el trabajo. Después de esto se recordarán los conceptos relacionados con las variedades y los ideales asociados a una variedad, para luego dar las definiciones de cero genérico y punto genérico y estudiar la relación entre ambos. Para terminar con las variedades se dará una pequeña definición sobre qué se entiende como dimensión de una variedad. Para finalizar se describirán los algoritmos para calcular el máximo común divisor en una variable y un algoritmo de pseudodivisión entre dos polinomios en $K[x_1, \ldots, x_n]$.

2.1. Dependencia algebraica y grado de trascendencia

En esta sección trabajaremos primero con el concepto de relación de dependencia abstracta para el cual obtendremos una serie de propiedades que luego llevaremos al caso específico y que a nosotros nos interesa que es la dependencia algebraica.
A partir de ésta, definiremos con rigurosidad el concepto de grado de trascendencia, para luego dar una serie de resultados sobre extensiones de cuerpos que necesitaremos en posteriores secciones. Para esta primera parte seguiremos el libro de P. M. Cohn [6].

Relación de dependencia abstracta

Definición 2.1.1. *Sea S un conjunto, entendemos por relación de dependencia en S a una aplicación $\mathbb{L} : \mathcal{P}(S) \to \mathcal{P}(S)$, que lleva subconjuntos de S en subconjuntos de S, donde si $y \in \mathbb{L}(X)$, diremos que y depende de X. La aplicación ha de cumplir lo siguiente:*

1. *Si $X = \{x_1, \ldots, x_n\}$, entonces $x_i \in \mathbb{L}(X)$.*
2. *Si $Y = \{y_1, \ldots, y_n\}$, $z \in \mathbb{L}(Y)$ y además $y_i \in \mathbb{L}(X)$ para todo i, entonces $z \in \mathbb{L}(X)$.*
3. *Si $y \in \mathbb{L}(\{x_1, \ldots, x_n\})$ pero $y \notin \mathbb{L}(\{x_2, \ldots, x_n\})$ entonces $x_1 \in \mathbb{L}(\{y, x_2, \ldots, x_n\})$.*

Nota 1. *De las condiciones 1 y 2 obtenemos que si y depende de X' y $X' \subseteq X$ entonces y depende de X.*

Proposición 1. *Se puede extender la noción de dependencia a conjuntos infinitos si decimos que y depende de $X \subseteq S$ si $\exists X' \subseteq X$ finito tal que y dependa de X'.*

Demostración: Veamos que con esta definición se verifican las tres condiciones.
Sea X un conjunto infinito. Para que se verifique la condición (1) hay que probar que todo elemento de X depende de un subconjunto finito de X, esto se verifica siempre que el subconjunto finito contenga al elemento, pues para conjuntos finitos es la condición (1).

Veamos la condición (2). Sea Y un conjunto infinito. Si $z \in \mathbb{L}(Y)$, entonces existe $Y' \subseteq Y$ finito tal que $z \in \mathbb{L}(Y')$, tenemos también que para todo elemento $y \in Y$, $y \in \mathbb{L}(X)$. Esto quiere decir que existe $X' \subseteq X$ finito tal que $y \in \mathbb{L}(X')$, en particular nos podemos quedar con $y \in Y'$,y podemos tomar la unión de los X' el cual seguirá siendo finito y por la nota 1 todos los y dependen de este conjunto. Por tanto podemos aplicar el caso finito y tenemos que $z \in \mathbb{L}(\bigcup X')$ y por tanto $z \in \mathbb{L}(X)$.

Veamos la condición (3). Si $y \in \mathbb{L}(X)$, pero $y \notin \mathbb{L}(X \setminus \{x\})$. Entonces existirá X' tal que $y \in \mathbb{L}(X')$, si $x \in X'$ lo dejamos como está, y si no entonces lo añadimos, por la nota 1 y seguirá siendo dependiente y es claro que $X' \cup \{x\}$ es finito. Dado que $y \notin \mathbb{L}(X \setminus \{x\})$ entonces $y \notin \mathbb{L}(X' \cup \{x\} \setminus \{x\})$ pues si no $y \in \mathbb{L}(X \setminus \{x\})$, entonces aplicando el caso finito de (3) tenemos que $x \in \mathbb{L}(\{y, X' \setminus \{x\}\})$ y por tanto $x \in \mathbb{L}(\{y, X \setminus \{x\}\})$. □

Ejemplo 2.1.1. *Consideremos la dependencia lineal en un espacio vectorial sobre un cuerpo, o más generalmente, en un modulo M sobre un cuerpo R. Recordemos que un elemento $y \in M$ es linealmente dependiente de un conjunto X si:*

$$y = \sum c_i x_i, \ \ para \ \ algun \ \ c_i \in R, \ \ x_i \in X.$$

Veamos que cumple las condiciones de relación de dependencia.

Condición (1): Tenemos que $x_i = \sum c_j x_j$ con $c_j = 0$ si $j \neq i$ y $c_i = 1$, el elemento neutro para la suma y el producto siempre siempre existen en un anillo.

Condición (2): Si $z = \sum a_i y_i$ e $y_i = \sum c_j x_j$, entonces $z = \sum\limits_i a_i \sum\limits_j c_j x_j$ y de aquí $z = \sum\limits_j (\sum\limits_i a_i c_j) x_j$, donde tenemos que $\sum\limits_i a_i c_j$ es un elemento del anillo y tenemos lo que queríamos.

Condición (3): Si $y = \sum\limits_{i=1} a_i x_i$, pero si eliminamos x_1 no hay dependencia,entonces ha de ser $a_1 \neq 0$ por tanto si reescribimos lo primero como $y - \sum\limits_{i=2} a_i x_i = a_1 x_1$ Como estamos en un cuerpo podemos multiplicar por el inverso y por tanto despejar x_1 con lo que obtenemos lo buscado.

Definición 2.1.2. *Sea $X = \{x_i | i \in I\} \subseteq S$, diremos que X es independiente si ningún x_i depende de $\{x_j | j \neq i\}$.*
Una familia independiente que genera S se llama base de S, lo que quiere decir que todo elemento de S depende de X.

Podemos reconocer las bases de la siguiente manera:

Proposición 2. *Sea S un conjunto con una relación de dependencia. Para $X \subseteq S$ las siguientes condiciones son equivalentes:*

1. *X es un subconjunto independiente maximal de S.*
2. *X es un generador minimal.*
3. *X es una base de S.*

Demostración: (1) $\Leftrightarrow$ (3). Sea X un subconjunto maximal independiente de S, veamos que todo elemento de S depende de X. Sea $y \in S$.
Si $y \in X$ entonces y depende de X por la condición 1.
Si $y \notin X$ entonces $X \cup \{y\}$ es dependiente por maximalidad, así que algún elemento depende del resto. Sea $x \in X$ dicho elemento, como X es independiente x no depende de $X \setminus \{x\}$ entonces por la propiedad 3, y depende de X. Y con ello se prueba que X genera S.
Probemos ahora la otra implicación, sea X una base, entonces es independiente pero todo $y \notin X$ es dependiente de X, así que X es maximal.

(2) $\Leftrightarrow$ (3). Sea X un generador minimal, hay que ver que es independiente. Si X fuera dependiente, tomamos $x \in X$ el elemento que depende del resto, entonces tendremos que todo elemento de X depende de $X \setminus \{x\}$ por tanto podemos aplicar la condición 2 y deducir que todo elemento que dependa de X dependerá también de $X \setminus \{x\}$ y por tanto será también generador. Esto contradice la minimalidad así que X es independiente y por tanto base.
Supongamos ahora que X es base, entonces es independiente, así que ningún elemento es dependiente del resto y por ello el conjunto es generador minimal. □

Definición 2.1.3. *Sea X un conjunto. Si el conjunto X es finito diremos que el cardinal de X, denotado por $|X|$, es el número de elementos del conjunto. Para extender la noción de cardinalidad a conjuntos infinitos se empieza definiendo la noción de comparación entre cardinales de conjuntos arbitrarios.*
Se dice que dos conjuntos A y B tienen el mismo cardinal si existe una biyección entre ambos. También se puede decir que ambos conjuntos son equipotentes.
Se dice que $|A| \leq |B|$ si existe una función inyectiva de A en B.
Se dice que $|A| < |B|$ si existe una función inyectiva pero no existe ninguna función biyectiva.

Lema 1. *Sea S un conjunto con una relación de dependencia. Sean $X \subseteq S$ independiente e Y un generador de S entonces $\exists Y' \subseteq Y \setminus X \cap Y' = \emptyset$ y $X \cup Y'$ es base de S, esto quiere decir que se puede completar cualquier conjunto independiente a una base añadiendo elementos de un conjunto generador. Además, si Y es finito, entonces X es finito y $|X \cup Y'| \leq |Y|$.*

Demostración: Sea $\mathcal{L} = \{Z \subseteq S \text{ independiente } \setminus X \subseteq Z \subseteq X \cup Y\}$. Podemos aplicar el lema de Zorn a $\mathcal{L}$, este lema nos dice que todo conjunto parcialmente ordenado en el que toda cadena tiene una cota superior, contiene al menos un elemento maximal. Puesto que el conjunto está parcialmente ordenado y el elemento $X \cup Y$ es cota superior, entonces se admite un elemento maximal al que llamaremos B. Por construcción del conjunto, B se compone de X y términos de Y, es decir,$B = X \cup Y'$, tomamos Y' de forma que $X \cap Y' = \emptyset$. Debido a la maximalidad todo elemento de Y depende de B, $\mathbb{L}(B) \supseteq \mathbb{L}(Y) = S$, y B es una base.
Supongamos ahora que Y es finito. Tenemos que ver que empezando con cualquier $X' \subseteq X$ finito podemos obtener una base añadiendo como mucho $|Y| - |X'|$ elementos.

Usaremos una inducción sobre $|X'|$; cuando $|X'| = 0$, por la primera parte elegimos $B \subseteq Y$ que sea base. Supondremos ahora $|X'| = r > 0$, por la hipótesis de inducción podemos construir una base con $n - (r-1)$ de Y y añadiendo $r-1$ elementos de X', sea $B_{r-1} = \{x_1, \ldots, x_{r-1}, y_r, \ldots, y_n\}$, $x_j \in X'$, $y_j \in Y$. Con otro elemento $x_r \in X'$ formamos el generador $B_{r-1} \cup \{x_r\}$ que contiene a $\{x_1, \ldots, x_r\}$ que es independiente. Por la primera parte existe una base $B_r \supseteq \{x_1, \ldots, x_r\}$, pero B_r no puede contener a todos los y_j porque la familia $\{x_1, \ldots, x_r, y_r, \ldots, y_n\}$ es dependiente (x_r depende del resto, pues el resto formaban una base). Por lo tanto se ha de eliminar un elemento de los y_j, y por tanto obtenemos una base de la forma: $B_r = \{x_1, \ldots, x_r, y_{r+1}, \ldots, y_n\}$,$x_j \in X'$,$y_j \in Y$ que esta en la forma que queremos y contiene como mucho n elementos. Por inducción obtenemos una base de como mucho $|Y|$ elementos, formada por los elementos de X' junto con elementos de Y. En particular, $|X'| \leqslant |Y|$ y como X' era cualquier subconjunto finito de X, entonces X tiene que ser finito y si la base es $X \cup Y'$, entonces $|X \cup Y'| \leqslant |Y|$. □

Corolario 2.1.1. *Sea S un conjunto con relación de dependencia. Si S tiene un generador C finito, entonces cualquier familia independiente tiene como mucho $|C|$ elementos y dos bases cualesquiera tienen el mismo número de elementos.*

Demostración: Por la última parte del lema anterior, el número de elementos en una familia independiente esta acotado por el número de elementos de un conjunto generador. En particular, dadas dos bases B, C, si B es finita, $|C| \leqslant |B|$ y también si C es finita, $|B| \leqslant |C|$, por el teorema de Bernstein $|B| = |C|$. □

Ahora trataremos de demostrar que dos bases cualesquiera, finitas o no, tienen el mismo cardinal. Para ello necesitamos un lema previo, el cual no demostraremos pues necesita conceptos de teoría de cardinales que no desarrollaremos pues exceden el ámbito del trabajo.

Lema 2. *Para cualquier cardinal infinito α,*

$$\aleph_0 \alpha = \alpha,$$

donde $\aleph_0$ denota el cardinal de $\mathbb{N}$

Proposición 3. *Sea S un conjunto con una relación de dependencia y supongamos que S tiene un conjunto minimal generador X. Si X es infinito, entonces cualquier conjunto generador de S tiene cardinal mayor. En particular, S no tiene conjuntos generadores finitos y dos conjuntos generadores minimales cualesquiera tienen el mismo cardinal.*

Demostración: Sea Y cualquier conjunto generador de S. Cada $y \in Y$ depende de X y también de un subconjunto $X_y \subseteq X$ finito. Veamos que $X = \bigcup_{y \in Y} X_y$. El conjunto generado por $\bigcup_{y \in Y} X_y$ contiene cada $y \in Y$ y por ello ha de ser S. Entonces $\bigcup_{y \in Y} X_y \subseteq X$ generando S y la igualdad se sigue de la minimalidad de X. Si Y fuera finito entonces X se expresaría como unión finita de conjuntos finitos, contradiciendo que X sea finito. Tenemos:

$$\alpha = |X| \leq \sum |X_y| \leq \aleph_0 \beta = \beta.$$

Donde la última igualdad se da por el lema anterior. Obtenemos $\alpha \leq \beta$; si Y fuera minimal, podemos intercambiar roles y obtener la otra desigualdad. □

Puesto que para una relación de dependencia los conceptos de conjuntos generadores minimales y de base son equivalentes, la proposición anterior equivale a decir que todos conjunto con relación de dependencia tiene una base y que dos bases cualesquiera tienen el mismo cardinal.

Dependencia algebraica

Definición 2.1.4. *Dada cualquier extensión de cuerpos E/K, sean $u_1, \ldots, u_m, v \in E$ diremos que v es algebraicamente dependiente de $u_1, \ldots, u_m$ sobre K si v es algebraico sobre $K(u_1, \ldots, u_m)$. Esto significa que v satisface una ecuación con coeficientes en $K(u_1, \ldots, u_m)$, es decir:*

$$a_0 v^d + a_1 v^{d-1} + \ldots + a_d = 0, \tag{2.1}$$

donde $a_i \in K[u_1, \ldots, u_m]$, $a_0 \neq 0$ y $d \geqslant 1$.

Proposición 4. *La dependencia algebraica es una relación de dependencia. Es decir verifica las condiciones 1-3.*

Demostración: Veamos que se verifican las tres condiciones:

1. u_i es algebraicamente dependiente de $u_1, \ldots, u_m$.
2. Si w es algebraicamente dependiente de $v_1, \ldots, v_n$ y cada v_i es algebraicamente dependiente de $u_1, \ldots, u_m$ entonces w es algebraicamente dependiente de $u_1, \ldots, u_m$.
3. Si v es algebraicamente dependiente de $u_1, \ldots, u_m$ pero no de $u_2, \ldots, u_m$ entonces u_1 es alegraicamente dependiente de $v, u_2, \ldots, u_m$.

La primera se prueba tomando la ecuación con coeficientes en $K[u_1, \ldots, u_m]$, $u_i - u_i = 0$, donde vemos que es de la forma de la definición con $d = 1, a_0 = 1, a_1 = u_1$.

Para probar la segunda tenemos que v_i es algebraico sobre $K(u_1, \ldots, u_m)$ y tenemos:

$$K(u_1, \ldots, u_m) \subseteq K(u_1, \ldots, u_m, v_1) \subseteq \ldots \subseteq K(u_1, \ldots, u_m, v_1, \ldots, v_n),$$

cada extensión es de grado finito por ser extensiones algebraicas, además como w es algebraico sobre $K(v_1, \ldots, v_n)$ obviamente lo será también de $K(u_1, \ldots, u_m, v_1, \ldots, v_n)$ y al igual que ante su grado de extensión es finito. Aplicando la fórmula de producto de grados a las extensiones,

$$K(u_1, \ldots, u_m) \subseteq K(u_1, \ldots, u_m, v_1, \ldots, v_n) \subseteq K(u_1, \ldots, u_m, v_1, \ldots, v_n, w),$$

obtenemos que el grado de la extensión $K(u_1, \ldots, u_m, v_1, \ldots, v_n, w)$ sobre $K(u_1, \ldots, u_m)$ es finito y por tanto w es algebraicamente dependiente de $u_1, \ldots, u_m$.

Para probar la tercera, tenemos por hipótesis una relación de la forma:

$$a_0 v^d + a_1 v^{d-1} + \ldots + a_d = 0, \;\; a_i \in K[u_1, \ldots, u_m].$$

Si reescribimos esta fórmula en términos de u_1, tendremos:

$$b_0 u_1^r + b_1 u_1^{r-1} + b_r = 0, \tag{2.2}$$

donde $b_i \in K[u_2, \ldots, u_m, v]$. Por hipótesis, $a_0 \neq 0$; si $b_i = 0 \; \forall i = 0, \ldots, r-1$, entonces $b_r = 0$ y por ello habría una relación de $u_2, \ldots, u_m, v$ y entonces v sería algebraicamente dependiente de $u_2, \ldots, u_r$ en contra de las hipótesis. Entonces no todos los b_i se anulan y la ecuación 2.2 nos dice que u_1 es algebraicamente dependiente de $u_2, \ldots, u_m, v$. Y queda probado. □

Ahora que hemos probado esto podemos utilizar todas las nociones probadas para las relaciones de dependencia, con lo que tenemos:

Definición 2.1.5. *Un subconjunto X de E es algebraicamente independiente sobre K si ningún elemento de X es algebraicamente dependiente del resto. Si el conjunto X es finito con $X = \{x_1, \ldots, x_n\}$ esta noción equivale a que los productos de potencias $x_1^{a_1} \ldots x_n^{a_n}$ sean linealmente independientes.*

Definición 2.1.6. *Sea $B \subseteq E$ algebraicamente independiente y tal que todo elemento de E es algebraicamente dependiente de B sobre K, entonces B se llama base de trascendencia de E sobre K.*

Por el lema 1 y la proposición 3:

Teorema 2.1.2. *Dada una extensión E/K, cualquier subconjunto algebraicamente independiente de E se puede completar a una base de trascendencia de E/K y dos bases cualesquiera tienen el mismo número de elementos.*

Definición 2.1.7. *El número de elementos de una base de trascendencia de E/K se llama grado de trascendencia o dimensión de E/K y se denota $tr.deg(E/K)$. Cualquier extensión de grado 0 se llama algebraica. Equivalentemente E/K es algebraica si todo elemento de E es algebraico sobre K.*

El grado de trascendencia cumple la siguiente fórmula:

Proposición 5. *Para tres cuerpos cualesquiera $K \subseteq E \subseteq F$ tenemos:*

$$tr.deg(F/K) = tr.deg(F/E) + tr.deg(E/K).$$

Demostración: Sea X una base de trascendencia para E/K e Y una para F/E. Entonces ningún elemento de Y está en E, pero lo está todo elemento de X por ello $X \cap Y = \emptyset$ y para tener lo que queremos vale probar que $X \cup Y$ es base de trascendencia de F/K. Cualquier elemento $z \in F$ es algebraico sobre $E(Y)$. Veremos que z es algebraicamente dependiente de un conjunto finito sobre K, sea $u_1, \ldots, u_r, y_1, \ldots, y_s$, donde $u_i \in E$ y $y_j \in Y$. Cada u_i es algebraicamente dependiente de X sobre K, de aquí z es algebraicamente dependiente por transitividad de $X \cup Y$ sobre K. Ahora debemos probar que $X \cup Y$ es algebraicamente independiente. Supongamos que no lo es, existe una relación polinomial:

$$f(x_1, \ldots, x_r, y_1, \ldots, y_s) = 0, \;\; x_i \in X, \;\; y_j \in Y,$$

con coeficientes en K. Sin embargo si reescribimos este polinomio en función de las y_i todos los coeficientes han de anularse, pues $x_i \in E$ debido a que Y es algebraicamente independiente sobre E y los coeficientes tienen que anularse. Pero estos coeficientes son términos en x_i, así que obtenemos una relación algebraica entre los x_i, que deben ser triviales y la relación f es la trivial. Por ello $X \cup Y$ es algebraicamente independiente sobre K, por ello es base de trascendencia para F/K y se da lo que queríamos. □

En particular, para extensiones algebraicas:

Corolario 2.1.3. *Una extensión algebraica de una extensión algebraica es a su vez algebraica.*

Definición 2.1.8. *Una extensión de cuerpos es trascendental si no es algebraica, es decir, si tiene grado de trascendencia positivo. Diremos que una extensión E/K tiene grado infinito de trascendencia si no existe un conjunto $X \subseteq E$ finito algebraicamente independiente con $E = K(X)$.*

Definición 2.1.9. *Un cuerpo K se dice que es algebraicamente cerrado si en $K[x]$ todo polinomio se puede descomponer en factores lineales. Es equivalente a decir que todo polinomio no constante posee al menos una raíz en K.*

Una vez definidos los conceptos de grado infinito de trascendencia y de cuerpo algebraicamente cerrado vamos a definir el concepto de cuerpo universal. Este cuerpo es importante pues las variedades van a estar definidas sobre un cuerpo universal el cual va ser extensión de un cuerpo base cualquiera K.

Definición 2.1.10. *Diremos que un cuerpo $\overline{K}$ es un cuerpo universal si es algebraicamente cerrado y tiene grado infinito de trascendencia sobre K.*

Lema 3. *Si existe un isomorfismo de cuerpos $K \cong K'$ un polinomio irreducible $\varphi(x)$ en $K[x]$ se lleva a un polinomio $\varphi'(x)$ en $K'[x]$ y si α es una raíz de $\varphi(x)$ en un cuerpo de extensión de K y α' una raíz de $\varphi'(x)$ en un cuerpo de extensión de K', entonces el isomorfismo $K \cong K'$ se puede extender a un isomorfismo $K(\alpha) \cong K'(\alpha')$, que lleva α en α'.*

Demostración: Los elementos de $K(\alpha)$ son de la forma $\sum c_k\alpha^k$ con $c_k \in K$ y operamos con ellos al igual que con los polinomios modulo $\varphi(x)$. Análogamente, los elementos de $K'(\alpha')$ son de la forma $\sum c'_k\alpha'^k$ con $c'_k \in K'$ y operamos con ellos al igual que con los polinomios modulo $\varphi'(x)$. Definimos la aplicación $f : \sum c_k\alpha^k \to \sum c'_k\alpha'^k$ (donde $g : c_k \to c'_k$ es el isomorfismo de la hipótesis). Veamos que esta aplicación está bien definida y es un isomorfismo.
Está bien definida pues a un elemento le corresponde una única imagen por como está definida la aplicación y que al ser $g : c_k \to c'_k$ isomorfismo la imagen de cada elemento c_k está bien definida.
Veamos que es inyectiva: Sean $u, v \in K(\alpha)$ con $u \neq v$ entonces u, v son de la forma $u = \sum c_k\alpha^k$, $v = \sum b_k\alpha^k$ donde al menos un $b_i \neq c_i$ pues si no tendríamos $u = v$, entonces tenemos que $b'_i \neq c'_i$, por ser g isomorfismo, si ahora tomamos $f(u) = \sum c'_k\alpha'^k$ y $f(v) = \sum b'_k\alpha'^k$ tenemos que son distintos pues $b'_i \neq c'_i$.
Es sobreyectiva pues todo elemento de $K'(\alpha')$ se escribe $\sum c'_k\alpha'^k$ y al ser g isomorfismo es sobreyectiva. Por tanto todo elemento de $K'(\alpha')$ esta asociado a uno de $K(\alpha)$, $\sum c_k\alpha^k$ pues g al ser isomorfismo es sobreyectiva también.
Para concluir que f es isomorfismo falta ver que conserva las operaciones. Sea $u = \sum c_k\alpha^k$ y $v = \sum c_k\alpha^k$, donde podemos suponer que ambos llegan hasta el mismo indice pues si uno llega a un índice menor que el otro se completará con ceros. Veamos que $f(u + v) = f(u) + f(v)$ con la suma definida en los polinomios en una variable modulo $\varphi(x)$ e $\varphi'(x)$.

$$f(u+v) = f(\sum c_k\alpha^k + \sum b_k\alpha^k) = f(\sum (c_k + b_k)\alpha^k) = \sum (c_k + b_k)'\alpha'^k,$$

donde tenemos que $b_k + c_k \in K$ por ser K cuerpo y por tanto tiene imagen por el isomorfismo.

$$f(u) + f(v) = f(\sum c_k\alpha^k) + f(\sum b_k\alpha^k) = \sum c'_k\alpha'^k + \sum b'_k\alpha'^k = \sum (c'_k + b'_k)\alpha'^k,$$

dado que g es isomorfismo conserva también operaciones y por ello
$(c_k + b_k)' = c'_k + b'_k$ y tenemos la igualdad.

Veamos que $f(u \cdot v) = f(u) \cdot f(v)$ con la suma definida en los polinomios en una variable modulo $\varphi(x)$ e $\varphi'(x)$.

$$f(u \cdot v) = f(\sum c_k \alpha^k \cdot \sum b_k \alpha^k) = f(\sum r_k \alpha^k) = \sum r'_k \alpha'^k,$$

donde r_k es una combinación lineal de productos $c_i b_j$.

$$f(u) \cdot f(v) = \sum c'_k \alpha'^k \cdot \sum b'_k \alpha'^k = \sum r'_k \alpha'^k,$$

donde r'_k es la misma combinación lineal que la de r_k. Donde tenemos que ambos r'_k son iguales pues el isomorfismo g lleva productos en productos y sumas en sumas y por ello lleva una combinación lineal en la otra. Con lo que se prueba que f es isomorfismo. Y es claro que este isomorfismo envía α en α'. □

Teorema 2.1.4. *Cualquier extensión de cuerpos $K(\alpha_1, \ldots, \alpha_n)$ obtenida añadiendo un número finito de elementos $\alpha_1, \ldots, \alpha_n$ a K es isomorfo a un subcuerpo de $\overline{K}$(cuerpo universal). Esto significa que si tomamos cualesquiera n elementos $\alpha_1, \ldots, \alpha_n$ de cualquier cuerpo de extensión Λ de K, entonces existe un isomorfismo $K(\alpha_1, \ldots, \alpha_n) \cong K(\alpha'_1, \ldots, \alpha'_n)$ que deja fijos los elementos de K y lleva los elementos $\alpha_1, \ldots, \alpha_n$ de Λ en $\alpha'_1, \ldots, \alpha'_n$ de $\overline{K}$.*

Demostración: Los elementos $\alpha_1, \ldots, \alpha_n$ se pueden ordenar de forma que $\alpha_1, \ldots, \alpha_r$ sean algebraicamente independientes sobre K mientras que los otros α_i son algebraicos sobre $K(\alpha_1, \ldots, \alpha_r)$. Ahora tomamos $\alpha'_1, \ldots, \alpha'_r$ algebraicamente independientes sobre K en $\overline{K}$. Lo podemos hacer pues $\overline{K}$ tiene grado infinito de trascendencia. Entonces existe un isomorfismo $K(\alpha_1, \ldots, \alpha_r) \cong K(\alpha'_1, \ldots, \alpha'_r)$ que deja los elementos de K fijos y lleva $\alpha_1, \ldots, \alpha_r$ en $\alpha'_1, \ldots, \alpha'_r$. Si $r = n$, hemos terminado. Si $r < n$, entonces α_{r+1} es un cero de un polinomio irreducible $\varphi(x)$ con coeficientes en $K(\alpha_1, \ldots, \alpha_r)$. A este polinomio le corresponde un polinomio irreducible $\varphi'(x)$ con coeficientes en $K(\alpha'_1, \ldots, \alpha'_r)$ que tiene un cero α'_{r+1} en $\overline{K}$. Por el lema anterior, el isomorfismo $K(\alpha_1, \ldots, \alpha_r) \cong K(\alpha'_1, \ldots, \alpha'_r)$ se puede extender a un isomorfismo $K(\alpha_1, \ldots, \alpha_{r+1}) \cong K(\alpha'_1, \ldots, \alpha'_{r+1})$ que lleva α_{r+1} en α'_{r+1}. Si continuamos aplicando este lema obtenemos el isomorfismo deseado $K(\alpha_1, \ldots, \alpha_n) \cong K(\alpha'_1, \ldots, \alpha'_n)$. □

2.2. Variedades e ideales asociados a una variedad

Comenzaremos la sección recordando el concepto de variedad algebraica afín de un subconjunto F del cuerpo de polinomios.

Definición 2.2.1. *Sea K un cuerpo y $\overline{K}$ un cuerpo universal sobre K. Sea F un subconjunto de $K[x_1, \ldots, x_n]$. La variedad de F en $\overline{K}^n$ es el conjunto denotado por $V_n(F)$ siguiente:*

$$V_n(F) = \{\boldsymbol{a} \in \overline{K}^n \ \ | f(\boldsymbol{a}) = 0 \ \ \forall f \in F\}.$$

Si no hay duda del espacio ambiente $\overline{K}^n$ se omitirá el subíndice.

Definición 2.2.2. *Una variedad V sobre K en $\overline{K}^n$ es cualquier conjunto de $\overline{K}^n$ que sea variedad de algún subconjunto de $K[x_1, \ldots, x_n]$. En adelante, no haremos referencia al cuerpo base y diremos simplemente variedad en $\overline{K}^n$.*

Lema 4. *Si $V, W \subset \overline{K}^n$ son variedades, entonces lo son también $V \cup W$ y $V \cap W$*

Demostración: Supongamos que $V = V(f_1, \ldots, f_s)$ y $W = V(g_1, \ldots, g_t)$. Veamos que:

$$V \cap W = V(f_1, \ldots, f_s, g_1, \ldots, g_t),$$

$$V \cup W = V(f_i g_j, 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t).$$

La primera igualdad es trivial pues $V \cap W$ significa que $f_1, \ldots, f_s$ y $g_1, \ldots, g_t$ se anulen todos, que es lo mismo a que se anule $f_1, \ldots, f_s, g_1, \ldots, g_t$.
Para la segunda, si $(a_1, \ldots, a_n) \in V$, entonces todos los f_i se anulan en este punto, lo que implica que todos los $f_i g_j$ también se anulan en $(a_1, \ldots, a_n)$. Por tanto $V \subset V(f_i g_j)$, y $W \subset V(f_i g_j)$ se obtiene de forma análoga. Por tanto $V \cup W \subset V(f_i g_j)$.
Para ver la otra contención, elegimos $(a_1, \ldots, a_n) \in V(f_i g_j)$. Si este pertenece a V hemos terminado, y si no, $f_{i_0}(a_1, \ldots, a_n) \neq 0$ para algún i_0. Dado que $f_{i_0} g_j$ se anula en $(a_1, \ldots, a_n)$ para todo j, entonces todos los g_j se tienen que anular en este punto, demostrando que $(a_1, \ldots, a_n) \in W$. Lo que muestra que $V(f_i g_j) \subset V \cup W$, esto concluye la demostración . □

Formaremos ahora el ideal $\mathcal{A} = (F)$. Vemos que los ceros comunes de $f_1, \ldots, f_r$, los polinomios de F, son ceros de todos los polinomios $f = f_1 g_1 + \cdots + f_r g_r$ del ideal $\mathcal{A}$. Por ello $V_n(F)$ se puede caracterizar también como el conjunto de ceros comunes de todos los polinomios de $\mathcal{A}$.
Si $\xi_1, \ldots, \xi_n$ son elementos de una extensión arbitraria, entonces por el teorema 2.1.4 podemos encontrar un isomorfismo de cuerpos que lleva los elementos $\xi_1, \ldots, \xi_n$ en elementos de $\overline{K}$. Para los siguientes teoremas por tanto no importa en que cuerpo de extensión estemos. Si $\xi_i \in \overline{K}$ entonces $\boldsymbol{\xi}$ es un punto del espacio afín $A_n(\overline{K})$.

Definición 2.2.3. *De entre todos los ideales que definen la misma variedad V, uno de ellos destaca, este es el conjunto de todos los polinomios f que toman el valor 0 en todos los puntos de V. A este ideal le llamaremos el ideal asociado a V. A este ideal lo denotaremos por $I_K(V) \subseteq K[x_1, \ldots, x_n]$, si no tenemos duda del cuerpo en el que trabajamos omitiremos el subíndice.*

Ahora daremos una descripción de las variedades y de los ideales en forma de aplicaciones

Teorema 2.2.1. *Las aplicaciones*

$$\boldsymbol{I} : variedades\ afines \to ideales$$

y

$$\boldsymbol{V} : ideales \to variedades\ afines,$$

invierten la inclusión, es decir, si $I_1 \subseteq I_2$, entonces $\boldsymbol{V}(I_1) \supseteq \boldsymbol{V}(I_2)$ y si $V_1 \subseteq V_2$, entonces $\boldsymbol{I}(V_1) \supseteq \boldsymbol{I}(V_2)$. Además para cualquier variedad V tenemos $\boldsymbol{V}(\boldsymbol{I}(V)) = V$, así que $\boldsymbol{I}$ es inyectiva.

Demostración: Primero supongamos que $I_1 \subseteq I_2$. Sea $\mathbf{x} \in \mathbf{V}(I_2)$, entonces $f(\mathbf{x}) = 0,\ \forall f \in I_2$. Como $I_1 \subseteq I_2$ en particular $f(\mathbf{x}) = 0,\ \forall f \in I_1$, así que $\mathbf{x} \in \mathbf{V}(I_1)$. Por tanto $\mathbf{V}(I_2) \subseteq \mathbf{V}(I_1)$.
Supongamos ahora que $V_1 \subseteq V_2$. Sea $f \in \mathbf{I}(V_1)$, entonces $f(\mathbf{x}) = 0\ ,\ \forall \mathbf{x} \in V_2$. Como $V_1 \subseteq V_2$, en particular $f(\mathbf{x}) = 0,\ \forall \mathbf{x} \in V_1$, lo que implica que $f \in \mathbf{I}(V_1)$. Con lo que $\mathbf{I}(V_2) \subseteq \mathbf{I}(V_1)$.

Veamos ahora la inyectividad de $\mathbf{I}$. Sea $V = \mathbf{V}(f_1, \ldots, f_s)$ una variedad afín y $\mathbf{x} \in V$, entonces $f(\mathbf{x}) = 0,\ \forall f \in \mathbf{I}(V)$. Aplicando la definición de variedad de un ideal tenemos que $\mathbf{x} \in \mathbf{V}(\mathbf{I}(V))$ y tenemos la inclusión $V \subseteq \mathbf{V}(\mathbf{I}(V))$. Para la otra inclusión tenemos que $f_1, \ldots, f_s \in \mathbf{I}(V)$ por

la definición de $\mathbf{I}$, por ello $\langle f_1, \ldots, f_s \rangle$ tiene que estar contenido en $\mathbf{I}(V)$. Dado que V invierte la inclusión se sigue que $\mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(\langle f_1, \ldots, f_s \rangle) = V$. Lo que prueba la igualdad $\mathbf{V}(\mathbf{I}(V)) = V$ y, en consecuencia $\mathbf{I}$ es inyectiva. □

Terminaremos la sección definiendo el concepto de variedad irreducible y dando un teorema muy importante con respecto a este tipo de variedades.

Definición 2.2.4. *Una variedad V que se puede representar como la unión de dos subvariedades (no vacías) y propias se llama reducible. Si queremos enfatizar que ambas variedades están definidas por ecuaciones en un cuerpo K diremos que V es reducible sobre K. Una variedad V que no es reducible diremos que es irreducible sobre K.*

Teorema 2.2.2. *Una variedad V es irreducible sobre K si y solo si $\boldsymbol{I}(V)$ es primo.*

Demostración: Primero supongamos que V es irreducible y sea $f \cdot g \in I(V)$. Tomamos $V_1 = V \cap V(f)$ y $V_2 = V \cap V(g)$, estas son variedades pues sabemos que la intersección de variedades es una variedad. Veamos que $V = V_1 \cup V_2$.

Es claro que $V_1 \cup V_2 \subseteq V$, pues $(V \cap V(f)) \cup (V \cap V(g)) = V \cap (V(f) \cup V(g)) \subseteq V$.

Probemos que $V \subseteq V_1 \cup V_2$. Hay que ver que $V \subseteq V(f) \cup V(g)$, por la fórmula anterior. Sea $\mathbf{x} \in V$. Dado que por definición de $I(V)$, $f \cdot g$ se anula en V. En particular, tendremos $(f \cdot g)(\mathbf{x}) = 0$, es decir, $f(\mathbf{x})g(\mathbf{x}) = 0$ como K es dominio de integridad y no hay divisores de cero por lo que $f(\mathbf{x}) = 0$ o $g(\mathbf{x}) = 0$, por lo tanto $\mathbf{x} \in V(f)$ o $\mathbf{x} \in V(g)$, lo que implica que $\mathbf{x} \in V(f) \cup V(g)$, con lo queda probado. Como tenemos $V = V_1 \cup V_2$ y sabemos que V es irreducible tiene que ser $V = V_1$ o $V = V_2$. Supongamos que $V = V_1$, el otro caso es análogo. $V = V \cap V(f) \Rightarrow V \subseteq V(f)$ y por ello f se tiene que anular en todo V lo que quiere decir que $f \in \mathbf{I}(V)$ y tenemos que este ideal es primo.
Supongamos ahora que $\mathbf{I}(V)$ es primo y sea $V = V_1 \cup V_2$. Supongamos que $V \neq V_1$, probemos que $\mathbf{I}(V) = \mathbf{I}(V_2)$. Como $V_2 \subseteq V$ y la aplicación $\mathbf{I}$ invierte la inclusión, $\mathbf{I}(V) \subseteq \mathbf{I}(V_2)$. Para la otra inclusión tenemos que $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$ dado que $V_1 \subsetneq V$ y la inyectividad de $\mathbf{I}$. Por ello podemos tomar $f \in \mathbf{I}(V_1) - \mathbf{I}(V)$. Ahora tomamos cualquier $g \in \mathbf{I}(V_2)$. Dado que $V = V_1 \cup V_2$, tenemos que $f \cdot g$ se anula en V (f se anula en V_1 y g en V_2), y por ello $f \cdot g \in \mathbf{I}(V)$. Pero hemos supuesto que $\mathbf{I}(V)$ es primo, así que o bien f o bien g pertenecen a $\mathbf{I}(V)$. Sabemos que $f \notin \mathbf{I}(V)$, y por ello, $g \in \mathbf{I}(V)$. Esto prueba que $\mathbf{I}(V) = \mathbf{I}(V_2)$, y como $\mathbf{I}$ es inyectiva tenemos que $V = V_2$. Por tanto V es una variedad irreducible. □

2.3. Ceros genéricos y puntos genéricos

Vamos a ver ahora un par de conceptos clave que son los ceros genéricos y los puntos genéricos. En esta sección seguiremos el libro de van der Waerden [3].

Comenzaremos la sección presentando la definición de cero genérico de un ideal.

Definición 2.3.1. *Un punto $\boldsymbol{\xi} \in \overline{K}^n$ se llama cero genérico de un ideal $\mathcal{P} \subset K[x_1, \ldots, x_n]$ si $f \in \mathcal{P}$ implica $f(\boldsymbol{\xi}) = 0$ y viceversa. Es decir, $\mathcal{P} = \boldsymbol{I}(\{\boldsymbol{\xi}\})$.*

Nuestro objetivo a partir de ahora es demostrar a partir de los ceros genéricos de un ideal que toda variedad es irreducible si y solo si tiene un punto genérico concepto que definiremos más adelante. Para ello iremos demostrando una serie de teoremas que nos irán acercando a lo buscado.

Teorema 2.3.1. *Si $\xi_1, \ldots, \xi_n$ son elementos de un cuerpo de extensión de K, entonces los polinomios $f \in K[x_1, \ldots, x_n]$ para los cuales $f(\boldsymbol{\xi}) = 0$, donde $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n)$ forman un ideal primo que es distinto de $K[x_1, \ldots, x_n]$.*

Demostración: Veamos primero que los polinomios con esta condición forman un ideal. Es decir, que la suma de dos elementos con esta condición también la verifica y que el producto de un elemento de esta forma con otro del cuerpo de polinomios pertenece al ideal. Sean $f(\mathbf{x}), g(\mathbf{x}) \in \mathcal{P}$ entonces $f(\mathbf{x}) + g(\mathbf{x})$ verifica que $f(\boldsymbol{\xi}) + g(\boldsymbol{\xi}) = 0$.
Sea $h(\mathbf{x}) \in K[x_1, \ldots, x_n]$ entonces $f(\mathbf{x})h(\mathbf{x})$ verifica $f(\boldsymbol{\xi})h(\boldsymbol{\xi}) = 0$. Y se verifica que es un ideal. Veamos que el ideal es primo. Si $f(\mathbf{x})g(\mathbf{x}) \in \mathcal{P}$ entonces $f(\boldsymbol{\xi})g(\boldsymbol{\xi}) = 0$, y si $f(\boldsymbol{\xi}) \neq 0$ entonces ha de ser $g(\boldsymbol{\xi}) = 0$ pues un cuerpo no tiene divisores de 0 y por tanto el ideal es primo.
Dado que $1 \notin \mathcal{P}$ tenemos que $\mathcal{P} \neq K[x_1, \ldots, x_n]$. □

Teorema 2.3.2. *Si $\mathcal{P}$ es el ideal primo del teorema anterior, entonces $\Lambda = K(\xi_1, \ldots, \xi_n)$ es isomorfo al cuerpo de fracciones, Π , del anillo cociente $\frac{K[x_1,\ldots,x_n]}{\mathcal{P}}$ y de forma que las clases de $x_1, \ldots, x_n$ corresponden a los elementos $\xi_1, \ldots, \xi_n$.*

Demostración: Sea $\mathcal{L} = K[\xi_1, \ldots, \xi_n]$. Entonces Λ es el cuerpo de fracciones de $\mathcal{L}$. Asignamos a cada elemento $f(\xi_1, \ldots, \xi_n) \in \mathcal{L}$ el elemento del anillo cociente $\frac{K[x_1,\ldots,x_n]}{\mathcal{P}}$ representado por $f(x_1, \ldots, x_n)$. Veamos que esta asignación es un isomorfismo.

Veamos primero que es biyectiva. Si tenemos dos polinomios iguales en $\mathcal{L}$, es decir, que $f(\boldsymbol{\xi}) - g(\boldsymbol{\xi}) = 0$, entonces por como se define $\mathcal{P}$ tenemos que $f(\mathbf{x}) - g(\mathbf{x}) \in \mathcal{P}$ y por tanto ambos son iguales en $\frac{K[x_1,\ldots,x_n]}{\mathcal{P}}$. En el sentido contrario si dos elementos son iguales en $\frac{K[x_1,\ldots,x_n]}{\mathcal{P}}$ entonces $f(\mathbf{x}) - g(\mathbf{x}) \in \mathcal{P}$ y esto implica que la resta se anula en $\boldsymbol{\xi}$ y entonces son iguales en Λ, por lo tanto esta correspondencia es biyectiva.
Es claro que la suma en un anillo va a la suma del otro y los productos en los productos. Por tanto la correspondencia conserva operaciones y se concluye que es un isomorfismo. y obtenemos que los anillos $\mathcal{L}$ y $\frac{K[x_1,\ldots,x_n]}{\mathcal{P}}$ son isomorfos. De aquí obtenemos que los cuerpos de fracciones de ellos,Λ y Π son también isomorfos. □

El teorema 2.3.1 nos dice que cada $\boldsymbol{\xi}$ es un cero genérico de un único ideal primo. El teorema 2.3.2 nos dice que $\boldsymbol{\xi}$ está únicamente determinado por $\mathcal{P}$ salvo isomorfismos.

Teorema 2.3.3. *Todo ideal primo distinto de $K[x_1, \ldots, x_n]$ tiene un cero genérico $\boldsymbol{\xi}$ en el cuerpo universal $\overline{K}$.*

Demostración: Construimos el anillo cociente $\mathcal{D} = \frac{K[x_1,\ldots,x_n]}{\mathcal{P}}$. Ahora denotamos por ξ_i a la clase de x_i modulo $\mathcal{P}$. Tenemos que $\mathcal{D}$ es isomorfo al anillo de polinomios $K[\xi_1, \ldots, \xi_n]$. Puesto que $\mathcal{P}$ es un ideal primo entonces $\mathcal{D}$ es un dominio de integridad y no posee divisores de 0. Por ello se admite la construcción del cuerpo de fracciones. Y por tanto $K[\xi_1, \ldots, \xi_n]$ también lo admite al ser isomorfo. Denotaremos por $\Lambda = K(\xi_1, \ldots, \xi_n)$ sabemos que Λ se puede relacionar por un isomorfismo con un subconjunto del cuerpo universal $\overline{K}$ por el teorema 2.1.4, y podemos

asumir que $\Lambda \subseteq \overline{K}$. El elemento $f(\xi_1, \ldots, \xi_n)$ es cero si y solo si el polinomio f pertenece a la clase del 0 modulo $\mathcal{P}$. De aquí, $\boldsymbol{\xi}$ es cero genérico de $\mathcal{P}$. □

Por el Teorema 2.3.3 todo ideal primo $\mathcal{P}$ tiene un cero genérico en $\overline{K}$ el cual está únicamente determinado salvo isomorfismo por el Teorema 2.3.2. Este punto $\boldsymbol{\xi}$ es un cero de $\mathcal{P}$ y por ello pertenece a la variedad $\mathbf{V}(\mathcal{P})$. El ideal $\mathbf{I}(\mathbf{V}(\mathcal{P})) = \mathcal{P}$, puesto que si un polinomio f se anula en todos los puntos de $\mathbf{V}(\mathcal{P})$, entonces en particular $f(\boldsymbol{\xi}) = 0$ y de aquí $f \in \mathcal{P}$. Dado que $\mathbf{I}(\mathbf{V}(\mathcal{P}))$ es primo, se sigue que $\mathbf{V}(\mathcal{P})$ es irreducible. Por ello tenemos lo siguiente:

Teorema 2.3.4. *Para cada ideal primo $\mathcal{P}$,$V(\mathcal{P})$ es irreducible y $\boldsymbol{I}(\boldsymbol{V}(\mathcal{P})) = \mathcal{P}$.*

Si empezamos con una variedad irreducible V, entonces $\mathbf{I}(V)$ es primo, por el teorema 2.2.2. Los puntos en los que se anula $\mathbf{I}(V)$ son precisamente los puntos de V. Si $\boldsymbol{\xi}$ es un cero genérico de $\mathcal{P}$, entonces $\boldsymbol{\xi}$ se llama punto genérico de M sobre K. Volviendo a las definiciones:

Definición 2.3.2. *Un punto $\boldsymbol{\xi}$ de V es un punto genérico de V sobre K si $\forall f \in K[x_1, \ldots, x_n]$ con $f(\boldsymbol{\xi}) = 0$ entonces $f(\boldsymbol{\sigma}) = 0 \ \ \forall \boldsymbol{\sigma} \in V$.*

Por el Teorema 2.3.3 toda variedad irreducible V tiene un punto genérico. En el otro sentido si una variedad v tiene un punto genérico $\boldsymbol{\xi}$, entonces $\mathbf{I}(V)$ es primo por el Teorema 2.3.1 y por ello V es irreducible. Con lo que obtenemos lo siguiente:

Teorema 2.3.5. *V tiene un punto genérico sobre K si y solo si V es irreducible sobre K.*

Nota 2. *Las nociones de punto genérico y cero genérico se pueden definir para una variedad y un ideal cualquiera. Sin embargo como hemos demostrado que si un ideal tiene un cero genérico ha de ser primo y si una variedad tiene un punto genérico esta ha de ser irreducible la definición solo tiene sentido en conjuntos de este tipo pues en variedades e ideales cualesquiera no van a existir puntos con estas propiedades.*

2.4. La dimensión

En esta sección continuaremos siguiendo el libro de van der Waerden [3]. Comenzaremos la sección demostrando el teorema de descomposición, clave para dar una definición del concepto de dimensión de una variedad. Empezaremos demostrando un lema previo:

Lema 5. *En todo conjunto no vacío de variedades existe una variedad minimal V^*, esto es, que no contiene a ninguna otra variedad del conjunto.*

Demostración: Recordaremos que de entre todos los ideales que definen la misma variedad V, uno de ellos destaca, este es el conjunto de todos los polinomios f que toman el valor 0 en todos los puntos de V, a este ideal le hemos llamado ideal asociado a V, denotado por $\mathbf{I}(V)$. Además hemos visto que $\mathbf{V}(\mathbf{I}(V)) = V$, por lo tanto V está únicamente determinada por $\mathbf{I}(V)$, y viceversa. Por lo tanto si tenemos un conjunto de variedades cada variedad V tiene un ideal asociado $\mathbf{I}(V)$, y a distintas V se le asocian distintos $\mathbf{I}(V)$ pues estas están únicamente determinadas. En el conjunto de estos ideales $\mathbf{I}(V)$ existe un ideal maximal $\mathbf{I}(V)^*$ el cual estará únicamente asociado a una variedad V^*. Esta variedad es minimal en el conjunto. Aquí utilizamos que $\mathbf{I}$ invierte la inclusión. □

Teorema 2.4.1. *Toda variedad V definida sobre K se puede representar como unión finita de variedades irreducibles, además si eliminamos términos redundantes la descomposición es única salvo reordenaciones.*

Demostración: Supongamos que existen variedades V que no se pueden representar como unión de variedades irreducibles, entonces en el conjunto de estas V hay una variedad minimal V^*. Esta variedad debe ser reducible y puede representarse como la unión de dos subvariedades propias V_1 y V_2. Dado que V^* es minimal, V_1 y V_2 se pueden representar como unión de variedades irreducibles, pero entonces V^* también se podrá representar así, con lo que se llega a contradicción.
Veamos la unicidad. Sea $V = V_1 \cup \ldots \cup V_r$ una descomposición y sea $V = V_1' \cup \ldots \cup V_s'$ otra descomposición. Es claro que V_1 está contenido en la unión de los V_i'. Está por ello contenido en un único V_i, dedo que hemos eliminado elementos redundantes y al ser las variedades irreducibles, que tomando una numeración adecuada será V_1. De forma similar V_1' está contenido en algún V_k: y tenemos la relación:

$$V_1 \subseteq V_1' \subseteq V_k.$$

Si ahora $k \neq 1$, entonces V_1 sería redundante en la descomposición, por ello $k = 1$ y $V_1 = V_1'$. Siguiendo de la misma manera encontramos que $V_2 = V_2', \ldots, V_r = V_r'$ y $r = s$. Lo que completa la prueba de la unicidad.

□

Definición 2.4.1. *Sea $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n)$ un punto genérico de una variedad irreducible V, esto es un cero genérico de $\boldsymbol{I}(V)$. Si r es el grado de trascendencia de $K(\xi_1, \ldots, \xi_n)$ sobre K entonces hay r elementos algebraicamente independientes. Además ya hemos visto que el grado de trascendencia no cambia si el punto genérico se lleva a otro punto genérico mediante un isomorfismo, entonces r solo depende de $\boldsymbol{I}(V)$ y tiene sentido definir por r a la dimensión del ideal $\boldsymbol{I}(V)$ o de la variedad irreducible V.*

La dimensión de un ideal primo $\mathcal{P} \neq K[x_1, \ldots, x_n]$ es un número entre 0 y n. Y asignaremos dimensión -1 al ideal unitario $K[x_1, \ldots, x_n]$.
Si $\boldsymbol{\xi}$ es un cero genérico de un ideal primo $\mathcal{P}$ y $\boldsymbol{\xi'}$ es un cero arbitrario del mismo ideal, entonces a cada polinomio $f(\boldsymbol{\xi}) \in K[\boldsymbol{\xi}]$ le corresponde el polinomio $f(\boldsymbol{\xi'}) \in K[\boldsymbol{\xi'}]$. Dado que $f(\boldsymbol{\xi}) = g(\boldsymbol{\xi})$ implica que $f(x) = g(x) \bmod \mathcal{P}$ y de aquí $f(\boldsymbol{\xi'}) = g(\boldsymbol{\xi'})$, se sigue que la correspondencia
$f(\boldsymbol{\xi}) \to f(\boldsymbol{\xi'})$ es inyectiva. Dado que esta correspondencia lleva sumas en sumas y productos en productos , es un homomorfismo:

$$K[\boldsymbol{\xi}] \sim K[\boldsymbol{\xi'}]. \tag{2.3}$$

Si esta correspondencia es además isomorfismo, es decir, si es sobreyectiva entonces por supuesto $\boldsymbol{\xi'}$ es también un cero genérico de $\mathcal{P}$, y viceversa.

Teorema 2.4.2. *Si un ideal primo $\mathcal{P}$ es cero-dimensional, todos sus ceros son ceros genéricos y equivalentes, es decir, que se obtienen de otros mediante un isomorfismo que deja fijos los elementos de K.*

Demostración: Si un ideal es cero-dimensional, por definición, todos los ceros genéricos $\boldsymbol{\xi}$ son algebraicos sobre K , por ello todas las funciones racionales en $\boldsymbol{\xi}$ son polinomios y $K(\boldsymbol{\xi}) = K[\boldsymbol{\xi}]$, Por ello $K[\boldsymbol{\xi}]$ es un cuerpo. Si ahora $\boldsymbol{\xi'}$ es un cero arbitrario, entonces el homomorfismo (2.3) es necesariamente un isomorfismo; de hecho un cuerpo no tiene homomorfismos excepto aquellos que son biyectivos y los que llevan el cuerpo entero al anillo nulo, y por ello se trata de un isomorfismo. □

Corolario 2.4.3. *Una variedad irreducible cero-dimensional consiste en finitos puntos que son conjugados sobre K*

Demostración: Las coordenadas $\xi_1, \ldots, \xi_n$ o $\xi'_1, \ldots, \xi'_n$ son algebraicas sobre K. Si consideramos ahora ceros sobre el cuerpo universal Ω, entonces estos ceros son conjugados sobre K. El número de estos puntos conjugados en Ω es como mucho igual al grado de trascendencia de $K(\boldsymbol{\xi})$ sobre K, y este número es finito por ser todos los ξ_i algebraicos. □

Para finalizar esta sección estamos en disposición de definir la dimensión de una variedad arbitraria.

Definición 2.4.2. *La dimensión de una variedad arbitraria V se define como la mayor de las dimensiones de sus componentes irreducibles.*

2.5. Algoritmos gcd y Pseudodivisión

Necesitaremos explicar un poco los algoritmos básicos que se van a usar. Uno de estos es un algoritmo para computar el máximo común divisor en una variable. Y el otro es un algoritmo de pseudodivisión entre dos polinomios en n variables.
Estos algoritmos se han sacado del libro de D. Cox, J. Little y O'Shea [4].

2.5.1. Algoritmo gcd

Definición 2.5.1. *Un máximo común divisor de dos polinomios $f, g \in K[x]$ es un polinomio h tal que:*

1. *El polinomio h divide a f y a g.*
2. *Si p es otro polinomio que divide a f y a g, entonces p divide a h.*

Cuando h tiene estas propiedades, escribiremos $h = \boldsymbol{gcd}(f, g)$Por lo tanto se hace necesario desarrollar algoritmos que nos ayuden a responder estas preguntas.

Aquí están las principales propiedades de **gcd**.

Proposición 6. *Sean $f, g \in K[x]$. Entonces:*

1. $\boldsymbol{gcd}(f, g)$ *existe y es único salvo multiplicación por una constante no nula de K.*
2. $\boldsymbol{gcd}(f, g)$ *es un generador del ideal $\langle f, g\rangle$.*
3. *Hay un algoritmo para encontrar $\boldsymbol{gcd}(f, g)$.*

Demostración: Consideramos el ideal $\langle f, g\rangle$. Dado que todo ideal de $K[x]$ es principal, existe $h \in K[x]$ tal que $\langle f, g\rangle = \langle h\rangle$. Veamos que $h = \mathbf{gcd}(f, g)$, primero vemos que h divide a f y a g dado que $f, g \in \langle h\rangle$. Con lo que se verifica la primera parte de la definición. Ahora supongamos que $p \in K[x]$ divide a f y a g. Esto significa que $f = C \cdot p$ y $g = D \cdot p$ para algunos $C, D \in K[x]$. Dado que $h \in \langle f, g\rangle$, existen $A, B \in K[x]$ tales que $A \cdot f + B \cdot g = h$. Si sustituimos, obtenemos

$$h = A \cdot f + B \cdot g = A \cdot C \cdot p + B \cdot D \cdot p = (A \cdot C + B \cdot D)p,$$

lo que muestra que p divide a h. Por tanto, $h = \mathbf{gcd}(f, g)$.
Con esto hemos probado la existencia, veamos ahora la unicidad. Supongamos que $h' = \mathbf{gcd}(f, g)$, entonces por la segunda parte de la definición, h y h' se dividirán el uno al otro. Lo que implica que h es h' multiplicado por una constante no nula. Lo que prueba la parte 1 de la proposición. La parte 2 se prueba directamente también por la forma en que hemos encontrado h.
La prueba de la existencia no es útil en la práctica pues depende de encontrar un generador de $\langle f, g\rangle$. Afortunadamente existe un algoritmo conocido como Algoritmo Euclídeo, que computa el máximo común divisor de dos polinomios en $K[x]$.
Sean $f, g \in K[x]$, donde $g \neq 0$, y escribimos $f = g \cdot q + r$, donde q y r son el resto y el cociente del algoritmo de división usual de polinomios en $K[x]$. Además denotaremos $r = remainder(f, g)$. Podemos ahora construir el Algoritmo Euclídeo para encontrar el $\mathbf{gcd}(f, g)$:

Entrada: f, g
Salida: h
$h := f$
$s := g$
mientras $s \neq 0$ **hacer**
$rem := remainder(h, s)$
$h := s$
$s := rem$

Para ver por qué este algoritmo computa el máximo común divisor, escribimos $f = q \cdot g + r$. Veamos $\mathbf{gcd}(f, g) = \mathbf{gcd}(f - q \cdot g, g) = \mathbf{gcd}(r, g)$.
Para probar basta probar por la parte 2 que $\langle f, g\rangle = \langle f - q \cdot g, g\rangle$.
Si $h \in \langle f, g\rangle$ será de la forma $h = Af + Bg$, donde $A, B \in K[x]$, entonces también $h = Af + Bg - q \cdot g \cdot A + q \cdot g \cdot A$. Reagrupando los términos $h = (B + q \cdot A)g + A(f - q \cdot g)$, dado que $(B + q \cdot A), A \in K[x]$ entonces $h \in \langle g, f - q \cdot g\rangle$.
Si $h \in \langle g, f - q \cdot g\rangle$ será de la forma $h = Ag + B(f - q \cdot g)$, donde $A, B \in K[x]$. Entonces $h = Ag + Bf - B \cdot q \cdot g$ y de aquí $h = (A - B \cdot q)g + Bf$, dado que $(A - B \cdot q), B \in K[x]$ entonces $h \in \langle f, g\rangle$. Con lo que queda demostrado.
Tenemos entonces que $\mathbf{gcd}(f, g) = \mathbf{gcd}(g, r)$. Tenemos que $deg(g) > deg(r)$ o $r = 0$. Si $r \neq 0$, podemos hacer los grados todavía más pequeños repitiendo este proceso. Por lo tanto, escribiremos $g = q' \cdot r + r'$, y argumentando como antes obtenemos $\mathbf{gcd}(g, r) = \mathbf{gcd}(r, r')$ donde $deg(r) > deg(r')$ o $r = 0$. Continuando de esta manera obtenemos

$$\mathbf{gcd}(f, g) = \mathbf{gcd}(g, r) = \mathbf{gcd}(r, r') = \mathbf{gcd}(r', r'') = \cdots , \tag{2.4}$$

donde los grados bajan $deg(g) > deg(r) > deg(r') > deg(r'') > \cdots$, o el proceso termina cuando uno de los $r, r', r'', \ldots$ es 0.
Ahora se va a explicar como funciona el Algoritmo Euclídeo. El algoritmo tiene variables h y s, podemos ver estas variables en la ecuación (2.4): los valores de h son el primer polinomio en cada **gcd** y los valores de s son los segundos. Lo que se hace exactamente en cada paso del mientras es pasar de un **gcd** al siguiente. El algoritmo termina dado que los grados siempre bajan, así que en algún momento $s = 0$. Cuando esto ocurre, tenemos $\mathbf{gcd}(h, 0) = \mathbf{gcd}(f, g)$, y dado que $\langle h, 0\rangle$ obviamente es igual a $\langle h\rangle$, tenemos que $\mathbf{gcd}(h, 0) = h$. Combinando estas dos últimas ecuaciones se sigue que $h = \mathbf{gcd}(f, g)$ cuando $s = 0$. Esto prueba que h es el máximo común divisor de f y g cuando el algoritmo termina, y se termina la demostración. □

Definición 2.5.2. *Un máximo común divisor de varios polinomios $f_1, \ldots, f_s \in K[x]$ es un polinomio h tal que:*

1. *El polinomio h divide a $f_1, \ldots, f_s$.*
2. *Si p es otro polinomio que divide $f_1, \ldots, f_s$ entonces p divide a h.*

Cuando h tiene estas propiedades, escribimos $h = \boldsymbol{gcd}(f_1, \ldots, f_s)$.

Ahora veremos las principales propiedades de **gcd**.

Proposición 7. *Sean $f_1, \ldots, f_s \in K[x]$, donde $s \geq 2$. Entonces:*

1. $\boldsymbol{gcd}(f_1, \ldots, f_s)$ *existe y es único salvo multiplicación por una constante no nula de K.*
2. $\boldsymbol{gcd}(f_1, \ldots, f_s)$ *es un generador del ideal $\langle f_1, \ldots, f_s \rangle$.*
3. *Si $s \geqslant 3$, entonces $\boldsymbol{gcd}(f_1, \ldots, f_s) = \boldsymbol{gcd}(f_1, \boldsymbol{gcd}(f_2, \ldots, f_s))$.*
4. *Hay un algoritmo para encontrar $\boldsymbol{gcd}(f_1, \ldots, f_s)$.*

Demostración: Las demostraciones de las partes 1 y 2 son similares a las de la proposición anterior. Para probar la parte 3, sea $h = \mathbf{gcd}(f_2, \ldots, f_s)$. Se prueba fácilmente mediante una inducción que $\langle f_1, h \rangle = \langle f_1, f_2, \ldots, f_s \rangle$. Por la parte 2 de esta proposición tenemos que $\langle \mathbf{gcd}(f_1, h) \rangle = \langle \mathbf{gcd}(f_1, \ldots, f_s) \rangle$. Entonces $\mathbf{gcd}(f_1, h) = \mathbf{gcd}(f_1, \ldots, f_s)$ dado que los elementos que generan un ideal son únicos salvo multiplicación por una constante, lo que prueba lo que queremos.
Finalmente hay probar que existe un algoritmo que encuentra $\mathbf{gcd}(f_1, \ldots, f_s)$. La idea es combinar la parte 3 con el Algoritmo Euclídeo. Por ejemplo para calcular $\mathbf{gcd}(f_1, \ldots, f_s)$, usamos la parte 3 dos veces y obtenemos:

$$\mathbf{gcd}(f_1, f_2, f_3, f_4) = \mathbf{gcd}(f_1, \mathbf{gcd}(f_2, f_3, f_4)) = \mathbf{gcd}(f_1, \mathbf{gcd}(f_2, \mathbf{gcd}(f_3, f_4))).$$

Por tanto si usamos el Algoritmo Euclídeo tres veces, obtenemos $\mathbf{gcd}(f_1, f_2, f_3, f_4)$. Si generalizamos esta idea obtenemos el algoritmo buscado. □

2.5.2 Algoritmo de pseudodivisión

La idea que subyace bajo el algoritmo de pseudodivisión es tratar de seguir lo más cerca posible el algoritmo de división polinomial en una variable.

Definición 2.5.3. *Sea*

$$f = \sum_{i=0}^{d} q_i(x_1, \ldots, x_{n-1}) x_n^i$$

un polinomio en $K[x_1, \ldots, x_n]$ con $q_d \neq 0$. El polinomio q_d se llama el coeficiente líder de f con respecto a x_n, denotado por $lc_n(f)$.

Definición 2.5.4. *El grado de f en x_n se denota por $deg_n(f)$. Por convenio se define $deg_n(0) = -1$.*

Proposición 8. *Para dos polinomios no nulos $f_1, f_2 \in K[x_1, \ldots, x_n]$, donde asumiremos que existen polinomios $pquo_n(f_1, f_2)$ y $prem_n(f_1, f_2)$ en $K[x_1, \ldots, x_n]$, llamados pseudocociente y pseudoresto con respecto a x_n, tales que:*

$$(lc_n(f_2))^d \cdot f_1 = pquo_n(f_1, f_2) \cdot f_2 + prem_n(f_1, f_2)$$

con $deg_n(prem_n(f_1, f_2)) \leq deg_n(f_2)$ y $d = max(deg_n(f_1) - deg_n(f_2) + 1, 0)$.
Además $prem_n(f_1, f_2) \in \langle f_1, f_2 \rangle$ en $K[x_1, \ldots, x_n]$.

Demostración: Los polinomios $q = pquo_n(f_1, f_2)$ y $r = prem_n(f_1, f_2)$ se pueden construir por el siguiente algoritmo llamado pseudodivisión con respecto a x_n.

Entrada: f_1, f_2
Salida: q, r

$r := f$
$q := 0$
mientras $r \neq 0$ **y** $deg_n(r) \geqslant deg_n(f_2)$ **hacer**
$\quad r := lc_n(f_2) \cdot r - lc_n(r) \cdot f_2 \cdot x_n^{deg_n(r) - deg_n(f_2)}$
$\quad q := lc_n(f_2) \cdot q + lc_n(r) \cdot x_n^{deg_n(r) - deg_n(f_2)}$

Vemos que obtenemos en el primer paso del algoritmo,

$$r := lc_n(f_2) \cdot f_2 - lc_n(f_2) \cdot f_2 \cdot x_n^{deg_n(r) - deg_n(f_2)},$$

$$q := c_n(f_2) \cdot 0 + lc_n(r) \cdot x_n^{deg_n(r) - deg_n(f_2)},$$

entonces obtenemos que $q \cdot f_2 + r = lc_n(f_2) \cdot f_2$, si seguimos se prueba que en cada paso se va obteniendo un $lc_n(f_2)$ más multiplicando, por tanto si aplicamos el algoritmo
$deg_n(f_1) - deg_n(f_2) + 1$ veces obtendremos lo buscado.
Para ver que $r \in \langle f_1, f_2 \rangle$, dado que $(lc_n(f_2))^d \cdot f_1 = q \cdot f_2 + r$, se sigue que

$$r = (lc_n(f_2))^d \cdot f_1 - q \cdot f_2 \in \langle f_1, f_2 \rangle.$$

□

Capítulo 3

Teorema de la Extensión y Hilbert's Nullstellensatz

En este capítulo buscaremos demostrar uno de los teoremas más importantes en la rama de la geometría algebraica, el Hilbert's Nullstellensatz. Para poder demostrar este teorema necesitamos otro teorema también de gran importancia llamado el teorema de la Extensión. Existen varias demostraciones de este teorema, una de ellas utiliza bases de Gröbner pero dado que estamos presentando un algoritmo alternativo a estas, se ha buscado un método que prescinde de ellas. En nuestro caso emplearemos resultantes, los cuales serán desarrollados en la primera sección. La demostración se ha seguido del libro de D. Cox, J. Little y O'Shea [4].

3.1. Resultantes

Para poder demostrar el teorema de la extensión necesitamos desarrollar el concepto de resultante y estudiar ciertas propiedades que estos poseen. Comenzamos desarrollando un lema previo:

Lema 6. *Sean $f, g \in K[x]$ polinomios de grados $l > 0$ y $m > 0$, respectivamente. Entonces f y g tienen un factor común si y solo si hay polinomios $A, B \in K[x]$ tal que:*

1. *A y B no son ambos nulos.*
2. *A tiene grado como mucho $m-1$ y B tiene grado como mucho $l-1$.*
3. *$A \cdot f + B \cdot g = 0$.*

Demostración: Primero suponemos que f y g tienen un factor común $h \in K[x]$. Entonces $f = hf_1$ y $g = hg_1$, donde $f_1, g_1 \in K[x]$. Tenemos que f_1 tiene grado como mucho $l-1$ y de forma similar $deg(g_1) \leq m-1$. Entonces:

$$g_1 \cdot f + (-f_1) \cdot g = g_1 \cdot hf_1 - f_1 \cdot hg_1 = 0,$$

y, por tanto, $A = g_1$ y $B = f_1$ cumplen las 3 propiedades.

Supongamos ahora que A y B cumplen las 3 propiedades. Por la primera, podemos asumir que $B \neq 0$. Si f y g no tuvieran un factor común, entonces su máximo común divisor es 1, así

que podemos encontrar polinomios $A', B' \in K[x]$ tal que $A'f + B'g = 1$ (Identidad de Bezout). Multiplicando por B y usando la propiedad 3 $Bg = -Af$:

$$B = (A'f + B'g)B = A'Bf + B'Bg = A'Bf - B'Af = (A'B - B'A)f.$$

Dado que hemos supuesto que B es no negativo, esta ecuación muestra que B tiene grado mayor que l, lo que contradice la propiedad 2. Por tanto debe existir un factor común a ambos polinomios. □

La idea es transformar $Af + Bg = 0$ en un sistema de ecuaciones lineales. Escribimos:

$$A = c_0x^{m-1} + \ldots + c_{m-1},$$

$$B = d_0x^{l-1} + \ldots + d_{l-1},$$

donde por ahora los $l + m$ coeficientes $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{l-1}$ son desconocidos. Nuestra meta es encontrar $c_i, d_i \in K$, no todos nulos, tal que la ecuación $Af + Bg = 0$ se verifique. Para conseguir un sistema de ecuaciones lineales, escribiremos f y g como sigue:

$$f = a_0x^l + \ldots + a_l, \quad a_0 \neq 0,$$

$$g = b_0x^m + \ldots + b_m, \quad b_0 \neq 0,$$

donde $a_i, b_i \in K$. Si sustituimos estas fórmulas por f, g, A y B en $Af + Bg = 0$ y comparamos los coeficientes de las potencias de x, entonces obtenemos el siguiente sistema de ecuaciones lineales con indeterminadas c_i, d_i y coeficientes $a_i, b_i \in K$:

$$\begin{array}{lllll}
a_0c_0 & + & b_0d_0 & = 0 & coeficiente\ de\ x^{l+m-1} \\
a_1c_0 + a_0c_1 & + & b_1d_0 + b_0d_1 & = 0 & coeficiente\ de\ x^{l+m-2} \\
\ddots & & \ddots & \vdots & \\
 & a_lc_{m-1} & + \quad b_md_{l-1} & = 0 & coeficiente\ de\ x^0.
\end{array}$$

Dado que hay $l + m$ ecuaciones lineales y $l + m$ incógnitas, sabemos por el álgebra lineal que hay una solución no nula si y solo si la matriz de coeficientes tiene determinante cero. Lo que nos lleva a la definición de resultante.

Definición 3.1.1. *Dados dos polinomios $f, g \in K[x]$ de grado positivo, escritos en la forma:*

$$f = a_0x^l + \ldots + a_l, \ \ a_0 \neq 0,$$

$$g = b_0x^m + \ldots + b_m, \ \ b_0 \neq 0.$$

Entonces definimos la matriz de Sylvester de f y g con respecto a x, denotada por $Syl(f, g, x)$ a la matriz $(l + m) \times (l + m)$:

$$Syl(f,g,x) = \underbrace{\begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \dots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix}}_{m \text{ columnas}} \underbrace{\qquad\qquad}_{l \text{ columnas}}, \tag{3.1}$$

donde los espacios vacíos se rellenan con ceros. la resultante de f y g con respecto a x, denotado por $Res(f,g,x)$ es el determinante de la matriz de Sylvester. Es decir,

$$Res(f,g,x) = det(Syl(f,g,x)).$$

Proposición 9. *Dados $f, g \in K[x]$ de grado positivo, la resultante $Res(f,g,x) \in K$ es un polinomio que evaluado en números enteros da un número entero. De hecho, f y g tienen un factor común en $K[x]$ si y solo si $Res(f,g,x) = 0$.*

Demostración: La fórmula estándar para el determinante de una matriz de dimensión $s \times s$, $A = (a_{ij})_{1 \le i,j \le s}$ es:

$$det(A) = \sum_{\sigma \, permutacin \, de \, \{1,\dots,s\}} sgn(\sigma) a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdots a_{s\sigma(s)},$$

donde $sgn(\sigma)$ es $+1$ si σ intercambia un número par de parejas de elementos de $\{1,\dots,s\}$ y -1 si σ intercambia un número impar de parejas. Esto muestra que el determinante es un polinomio que evaluado en números enteros da un número entero pues de hecho sus coeficientes son ± 1. De lo que se sigue por la definición de resultante que este también lo es.

Para la segunda parte tenemos que la resultante es cero si y solo si el sistema de ecuaciones anterior a la definición de resultante tiene determinante cero. Lo cual ocurre si y solo si el sistema tiene una solución no nula. Y hemos observado antes que esto equivale a la existencia de A y B como en el lema 6, aplicando este lema concluimos que f y g tienen un factor común. □

Proposición 10. *Dados $f, g \in K[x]$ de grado positivo, hay polinomios $A, B \in K[x]$ tales que:*

$$Af + Bg = Res(f,g,x).$$

Además, los coeficientes de A y B son polinomios de valores enteros en los coeficientes de f y g.

Demostración: La definición de resultante estaba basada en la ecuación $Af + Bg = 0$. En esta demostración aplicaremos los mismos métodos a la ecuación:

$$A'f + B'g = 1. \tag{3.2}$$

La proposición es trivial si $Res(f,g,x)=0$ (elegimos $A=B=0$), así que suponemos ahora que $Res(f,g,x)\neq 0$. Escribimos:

$$f=a_0x^l+\ldots+a_l, \qquad a_0\neq 0,$$

$$g=b_0x^m+\ldots+b_m, \qquad b_0\neq 0,$$

$$A'=c_0x^{m-1}+\ldots+c_{m-1},$$

$$B'=d_0x^{l-1}+\ldots+d_{l-1},$$

donde los coeficientes $c_0,\ldots,c_{m-1},d_0,\ldots,d_{l-1}$ son indeterminadas en K. Si sustituimos estas fórmulas en (3.2) y comparamos los coeficientes de las potencias de x, entonces obtenemos el siguiente sistema de ecuaciones lineales con indeterminadas c_i,d_i y coeficientes $a_i,b_i\in K$:

$$\begin{array}{lllll}
a_0c_0 & + & b_0d_0 & = 0 & coeficiente\ de\ x^{l+m-1}\\
a_1c_0+a_0c_1 & + & b_1d_0+b_0d_1 & = 0 & coeficiente\ de\ x^{l+m-2}\\
\ddots & & \ddots & \vdots & \\
 & a_lc_{m-1} + & b_md_{l-1} & = 1 & coeficiente\ de\ x^0.
\end{array}$$

Estas ecuaciones son las mismas que las calculadas antes de la definición de resultante excepto por el 1 en la última ecuación. Por tanto, la matriz de coeficientes es la matriz de Sylvester de f y g, y entonces que $Res(f,g,x)\neq 0$ garantiza que el sistema anterior tiene solución única en K. En esta situación, podemos usar la regla de Cramer para dar una fórmula para la única solución. La regla de Cramer nos dice que la i-ésima indeterminada es una razón entre dos determinantes , donde el denominador es el determinante de la matriz de coeficientes y el numerador es el determinante de la matriz donde la i-ésima columna de la matriz de coeficientes se sustituye por el lado derecho de la ecuación.En nuestro caso obtenemos fórmulas para los $c_i's$ y $d_i's$. Por ejemplo, la primera indeterminada c_0 viene dada por:

$$c_0=\frac{1}{Res(f,g,x)}det\begin{pmatrix}
0 & & & & b_0 & & \\
0 & a_0 & & & \vdots & \ddots & \\
\vdots & \vdots & \ddots & & \vdots & & b_0\\
0 & a_l & & a_0 & b_m & & \vdots\\
\vdots & & \ddots & \vdots & & \ddots & \vdots\\
1 & & & a_l & & & b_m
\end{pmatrix}.$$

Dado que el determinante es un polinomio de valores enteros en sus entradas, se sigue que:

$$c_0=\frac{un\ polinomio\ de\ valores\ enteros\ en\ a_i,b_i}{Res(f,g,x)}.$$

Hay formulas similares para el resto de $c_i's$ y $d_i's$. Dado que $A'=c_0x^{m-1}+\ldots+c_{m-1}$, podemos extraer el denominador común $Res(f,g,x)$ y escribir A' en la forma:

$$A'=\frac{1}{Res(f,g,x)}A,$$

donde $A \in K[x]$ y los coeficientes de A son polinomios de valores enteros en a_i y b_i. De forma similar, podemos escribir:

$$B' = \frac{1}{Res(f,g,x)}B,$$

donde $B \in K[x]$ tiene las mismas propiedades que A. Dado que A' y B' satisfacen $A'f + B'g = 1$, podemos multiplicar por $Res(f,g,x)$ para obtener:

$$Af + Bg = Res(f,g,x).$$

Dado que A y B tienen las propiedades pedidas en la proposición se termina la demostración. □

Lo que haremos ahora es adaptar la teoría de resultantes a polinomios en n variables. Supongamos $f, g \in K[x_1, \ldots, x_n]$ de grado positivo en x_1. Escribimos:

$$f = a_0 x_1^l + \ldots + a_l, \qquad a_0 \neq 0,$$

$$g = b_0 x_1^m + \ldots + b_m, \qquad b_0 \neq 0,$$

donde $a_i, b_i \in K[x_2, \ldots, x_n]$, y definimos la resultante de f y g con respecto a x_1 como el determinante:

$$Res(f,g,x_1) = det \underbrace{\begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ldots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix}}_{m \text{ columnas}} \underbrace{\qquad\qquad}_{l \text{ columnas}},$$

donde los espacios vacíos se completan con ceros. Para resultantes de polinomios en varias variables, los resultados obtenidos anteriormente se traducen en:

Proposición 11. *Sean $f, g \in K[x_1, \ldots, x_n]$ con grado positivo en x_1. Entonces:*

1. *$Res(f,g,x_1)$ está en el primer ideal de eliminación $\langle f, g\rangle \cap K[x_2, \ldots, x_n]$.*
2. *$Res(f,g,x_1) = 0$ si y solo si f y g tienen un factor común en $K[x_1, \ldots, x_n]$ con grado positivo en x_1.*

Demostración: Cuando escribimos f, g en términos de x_1, los coeficientes a_i, b_i pertenecen a $K[x_2, \ldots, x_n]$. Dado que la resultante es un polinomio de valores enteros en a_i, b_i por la proposición 9, se sigue que $Res(f,g,x_1) \in K[x_2, \ldots, x_n]$. También sabemos que

$$Af + Bg = Res(f,g,x_1),$$

donde A y B son polinomios en x_1 cuyos coeficientes son de nuevo polinomios con valores enteros en a_i, b_i por la proposición 10. Por tanto $A, B \in K[x_2, \ldots, x_n][x_1] = K[x_1, \ldots, x_n]$ y por la ecuación de arriba $Res(f, g, x_1) \in \langle f, g \rangle$. Lo que prueba la primera parte de la proposición.

Para probar la segunda parte, usaremos la proposición 9 para interpretar la anulación de la resultante en términos de factores comunes. Anteriormente hemos trabajado con polinomios en una variable con coeficientes es un cuerpo. Dado que f y g son polinomios en x_1 con coeficientes en $K[x_2, \ldots, x_n]$, el cuerpo en el que los coeficientes están es $K(x_2, \ldots, x_n)$. Entonces la proposición 9 aplicada a $f, g \in K(x_2, \ldots, x_n)[x_1]$, nos dice que $Res(f, g, x_1) = 0$ si y solo si f y g tienen un factor común en $K(x_2, \ldots, x_n)[x_1]$ que tiene grado positivo en x_1. Pero ya sabemos que esto es equivalente a tener un factor común en $K[x_1, \ldots, x_n]$ de grado positivo en x_1. Con lo que se concluye la demostración. □

En un cuerpo algebraicamente cerrado, dos polinomios en $K[x]$ tienen un factor común si y solo si tienen una raíz común. Con lo que obtenemos el siguiente corolario.

Corolario 3.1.1. *Si $f, g \in K[x]$ un cuerpo algebraicamente cerrado, entonces $Res(f, g, x) = 0$ si y solo si f y g tienen una raíz común en K*

Veremos ahora como se pueden usar los resultantes para demostrar el teorema de la extensión.

Proposición 12. *Sea K un cuerpo algebraicamente cerrado. Dados $f, g \in K[x_1, \ldots, x_n]$, escribimos:*

$$f = a_0 x_1^l + \ldots + a_l, \qquad a_0 \neq 0,$$

$$g = b_0 x_1^m + \ldots + b_m, \qquad b_0 \neq 0,$$

donde $a_i, b_i \in K[x_2, \ldots, x_n]$. Si $Res(f, g, x_1) \in K[x_2, \ldots, x_n]$ se anula en $(c_2, \ldots, c_n) \in K^{n-1}$, entonces ocurre una de las dos cosas siguientes:

1. *O bien a_0, o bien b_0 se anulan en $(c_2, \ldots, c_n)$.*
2. *Existe $c_1 \in K$ tal que f y g se anulan en $(c_1, \ldots, c_n) \in K^n$.*

Demostración: Introduciremos primero algo de notación para simplificar la demostración. Sea $\mathbf{c} = (c_2, \ldots, c_n)$, y sea $f(x_1, \mathbf{c}) = f(x_1, c_2, \ldots, c_n)$. Basta con probar que $f(x_1, \mathbf{c})$ y $g(x_1, \mathbf{c})$ tienen una raíz común cuando $a_0(\mathbf{c})$ y $b_0(\mathbf{c})$ son ambas no nulas. Para probar esto, escribimos:

$$f(x_1, \mathbf{c}) = a_0(\mathbf{c}) x_1^l + \ldots + a_l(\mathbf{c}), \qquad a_0(\mathbf{c}) \neq 0,$$

$$g(x_1, \mathbf{c}) = b_0(\mathbf{c}) x_1^m + \ldots + b_m(\mathbf{c}), \qquad b_0(\mathbf{c}) \neq 0.$$

Por hipótesis, $h = Res(f, g, x_1)$ se anula en $\mathbf{c}$. Por tanto, si evaluamos el determinante que devuelve la resultante en el punto $\mathbf{c}$, obtenemos:

$$0 = h(\mathbf{c}) = det \underbrace{\begin{pmatrix} a_0(\mathbf{c}) & & & b_0(\mathbf{c}) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_0(\mathbf{c}) & \vdots & & b_0(\mathbf{c}) \\ a_l(\mathbf{c}) & & \vdots & b_m(\mathbf{c}) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l(\mathbf{c}) & & & b_m(\mathbf{c}) \end{pmatrix}}_{m \ \ columnas \qquad\qquad l \ \ columnas}. \tag{3.3}$$

De las ecuaciones anteriores, la resultante de $f(x_1, \mathbf{c})$ y $g(x_1, \mathbf{c})$ es exactamente el determinante que aparece antes, y se sigue que

$$0 = h(\mathbf{c}) = Res(f(x_1, \mathbf{c}), g(x_1, \mathbf{c})).$$

Entonces el corolario 3.1.1 implica que $f(x_1, \mathbf{c})$ y $g(x_1, \mathbf{c})$ tiene una raíz común, y se concluye la demostración. □

3.2. Teorema de la Extensión

Ahora que tenemos todos los ingredientes pasaremos a demostrar el teorema de la extensión pero antes de ir al caso general probaremos el caso en que el ideal está generado por dos polinomios.

Teorema 3.2.1. ***(El Teorema de la Extensión para dos polinomios)****. Sea* $I = \langle f, g\rangle \subset K[x_1, \ldots, x_n]$ *y sea* $I_1 = I \cap K[x_2, \ldots, x_n]$ *también llamado primer ideal de eliminación de* I*. Escribimos:*

$$f = a_0 x_1^l + \ldots + a_l, \qquad a_0 \neq 0,$$
$$g = b_0 x_1^m + \ldots + b_m, \qquad b_0 \neq 0,$$

donde $a_i, b_i \in K[x_2, \ldots, x_n]$*. Supongamos que tenemos* $(c_2, \ldots, c_n) \in \boldsymbol{V}(I_1)$*. Si* $(c_2, \ldots, c_n) \notin \boldsymbol{V}(a_0, b_0)$*, entonces existe* $c_1 \in K$ *tal que* $(c_1, \ldots, c_n) \in \boldsymbol{V}(I)$*.*

Demostración: Usaremos la notación $\mathbf{c} = (c_2, \ldots, c_n)$. Por la proposición 11, sabemos que $Res(f, g, x_1) \in I_1$, así que la resultante se anula en la solución parcial $\mathbf{c}$. Si ni a_0 ni b_0 se anulan en $\mathbf{c}$, entonces el c_1 requerido existe por la proposición 12.
Por hipótesis sabemos que ambos no se anulan en $\mathbf{c}$ sin embargo podría darse el caso que uno de los dos se anulase. Supongamos que $a_0(\mathbf{c}) \neq 0$ pero $b_0(\mathbf{c}) = 0$. Entonces $g(x_1, \mathbf{c})$ tiene grado en x_1 estrictamente menor que m. En este caso, el determinante de (3.3) es $(l+m) \times (l+m)$, lo que lo hace demasiado grande para ser la resultante de $f(x_1, \mathbf{c})$ y $g(x_1, \mathbf{c})$.
La idea para demostrar esto es que dado que $\mathbf{V}(f, g)$ depende del ideal $\langle f, g\rangle$, podemos usar una base diferente del ideal cuando $a_0(\mathbf{c}) \neq 0$ y $b_0(\mathbf{c}) = 0$. Si N es cualquier entero positivo. Hay que probar

$$\langle f, g\rangle = \langle f, g + x_1^N f\rangle. \tag{3.4}$$

Si $h \in \langle f, g\rangle$ será de la forma $h = Af + Bg$, donde $A, B \in K[x_1, \ldots, x_n]$, entonces también $h = Af + Bg - Bx_1^N f + Bx_1^N f$. Reagrupando los términos $h = (A - Bx_1^N)f + B(g + x_1^N f)$,dado

que $(A - Bx_1^N), B \in K[x_1, \ldots, x_n]$ entonces $h \in \langle f, g + x_1^N f\rangle$.
Si $h \in \langle f, g+x_1^N f\rangle$ será de la forma $h = Af+B(g+x_1^N f)$, donde $A, B \in K[x_1, \ldots, x_n]$. Entonces $h = Af + Bg + Bx_1^N f$ y de aquí $h = (A + Bx_1^N)f + Bg$, dado que $(A + Bx_1^N), B \in K[x_1, \ldots, x_n]$ entonces $h \in \langle f, g\rangle$. Con lo que queda demostrado.

Ahora elegimos N lo suficientemente grande de manera que $x_1^N f$ tenga grado más grande en x_1 que g. Entonces el coeficiente líder de $g + x_1^N f$ con respecto a x_1 es a_0, el cual es no nulo en $\mathbf{c}$. Esto nos permite aplicar el argumento previo a f y $g + x_1^N f$, obteniendo $c_1 \in K$ con $(c_1, \mathbf{c}) \in \mathbf{V}(f, g + x_1^N f)$. Por (3.4), esto implica $(c_1, \mathbf{c}) \in \mathbf{V}(f, g)$, y el teorema queda probado. El caso $a_0(\mathbf{c}) = 0$ y $b_0(\mathbf{c}) \neq 0$ es análogo. □

Nota 3. *Vemos que la prueba no sería válida en el caso en que a_0 y b_0 se anulen ambos en $\mathbf{c}$. La razón de esto es que obviamente en este caso la solución parcial podría no extender.*

Pasaremos ahora a probar el teorema de la Extensión para un ideal arbitrario $\langle f_1, \ldots, f_s\rangle \subset K[x_1, \ldots, x_n]$. El problema inmediato que tenemos es que solamente hemos definido la resultante de dos polinomios. La manera de definirlo es introduciendo nuevas variables $u_2, \ldots, u_s$ y metiendo $f_2, \ldots, f_s$ en un único polinomio

$$u_2 f_2 + \ldots + u_s f_s \in K[u_2, \ldots, u_s, x_1, \ldots, x_n].$$

Podemos englobar a f_1 también dentro de este anillo. Por la proposición 11, la resultante de f_1 y $u_2 f_2 + \ldots + u_s f_s$ pertenece a $K[u_2, \ldots, u_s, x_2, \ldots, x_n]$. Para obtener polinomios en $x_2, \ldots, x_n$, expandimos la resultante en términos de potencias de $u_2, \ldots, u_s$. Esto significa escribir

$$Res(f_1, u_2 f_2 + \ldots + u_s f_s, x_1) = \sum_\alpha h_\alpha(x_2, \ldots, x_n) u^\alpha, \tag{3.5}$$

donde u^α es el monomio $u_2^{\alpha_2} \cdots u_s^{\alpha_s}$ y $h_\alpha \in K[x_2, \ldots, x_n]$ para todo α. Llamamos a los polinomios h_α resultantes generalizados de $f_1, \ldots, f_s$.

Ejemplo 3.2.1. *Como ejemplo computaremos la resultante generalizado de*

$$f_1 = x^2 + y + z - 1,$$
$$f_2 = x + y^2 + z - 1,$$
$$f_3 = x + y^2 + z - 1.$$

Si computamos la resultante $Res(f, u_2 f_2 + u_3 f_3, x)$ y luego reordenamos los términos en función de las u_i obtenemos lo siguiente:

$$\begin{aligned} Res(f_1, u_2 f_2 + u_3 f_3, x) = (&y^4 + 2y^2 z - 2y^2 + x^2 + y - z)u_2^2 \\ &+2(y^2 z^2 + y^3 + z^3 - y^2 - z^2 + yz)u_2 u_3 \\ &+(z^4 + 2yz^2 + y^2 - 2z^2 - y + z. \end{aligned}$$

De aquí se sigue que los resultantes generalizados vienen dados por

$$h_{20} = y^4 + 2y^2 z - 2y^2 + z^2 + y - z,$$

$$h_{11} = 2(y^2z^2 + y^3 + z^3 - y^2 - z^2 + yz,$$
$$h_{02} = z^4 + 2yz^2 + y^2 - 2z^2 - y + z.$$

Vemos que estos pueden variar en función del orden. Por tanto en la práctica apenas se usan pero nos sirven para demostrar el teorema de la Extensión.

Teorema 3.2.2. ***(El Teorema de la Extensión)****. Sea $I = \langle f_1, \ldots, f_s\rangle \subset K[x_1, \ldots, x_n]$ y sea I_1 el primer ideal de eliminación de I. Para cada $1 \leq i \leq s$, escribimos f_i en la forma*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ terminos con grado en } x_1 \ < N_i,$$

donde $N_i \geq 0$ y $g_i \in K[x_2, \ldots, x_n]$ es no nulo. Supongamos que tenemos una solución parcial $(c_2, \ldots, c_n) \in \boldsymbol{V}(I_1)$. Si $(c_2, \ldots, c_n) \notin \boldsymbol{V}(g_1, \ldots, g_s)$, entonces existe $c_1 \in K$ tal que $(c_1, c_2, \ldots, c_n) \in \boldsymbol{V}(I)$.

Demostración: Como siempre fijamos $\mathbf{c} = (c_2, \ldots, c_n)$. Buscamos una raíz común c_1 de $f_1(x_1, \mathbf{c}), \ldots, f_s(x_1, \mathbf{c})$. El caso $s = 2$ se trató en el teorema anterior, el cual también cubre el caso $s = 1$ dado que $\mathbf{V}(f_1) = \mathbf{V}(f_1, f_1)$. Queda de probar el caso $s \geq 3$.

Dado que $\mathbf{c} \notin \mathbf{V}(g_1, \ldots, g_s)$, asumiremos que $g_1(\mathbf{c}) \neq 0$. Sean $h_\alpha \in K[x_2, \ldots, x_n]$ los resultantes generalizados de $f_1, \ldots, f_s$. Por tanto,

$$Res(f_1, u_2f_2 + \ldots + u_sf_s, x_1) = \sum_\alpha h_\alpha u^\alpha. \tag{3.6}$$

Vamos a demostrar ahora que los h_α pertenecen al primer ideal de eliminación I_1. Dado que estamos computando los resultantes en el anillo $K[u_2, \ldots, u_s, x_1, \ldots, x_n]$, se sigue de la proposición 11 que

$$Af_1 + B(u_2f_2 + \ldots + u_sf_s, x_1) = Res(f_1, u_2f_2 + \ldots + u_sf_s, x_1) \tag{3.7}$$

para algunos polinomios $A, B \in K[u_2, \ldots, u_s, x_1, \ldots, x_n]$. Ahora escribimos $A = \sum_\alpha A_\alpha u^\alpha$ y $B = \sum_\beta B_\beta u^\beta$, donde $A_\alpha, B_\beta \in K[x_1, \ldots, x_n]$. Probaremos que $h_\alpha \in \langle f_1, \ldots, f_s\rangle = I$ comparando los coeficientes de u^α en (3.7). Dado que $h_\alpha \in K[x_2, \ldots, x_n]$, probar lo anterior demostraría que $h_\alpha \in I_1$.
Para comparar los coeficientes, necesitamos escribir todo agrupando los u^α. Fijamos $e_2 = (1, 0, \ldots, 0), \ldots, e_s = (0, \ldots, 0, 1)$, de tal forma que $u_2f_2 + \ldots + u_sf_s = \sum_{i\geq 2} u^{e_i}f_i$. Entonces la ecuación (3.7) se puede escribir

$$\begin{aligned}
\sum_\alpha h_\alpha u^\alpha &= (\sum_\alpha A_\alpha u^\alpha)f_1 + (\sum_\beta B_\beta u^\beta)(\sum_{i\geq 2} u^{e_i}f_i) \\
&= \sum_\alpha (a_\alpha f_1)u^\alpha + \sum_{i\geq 2.\beta} B_\beta f_i u^{\beta+e_i} \\
&= \sum_\alpha (A_\alpha f_1)u^\alpha + \sum_\alpha (\sum_{i\geq 2.\beta \ \ \beta+e_i=\alpha} B_\beta f_i)u^\alpha \\
&= \sum_\alpha (A_\alpha f_1 + \sum_{i\geq 2.\beta \ \ \beta+e_i=\alpha} B_\beta f_i)u^\alpha.
\end{aligned}$$

Si igualamos los coeficientes de u^α, obtenemos

$$h_\alpha = A_\alpha f_1 + \sum_{i \geq 2. \beta \quad \beta + e_i = \alpha} B_\beta f_i,$$

lo que prueba que $h_\alpha \in I$. Como hemos visto, esto prueba que $h_\alpha \in I_1$ para todo α. Dado que $\mathbf{c} \in \mathbf{V}(I_1)$, se sigue que $h_\alpha(\mathbf{c}) = 0$ para todo α. Entonces (3.6)nos dice que la resultante $h = Res(f_1, u_2 f_2 + \ldots + u_s f_s, x_1)$ se anula cuando se evalúa en $\mathbf{c}$. Si $h(\mathbf{c}, u_2, \ldots, u_s)$ denota el polinomio en $K[x_1, u_2, \ldots, u_s]$ que conseguimos cuando sustituimos $\mathbf{c} = (c_2, \ldots, c_n)$ para $(x_2, \ldots, x_n)$, entonces tenemos

$$h(\mathbf{c}, u_2, \ldots, u_s) = 0. \tag{3.8}$$

Supondremos lo siguiente con respecto a f_2:

$$g_2(\mathbf{c}) \neq 0 \ \textit{y} \ f_2 \ \textit{tiene grado mayor que} \ f_3, \ldots, f_s \ \textit{en} \ x_1. \tag{3.9}$$

Veamos que esto implica que

$$h(\mathbf{c}, u_2, \ldots, u_s) = Res(f_1(x_1, \mathbf{c}), u_2 f_2(x_1, \mathbf{c}) + \ldots + u_s f_s(x_1, \mathbf{c}), x_1). \tag{3.10}$$

Si evaluamos el determinante definiendo a $h = Res(f_1, u_2 f_2 + \ldots + u_s f_s, x_1)$ en $\mathbf{c}$, se sigue que $h(\mathbf{c}, u_2, \ldots, u_s)$ está dado por un cierto determinante. Es más, este determinante es la resultante en (3.10) siempre que el coeficiente líder de f_1 y $u_2 f_2 + \ldots + u_s f_s$ no se anulen en $\mathbf{c}$. Esto es verdadero para f_1 dado que $g_1(\mathbf{c}) \neq 0$. Para $u_2 f_2 + \ldots + u_s f_s$, la suposición (3.9) implica que su coeficiente líder es $u_2 g_2$, y (3.9) también nos dice que el coeficiente líder no se anula dado que $g_2(\mathbf{c}) \neq 0$. Esto prueba (3.10).
Si combinamos (3.8) y (3.10), entonces obtenemos

$$Res(f_1(x_1, \mathbf{c}), u_2 f_2(x_1, \mathbf{c}) + \ldots + u_s f_s(x_1, \mathbf{c}), x_1) = 0.$$

Los polinomios $f_1(x_1, \mathbf{c})$ y $u_2 f_2(x_1, \mathbf{c}) + \ldots + u_s f_s(x_1, \mathbf{c})$ pertenecen a $K[x_1, u_2, \ldots, u_s]$, así que por la proposición (11), la anulación de sus resultantes implica que tienen un factor común F de grado positivo en x_1. Dado que F divide a $f_1(x_1, \mathbf{c})$ se sigue que F es un polinomio en $K[x_1]$. Veamos que F divide a todos $f_2(x_1, \mathbf{c}), \ldots, f_s(x_1, \mathbf{c})$. Sabemos que F divide a $u_2 f_2(x_1, \mathbf{c})$, lo que significa que

$$F(x_1) A(x_1, u_2, \ldots, u_s) = u_2 f_2(x_1, \mathbf{c}) + \ldots + u_s f_s(x_1, \mathbf{c}), \tag{3.11}$$

para algún $A \in K[x_1, u_2, \ldots, u_s]$. Comparando los coeficientes de $u_2, \ldots, u_s$ se llega a que F divide $f_2(x_1, \mathbf{c}), \ldots, f_s(x_1, \mathbf{c})$.
Dado que F también divide a $f_1(x_1, \mathbf{c})$, vemos que F es un factor común de grado positivo de todos los $f_i(x_1, \mathbf{c})'s$. Ahora sea c_1 una raíz de F (esta existe pues estamos en un cuerpo algebraicamente cerrado). Entonces c_1 es automáticamente raíz de todos los $f_i(x_1, \mathbf{c})'s$, lo que prueba el teorema de la Extensión cuando se verifica (3.9).
Ahora veamos que pasa cuando (3.9) no se cumple para $f_1, \ldots, f_s$, entonces es fácil encontrar una nueva base para la cual (3.9) se cumple. La idea es sustituir f_2 por $f_2 + x_1^N f_1$, donde N es un entero positivo. Hay que demostrar que

$$I = \langle f_1, f_2 + x_1^N f_1, f_3, \ldots, f_s \rangle.$$

La demostración es idéntica a la hecha para probar que $\langle f, g \rangle = \langle f, g + x_1^N f \rangle$.

Si N es suficientemente grande, el coeficiente líder de $f_2 + x_1^N f_1$ será g_1, el cual sabemos que no se anula en $\mathbf{c}$. Haciendo N más grande si es necesario, podemos asumir que $f_2 + x_1^N f_1$ tiene grado más grande en x_1 que $f_3, \ldots, f_s$. Entonces el argumento previo nos da c_1 el cual es raíz de $f_1(x_1, \mathbf{c}), f_2(x_1, \mathbf{c}) + x_1^N f_1(x_1, \mathbf{c}), f_3(x_1, \mathbf{c}), \ldots, f_s(x_1, \mathbf{c})$. Se comprueba entonces que que c_1 es raíz de todos los $f_i(x_1, \mathbf{c})'s$. Lo que concluye la demostración del teorema de la Extensión. □

El teorema de la Extensión es especialmente fácil de usar si uno de los coeficientes líder es constante.

Corolario 3.2.3. *Sea $I = \langle f_1, \ldots, f_s \rangle \subset K[x_1, \ldots, x_n]$, y supondremos que para algunos i, f_i es de la forma*

$$f_i = cx_1^N + \text{ términos con grado en } x_1 < N,$$

donde $c \in K$ es no nulo y $N > 0$. Si I_1 es el primer ideal de eliminación de I y $(a_2, \ldots, a_n) \in \boldsymbol{V}(I_1)$, entonces existe $a_1 \in K$ tal que $(a_1, a_2, \ldots, a_n) \in \boldsymbol{V}(I)$.

Demostración: Se sigue inmediatamente del teorema de la Extensión: dado que $g_i = c \neq 0$ implica que $\mathbf{V}(g_1, \ldots, g_s) = \emptyset$, tenemos $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$ para todas las soluciones parciales. □

En el caso en que uno de los coeficientes sea una constante no nula los $g_i's$ nunca se pueden anular a la vez en el punto $(a_2, \ldots, a_n)$, y como consecuencia las soluciones parciales siempre se pueden extender en este caso. Tenemos por tanto la siguiente versión geométrica del corolario anterior.

Corolario 3.2.4. *Sea $V = \boldsymbol{V}(f_1, \ldots, f_s) \subset K^n$, y suponemos que para algún i, f_i es de la forma*

$$f_i = cx_1^N + \text{ términos con grado en } x_1 < N,$$

donde $c \in K$ es no nula y $N > 0$. Si I_1 es el primer ideal de eliminación, entonces en K^{n-1}

$$\pi_1(V) = \boldsymbol{V}(I_1),$$

donde π_1 es la proyección en las últimas $n-1$ componentes.

3.3. Hilbert's Nullstellensatz

Ahora ya tenemos los ingredientes necesarios para poder demostrar el Hilbert's Nullstellensatz. Daremos tres versiones que son equivalentes del mismo, cada una de ellas útil en distintas situaciones.

Teorema 3.3.1 (**Nullstellensatz débil**)**.** *Sea K un cuerpo algebraicamente cerrado y sea $I \subseteq K[x_1, \ldots, x_n]$ un ideal con $\boldsymbol{V}(I) = \emptyset$. Entonces $I = K[x_1, \ldots, x_n]$.*

Demostración: Para probar esto, veremos que $1 \in I$. Con esto tenemos lo que queremos pues si $1 \in I$ entonces $f = f \cdot 1 \in I$ y por tanto $f \in I$ para cada $f \in K[x_1, \ldots, x_n]$.
Lo probaremos por inducción sobre n, el número de variables. Si $n = 1$ y $I \subseteq K[x]$ satisface $\mathbf{V}(I) = \emptyset$ como sabemos que $K[x]$ es dominio de ideales principales podemos escribir $I = \langle f \rangle$. Entonces $\mathbf{V}(I)$ es el conjunto de raíces de f, dado que K es algebraicamente cerrado todo polinomio no constante tiene una raíz. Por ello la única forma de que $\mathbf{V}(I) = \emptyset$ es que f sea una

constante no nula. En este caso $1/f \in K$, por ello $1 = (1/f) \cdot f \in I$, con lo que terminamos.
Supongamos ahora el resultado cierto para $n-1$ variables que escribiremos $K[x_2, \ldots, x_n]$. Consideramos cualquier ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq K[x_1, \ldots, x_n]$ para el cual $\mathbf{V}(I) = \emptyset$. Asumiremos que f_1 es no constante pues si no no hay nada que demostrar. Así que supongamos que f_1 tiene grado total $N \geqslant 1$. Ahora haremos un cambio de coordenadas para escribir f_1 con una forma que nos interesa:

$$\begin{aligned} x_1 &= \tilde{x_1}, \\ x_2 &= \tilde{x_2} + a_2\tilde{x_1}, \\ &\vdots \\ x_n &= \tilde{x_n} + a_n\tilde{x_1}, \end{aligned}$$

donde los a_i son constantes en K que debemos determinar. Sustituimos para $x_1, \ldots, x_n$ así que f_1 tiene la forma:

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= f_1(\tilde{x_1}, \ldots, \tilde{x_n} + a_n\tilde{x_1}) \\ &= c(a_2, \ldots, a_n)\tilde{x_1}^N + \ \textit{términos con grado } < N \textit{ en } x_1. \end{aligned}$$

Hay que probar que $c(a_2, \ldots, a_n)$ es una expresión polinomial no nula en $a_2, \ldots, a_n$. Si escribimos $f = h_N + h_{N-1} + \ldots + h_0$, donde cada h_i es un polinomio homogéneo de grado i. Veamos que tras el cambio de coordenadas descrito, el coeficiente $c(a_1, \ldots, a_n)$ de $\tilde{x_1}^N$ en $\tilde{f}$ es $h_N(1, a_2, \ldots, a_n)$. Si elegimos un monomio cualquiera de h_N será de la forma $cx_1^{\alpha_1} \cdots x_n^{\alpha_n}$, donde $\alpha_1 + \ldots + \alpha_n = N$. Si aplicamos el cambio de variables obtenemos $c\tilde{x_1}^{\alpha_1} \cdot (\tilde{x_2} + a_2\tilde{x_1})^{\alpha_2} \cdots (\tilde{x_n} + a_n\tilde{x_1})^{\alpha_n}$. Vemos el único término que llega a grado N en $\tilde{x_1}$ será $c\tilde{x_1}^{\alpha_1} a_2^{\alpha_2} \tilde{x_1}^{\alpha_2} \cdots a_n^{\alpha_n} \tilde{x_1}^{\alpha_n}$ lo que claramente nos da $ca_2^{\alpha_2} \cdots a_n^{\alpha_n} x_1^N$ y por tanto vemos que claramente el coeficiente líder es el del monomio evaluado en $(1, a_2, \ldots, a_n)$. Esto ocurrirá en todos los monomios pues le hemos elegido arbitrario. Con lo que se obtiene que el coeficiente líder de $\tilde{x_1}^N$ es $h_N(1, a_2, \ldots, a_n)$ ver que este es no nulo es fácil pues dado que h_N es homogéneo si una constante la convertimos en 1 los monomios no se pueden anular entre si pues los exponentes del resto de variables han de ser distintos.

Dado que un cuerpo algebraicamente cerrado es infinito y $c(a_2, \ldots, a_n)$ es una expresión polinomial no nula podemos elegir $a_2, \ldots, a_n$ de tal forma que $c(a_2, \ldots, a_n) \neq 0$.
Con esta elección de $a_2, \ldots, a_n$, bajo el cambio de coordenadas descrito anteriormente, todo polinomio $f \in K[x_1, \ldots, x_n]$ se lleva a un polinomio $\tilde{f} \in K[\tilde{x_1}, \ldots, \tilde{x_n}]$. Hay que probar que el conjunto $\tilde{I} = \{\tilde{f} : f \in I\}$ es un ideal en $K[\tilde{x_1}, \ldots, \tilde{x_n}]$. Lo primero es tener en cuenta que el cambio de variables es una transformación lineal entre los cuerpos de polinomios $K[x_1, \ldots, x_n]$ y $K[\tilde{x_1}, \ldots, \tilde{x_n}]$ por tanto se verificará que $\tilde{f} + \tilde{g} = \widetilde{f+g}$ y también $\tilde{f} \cdot \tilde{g} = \widetilde{f \cdot g}$. Para ver que $\tilde{I}$ veamos primero que si $\tilde{f}, \tilde{g} \in \tilde{I}$ entonces $\tilde{f} + \tilde{g} \in \tilde{I}$. Dado que $\tilde{f} + \tilde{g} = \widetilde{f+g}$, entonces para ver que pertenece a $\tilde{I}$ hay que ver que $f + g \in I$ lo cual es claro pues I es un ideal y la suma de elementos del ideal está en el ideal. Veamos ahora que si $g \in K[\tilde{x_1}, \ldots, \tilde{x_n}]$ es un polinomio cualquiera, entonces $g \cdot \tilde{f} \in \tilde{I}$. Claramente g tendrá asociado un polinomio $g' \in K[x_1, \ldots, x_n]$ tal que $g = \tilde{g'}$ entonces $g \cdot \tilde{f} = \widetilde{g' \cdot f}$. Entonces hay que ver que $g' \cdot f \in I$ lo cual se verifica de nuevo dado que I es un ideal. Con lo que queda probado que $\tilde{I}$ es un ideal.

Vemos que se cumple también que $\mathbf{V}(\tilde{I}) = \emptyset$ dado que si las ecuaciones transformadas tuvieran solución también la tendrían las originales. Es más, si podemos demostrar que $1 \in \tilde{I}$, entonces

$1 \in I$ dado que las constantes no se ven afectadas por la operación $\tilde{}$.
Probaremos ahora que $1 \in \tilde{I}$. Hemos visto que $f_1 \in I$ se transforma en $\tilde{f_1} \in \tilde{I}$ con la propiedad

$$\tilde{f_1}(\tilde{x_1}, \ldots, \tilde{x_n}) = c(a_2, \ldots, a_n)\tilde{x_1}^N + \ \textit{términos con grado} \ < N \ \textit{en} \ x_1,$$

donde $c(a_2, \ldots, a_n) \neq 0$. Esto nos permite usar el corolario 3.2.4, para relacionar $\mathbf{V}(\tilde{I})$ con su proyección en el espacio de coordenadas $\tilde{x_2}, \ldots, \tilde{x_n}$. Sea

$$\pi_1 : K^n \longrightarrow K^{n-1},$$

la proyección sobre las últimas $n-1$ componentes. Si consideramos $\tilde{I_1} = \tilde{I} \cap K[\tilde{x_2}, \ldots, \tilde{x_n}]$ el primer ideal de eliminación, entonces el corolario 3.2.4 nos dice que las soluciones parciales en K^{n-1} siempre extienden y de hecho $\mathbf{V}(\tilde{I_1}) = \pi_1(\mathbf{V}(\tilde{I}))$. Esto implica que

$$\mathbf{V}(\tilde{I_1}) = \pi_1(\mathbf{V}(\tilde{I})) = \pi_1(\emptyset) = \emptyset.$$

Por la hipótesis de inducción, se verifica que $\tilde{I_1} = K[\tilde{x_2}, \ldots, \tilde{x_n}]$. Pero esto implica que $1 \in \tilde{I_1} \subset \tilde{I}$, con lo que se termina la demostración. □

Pasemos ahora a enunciar y demostrar el Hilbert's Nullstellensatz.

Teorema 3.3.2. ***(Hilbert's Nullstellensatz).*** *Sea K un cuerpo algebraicamente cerrado. Sean $f, f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ tales que $f \in \boldsymbol{I}(\boldsymbol{V}(f_1, \ldots, f_s))$, entonces existe un entero $m \geq 1$ tal que*

$$f^m \in \langle f_1, \ldots, f_s \rangle,$$

(y viceversa).

Demostración: Dado un polinomio f que se anula en todos los ceros comunes de los polinomios $f_1, \ldots, f_s$, debemos demostrar que existe un entero $m \geq 1$ y polinomios $A_1, \ldots, A_s$ tal que

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

La prueba más directa está basada en un truco ingenioso. Consideramos el ideal

$$\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset K[x_1, \ldots, x_n, y],$$

donde $f, f_1, \ldots, f_s$ son como antes. Veamos que $\mathbf{V}(\tilde{I}) = \emptyset$.
Para ver esto, sea $(a_1, \ldots, a_n, a_{n+1}) \in K^{n+1}$. Pueden pasar dos casos:
Caso 1: Si $(a_1, \ldots, a_n)$ no es cero común de $f_1, \ldots, f_s$ entonces $f(a_1, \ldots, a_n) = 0$ dado que f se anula en los ceros comunes de $f_1, \ldots, f_s$. Por tanto, el polinomio $1 - yf$ toma el valor $1 - a_{n+1}f(a_1, \ldots, a_n) = 1 \neq 0$ en el punto $(a_1, \ldots, a_n, a_{n+1})$. En particular,
$(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$.
Caso 2: Si $(a_1, \ldots, a_n)$ no es un cero común de $f_1, \ldots, f_s$ entonces para algún i, tenemos $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$. En particular, concluimos también que $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$.
Dado que $(a_1, \ldots, a_n, a_{n+1}) \in K^{n+1}$ es arbitrario, se concluye que $\mathbf{V}(\tilde{I}) = \emptyset$. Ahora aplicamos el Hilbert's Nullstellensatz débil para concluir que $1 \in \tilde{I}$. Esto significa

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf),$$

para algunos $p_i, q \in K[x_1, \ldots, x_n, y]$. Ahora elegimos $y = 1/f(x_1, \ldots, x_n)$. Entonces la relación de arriba implica que

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i.$$

Si multiplicamos a ambos lados de la ecuación por una potencia f^m, donde m se elige suficientemente grande para eliminar todos los denominadores. Lo que nos lleva a

$$f^m = \sum_{i=1}^{s} A_i f_i,$$

para algunos polinomios $A_i \in K[x_1, \ldots, x_n]$, lo que teníamos que probar. □

Ahora daremos otra versión de este teorema que se utiliza en la práctica para calcular el radical de un ideal.

Teorema 3.3.3. ***(Hilbert's Nullstellenzatz fuerte).*** *Sea K un cuerpo algebraicamente cerrado. Si I es un ideal en $K[x_1, \ldots, x_n]$, entonces*

$$\boldsymbol{I}(\boldsymbol{V}(I)) = \sqrt{I}.$$

Demostración: Tenemos que $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$ dado que $f \in \sqrt{I}$ implica que $f^m \in I$ para algún m. Por tanto f^m se anula en $\mathbf{V}(I)$, lo que implica que f se anula en $\mathbf{V}(I)$. Y por tanto $f \in \mathbf{I}(\mathbf{V}(I))$.
Para la otra contención, supongamos que $f \in \mathbf{I}(\mathbf{V}(I))$. Entonces, por definición, f se anula en $\mathbf{V}(I)$. Por el Hilbert's Nullstellensatz, entonces existe un entero $m \geq 1$ tal que $f^m \in I$. Pero esto significa que $f \in \sqrt{I}$. Dado que f era arbitrario, $\mathbf{I}(\mathbf{V}(I)) \subset \sqrt{I}$. Lo que completa la demostración. □

Capítulo 4

Cadenas regulares

Una vez definidos todos los conceptos que necesitamos y los teoremas mas importantes que utilizaremos pasamos a introducir el concepto en el que se centra el trabajo y sobre el que se basan los algoritmos que se van a desarrollar. En este capítulo y los siguientes se ha seguido el artículo de Kalkbrenner [1].

4.1. Cadenas regulares y ceros regulares

Las variedades normalmente se representan como conjuntos de ceros de un número finito de polinomios. Aquí se va a utilizar una representación diferente para las variedades. Dado que toda variedad irreducible está únicamente determinada por uno de sus puntos genéricos, entonces representaremos las variedades mediante los puntos genéricos de sus componentes irreducibles. Para encontrar esta representación definiremos un tipo de subconjuntos del cuerpo de polinomios al que llamaremos cadenas regulares. Estas cadenas regulares tendrán asociadas un conjunto de puntos de $\overline{K}^n$ a los que llamaremos ceros regulares de una cadena regular. Como ya hemos visto, todo punto de $\overline{K}^n$ es punto genérico de una variedad irreducible, por tanto a partir de cada uno de los ceros regulares obtendremos la descripción de una variedad irreducible. Por lo tanto el objetivo será encontrar un conjunto de cadenas regulares de forma que los ceros regulares de estas nos describan cada una de las componentes irreducibles de la variedad.

Definición 4.1.1 (**Cadena regular**). *Vamos a dar una definición inductiva de las cadenas regulares, comenzaremos con el caso $n = 0$. El conjunto vacío es la única cadena regular en K y el conjunto $\overline{K}^0$ que contiene solamente la lista vacía es llamado conjunto de ceros regulares de $\emptyset$, denotado por $RZ_0(\emptyset)$.*
Ahora sea n un número natural cualquiera. Un subconjunto $R \subseteq K[x_1, \ldots, x_n]$ es una cadena regular si:

1. *$R \cap K[x_1, \ldots, x_{n-1}]$ es una cadena regular en $K[x_1, \ldots, x_{n-1}]$*
2. *$R - K[x_1, \ldots, x_{n-1}]$ tiene como mucho un elemento.*
3. *Si $\exists f \in R - K[x_1, \ldots, x_{n-1}]$, entonces $lc_n(f)(a_1, \ldots, a_{n-1}) \neq 0$ para todo $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R \cap K[x_1, \ldots, x_{n-1}])$.*

Donde $RZ_{n-1}(R \cap K[x_1, \ldots, x_{n-1}])$ es el conjunto de ceros regulares de $R \cap K[x_1, \ldots, x_{n-1}]$.

Notación. *A partir de ahora denotaremos al conjunto $R \cap K[x_1, \ldots, x_k]$ por R_k.*

Nos surge ahora el problema de describir el conjunto RZ_{n-1} para poder saber si un conjunto es de verdad una cadena regular. De las propiedades 1 y 2 de la definición anterior se puede ver que las cadenas regulares son conjuntos triangulares pues solo se va añadiendo un polinomio en cada variable. Por tanto tiene sentido definir los ceros regulares de la siguiente forma:

Definición 4.1.2 (**Ceros regulares**). *El conjunto de ceros regulares de una cadena regular $R \subseteq K[x_1, \ldots, x_n]$ se define de dos formas distintas en función de R.*

***Caso 1**: Si $R \subseteq K[x_1, \ldots, x_{n-1}]$ entonces:*
$RZ_n(R) = \{(a_1, \ldots, a_n) | (a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1}), a_n \in \overline{K}$ *trascendente sobre* $K(a_1, \ldots, a_{n-1})\}$.

***Caso 2**: Si existe $f \in R - K[x_1, \ldots, x_n]$ entonces:*

$$RZ_n(R) = \{(a_1, \ldots, a_n) | (a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1}), a_n \in \overline{K}, \text{ y } f(a_1, \ldots, a_n) = 0\}.$$

Es claro por definición que $RZ_n(R)$ es no vacío para toda cadena regular $R \subseteq K[x_1, \ldots, x_n]$.

Nota 4. *Veamos que la cadena regular vacía en cualquier dimensión es de verdad una cadena regular y que:*
$RZ_n(\emptyset) = \{(a_1, \ldots, a_n) |$ $a_1, \ldots, a_n \in \overline{K}$ *y* a_i *trascendente sobre* $K(a_1, \ldots, a_{i-1})$ *para todo* $i \in \{1, \ldots, n\}\}$.

Lo probaremos por inducción sobre n. Veamos primero el caso $n = 1$, tenemos que $\emptyset \cap K = \emptyset$, el cual es cadena regular por definición, por lo que se verifica 1. Dado que $\emptyset - K$ no tiene elementos se verifican 2 y 3. Para ver cuales son los ceros regulares, dado que $\emptyset \subseteq K$,

$$RZ_1(\emptyset) = \{a_1 | a_1 \in \overline{K} \text{ trascendente sobre } K\}.$$

Por lo que se verifica el caso $n = 1$.
Suponemos que se verifica para el caso $n - 1$. Lo probaremos para la cadena regular vacía en $K[x_1, \ldots, x_n]$. Dado que $\emptyset \cap K[x_1, \ldots, x_{n-1}] = \emptyset$, el cual por hipótesis de inducción es una cadena regular. Además como $\emptyset - K[x_1, \ldots, x_{n-1}]$ no tiene elementos se verifican 2 y 3. Para ver cuales son los ceros regulares tenemos que como $\emptyset \subseteq K[x_1, \ldots, x_{n-1}]$:
$RZ_n(\emptyset) = \{(a_1, \ldots, a_n) | (a_1, \ldots, a_{n-1}) \in RZ_{n-1}(\emptyset), a_n \in \overline{K}$ *trascendente sobre* $K(a_1, \ldots, a_{n-1})\}$.
Con lo que por la hipótesis de inducción $(a_1, \ldots, a_{n-1})$ verifican las hipótesis y también lo hace a_n con lo que se prueba para cualquier n.

Para ver como funcionan estos conceptos vamos a ver una serie de ejemplos.

Ejemplo 4.1.1. *Estudiemos si los siguientes subconjuntos de $\mathbb{Q}[x_1, x_2, x_3]$ son cadenas regulares o no, y calculemos sus ceros regulares si lo son.*

$$R_1 = \{x_2^2 - x_1^2, x_3, x_3 + 1\},$$

$$R_2 = \{x_2^2 - x_1^2, (x_2 - x_1)x_3\},$$

$$R_3 = \{x_2^2 - x_1^2, x_3 - x_1\},$$
$$R_4 = \{x_2^2 - x_1^2, (x_3 - x_1)x_2\}.$$

Vemos primero que $R_i \cap \mathbb{Q}[x_1, x_2] = \{x_2^2 - x_1^2\}\ \forall i = 1, 2, 3, 4$. *Veamos que esto es una cadena regular, aplicando la definición:* $\{x_1^2 - x_2^2\} \cap \mathbb{Q}[x_1] = \emptyset$, *por la nota anterior es cadena regular en* $\mathbb{Q}[x_1]$ *y además:*
$RZ_1(\emptyset) = \{a_1 | a_1 \in \overline{\mathbb{Q}}$ *trascendente sobre* $\mathbb{Q}\}$.
Ahora pasamos a ver que $\{x_2^2 - x_1^2\}$ *es cadena regular, hemos probado ya la condición (1). La condición (2) se verifica dado que* $\{x_2^2 - x_1^2\} - \mathbb{Q}[x_1]$ *tiene solo un elemento. Para la condición (3) tenemos que* $lc_2(x_2^2 - x_1^2) = 1$ *por lo que evaluado en* $RZ_1(\emptyset)$ *es distinto de 0. Con lo que se verifica que* $\{x_2^2 - x_1^2\}$ *es cadena regular. Veamos cuales son los ceros regulares. Como* $\exists f \in \{x_2^2 - x_1^2\} - \mathbb{Q}[x_1]$ *se define*

$$RZ_2(\{x_2^2 - x_1^2\}) = \{(a_1, a_2) | a_1 \in RZ_1(\emptyset), a_2 \in \overline{\mathbb{Q}}, a_2^2 - a_1^2 = 0\},$$

con lo que por como definimos $RZ_1(\emptyset)$ *y despejando la ecuación tenemos que:*

$$RZ_2(\{x_2^2 - x_1^2\}) = \{(a, a) | a \in \overline{\mathbb{Q}} \text{ trascendente sobre } \mathbb{Q}\} \cup \{(a, -a) | a \in \overline{\mathbb{Q}} \text{ trascendente sobre } \mathbb{Q}\}.$$

Una vez visto esto veamos si los conjuntos originales son o no cadenas regulares. Ya hemos visto que la condición (1) se cumple para todas. Vemos que R_1 *no es cadena regular pues* $R_1 - \mathbb{Q}[x_1, x_2]$ *tiene dos elementos.*
Tenemos que R_2 *si que verifica la condición (2) pues* $R_2 - \mathbb{Q}[x_1, x_2]$ *tiene un elemento. Sin embargo veamos que no verifica (3), tenemos* $f = (x_2 - x_1)x_3 \in R_2 - \mathbb{Q}[x_1, x_2]$, *y vemos que* $lc_3(f) = x_2 - x_1$ *sin embargo este se anula para los puntos de la forma* $(a, a) \in RZ_2(\{x_2^2 - x_1^2\})$ *y no se verifica (3).*
Tenemos que R_3 *si que verifica la condición (2) pues* $R_3 - \mathbb{Q}[x_1, x_2]$ *tiene un elemento. En este caso si que se verifica (3), tenemos* $f = x_3 - x_1 \in R_3 - \mathbb{Q}[x_1, x_2]$, *y vemos que* $lc_3(f) = 1$ *el cual es distinto de 0 para todo punto de* $RZ_2(\{x_2^2 - x_1^2\})$. *Calculemos entonces* $RZ_3(R_3)$, *puesto que* $\exists f \in R_3 - \mathbb{Q}[x_1, x_2]$ *tenemos que:*

$$RZ_3(R_3) = \{(a_1, a_2, a_3) | (a_1, a_2) \in RZ_2(\{x_2^2 - x_1^2\}), a_3 \in \overline{\mathbb{Q}}, a_3 - a_1 = 0\},$$

con lo que por como definimos $RZ_2(\{x_2^2 - x_1^2\})$ *y despejando la ecuación tenemos que:*

$$RZ_3(R_3) = \{(a, a, a) | a \in \overline{\mathbb{Q}} \text{ trascendente sobre } \mathbb{Q}\} \cup \{(a, -a, a) | a \in \overline{\mathbb{Q}} \text{ trascendente sobre } \mathbb{Q}\}.$$

Tenemos que R_4 *si que verifica la condición (2) pues* $R_4 - \mathbb{Q}[x_1, x_2]$ *tiene un elemento. En este caso si que se verifica (3), tenemos* $f = x_2(x_3 - x_1) \in R_4 - \mathbb{Q}[x_1, x_2]$, *y vemos que* $lc_3(f) = x_2$ *esto se anula en cualquier punto de la forma* $(a, 0)$ *sin embargo tenemos que este no pertenece a* $RZ_2(\{x_2^2 - x_1^2\})$ *pues el elemento 0 no es trascendente sobre* $\mathbb{Q}$, *por tanto se verifica (3). Calculemos entonces* $RZ_3(R_4)$, *puesto que* $\exists f \in R_3 - \mathbb{Q}[x_1, x_2]$ *tenemos que:*

$$RZ_3(R_4) = \{(a_1, a_2, a_3) | (a_1, a_2) \in RZ_2(\{x_2^2 - x_1^2\}), a_3 \in \overline{\mathbb{Q}}, a_2(a_3 - a_1) = 0\},$$

con lo que por como definimos $RZ_2(\{x_2^2 - x_1^2\})$, *tenemos que* $a_2 \neq 0$ *y ha de ser* $a_3 - a_1 = 0$ *por lo que nos queda:*

$$RZ_3(R_4) = \{(a, a, a) | a \in \overline{\mathbb{Q}} \text{ trascendente sobre } \mathbb{Q}\} \cup \{(a, -a, a) | a \in \overline{\mathbb{Q}} \text{ trascendente sobre } \mathbb{Q}\}.$$

Hay que notar que por ejemplo el $(0,0,a)$ es un cero común a los polinomios en R_4 pero sin embargo este no pertenece a $RZ_3(R_4)$. Dado que a nosotros lo que nos va a importar de las cadenas regulares son sus ceros regulares, las cadenas R_3 y R_4 van a representar a la misma variedad aunque sean distintas.

Dado que buscamos encontrar las variedades irreducibles que tienen un punto genérico dentro de los ceros regulares de una cadena regular tiene sentido definir el siguiente conjunto:

Definición 4.1.3. *Sea $n \in \mathbb{N}$. Si $R \subseteq K[x_1, \ldots, x_n]$ es una cadena regular llamamos conjunto de variedades irreducibles asociadas con R, denotadas por $AIV_n(R)$, al conjunto:*

$$AIV_n(R) = \{V | V \text{ es irreducible con un punto genérico en } RZ_n(R)\}.$$

Nota 5. *Veamos que $AIV_n(\emptyset) = \{\overline{K}^n\}$, veamos primero que la variedad $\overline{K}^n$ tiene un punto genérico en $RZ_n(\emptyset)$,ya hemos visto que los puntos de $RZ_n(\emptyset)$ son de la forma $(a_i, \ldots, a_n)$, con a_i trascendente sobre $K(a_1, \ldots, a_{i-1})$, además esto implica que a_i trascendente sobre $K(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. Veamos que los puntos de esta forma son puntos genéricos de $\overline{K}^n$, tenemos que el único polinomio que se anula en un punto de esta forma es el polinomio nulo pues si no tendríamos una relación algebraica y no serían trascendentes entre si, y es claro que todo punto de la variedad se anula en el polinomio nulo así que se verifica la condición de punto genérico. Ahora tenemos que ver que ninguna otra variedad irreducible tiene un punto genérico con la forma de arriba. Es claro que ninguna otra variedad tiene un punto genérico de esa forma pues estaría definida por una serie de polinomios no nulos y si un punto de esta forma los anulara entonces existiría una dependencia algebraica y no serían trascendentes entre si.*
Debido a esto tiene sentido definir $AIV_0(\emptyset) = \{\overline{K}^0\}$.

Definición 4.1.4. *Para todo $n \in \mathbb{N}$ y toda cadena regular R llamaremos a la variedad representada por R y la denotaremos por $Rep_n(R)$ a:*

$$Rep_n(R) = \bigcup_{V \in AIV_n(R)} V.$$

Ejemplo 4.1.2. *Sean R_3 y R_4 las cadenas regulares del ejemplo anterior. Recordemos que los ceros regulares de estas cadenas son:*

$$RZ_3(R_3) = \{(a,a,a) | a \in \overline{\mathbb{Q}} \text{ trascendente sobre } \mathbb{Q}\} \cup \{(a,-a,a) | a \in \overline{\mathbb{Q}} \text{ trascendente sobre } \mathbb{Q}\}.$$

Por lo tanto la variedad representada por R_3 y R_4 será la que tenga como componentes irreducibles las variedades irreducibles dadas por los puntos genéricos (a,a,a) y $(a,-a,a)$.

4.2. El problema

Una vez que hemos definido el concepto de Rep_n que será una unión de variedades irreducibles con un punto genérico en los ceros regulares de una cadena regular nos surge la siguiente pregunta. ¿Se podrá representar cualquier variedad en términos de una unión de estos representantes?.

Es decir, podremos encontrar un algoritmo que resuelva el siguiente problema:
Entrada: $F = \{f_1, \ldots, f_k\} \neq \emptyset$ subconjunto finito de $K[x_1, \ldots, x_n]$
Salida:$M = \{R_1, \ldots, R_l\}$ un conjunto (posiblemente vacío) de cadenas regulares de $K[x_1, \ldots, x_n]$ tales que:

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i).$$

Veremos en el último capítulo que algunos de los problemas más importantes en la teoría de ideales se puede resolver si conseguimos solucionar este problema. Para todos los problemas que vamos a resolver mediante el uso de cadenas regulares ya se han desarrollado algoritmos que los resuelven sin embargo la mayoría se basan en la utilización de bases de Gröbner.

Capítulo 5

Algoritmos para computar módulo una cadena regular

Antes de poder dar una solución algorítmica para el problema planteado en la sección anterior necesitamos desarrollar una serie de algoritmos que nos permita computar en cuerpos de extensión dados por cadenas regulares. Estos algoritmos se desarrollarán siguiendo la idea que se muestra en el siguiente ejemplo.

Ejemplo 5.0.1. *Queremos decidir para que ceros b del polinomio $x^6-10x^4+31x^2-30$ se verifica que $b^2-3=0$.*
Una estrategia posible es descomponer $x^6-10x^4+31x^2-30$ en factores irreducibles, en este caso x^2-2, x^2-3, x^2-5 y decidir la pregunta en cada uno de los cuerpos de extensión $\frac{\mathbb{Q}[x]}{x^2-2}$, $\frac{\mathbb{Q}[x]}{x^2-3}$, $\frac{\mathbb{Q}[x]}{x^2-5}$ por separado.

*Otra manera es sustituir el proceso de factorización por computaciones en términos del máximo común divisor: **gcd**$(x^6-10x^4+31x^2-30, x^2-3) = x^2-3$, entonces encontramos la descomposición $x^6-10x^4+31x^2-30 = (x^2-3)(x^4-7x^2+10)$ y x^4-7x^2+10 y x^2-3 son relativamente primos. Por tanto sabemos que $a^2-3=0$ si y solo si a es cero de x^2-3, $a^2-3\neq 0$ si y solo si a es cero de x^4-7x^2+10.*

5.1. Especificaciones de los algoritmos

En lo que se va a centrar esta sección es en desarrollar unos algoritmos que sigan la estrategia utilizada en el ejemplo anterior pero extendida a cadenas regulares y a polinomios en varias variables. Para ello debemos crear dos algoritmos llamados **common**$_n$ y **separate**$_n$ que satisfacen las siguientes especificaciones:

Algoritmo common$_n$:
Entrada: R, una cadena regular en $K[x_1,\ldots,x_n]$, y g un polinomio en $K[x_1,\ldots,x_n]$.
Salida: O, un conjunto de cadenas regulares en $K[x_1,\ldots,x_n]$ tales que:

$$\{a \in RZ_n(R) \mid g(a)=0\} = \bigcup_{R'\in O} RZ_n(R').$$

Algoritmo separate$_n$:
Entrada: R, una cadena regular en $K[x_1,\ldots,x_n]$, y g un polinomio en $K[x_1,\ldots,x_n]$.
Salida: O, un conjunto de cadenas regulares en $K[x_1,\ldots,x_n]$ tales que:

$$\{a \in RZ_n(R) \mid g(a) \neq 0\} = \bigcup_{R' \in O} RZ_n(R').$$

Como se puede ver estos algoritmos separan los ceros regulares de una cadena regular en dos conjuntos distintos, aquellos que son ceros también de un polinomio g y aquellos que no lo son, y los expresa en términos de un conjunto de cadenas regulares. Relacionando con el primer ejemplo vemos que $R = \{x^6 - 10x^4 + 31x^2 - 30\}$, $g = x^2 - 3$, $\mathbf{common}_1(R, g) = \{x^2 - 3\}$ y $\mathbf{separate}_1(R, g) = \{x^4 - 7x^2 + 10\}$.

Veamos ahora un ejemplo más complejo para ver como funcionan estos algoritmos para resolver el problema planteado antes:

Ejemplo 5.1.1. *Sea R la cadena regular $\{x_2^2 + x_1^2, x_3^2 - x_1x_3 - x_3 + x_1\}$ en $\mathbb{Q}[x_1, x_2, x_3]$. ¿Para cuales $(a_1, a_2, a_3) \in RZ_3(R)$ se verifica $a_1^2a_2^{-2} + a_3 = 0$? Supongamos que ya se han encontrado algoritmos que satisfacen las especificaciones.*
*Este problema se resuelve en términos de **common**$_3$ y **separate**$_3$. Primero veamos cuando existe a_2^{-1} para cada $(a_1, a_2, a_3) \in RZ_3(R)$, computando **common**$_3(R, x_2)$ obtenemos el vacío, por lo tanto $a_2 \neq 0$ y a_2^{-1} existe para cada $(a_1, a_2, a_3) \in RZ_3(R)$. Dado que ya sabemos que $a_2 \neq 0$ para cada $(a_1, a_2, a_3) \in RZ_3(R)$, podemos multiplicar por a_2^2 y ver cuando se verifica que $a_1 + a_3a_2^2 = 0$. Computando **common**$_3(R, x_1^2 + x_3x_2^2)$ obtenemos el conjunto $R' := \{x_2^2 + x_1^2, x_1^2 + x_3x_2^2\}$ y si hacemos **separate**$_3(R, x_1^2 + x_3x_2^2)$ obtenemos el conjunto $R'' := \{x_2^2 + x_1^2, x_2^2x_3 - x_2^2x_1 - x_2^2 - x_1^2\}$. Por tanto obtenemos:*

$$a_1^2a_2^{-2} + a_3 = 0 \ \textit{si y solo si} \ (a_1, a_2, a_3) \in RZ_3(R'),$$

$$a_1^2a_2^{-2} + a_3 \neq 0 \ \textit{si y solo si} \ (a_1, a_2, a_3) \in RZ_3(R'').$$

Volviendo al primer ejemplo se encontraron dos factores de los polinomios $x^6 - 10x^4 + 31x^2 - 30$ computando el máximo común divisor. Un algoritmo para calcular un máximo común divisor generalizado a n variables es una parte muy importante en los algoritmos **common**$_n$ y **separate**$_n$. Definimos para cada número natural n un algoritmo llamado **ggcd**$_n$ que es máximo común divisor generalizado que satisface la siguiente especificación:

Algoritmo ggcd$_n$:
Entrada: R, una cadena regular en $K[x_1,\ldots,x_{n-1}]$, y F un subconjunto finito no vacío de $K[x_1,\ldots,x_n]$.
Salida: O, donde $O = \{(R_1, g_1),\ldots,(R_l, g_l)\}$ y $R_1,\ldots,R_l$ son cadenas regulares en $K[x_1,\ldots,x_{n-1}]$ y $g_1,\ldots,g_l$ son polinomios en $K[x_1,\ldots,x_n]$ verificando lo siguiente:

1. $RZ_{n-1}(R) = RZ_{n-1}(R_1) \cup \ldots \cup RZ_{n-1}(R_l)$.
2. Para todo $i \in \{1,\ldots,l\}$ y cada $a = (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(R_i)$:
   a) Si $g_i \neq 0$ entonces $lc_n(g_i)(a) \neq 0$,

b) El polinomio $g_i(a, x_n)$ es el máximo común divisor de los polinomios en $\{f(a, x_n) \mid f \in F\}$ (salvo una constante multiplicativa).

3. Para todo $i \in \{1, \ldots, l\}$, g_i se anula en $Rep_n(R_i) \cap V_n(F)$.

5.2. Construcción de los algoritmos

Construiremos los algoritmos de forma inductiva:
Primero construimos el algoritmo $\mathbf{ggcd}_n$ para $n = 1$.
En este caso puesto que la entrada de $\mathbf{ggcd}_n$ es una cadena en $K[x_1, \ldots, x_{n-1}]$, entonces la entrada de $\mathbf{ggcd}_1$ la entrada será una cadena en K y por definición la única cadena en K es la cadena vacía. Y los el conjunto de polinomios F estará en $K[x_1]$ por tanto tiene sentido definir la salida de $\mathbf{ggcd}_1$ como:

Algoritmo $\mathbf{ggcd}_1$:
$\mathbf{ggcd}_1(\emptyset, F)$
$O := \{(\emptyset, \mathbf{gcd}(F))\}$

Donde la notación $\emptyset$ indica la cadena vacía y **gcd** denota al máximo común divisor usual entre polinomios en una variable. Probaremos que verifica las especificaciones en la siguiente sección donde se justificará la terminación y la corrección de los algoritmos desarrollados en esta sección.
Construiremos ahora los algoritmos $\mathbf{common}_n$ y $\mathbf{separate}_n$ en función de $\mathbf{ggcd}_n$:

Algoritmo $\mathbf{common}_n$:
$\mathbf{common}_n(R, g)$
$\{(S_1, g_1), \ldots, (S_r, g_r)\} := \mathbf{ggcd}_n(R \cap K[x_1, \ldots, x_{n-1}], R - K[x_1, \ldots, x_{n-1}] \cup \{g\})$
si $R - K[x_1, \ldots, x_{n-1}] = \emptyset$
entonces
$O := \{S_j \mid j \in \{1, \ldots, r\} \ y \ g_j = 0\}$.
si no
$O := \{S_j \cup \{g_j\} \mid j \in \{1, \ldots, r\} \ y \ g_j \notin K[x_1, \ldots, x_{n-1}]\}$.

Observamos que el conjunto O puede ser vacío si para el primer caso todos los $g_j \neq 0$, o si en el segundo caso para todo j, $g_j \in K[x_1, \ldots, x_{n-1}]$.

Algoritmo $\mathbf{separate}_n$:
$\mathbf{separate}_n(R, g)$
$\{(S_1, g_1), \ldots, (S_r, g_r)\} := \mathbf{ggcd}_n(R \cap K[x_1, \ldots, x_{n-1}], R - K[x_1, \ldots, x_{n-1}] \cup \{g\})$
si $R - K[x_1, \ldots, x_{n-1}] = \emptyset$
entonces
$O := \{S_j \mid j \in \{1, \ldots, r\} \ y \ g_j \neq 0\}$
si no
f:= el único elemento en $R - K[x_1, \ldots, x_{n-1}]$
$J := \{j \in \{1, \ldots, r\} \mid g_j \notin K[x_1, \ldots, x_{n-1}] \ y \ deg_n(g_j) < deg_n(f)\}$
$O := \{S_j \cup \{f\} \mid j \in \{1, \ldots, r\} \ y \ g_j \in K[x_1, \ldots, x_{n-1}]\} \cup$

$$\bigcup_{j\in J} separate_n(S_j \cup \{pquo(f, g_j)\}, g)$$

Observamos que el conjunto O puede ser vacío si en el primer caso todos los $g_j = 0$, o si en el segundo caso si para todo j, $g_j \notin K[x_1, \ldots, x_{n-1}]$ y $deg_n(g_j) \geqslant deg_n(f)$.

Podemos ahora definir $\mathbf{ggcd}_{n+1}$ en función de estos dos algoritmos:

Algoritmo $\mathbf{ggcd}_{n+1}$:
$\mathbf{ggcd}_{n+1}(R, F)$
si $|F - \{0\}| \geqslant 2$ **o** existe un polinomio g no nulo de F y un $a \in RZ_n(R)$ tal que $lc_{n+1}(g)(a) = 0$
entonces
f:= un elemento no nulo de F con grado minimal en x_{n+1}
$F' := F - \{f\}$
$M' := \mathbf{common}_n(R, lc_{n+1}(f))$
$M'' := \mathbf{separate}_n(R, lc_{n+1}(f))$
$f' := f - lc(f) \cdot x_{n+1}^{deg_{n+1}(f)}$
$F'' := \{prem_{n+1}(g, f) \mid g \in F'\}$
$O := \bigcup_{S'\in M'} \mathbf{ggcd}_{n+1}(S', F' \cup \{f'\}) \cup \bigcup_{S''\in M''} \mathbf{ggcd}_{n+1}(S'', F'' \cup \{f\})$
si no
si existe un elemento no nulo $f \in F$
entonces
$O := \{(R, f)\}$
si no
$O := \{(R, 0)\}$

Veamos ahora un ejemplo para ver como funcionan estos algoritmos:

Ejemplo 5.2.1. *Computaremos el máximo común divisor de $x_2^2 - x_1$ y $x_1x_2 + x_1^2$ módulo $x_1^4 - x_1^3$. Con lo que computaremos $\boldsymbol{ggcd}_2(\{x_1^4 - x_1^3\}, \{x_2^2 - x_1, x_1x_2 + x_1^2\})$.*
Como $|F - \{0\}| \geqslant 2$:
$f := x_1x_2 + x_1^2$
$F' := x_2^2 - x_1$
$M' := \boldsymbol{common}_1(\{x_1^4 - x_1^3\}, x_1)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1^4 - x_1^3, x_1\}) := \{(\emptyset, x_1)\}$
Como $R - K \neq \emptyset$ y $x_1 \notin K$
$O := \{\emptyset \cup \{x_1\}\} = \{x_1\}$
$M' := \{x_1\}$
$M'' := \boldsymbol{separate}_1(\{x_1^4 - x_1^3\}, x_1)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1^4 - x_1^3, x_1\}) := \{(\emptyset, x_1)\}$
Como $R - K \neq \emptyset$ y $deg_1(x_1) < deg_1(x_1^4 - x_1^3)$
$J := \{1\}$
$O := \boldsymbol{separate}_1(\emptyset \cup \{pquo(x_1^4 - x_1^3\}, x_1) = \boldsymbol{separate}_1(\{x_1^3 - x_1^2\}, x_1)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1^3 - x_1^2, x_1\}) := \{(\emptyset, x_1)\}$
Como $R - K \neq \emptyset$ y $deg_1(x_1) < deg_1(x_1^3 - x_1^2)$
$J := \{1\}$

$O := \boldsymbol{separate}_1(\{pquo(x_1^3 - x_1^2\}, x_1) = \boldsymbol{separate}_1(\{x_1^2 - x_1\}, x_1)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1^2 - x_1, x_1\}) := \{(\emptyset, x_1)\}$
Como $R - K \neq \emptyset$ *y* $deg_1(x_1) < deg_1(x_1^2 - x_1)$
$J := \{1\}$
$O := \boldsymbol{separate}_1(\{pquo(x_1^2 - x_1\}, x_1) = \boldsymbol{separate}_1(\{x_1 - 1\}, x_1)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1 - 1, x_1\}) := \{(\emptyset, 1)\}$
Como $R - K \neq \emptyset$ *y* $1 \in K$
$J := \emptyset$
$O := \{\emptyset \cup \{x_1 - 1\}\} = \{x_1 - 1\}$

$M'' := \{x_1 - 1\}$
$f' := x_1x_2 + x_1^2 - x_1x_2 = x_1^2$
$F'' := \{prem_2(x_2^2 - x_1, x_1x_2 + x_1^2)\} = \{x_1^4 - x_1^3\}$
$O := \boldsymbol{ggcd}_2(\{x_1\}, \{x_2^2 - x_1, x_1^2\}) \cup \boldsymbol{ggcd}_2(\{x_1 - 1\}, \{x_1^4 - x_1^3, x_1x_2 + x_1^2\})$

Calculemos primero $\boldsymbol{ggcd}_2(\{x_1\}, \{x_2^2 - x_1, x_1^2\})$*:*
Como $|F - \{0\}| \geqslant 2$*:*
$f := x_1^2$
$F' := x_2^2 - x_1$
$M' := \boldsymbol{common}_1(\{x_1\}, x_1^2)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1, x_1^2\}) := \{(\emptyset, x_1)\}$
Como $R - K \neq \emptyset$ *y* $x_1 \notin K$
$O := \{\emptyset \cup \{x_1\}\} = \{x_1\}$
$M' := \{x_1\}$
$M'' := \boldsymbol{separate}_1(\{x_1\}, x_1^2)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1, x_1^2\}) := \{(\emptyset, x_1)\}$
Como $R - K \neq \emptyset$ *y* $deg_1(x_1) \not< deg_1(x_1)$
Además $x_1 \notin K$ *por tanto:*
$O := \emptyset$ *(O es el conjunto vacío)*
$M'' := \emptyset$ *(M'' es el conjunto vacío)*
$f' := x_1^2 - x_1^2 = 0$
$F'' := \{prem_2(x_2^2 - x_1, x_1^2)\} = \{0\}$
$O := \boldsymbol{ggcd}_2(\{x_1\}, \{x_2^2 - x_1\} \cup \{0\}) \cup \emptyset = \boldsymbol{ggcd}_2(\{x_1\}, \{x_2^2 + x_1, 0\})$
Como $|F - \{0\}| \not\geqslant 2$ *y* $lc_2(x_2^2 - x_1) = 1 \neq 0$ *para todo* $a \in RZ_1(\{x_1\})$
Como existe $f \neq 0$ *en* F *entonces:*
$O := \{(\{x_1\}, x_2^2 - x_1)\}$
Por tanto $\boldsymbol{ggcd}_2(\{x_1\}, \{x_2^2 - x_1, x_1^2\}) = \{(\{x_1\}, x_2^2 - x_1)\}$.

Calculemos ahora $\boldsymbol{ggcd}_2(\{x_1 - 1\}, \{x_1^4 - x_1^3, x_1x_2 + x_1^2\})$*:*
Como $|F - \{0\}| \geqslant 2$*:*
$f := x_1^4 - x_1^3$
$F' := x_1x_2 + x_1^2$
$M' := \boldsymbol{common}_1(\{x_1 - 1\}, x_1^4 - x_1^3)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1^4 - x_1^3, x_1 - 1\}) := \{(\emptyset, x_1 - 1)\}$
Como $R - K \neq \emptyset$ *y* $x_1 - 1 \notin K$
$O := \{\emptyset \cup \{x_1 - 1\}\} = \{x_1 - 1\}$
$M' := \{x_1 - 1\}$

$M'' := \textbf{\textit{separate}}_1(\{x_1 - 1\}, x_1^4 - x_1^3)$
$\quad \textbf{\textit{ggcd}}_1(\emptyset, \{x_1^4 - x_1^3, x_1 - 1\}) := \{(\emptyset, x_1 - 1)\}$
$\quad$ *Como* $R - K \neq \emptyset$, $x_1 - 1 \notin K$ *y* $deg_1(x_1 - 1) \not< deg_1(x_1 - 1)$
$\quad O := \emptyset$ *(O es el conjunto vacío)*
$M'' := \emptyset$ *(M'' es el conjunto vacío)*
$f' := x_1^4 - x_1^3 - (x_1^4 - x_1^3) = 0$
$F'' := \{prem_2(x_1x_2 + x_1^2, x_1^4 - x_1^3)\} = \{0\}$
$O := \textbf{\textit{ggcd}}_2(\{x_1 - 1\}, \{x_1x_2 + x_1^2, 0\}\}) \cup \emptyset = \textbf{\textit{ggcd}}_2(\{x_1 - 1\}, \{0, x_1x_2 + x_1^2\})$
$\quad$ *Como* $|F - \{0\}| \not\geq 2$ *y tenemos que* $RZ_1(\{x_1 - 1\}) = 1$ *y por tanto*
$\quad lc_2(x_1x_2 + x_1^2)(1) = 1 \neq 0$
$\quad$ *Como existe* $f \neq 0$ *en* F *entonces:*
$\quad O := \{(\{x_1 - 1\}, x_1x_2 + x_1^2)\}$

Por lo tanto $\textbf{\textit{ggcd}}_2(\{x_1^4 - x_1^3\}, \{x_2^2 - x_1, x_1x_2 + x_1^2\}) = \{(\{x_1\}, x_2^2 - x_1), (\{x_1 - 1\}, x_1x_2 + x_1^2)\}$.

5.3. Justificación de la terminación y corrección de los algoritmos

Para demostrar la terminación de los tres algoritmos supondremos que $\textbf{ggcd}_n$ termina y satisface las especificaciones, y procederemos de manera inductiva. Por tanto primero tenemos que demostrar el caso inicial, es decir que $\textbf{ggcd}_1$ termina, que su salida es una cadena regular y que verifica las especificaciones. Dado que simplemente el algoritmo es:

$\textbf{ggcd}_1(\emptyset, F)$
$O := \{(\emptyset, \textbf{gcd}(F))\}$

claramente el algoritmo termina y la salida está compuesta por un par de cadena regular (la cadena vacía) y polinomio. Veamos que verifica las especificaciones:

Verifica la especificación 1 pues claramente $RZ_0(\emptyset) = RZ_0(\emptyset)$.
Dado que $RZ_0(\emptyset)$ es la lista vacía por definición, entonces si $g_j \neq 0$ entonces $lc_1(g_j)(a) \neq 0$ para todo $a \in RZ_0(\emptyset)$. Se verifica la especificación 2a).
La especificación 2b) se traduce en este caso a que $g_1(x_1)$ es el máximo común divisor de $\{f(x_1) \mid f \in F\}$, es decir que $g_1 = \textbf{gcd}(F)$, y por lo tanto se verifica.
La especificación 3 se verifica pues ya vimos que $AIV_n(\emptyset) = \{\overline{K}^n\}$, en nuestro caso
$AIV_1(\emptyset) = \{\overline{K}\}$, con lo que por definición de Rep_n, $Rep_1(\emptyset) = \overline{K}$, por tanto hay que ver que $\textbf{gcd}(F)$ se anula en $V_n(F)$. Por definición $V_n(F)$ son los puntos donde se anulan todos los polinomios de F y por lo tanto son los puntos que son raíces de todos los polinomios. Por tanto por las propiedades de **gcd** estos puntos tienen que ser raíces de $\textbf{gcd}(F)$ y por tanto $\textbf{gcd}(F)$ se anula en $V_n(F)$.

5.3.1 Algoritmo $\textbf{common}_n$

Sean R una cadena regular en $K[x_1, \ldots, x_n]$ y $g \in K[x_1, \ldots, x_n]$ un polinomio, los cuales son los argumentos de entrada.
Vemos que el algoritmo termina si termina el algoritmo $\textbf{ggcd}_n$. Hemos supuesto que este algoritmo termina por tanto $\textbf{common}_n$ termina.

Veamos que el conjunto O definido en el algoritmo es un conjunto de cadenas regulares. Debido a las especificaciones de $\mathbf{ggcd}_n$ los elementos S_j son cadenas regulares en $K[x_1,\ldots,x_{n-1}]$ y los elementos g_j son polinomios en $K[x_1,\ldots,x_n]$. Por tanto en caso de que $R-K[x_1,\ldots,x_{n-1}]=\emptyset$ claramente O es un conjunto de cadenas regulares. En caso contrario, tendremos O compuesto por $S_j\cup\{g_j\}$, veamos que es una cadena regular. Como $g_j\notin K[x_1,\ldots,x_{n-1}]$ tenemos que $(S_j\cup\{g_j\})\cap K[x_1,\ldots,x_{n-1}]=S_j$ y por tanto es cadena regular.
$(S_j\cup\{g_j\})-K[x_1,\ldots,x_n]$ tiene solo un elemento g_j. Hay que comprobar que $lc_n(g_j)(a)\neq 0$ con $a\in RZ_{n-1}(S_j)$. Como $g_j\notin K[x_1,\ldots,x_{n-1}]$, entonces en particular $g_j\neq 0$. Por la especificación 2a) de $\mathbf{ggcd}_n$, $lc_n(g_j)(a)\neq 0$ para todo $a\in RZ_{n-1}(S_j)$.
Podría darse el caso en que el conjunto O fuera vacío, pero no hay problema puesto que la salida puede ser vacía.

Veamos ahora que el algoritmo verifica las especificaciones. Denotamos por
$R_{n-1}=R\cap K[x_1,\ldots,x_{n-1}]$. Distinguiremos los dos casos que hay en el algoritmo.

Caso 1: $R-K[x_1,\ldots,x_{n-1}]=\emptyset$
En este caso $R_{n-1}=R$, por construcción del algoritmo:
$\{(S_1,g_1),\ldots,(S_l,g_l)\}:=\mathbf{ggcd}_n(R,\{g\})$, que verifica:

1. $RZ_{n-1}(R)=RZ_{n-1}(S_1)\cup\ldots\cup RZ_{n-1}(S_l)$.
2. Para todo $j\in\{1,\ldots,l\}$ y cada $a=(a_1,\ldots,a_{n-1})\in RZ_{n-1}(S_j)$:
   a) Si $g_j\neq 0$ entonces $lc_n(g_j)(a_1,\ldots,a_{n-1})\neq 0$,
   b) El polinomio $g_j(a_1,\ldots,a_{n-1},x_n)=g(a_1,\ldots,a_{n-1},x_n)$ (salvo una constante multiplicativa).
3. Para todo $j\in\{1,\ldots,l\}$, g_j se anula en $Rep_n(S_j)\cap V_n(\{g\})$.

Además al entrar en la primera parte del condicional

$$O:=\{S_j\mid j\in\{1,\ldots,l\},\ g_j=0\}. \tag{5.1}$$

Sea $a=(a_1,\ldots,a_n)\in\overline{K}^n$. Se probará que

$$\bigcup_{R'\in O}RZ_n(R')=\{a\in RZ_n(R)\mid g(a)=0\},$$

mediante los siguientes pasos:

1. $a\in\bigcup_{R'\in O}RZ_n(R')$.
2. $\exists\ j\in\{1,\ldots,r\}$ con $g_j=0$ y $a\in RZ_n(S_j)$.
3. $\exists\ j\in\{1,\ldots,r\}$ con $g_j(a_1,\ldots,a_{n-1},x_n)=0$, $(a_1,\ldots,a_{n-1})\in RZ_{n-1}(S_j)$, y a_n trascendente sobre $K(a_1,\ldots,a_{n-1})$.
4. $\exists\ j\in\{1,\ldots,r\}$, $(a_1,\ldots,a_{n-1})\in RZ_{n-1}(S_j)$, y a_n trascendente sobre $K(a_1,\ldots,a_{n-1})$, y $g(a_1,\ldots,a_{n-1},x_n)=0$

5. $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R \cap K[x_1, \ldots, x_{n-1}])$, a_n trascendente sobre $K(a_1, \ldots, a_{n-1})$, y $g(a) = 0$.

6. $a \in RZ_n(R)$ y $g(a) = 0$.

$1 \Leftrightarrow 2$: Es evidente de (5.1).

$2 \Rightarrow 3$: Por especificación de $\mathbf{ggcd}_n$ tenemos que S_j son cadenas en $K[x_1, \ldots, x_{n-1}]$, por tanto por definición de cero regular $a = (a_1, \ldots, a_n) \in RZ_n(S_j)$ si y solo si
$(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$, a_n trascendente sobre $K(a_1, \ldots, a_{n-1})$. Además tenemos que si $g_j = 0$ entonces $g_j(a_1, \ldots, a_{n-1}, x_n) = 0$.
$3 \Rightarrow 2$: Falta probar que si $g_j(a_1, \ldots, a_{n-1}, x_n) = 0$ entonces $g_j = 0$. Si $g_j(a_1, \ldots, a_{n-1}, x_n) = 0$ entonces $lc_n(g_j)(a_1, \ldots, a_{n-1}) = 0$ con $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$ y por lo tanto habría entrado en la primera parte del condicional en $\mathbf{ggcd}_n$, a no ser que $g_j = 0$ que es la única posibilidad.

$3 \Leftrightarrow 4$: Por 2b) escrito antes, tenemos que $g_j(a_1, \ldots, a_{n-1}, x_n) = g(a_1, \ldots, a_n, x_n)$ y de aquí $g_j(a_1, \ldots, a_{n-1}, x_n) = 0$ si y solo si $g(a_1, \ldots, a_{n-1}, x_n) = 0$.

$4 \Rightarrow 5$: Tenemos que por la especificación 1 escrita antes, $\exists\ j \in \{1, \ldots, r\}$ tal que
$(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$ si y solo si $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1})$. Ahora si
$g(a_1, \ldots, a_{n-1}, x_n) = 0$ entonces $g(a) = 0$.
$5 \Rightarrow 4$: Falta probar que si $g(a) = 0$ entonces $g(a_1, \ldots, a_{n-1}, x_n) = 0$. Si $g(a) = 0$ dado que a_n es trascendente sobre $K(a_1, \ldots, a_{n-1})$ entonces se ha de tener que $g(a_1, \ldots, a_{n-1}, x_n) = 0$, pues si no a_n no sería trascendente sobre $K(a_1, \ldots, a_{n-1})$.

$5 \Leftrightarrow 6$: Aplicando la definición de cero regular a la cadena R obtenemos lo que queremos.

Notemos que hemos supuesto que existe $a \in \bigcup_{R' \in O} RZ_n(R')$ para demostrar una implicación y que existe $a \in RZ_n(R)$ tal que $g(a) = 0$. Sin embargo podría darse el caso en que fueran vacíos, pero esto no presenta problema pues al ser una equivalencia también queda demostrado por contrarrecíproco, que si un conjunto es vacío también lo será el otro.
Con esto finaliza la demostración de la primera parte del algoritmo.

Caso 2: $R - K[x_1, \ldots, x_{n-1}] \neq \emptyset$
Denotaremos el elemento de $R - K[x_1, \ldots, x_n]$ por f.
Por construcción del algoritmo:
$\{(S_1, g_1), \ldots, (S_l, g_l)\} := \mathbf{ggcd}_n(R_{n-1}, \{f, g\})$, que verifica:

1. $RZ_{n-1}(R_{n-1}) = RZ_{n-1}(S_1) \cup \ldots \cup RZ_{n-1}(S_l)$.

2. Para todo $j \in \{1, \ldots, l\}$ y cada $a = (a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$:

   a) Si $g_j \neq 0$ entonces $lc_n(g_j)(a) \neq 0$,

   b) El polinomio $g_j(a_1, \ldots, a_{n-1}, x_n) = \mathbf{gcd}(f(a_1, \ldots, a_{n-1}, x_n), g(a_1, \ldots, a_{n-1}, x_n))$ (salvo una constante multiplicativa).

3. Para todo $j \in \{1, \ldots, l\}$, g_j se anula en $Rep_n(S_j) \cap V_n(\{f, g\})$.

Además al entrar en la segunda parte del condicional

$$O := \{S_j \cup \{g_j\} \mid j \in \{1, \ldots, l\},\ g_j \notin K[x_1, \ldots, x_{n-1}]\}. \tag{5.2}$$

Sea $a = (a_1, \ldots, a_n) \in \overline{K}^n$. Se probará que

$$\bigcup_{R' \in O} RZ_n(R') = \{a \in RZ_n(R) \mid g(a) = 0\},$$

mediante los siguientes pasos:

1. $a \in \bigcup_{R' \in O} RZ_n(R')$.
2. $\exists\ j \in \{1, \ldots, r\}$ con $g_j \notin K[x_1, \ldots, x_{n-1}]$ y $a \in RZ_n(S_j \cup \{g_j\})$.
3. $\exists\ j \in \{1, \ldots, r\}$ con $g_j \notin K[x_1, \ldots, x_{n-1}]$, $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$, y $g_j(a) = 0$.
4. $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1})$ y $f(a) = g(a) = 0$.
5. $a \in RZ_n(R)$ y $g(a) = 0$.

$1 \Leftrightarrow 2$: Es evidente por (5.2).

$2 \Leftrightarrow 3$: Por la definición de cero regular de una cadena tenemos, dado que S_j es una cadena en $K[x_1, \ldots, x_{n-1}]$, los ceros regulares serán de la forma $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$ y $g_j(a) = 0$. Y tenemos la equivalencia.

$3 \Rightarrow 4$: Por la especificación 1 escrita antes, $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1})$ si y solo si existe $j \in \{1, \ldots, r\}$ con $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$. Veamos que si $g_j \notin K[x_1, \ldots, x_{n-1}]$ y $g_j(a) \neq 0$ entonces $f(a) = g(a) = 0$. Tenemos que si $g_j(a) = 0$ entonces a_n es raíz de $g_j(a_1, \ldots, a_{n-1}, x_n)$. Al ser máximo común divisor de $f(a_1, \ldots, a_{n-1}, x_n)$ y de $g(a_1, \ldots, a_{n-1}, x_n)$, por la especificación 2b) escita antes, entonces a_n será raíz de ambos y por tanto $f(a) = g(a) = 0$.
$4 \Rightarrow 3$: Supongamos que $f(a) = g(a) = 0$, veamos que $g_j \notin K[x_1, \ldots, x_{n-1}]$ y $g_j(a) = 0$. Dado que a_n es raíz de $f(a_1, \ldots, a_{n-1}, x_n)$ y de $g(a_1, \ldots, a_{n-1}, x_n)$ también lo será de máximo común divisor y por tanto $g_j(a) = 0$. Supongamos ahora que $g_j \in K[x_1, \ldots, x_{n-1}]$ entonces $lc_n(g_j) = g_j$ y por tanto $lc_n(g_j)(a_1, \ldots, a_{n-1}) = 0$ lo cual por la especificación 2a) no puede pasar si $g_j \neq 0$. Sin embargo si $g_j = 0$ entonces $f(a_1, \ldots, a_{n-1}, x_n) = 0$, por ser el máximo común divisor igual a cero. Entonces, o bien $f \in K[x_1, \ldots, x_{n-1}]$ lo cual es una contradicción dado que estamos en el caso 2, o bien $lc_n(f)(a_1, \ldots, a_{n-1}) = 0$ lo cual entra en contradicción con la definición de la cadena regular R. Por tanto se ha de tener que $g_j \notin K[x_1, \ldots, x_{n-1}]$.

$4 \Leftrightarrow 5$: Por definición de cadena regular es claro que

$$(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R \cap K[x_1, \ldots, x_{n-1}])\ \ y\ \ f(a) = 0\ \ si\ \ y\ \ solo\ \ si\ \ a \in RZ_n(R).$$

Notemos que hemos supuesto que existe $a \in \bigcup_{R' \in O} RZ_n(R')$ para demostrar una implicación y que existe $a \in RZ_n(R)$ tal que $g(a) = 0$. Sin embargo podría darse el caso en que fueran

vacíos, pero esto no presenta problema pues al ser una equivalencia también queda demostrado por contrarrecíproco, que si un conjunto es vacío también lo será el otro. Con lo que termina la demostración de la corrección del algoritmo.

5.3.2 Algoritmo separate$_n$

Antes de comenzar la demostración de la terminación y la corrección del algoritmo demostraremos un lema que emplearemos varias veces en la demostración de la corrección algoritmo.

Lema 7. *Si g es un polinomio en $K[x_1,\ldots,x_n]$ con $lc_n(g)(a_1,\ldots,a_{n-1}) \neq 0$. Si f es otro polinomio en $K[x_1,\ldots,x_n]$ tal que $g(a_1,\ldots,a_{n-1},x_n)$ divide a $f(a_1,\ldots,a_{n-1},x_n)$ entonces $prem(f,g)(a_1,\ldots,a_{n-1},x_n) = 0$ y por tanto $pquo(f,g)(a_1,\ldots,a_{n-1},x_n)$ divide a $f(a_1,\ldots,a_{n-1},x_n)$*

Demostración: Por definición de pseudodivisión tenemos:

$$(lc_n(g))^d \cdot f = pquo_n(f,g)\cdot g + prem_n(f,g),$$

con $deg_n(prem_n(f,g)) \leq deg_n(g)$ y $d = max(deg_n(f) - deg_n(g) + 1, 0)$. Denotaremos por q al pseudocociente y por r al pseudoresto, entonces tenemos:
$(lc_n(g))^d(a_1,\ldots,a_{n-1})\cdot g(a_1,\ldots,a_{n-1},x_n) = q(a_1,\ldots,a_{n-1},x_n)\cdot g(a_1,\ldots,a_{n-1},x_n)$
$+r(a_1,\ldots,a_{n-1},x_n)$,
dado que tenemos que $lc(g)(a_1,\ldots,a_{n-1}) \neq 0$ y es además una constante en $K(a_1,\ldots,a_{n-1})$ y los demás son polinomios en una variable en el cuerpo de extensión $K(a_1,\ldots,a_{n-1})$ lo podemos reescribir como:

$$c\cdot F(x) = Q(x)\cdot G(x) + R(x),$$

con $deg(R) < deg(G)$. Como $F(x)$ es divisible por $G(x)$ tenemos que $F(x) = G(x)\cdot H(x)$. Por tanto:

$$c\cdot G(x)\cdot H(x) = G(x)Q(x) + R(x),$$

con lo que tenemos que:

$$G(x)\cdot(c\cdot H(x) - Q(x)) = R(x),$$

pero esto nos dice que si $c\cdot H(x) - Q(x) \neq 0$ entonces $deg_n(R(x)) \geq deg_n(G(x))$ lo cual no puede ocurrir. Por lo tanto $c\cdot H(x) - Q(x) = 0$ y en consecuencia $R(x) = 0$. Esto demuestra que $r(a_1,\ldots,a_{n-1},x_n) = 0$ y en consecuencia $pquo(f,g)(a_1,\ldots,a_{n-1},x_n)$ divide a $f(a_1,\ldots,a_{n-1},x_n)$. □

Sean R una cadena regular en $K[x_1,\ldots,x_n]$ y $g \in K[x_1,\ldots,x_n]$ un polinomio, los cuales solo los argumentos de entrada. Denotaremos por $R_{n-1} = R \cap K[x_1,\ldots,x_{n-1}]$. Distinguiremos los dos casos ya pues la terminación no es tan clara como en el caso anterior.
Caso 1: $R - K[x_1,\ldots,x_{n-1}] = \emptyset$.
En este caso $R_{n-1} = R$, por construcción del algoritmo:
$\{(S_1,g_1),\ldots,(S_l,g_l)\} := \mathbf{ggcd}_n(R,\{g\})$, que verifica:

1. $RZ_{n-1}(R) = RZ_{n-1}(S_1)\cup\ldots\cup RZ_{n-1}(S_l)$.
2. Para todo $j\in\{1,\ldots,l\}$ y cada $a = (a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j)$:
   a) Si $g_j \neq 0$ entonces $lc_n(g_j)(a_1,\ldots,a_{n-1}) \neq 0$,

b) El polinomio $g_j(a_1,\ldots,a_{n-1},x_n) = g(a_1,\ldots,a_{n-1},x_n)$ (salvo una constante multiplicativa).

3. Para todo $j \in \{1,\ldots,l\}$, g_j se anula en $Rep_n(S_j) \cap V_n(\{g\})$.

Además al entrar en la primera parte del condicional

$$O := \{S_j \mid j \in \{1,\ldots,l\},\ g_j \neq 0\}. \tag{5.3}$$

En este caso la terminación se deduce de la terminación de $\mathbf{ggcd}_n$.
Por la especificación del algoritmo $\mathbf{ggcd}_n$ los elementos de salida S_j son cadenas regulares y por lo tanto lo será cada uno de los elementos de O por (5.3).

Sea $a = (a_1,\ldots,a_n) \in \overline{K}^n$. Se probará que

$$\bigcup_{R' \in O} RZ_n(R') = \{a \in RZ_n(R) \mid g(a) \neq 0\},$$

mediante los siguientes pasos:

1. $a \in \bigcup_{R' \in O} RZ_n(R')$.
2. $\exists\ j \in \{1,\ldots,r\}$ con $g_j \neq 0$ y $a \in RZ_n(S_j)$.
3. $\exists\ j \in \{1,\ldots,r\}$ con $g_j \neq 0$, $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j)$, y a_n trascendente sobre $K(a_1,\ldots,a_{n-1})$.
4. $\exists\ j \in \{1,\ldots,r\}$ con $g_j(a_1,\ldots,a_{n-1},x_n) \neq 0$, $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j)$, y a_n trascendente sobre $K(a_1,\ldots,a_{n-1})$.
5. $\exists\ j \in \{1,\ldots,r\}$ con $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j)$, a_n trascendente sobre $K(a_1,\ldots,a_{n-1})$, y $g(a_1,\ldots,a_{n-1},x_n) \neq 0$.
6. $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(R_{n-1})$, a_n trascendente sobre $K(a_1,\ldots,a_{n-1})$, y $g(a) \neq 0$.
7. $a \in RZ_n(R)$ y $g(a) \neq 0$.

$1 \Leftrightarrow 2$: Es evidente de (5.3).

$2 \Leftrightarrow 3$: Puesto que por especificación de $\mathbf{ggcd}_n$, S_j es una cadena en $K[x_1,\ldots,x_{n-1}]$, tenemos que $a \in RZ_n(S_j)$ si y solo si $(a_1,\ldots,a_{n-1}) \in RZ(S_j)$ y a_n es trascendente sobre $K(a_1,\ldots,a_{n-1})$.

$3 \Leftrightarrow 4$: Si $g_j \neq 0$ por la especificación 2a), tenemos que $lc_n(g_j)(a_1,\ldots,a_{n-1}) \neq 0$ para todo $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j)$, lo que implica que $g_j(a_1,\ldots,a_{n-1},x_n) \neq 0$ para todo $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j)$. La otra implicación es evidente pues si $g_j(a_1,\ldots,a_{n-1},x_n) \neq 0$, entonces $g_j \neq 0$.

$4 \Leftrightarrow 5$: Por la especificación de 2b) escrita antes, sabemos que

$$g_j(a_1,\ldots,a_{n-1},x_n) = g(a_1,\ldots,a_{n-1},x_n).$$

Por tanto tenemos que si uno es distinto de 0 el otro también lo es.

$5 \Leftrightarrow 6$: Por la especificación 1 escrita antes tenemos que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1})$ si y solo si existe $j \in \{1, \ldots, r\}$ tal que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$. Si $g(a) \neq 0$ entonces es claro que $g(a_1, \ldots, a_{n-1}, x_n) \neq 0$. Supongamos ahora que $g(a_1, \ldots, a_{n-1}, x_n) \neq 0$, entonces ha de ser $g(a) \neq 0$ pues si no a_n no sería trascendente sobre $K(a_1, \ldots, a_{n-1})$.

$6 \Leftrightarrow 7$: Por definición de cero regular es claro que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1})$ y a_n trascendente sobre $K(a_1, \ldots, a_{n-1})$ si y solo si $a \in RZ_n(R)$.

Notemos que hemos supuesto que existe $a \in \bigcup_{R' \in O} RZ_n(R')$ para demostrar una implicación y que existe $a \in RZ_n(R)$ tal que $g(a) = 0$. Sin embargo podría darse el caso en que fueran vacíos, pero esto no presenta problema pues al ser una equivalencia también queda demostrado por contrarrecíproco, que si un conjunto es vacío también lo será el otro.
Con esto termina la demostración para el primer caso.

Caso 2: $R - K[x_1, \ldots, x_{n-1}] \neq \emptyset$.
Denotaremos es este caso al único elemento de $R - K[x_1, \ldots, x_{n-1}]$ por f.
Por construcción del algoritmo:
$\{(S_1, g_1), \ldots, (S_l, g_l)\} := \mathbf{ggcd}_n(R_{n-1}, \{f, g\})$, que verifica:

1. $RZ_{n-1}(R_{n-1}) = RZ_{n-1}(S_1) \cup \ldots \cup RZ_{n-1}(S_l)$.
2. Para todo $j \in \{1, \ldots, l\}$ y cada $a = (a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$:
   a) Si $g_j \neq 0$ entonces $lc_n(g_j)(a) \neq 0$,
   b) El polinomio $g_j(a_1, \ldots, a_{n-1}, x_n) = \mathbf{gcd}(f(a_1, \ldots, a_{n-1}, x_n), g(a_1, \ldots, a_{n-1}, x_n))$ (salvo una constante multiplicativa).
3. Para todo $j \in \{1, \ldots, l\}$, g_j se anula en $Rep_n(S_j) \cap V_n(\{f, g\})$.

Además al entrar en la segunda parte del condicional:

$$J := \{j \mid g_j \notin K[x_1, \ldots, x_{n-1}],\ deg_n(g_j) < deg_n(f)\} \tag{5.4}$$

$$O := \{S_j \cup \{f\} \mid j \in \{1, \ldots, r\}\ y\ g_j \in K[x_1, \ldots, x_{n-1}]\} \cup \bigcup_{j \in J} \mathbf{separate}_n(S_j \cup \{pquo(f, g_j)\}, g) \tag{5.5}$$

Para demostrar la terminación y la corrección trabajaremos mediante una inducción sobre el $deg_n(f)$.
Caso base: Sea $n = 1$.
Lo primero es ver la terminación. Veamos que $J = \emptyset$. Tenemos que g_j tiene algún término en la variable x_n, pues $g_j \notin K[x_1, \ldots, x_{n-1}]$ por (5.4), por tanto $0 < deg_n(g_j)$. Además $deg_n(f) = 1$ por hipótesis y entonces no puede ser $0 < deg_n(g_j) < deg_n(f) = 1$. Con lo que $J = \emptyset$ y tenemos que entonces $\mathbf{separate}_n$ termina por la finalización de $\mathbf{ggcd}_n$
Veamos que todo elemento de O es cadena regular. Observamos que los elemento de O son de

la forma $S_j \cup \{f\}$, veamos que son cadenas regulares. Obtenemos intersecando el conjunto con $K[x_1, \ldots, x_{n-1}]$ el conjunto S_j que sabemos que es cadena regular por especificación de $\mathbf{ggcd}_n$. Además claramente solo existe un elemento en $S_j \cup \{f\} - K[x_1, \ldots, x_{n-1}]$. Solo falta comprobar que $lc_n(f)(a_1, \ldots, a_{n-1}) \neq 0$ para todo $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$. Sabemos que por ser R cadena regular, $lc_n(f)(a_1, \ldots, a_{n-1}) \neq 0$ para todo $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R \cap K[x_1, \ldots, x_{n-1}])$. Sabemos que

$$RZ_{n-1}(R_{n-1}) = \bigcup_{j=1}^{r} RZ_{n-1}(S_j),$$

por especificación de $\mathbf{ggcd}_n$, por tanto tiene que ser $lc_n(f)(a_1, \ldots, a_{n-1}) \neq 0$ para todo $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$. Con lo que O está formado por cadenas regulares.
Veamos ahora la corrección del algoritmo. Tendremos en cuenta que $J = \emptyset$ y que $deg_n(f) = 1$. Sea $a = (a_1, \ldots, a_n) \in \overline{K}^n$. Se probará que

$$\bigcup_{R' \in O} RZ_n(R') = \{a \in RZ_n(R) \mid g(a) \neq 0\},$$

mediante los siguientes pasos:

1. $a \in \bigcup_{R' \in O} RZ_n(R')$
2. $\exists\ j \in \{1, \ldots, r\}$ con $g_j \in K[x_1, \ldots, x_{n-1}]$ y $a \in RZ_n(S_j \cup \{f\})$
3. $\exists\ j \in \{1, \ldots, r\}$ con $g_j \in K[x_1, \ldots, x_{n-1}]$, $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$, $f(a) = 0$, y $f(a_1, \ldots, a_{n-1}, x_n) \neq 0$
4. $\exists\ j \in \{1, \ldots, r\}$ con $g_j(a_1, \ldots, a_{n-1}, x_n) \in \overline{K} - \{0\}$, $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$, $f(a) = 0$, y $f(a_1, \ldots, a_{n-1}, x_n) \neq 0$
5. $\exists\ j \in \{1, \ldots, r\}$ con $g_j(a) \neq 0$, $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$, $f(a) = 0$, y $f(a_1, \ldots, a_{n-1}, x_n) \neq 0$
6. $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R \cap K[x_1, \ldots, x_{n-1}])$, $f(a) = 0$, $f(a_1, \ldots, a_{n-1}, x_n) \neq 0$, y $g(a) \neq 0$
7. $a \in RZ_n(R)$ y $g(a) \neq 0$.

$1 \Leftrightarrow 2$: Es evidente de (5.5) y de $J = \emptyset$

$2 \Rightarrow 3$: Hemos probado anteriormente que $S_j \cup \{f\}$ es cadena regular. Y sabemos por la definición de cadena regular que $lc_n(f)(a_1, \ldots, a_{n-1}) \neq 0$ por tanto también $f(a_1, \ldots, a_{n-1}, x_n) \neq 0$. Por definición de cero regular tenemos también $f(a) = 0$.
$3 \Rightarrow 2$: Es evidente de la definición de cero regular de una cadena regular.

$3 \Rightarrow 4$: Por la especificación 2b) escrita antes, dado que $f(a_1, \ldots, a_{n-1}, x_n) \neq 0$ al ser uno de los dos polinomios distinto de 0 también lo será el máximo común divisor, es decir $g_j(a_1, \ldots, a_{n-1}, x_n) \neq 0$. Además puesto que g_j no tiene variable en x_n, $g_j(a_1, \ldots, a_{n-1}, x_n) \in \overline{K}$.
$4 \Rightarrow 3$: Si $g_j(a_1, \ldots, a_{n-1}, x_n) \in \overline{K} - \{0\}$ entonces $g_j \neq 0$ y entonces por la especificación 2b) escrita antes, $lc_n(g_j)(a_1, \ldots, a_{n-1}) \neq 0$. Por tanto g_j solo puede ser un polinomio en $K[x_1, \ldots, x_{n-1}]$,

pues para que $g_j(a_1,\ldots,a_{n-1},x_n) \in \overline{K}$ se tendrían que anular todos los coeficientes de la variable x_n, pero esto no puede pasar pues $lc_n(g_j)(a_1,\ldots,a_{n-1}) \neq 0$. Y por tanto $g_j \in K[x_1,\ldots,x_{n-1}]$

$4 \Rightarrow 5$: Si $g_j(a_1,\ldots,a_{n-1},x_n) \in \overline{K} - \{0\}$ entonces no hay ningún término en la variable x_n y por tanto aunque sustituyamos x_n por cualquier valor a_n no va a cambiar el valor de $g_j(a_1,\ldots,a_{n-1},x_n)$, dado que este es distinto de 0, también lo será $g_j(a)$.
$5 \Rightarrow 4$: Es claro que si $g_j(a) \neq 0$ entonces $g_j(a_1,\ldots,a_{n-1},x_n) \neq 0$. Veamos que pertenece a $\overline{K}$, utilizando la especificación 2b) escrita antes, dado que $deg_n(f) = 1$, entonces $g_j(a_1,\ldots,a_{n-1},x_n)$ es de grado como mucho 1 en x_n por ser divisor de $f(a_1,\ldots,a_{n-1},x_n)$. Si $g_j(a_1,\ldots,a_{n-1},x_n)$ fuera de grado 1 entonces para dividir a f tiene que ser $g_j(a_1,\ldots,a_{n-1},x_n) = C\cdot f(a_1,\ldots,a_{n-1},x_n)$, con $C \in K(a_1,\ldots,a_{n-1})$. Puesto que $f(a) = 0$ entonces por esto $g_j(a) = 0$ y llegamos a contradicción. Por tanto g_j tiene que ser de grado 0 en x_n, y por tanto $g_j(a_1,\ldots,a_{n-1},x_n) \in \overline{K}$.

$5 \Rightarrow 6$: Por la especificación 1 escrita antes, tenemos que $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(R_{n-1})$ si y solo si existe $j \in \{1,\ldots,r\}$ tal que $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j)$. Si $g(a) \neq 0$, entonces tenemos que a_n no es raíz de $g(a_1,\ldots,a_{n-1},x_n)$ pero lo es de $f(a_1,\ldots,a_{n-1},x_n)$ pues $f(a) = 0$. Debido a esto a_n no será raíz del máximo común divisor de ambos, es decir, $g_j(a_1,\ldots,a_{n-1},x_n)$ y por tanto $g_j(a) \neq 0$.
$6 \Rightarrow 5$: Si $g_j(a) \neq 0$ entonces a_n no es raíz de $g_j(a_1,\ldots,a_{n-1},x_n)$ y dado que este es máximo común divisor no lo será de uno de los dos polinomios. Dado que es raíz de $f(a_1,\ldots,a_{n-1},x_n)$, pues $f(a) = 0$, entonces ha de ser $g(a) \neq 0$.

$6 \Leftrightarrow 7$: Por definición de cadena regular es claro que

$$(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(R \cap K[x_1,\ldots,x_{n-1}]) \ \ y \ \ f(a) = 0 \ \ si \ \ y \ \ solo \ \ si \ \ a \in RZ_n(R).$$

Nota 6. *Hay que resaltar que para esta demostración solo hemos utilizado que $deg_n(f) = 1$ para demostrar $5 \Rightarrow 4$. Esto nos será útil pues podremos demostrar $1 \Rightarrow 7$ un caso particular del caso general con esta misma demostración.*

Notemos que hemos supuesto que existe $a \in \bigcup_{R' \in O} RZ_n(R')$ para demostrar una implicación y que existe $a \in RZ_n(R)$ tal que $g(a) = 0$. Sin embargo podría darse el caso en que fueran vacíos, pero esto no presenta problema pues al ser una equivalencia también queda demostrado por contrarrecíproco, que si un conjunto es vacío también lo será el otro.
Con lo que queda demostrado el caso $deg_n(f) = 1$.

Caso general: Supongamos ahora que tenemos $deg_n(f) > 1$ y que el algoritmo $\mathbf{separate}_n$ termina y verifica la especificaciones para cualquier $m < n$. Para probar la terminación, por (5.5) observamos que el algoritmo termina si este termina para cada $j \in J$ con entrada $S_j \cup \{pquo(f,g)\}$ y g y además $g_j \notin K[x_1,\ldots,x_{n-1}]$. Sea $j \in J$ y denotamos por $q_j = pquo(f,g_j)$. Primero hay que demostrar que $S_j \cup \{q_j\}$ es una cadena regular en $K[x_1,\ldots,x_n]$. Por especificación de $\mathbf{ggcd}_n$, S_j es una cadena regular de $K[x_1,\ldots,x_{n-1}]$. Probemos ahora que $lc_n(q_j)(a_1,\ldots,a_{n-1}) \neq 0$ para todo $(a_1,\ldots,a_{n-1}) \in RZ_{n-1}(S_j)$. Por definición de pseudodivisión tenemos que:

$$(lc_n(g_j))^d \cdot f = q_j \cdot g_j + prem_n(f,g_j),$$

donde por ser $deg_n(f) > deg_n(g_j)$, tenemos que $d := deg_n(f) - deg_n(g_j) + 1$. Dado que $deg_n(g_j) < deg_n(f)$ y además $deg_n(g_j) + deg_n(q_j) = deg_n(f)$, tenemos que $q_j \notin K[x_1,\ldots,x_{n-1}]$.

Es evidente que en g_j, $lc_n(g_j)$ solo multiplica una vez a la variable x_n con mayor grado. Por tanto tendremos que:

$$lc_n(q_j) = lc_n(g_j)^{d-1} \cdot lc_n(f). \tag{5.6}$$

Por la especificación 2a) escrita antes, tenemos que $lc_n(g_j)(a_1, \ldots, a_{n-1}) \neq 0$ para todo $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$, pues $g_j \notin K[x_1, \ldots, x_{n-1}]$ y en particular $g_j \neq 0$. además por la especificación 1 de antes, tenemos que si $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$ entonces $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1})$, y por la definición de cadena regular tenemos que $lc_n(f)(a_1, \ldots, a_{n-1}) \neq 0$. Por tanto tendremos que al ser $lc_n(g_j)(a_1, \ldots, a_{n-1}) \neq 0$ y $lc_n(f)(a_1, \ldots, a_{n-1}) \neq 0$, por (5.6), también $lc_n(q_j)(a_1, \ldots, a_{n-1}) \neq 0$. Y hemos probado que $S_j \cup \{q_j\}$ es una cadena regular.

Veamos ahora la terminación, se sigue de (5.4) que $g_j \notin K[x_1, \ldots, x_{n-1}]$ y dado que $deg_n(g_j) + deg_n(q_j) = deg_n(f)$, entonces $deg_n(q_j) < deg_n(f)$. Por lo tanto se reduce el grado del polinomio que no pertenece a $K[x_1, \ldots, x_{n-1}]$ y por tanto la terminación de $\mathbf{separate}_n$ con entrada $S_j \cup \{q_j\}$ y g está garantizada por la hipótesis de inducción. Lo que prueba la terminación.

Para ver que todo elemento de O es cadena regular, vemos que

$$O := \{S_j \cup \{f\} \mid j \in \{1, \ldots, r\} \ y \ g_j \in K[x_1, \ldots, x_{n-1}]\} \cup \bigcup_{j \in J} \mathbf{separate}_n(S_j \cup \{pquo(f, g_j)\}, g),$$

Ya comprobamos que $S_j \cup \{f\}$ era cadena regular para el caso $n = 1$, sin embargo no utilizamos que $deg_n(f) = 1$ por tanto la prueba para este caso es la misma. Para la segunda parte podemos aplicar la hipótesis de inducción y por tanto la salida de $\mathbf{separate}_n(S_j \cup \{q_j\}, g)$ está compuesta también por cadenas regulares.

Falta probar que

$$\{a \in RZ_n(R) \mid g(a) \neq 0\} = \bigcup_{R' \in O} RZ_n(R').$$

Lo probaremos por doble contención:

$\supseteq$: Sea $a \in \bigcup_{R' \in O} RZ_n(R')$. O bien existe $j \in \{1, \ldots, r\}$ con $g_j \in K[x_1, \ldots, x_{n-1}]$ y $a \in RZ_n(S_j \cup \{f\})$, o bien existe un $j \in J$ y un $R_j \in O_j$ tal que $a \in RZ_n(R_j)$, donde O_j denota el conjunto salida de $\mathbf{separate}_n$ con entrada $S_j \cup \{q_j\}$ y g. Veamos los dos casos por separado.

Caso 1: Si existe $j \in \{1, \ldots, r\}$ con $g_j \in K[x_1, \ldots, x_{n-1}]$ y $a \in RZ_n(S_j \cup \{f\})$ como ya vimos en la nota (6) en la demostración del caso $n = 1$ vemos que la condición de que $deg_n(f) = 1$ solo se utiliza para probar $5 \Rightarrow 4$, como nosotros en este caso solo queremos probar $1 \Rightarrow 7$, podemos utilizar la misma demostración.

Caso 2: Si existe un $j \in J$ y un $R_j \in O_j$ tal que $a \in RZ_n(R_j)$. Por la hipótesis de inducción,

$$\{a \in RZ_n(S_j \cup \{q_j\} \mid g(a) \neq 0\} = \bigcup_{R_j \in O_j} RZ_n(R_j),$$

por tanto si $a \in RZ_n(R_j)$ entonces:

$$a \in RZ_n(S_j \cup \{q_j\}) \ y \ g(a) \neq 0.$$

Por la especificación 2b) escrita antes tenemos que $g_j(a_1, \ldots, a_{n-1}, x_n)$ divide a $f(a_1, \ldots, a_{n-1}, x_n)$, y por tanto podemos aplicar el lema 7 y obtenemos que $q_j(a_1, \ldots, a_{n-1}, x_n)$ divide a $f(a_1, \ldots, a_{n-1}, x_n)$. Por definición de cero regular tenemos que si $(a_1, \ldots, a_n) \in RZ_n(S_j \cup \{q_j\})$ entonces $q_j(a_1, \ldots, a_n) = 0$ y por tanto a_n será raíz de $q_j(a_1, \ldots, a_{n-1}, x_n)$. Esto implica que lo será también de un múltiplo suyo y obtenemos $f(a_1, \ldots, a_n) = 0$. Sabemos que $(a_1, \ldots, a_{n-1}) \in RZ_n(S_j)$ y por la especificación 1 escrita antes tenemos que $(a_1, \ldots, a_{n-1}) \in RZ_n(R_{n-1})$. Por lo tanto junto a que $f(a) = 0$ obtenemos que $a \in RZ_n(R)$, además ya teníamos que $g(a) \neq 0$.

$\subseteq$: Sea $a \in RZ_n(R)$ y $g(a) \neq 0$. Sabemos que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R_{n-1})$, entonces por la especificación 1 tenemos que existe un $j \in \{1, \ldots, r\}$ tal que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$. Distinguiremos dos casos:

Caso 1:Si $g_j \in K[x_1, \ldots, x_{n-1}]$ entonces $S_j \cup \{f\} \in O$. Tenemos que $f(a) = 0$, por definición de cero regular. Por tanto $a \in RZ_n(S_j \cup \{f\})$ y tenemos que $a \in \bigcup_{R' \in O} RZ_n(R')$.

Caso 2: Si $g_j \notin K[x_1, \ldots, x_{n-1}]$. Tenemos que $g(a) \neq 0$, que $f(a) = 0$, por definición de cero regular, y que el polinomio $g_j(a_1, \ldots, a_{n-1}, x_n)$ es el máximo común divisor de $f(a_1, \ldots, a_{n-1}, x_n)$ y $g(a_1, \ldots, a_{n-1}, x_n)$. Observamos que $g_j(a) \neq 0$ pues si fuera igual a cero entonces cualquier múltiplo suyo también se anularía en a_n y tendría que ser $g(a) = 0$, lo que es una contradicción. Además tenemos que

$$deg_n(g_j(a_1, \ldots, a_{n-1}, x_n)) < deg_n(f(a_1, \ldots, a_{n-1}, x_n)), \tag{5.7}$$

es claro que es menor o igual pues uno es divisor del otro, pero la igualdad no se da pues entonces serían el mismo polinomio salvo una constante multiplicativa y entonces se anularían en los mismos puntos lo cual no ocurre, pues hemos visto que $f(a) = 0$ y $g_j(a) \neq 0$. Utilizando que $lc_n(g_j)(a_1, \ldots, a_{n-1}) \neq 0$, por la especificación 2a) escrita antes, junto con (5.7) obtenemos que $deg_n(g_j) < deg_n(f)$. De aquí por tanto $j \in J$. Como $g_j(a_1, \ldots, a_{n-1}, x_n)$ divide a $f(a_1, \ldots, a_{n-1}, x_n)$, tenemos que $prem(f, g_j)(a_1, \ldots, a_{n-1}, x_n) = 0$ por el lema 7. Por tanto tenemos que:

$$(lc_n(g_j(a_1, \ldots, a_{n-1}))^d \cdot f(a_1, \ldots, a_{n-1}, x_n) = q_j(a_1, \ldots, a_{n-1}, x_n) \cdot g_j(a_1, \ldots, a_{n-1}, x_n),$$

como $g_j(a) \neq 0$ y $f(a) = 0$, tiene que ser $q_j(a) = 0$. Por definición de cero regular, $a \in RZ_n(S_j \cup \{q_j\})$. Puesto que $g(a) \neq 0$ podemos aplicar la hipótesis de inducción aplicada a $\mathbf{separate}_n$ con entrada $S_j \cup \{q_j\}$ y g., que nos dice que:

$$\{a \in RZ_n(S_j \cup \{q_j\} \mid g(a) \neq 0\} = \bigcup_{R_j \in O_j} RZ_n(R_j),$$

y tenemos que a pertenecerá a los ceros regulares de una cadena regular perteneciente a O_j. Por tanto como este es subconjunto de O obtenemos que $a \in \bigcup_{R' \in O} RZ_n(R')$.

Notemos que hemos supuesto que existe $a \in \bigcup_{R' \in O} RZ_n(R')$ para demostrar una implicación y que existe $a \in RZ_n(R)$ tal que $g(a) = 0$. Sin embargo podría darse el caso en que fueran vacíos, pero esto no presenta problema pues al ser una equivalencia también queda demostrado por contrarrecíproco, que si un conjunto es vacío también lo será el otro.
Con lo que se demuestra la corrección del algoritmo.

5.3.3 Algoritmo $\mathbf{ggcd}_{n+1}$

Para demostrar la terminación y la corrección del algoritmo $\mathbf{ggcd}_{n+1}$ definiremos un nuevo concepto.
Sea G un subconjunto no vacío de $K[x_1, \ldots, x_{n+1}]$. Entonces:

$$sumdeg(G) := \sum_{g \in G} (deg_{n+1}(g) + 1).$$

Nota 7. *Como ya hemos estipulado en la sección inicial, tomamos $deg_{n+1}(0) = -1$, de esta forma no tenemos problema con la definición de sumdeg.*

Sean R una cadena regular en $K[x_1, \ldots, x_n]$ y sea F un conjunto de polinomios en $K[x_1, \ldots, x_{n+1}]$ los argumentos de entrada. Probaremos la terminación y corrección del algoritmo mediante una inducción sobre $sumdeg(F)$.
Probaremos primero el caso $sumdeg(F) = 0$:
Lo primero que observamos es que si $sumdeg(F) = 0$ tiene que ser $deg_{n+1}(g) = -1$. Por la definición de deg tenemos que esto pasa si y solo si $F := \{0\}$. Para este caso la terminación es clara y el conjunto de salida será $O := \{(R, 0)\}$. Claramente este conjunto de salida está compuesto por una cadena regular y un polinomio. Veamos que se verifican las tres especificaciones:

Escribimos $O := \{(R_1, g_1)\}$, con $R_1 = R$ y $g_1 = 0$ Tenemos que $RZ_n(R) = RZ_n(R_1)$, puesto que $g_1 = 0$ la especificación 2a) no se tiene que verificar y dado que $g_1(a, x_{n+1}) = 0$ para todo $a \in RZ_n(R_1)$ se verifica que es el máximo común divisor de $\{f(a, x_n) \mid f \in F\}$ pues $F = \{0\}$. La propiedad 3 se verifica también pues g_1 se anula siempre.

Supondremos ahora que $sumdeg(F) = k > 0$ y que la terminación y la corrección se verifican para cualquier $m < k$.
El primer problema con el que nos encontramos es saber si las condiciones impuestas en el condicional son computables o no. Es evidente que la condición $|F - \{0\}| \geq 2$ es computable. Lo que no está tan claro es saber si existe algún $a \in RZ_n(R)$ tal que $lc_{n+1}(g)(a) = 0$ es un problema computable o no. Tenemos que $lc_{n+1}(g)$ es un polinomio en $K[x_1, \ldots, x_n]$ y la cadena regular de entrada R es una cadena regular en $K[x_1, \ldots, x_n]$. Por lo tanto podemos computar $\mathbf{common}_n(R, lc_{n+1}(g))$ esto nos dará un conjunto $O := \{R_1, \ldots, R_l\}$ de cadenas regulares verificando:

$$\{a \in RZ_n(R) \mid lc_{n+1}(g)(a) = 0\} = \bigcup_{R' \in O} RZ_n(R').$$

Con esto vemos que se puede resolver el problema pues si $O = \emptyset$ entonces no existe ningún $a \in RZ_n(R)$ tal que $lc_n(g)(a) = 0$ y entraría en la segunda parte del condicional. Si $O \neq \emptyset$ entrará en la primera parte.

Para probar ahora la terminación y la corrección del algoritmo distinguiremos dos casos. El primero que exista exactamente un polinomio no nulo $g \in F$ y $lc(g)(a) \neq 0$ para todo $a \in RZ_n(R)$, es decir que no entra en la primera parte del condicional. El segundo caso será cualquier otra situación distinta a la anterior.

Caso 1: Supongamos que existe un único $g \in F$ no nulo con $lc(g)(a) \neq 0$ para todo $a \in RZ_n(R)$. El algoritmo termina en este caso, además el conjunto de salida será $O := \{(R, g)\}$, el cual claramente está formado por una cadena regular y un polinomio. Veamos que se verifican las especificaciones:
Escribimos $O := \{(R_1, g_1)\}$, con $R_1 = R$ y $g_1 = g$. Tenemos que $RZ_n(R) = RZ_n(R_1)$ con lo que se verifica la primera especificación. Por estar en el caso 1, $g_1 \neq 0$ por tanto tiene que ser $lc_{n+1}(g_1)(a) \neq 0$ para todo $a \in RZ_n(R_1)$, pero esto se verifica también por estar en el caso 1. La especificación 2b) se cumple pues al ser el conjunto $F = \{g\}$, como $g_1 = g$ tenemos que $g_1(a_1, \ldots, a_n, x_{n+1}) = g(a_1, \ldots, a_n, x_{n+1}$ y el máximo común divisor de un elemento es él mismo con lo que se verifica la especificación. La tercera especificación se verifica pues al anularse g_1 en todo $V_{n+1}(F)$ también lo hará en un subconjunto suyo, en particular se anulará en $Rep_{n+1}(R) \cap V_{n+1}(F)$.

Caso 2: O bien $|F - \{0\}| \geq 2$, o bien existe un polinomio no nulo $g \in F$ y un $a \in RZ_n(R)$ tal que $lc(g)(a) = 0$.
En este caso tenemos:
f:= un elemento no nulo de F con grado mínimo en x_{n+1}
$F' := F - \{f\}$
$M' := \mathbf{common}_n(R, lc_{n+1}(f))$
$M'' := \mathbf{separate}_n(R, lc_{n+1}(f))$
$f' := f - lc_{n+1}(f) \cdot x_{n+1}^{deg_{n+1}(f)}$
$F'' := \{prem_{n+1}(g, f) \mid g \in F'\}$
$O := \bigcup_{S' \in M'} \mathbf{ggcd}_{n+1}(S', F' \cup \{f'\}) \cup \bigcup_{S'' \in M''} \mathbf{ggcd}_{n+1}(S'', F'' \cup \{f\})$
Se sigue de la ya demostrada terminación de $\mathbf{common}_n$ y $\mathbf{separate}_n$, que el algoritmo termina con los argumentos de entrada R y F si termina para cada $S' \in M'$ con argumentos de entrada S' y $F' \cup \{f'\}$ y para todo $S'' \in M''$ con conjuntos de entrada S'' y $F'' \cup \{f\}$.

Sea $S' \in M'$. Tenemos que $sumdeg(F' \cup \{f'\}) = sumdeg(F') + deg_{n+1}(f') + 1$. Puesto que $f' = f - lc_{n+1}(f) \cdot x_{n+1}^{deg_{n+1}(f)}$, lo cual implica que a f le eliminas todo el término en la variable x_{n+1} con exponente más alto, por tanto $deg_{n+1}(f') < deg_{n+1}(f)$, con lo que se tiene

$$sumdeg(F') + deg_{n+1}(f') + 1 < sumdeg(F') + deg_{n+1}(f) + 1. \tag{5.8}$$

. Dado que $F' = F - \{f\}$ tenemos por tanto que $sumdeg(F') + deg_{n+1}(f) + 1 = sumdeg(F)$. Aplicando (5.8) obtenemos $sumdeg(F' \cup \{f'\}) < sumdeg(F)$, y podemos aplicar la hipótesis de inducción a $\mathbf{ggcd}_{n+1}(S', F' \cup \{f'\})$ y concluir que el algoritmo termina para todo $S' \in M'$.

Sea $S'' \in M''$. Dado que aplicamos $\mathbf{separate}_n$ para calcular M'', vemos que por las especificaciones se verifica que $lc_{n+1}(f)(a) \neq 0$ para cada $a \in RZ_n(S'')$. Distinguiremos ahora dos casos:

Caso 1: Si $F'' \subseteq \{0\}$ entonces si computamos el algoritmo $\mathbf{ggcd}_{n+1}$ con entradas S'' y $F'' \cup \{f\}$, entonces este entrará en la segunda parte del condicional y por tanto termina.

Caso 2: Si existe un $g \in F''$ no nulo entonces $deg_{n+1}(g) > deg_{n+1}(f)$ pues f se elige de grado mínimo en x_{n+1}. Por definición de pseudodivisión, $deg_{n+1}(prem_{n+1}(g,f)) < deg_{n+1}(g)$ como F'' se compone de estos pseudorestos, tenemos que $sumdeg(F'') < sumdeg(F')$. Por tanto tendremos que:

$$sumdeg(F'' \cup \{f\}) < sumdeg(F' \cup \{f\}) = sumdeg(F).$$

Por lo que podemos aplicar la hipótesis de inducción a $\mathbf{ggcd}_{n+1}(S', F' \cup \{f'\})$ y concluir que el algoritmo termina para todo $S'' \in M''$. Lo que concluye la demostración de la terminación.

Veamos ahora que todo elemento del conjunto O de salida es de la forma (R', g') con R' una cadena regular y g' un polinomio. Ya lo hemos probado para los casos de la segunda parte del condicional. Para el otro caso tenemos que:

$$O := \bigcup_{S' \in M'} \mathbf{ggcd}_{n+1}(S', F' \cup \{f'\}) \cup \bigcup_{S'' \in M''} \mathbf{ggcd}_{n+1}(S'', F'' \cup \{f\}), \tag{5.9}$$

entonces cada elemento de O tendrá la forma (R', g') si lo tienen las dos partes. Ya hemos visto que podemos aplicar la hipótesis de inducción a cada una de las partes y por tanto todos los elementos de O tienen la forma que queremos.

Veamos ahora que $\mathbf{ggcd}_{n+1}$ cumple las especificaciones:
Para la segunda parte del condicional ya hemos probado que se verifican todas las especificaciones por lo que nos centraremos en la primera parte del condicional. Para la primera especificación vemos que $\mathbf{common}_n$ con entrada R y $lc_{n+1}(f)$ tiene como especificación:

$$\{a \in RZ_n(R) \mid lc_{n+1}(f)(a) = 0\} = \bigcup_{S' \in M'} RZ_n(S'),$$

y $\mathbf{separate}_n$ con entrada R y $lc_{n+1}(f)$ tiene como especificaciones:

$$\{a \in RZ_n(R) \mid lc_{n+1}(f)(a) \neq 0\} = \bigcup_{S'' \in M''} RZ_n(S'').$$

Por tanto tenemos que:

$$RZ_n(R) = \bigcup_{S' \in M'} RZ_n(S') \cup \bigcup_{S'' \in M''} RZ_n(S'').$$

Dado que podemos aplicar la hipótesis de inducción a $\mathbf{ggcd}_{n+1}$ con entrada $S' \in M'$ y $F' \cup \{f'\}$ tenemos que:

$$RZ(S') = \bigcup_{(R',g') \in O'} RZ_n(R'),$$

siendo O' el conjunto salida de $\mathbf{ggcd}_n(S', F' \cup \{f'\})$. Aplicando la hipótesis de inducción a $\mathbf{ggcd}_n$ con entrada S'' y $F'' \cup \{f\}$ obtenemos que:

$$RZ(S'') = \bigcup_{(R'',g'') \in O''} RZ_n(R''),$$

siendo O'' el conjunto salida de $\mathbf{ggcd}_n(S'', F'' \cup \{f\})$ con lo que obtenemos que $RZ_n(R)$ se puede escribir como una unión de ceros regulares de cadenas pertenecientes a O.

Para las siguientes especificaciones denotaremos por (R', g') un elemento del conjunto de salida O y sea $a \in RZ_n(R')$. Veamos ahora que si $g' \neq 0$ entonces $lc_{n+1}(g')(a) \neq 0$ para todo $a \in RZ_n(R')$. Dado que O es de la forma (5.9) vemos que tanto si (R', g') pertenece a una parte como a la otra por la hipótesis de inducción obtenemos que $lc_{n+1}(g')(a) \neq 0$ para todo $a \in RZ_n(R')$.

Para demostrar la especificación 2b) y para la especificación 3) distinguiremos dos casos, cuando existe $S' \in M'$ con $(R', g') \in \mathbf{ggcd}_{n+1}(S', F' \cup \{f'\})$ y cuando existe $S'' \in M''$ con $(R', g') \in \mathbf{ggcd}_{n+1}(S'', F'' \cup \{f\})$.

Caso 1: Demostremos primero la especificación 2b).Sea $a \in RZ_n(R')$. Por especificación de $\mathbf{common}_n$ con entrada R y $lc_{n+1}(f)$ se tiene que:

$$\{a \in RZ_n(R) \mid lc_{n+1}(f)(a) = 0\} = \bigcup_{S' \in M'} RZ_n(S'),$$

por lo tanto $lc_{n+1}(f)(b) = 0$ para todo $b \in RZ_n(S')$. Por la hipótesis de inducción tenemos que la especificación 1 de $\mathbf{ggcd}_n$ con entrada S' y $F' \cup \{f'\}$ es $RZ_n(S') = \bigcup_{(R',g') \in O'} RZ_n(R')$ y por tanto $RZ_n(R') \subseteq RZ_n(S')$. Junto a que $lc_{n+1}(f)(b) = 0$ para todo $b \in RZ_n(S')$ se tiene que $lc_{n+1}(f)(a) = 0$. Como $f' = f - lc_{n+1}(f) \cdot x_{n+1}^{deg_{n+1}(f)}$, entonces

$$f'(a, x_{n+1}) = f(a, x_{n+1}) - lc_{n+1}(f)(a) \cdot x_{n+1}^{deg_{n+1}(f)},$$

y de aquí puesto que $lc_{n+1}(f)(a) = 0$ tenemos $f'(a, x_{n+1}) = f(a, x_{n+1})$. Como aplicamos $\mathbf{ggcd}_{n+1}$ al conjunto $F' \cup \{f'\}$ y tenemos que F' es $F - \{f\}$ entonces si

$$g'(a, x_{n+1}) = \mathbf{gcd}(\{g(a, x_{n+1}) \mid g \in F' \cup \{f'\}),$$

también será máximo común divisor de $\{g(a, x_{n+1}) \mid g \in F)$ pues ambos conjuntos coinciden para $a \in RZ_n(S')$ con lo que se prueba la condición 2(b).

Sea $a \in RZ_n(R')$ ya hemos visto que $lc_{n+1}(f)(a) = 0$. Por definición de Rep_{n+1} obtenemos que a será cero genérico de una variedad irreducible V de las que componen $Rep_{n+1}(R')$. Por lo tanto por definición de cero genérico de una variedad tendremos que $lc(f)(c) = 0$ para todo $c \in V$. De aquí se deduce que $lc_{n+1}(f)$ se anula en $Rep_{n+1}(R')$. Si utilizamos la hipótesis de inducción vemos que g' se anula en $Rep_{n+1}(R') \cap V_{n+1}(F' \cup \{f'\})$. Veamos que g' se anula en $Rep_{n+1}(R') \cap V_{n+1}(F)$. Sea $b \in Rep_{n+1}(R') \cap V(F)$. Entonces para todo $h \in F$, con $h \neq f$, $h(b) = 0$. Además $f(b) = 0$, por tanto $f'(b) + lc_{n+1}(f)(b) x_{n+1}^{deg_{n+1}} = 0$. Puesto que ya

hemos visto que $lc_{n+1}(f)$ se anula en $Rep_n(R')$ tenemos que dado que $b \in Rep_{n+1}(R')$ entonces $lc_{n+1}(f)(b) = 0$ y por lo tanto ha de ser $f'(b) = 0$. Si juntamos esto a que $h(b) = 0$ para todo $h \in F$, con $h \neq f$ obtenemos que $b \in V(F' \cup \{f'\})$ y por hipótesis $g'(b) = 0$. Por lo tanto g' se anula en $Rep_{n+1}(R') \cap V(F)$. Con lo que se prueba la tercera especificación.

Caso 2: Si existe $S'' \in M''$ con $(R', g') \in \mathbf{ggcd}_{n+1}(S'', F'' \cup \{f\})$. Demostremos primero la especificación 2b). Sea $a \in RZ_n(R')$. Por especificación de $\mathbf{separate}_n$ con entrada R y $lc_{n+1}(f)$ se tiene que:

$$\{a \in RZ_n(R) \mid lc_{n+1}(f)(a) \neq 0\} = \bigcup_{S'' \in M''} RZ_n(S''),$$

por lo tanto $lc_{n+1}(f)(b) \neq 0$ para todo $b \in RZ_n(S'')$. Por la hipótesis de inducción tenemos que la especificación 1 de $\mathbf{ggcd}_n$ con entrada S'' y $F'' \cup \{f\}$ es $RZ_n(S'') = \bigcup_{(R',g') \in O''} RZ_n(R')$ y por tanto $RZ_n(R') \subseteq RZ_n(S'')$. Junto a que $lc_{n+1}(f)(b) \neq 0$ para todo $b \in RZ_n(S'')$ se tiene que $lc_{n+1}(f)(a) \neq 0$. Por las especificaciones del algoritmo de pseudodivisión:

$$(lc_n(f))^d \cdot g = pquo_n(g, f) \cdot f + prem_n(g, f),$$

dado que $lc_{n+1}(f)(a) \neq 0$, tenemos que la parte izquierda es no nula, por lo tanto si un polinomio divide a la parte de la izquierda y también divide a f ha de dividir también al pseudoresto lo que nos asegura entonces que el máximo común divisor de $\{h(a, x_{n+1}) \mid h \in F\}$ es el mismo que el de $\{h(a, x_{n+1}) \mid h \in F'' \cup \{f\}\}$. Entonces si ahora aplicamos la hipótesis de inducción a $\mathbf{ggcd}_n(S'', F'' \cup \{f\})$ tenemos que g' verifica la condición 2(b) para $F'' \cup \{f\}$ y por lo anterior también lo verificará para F.

Falta ver la especificación 3, es decir hay que probar que g' se anula en $Rep_{n+1}(R') \cap V(F)$. Sea $b \in Rep_{n+1}(R') \cap V(F)$. Dado que tenemos:

$$(lc_n(f))^d \cdot g = pquo_n(g, f) \cdot f + prem_n(g, f),$$

como b anula todo polinomio g que es pseudodividendo y también anula f entonces b también anulará cada cada pseudoresto, con lo que se obtendrá que $b \in Rep_n(R') \cap V_{n+1}(F)$. Si aplicamos la hipótesis de inducción obtenemos que g' se anula en $Rep_n(R') \cap V_n(F'' \cup \{f\})$, por lo que $g'(b) = 0$ y por tanto g' se anula en $Rep_{n+1}(R') \cap V(F)$. Con lo que se concluye la prueba de la corrección para $\mathbf{ggcd}_{n+1}$.

Capítulo 6

Computación de cadenas regulares

En esta sección emplearemos el algoritmo $\mathbf{ggcd}_n$ desarrollado en secciones anteriores para resolver el problema de encontrar un conjunto de cadenas regulares $M = \{R_1, \ldots, R_l\}$ de forma que se verifique

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i),$$

siendo F un subconjunto de $K[x_1, \ldots, x_n]$. Para ello desarrollaremos un nuevo algoritmo llamado $\mathbf{solve}_n$ que nos dará una solución a esto.

6.1. Especificaciones del algoritmo $\mathbf{solve}_n$

Antes de describir el algoritmo definiremos un nuevo orden parcial para los elementos de $\overline{K}^n$.

Definición 6.1.1. *Sean $a := (a_1, \ldots, a_n)$ y $b := (b_1, \ldots, b_n)$ elementos de $\overline{K}^n$. Entonces diremos que a es menor que b y lo denotaremos $a \prec b$ si existe un $i \in \{1, \ldots, n\}$ tal que para todo $j \in \{1, \ldots, i-1\}$ se verifica que $K(a_1, \ldots, a_j)$ y $K(b_1, \ldots, b_j)$ tienen el mismo grado de trascendencia y $K(a_1, \ldots, a_i)$ tiene grado de trascendencia menor que $K(b_1, \ldots, b_i)$.*

Nota 8. *Realmente lo anterior no se trata de un orden parcial, para que podamos hablar de un orden parcial debemos definir $\preceq$, donde $a \preceq b$ si $a \prec b$ o $a = b$. Además vemos que podría ocurrir que ni $a \prec b$ ni tampoco $b \prec a$, diremos entonces que a y b son similares y lo denotaremos por*

$$a \sim b.$$

Nota 9. *Vemos que decir que $a \preceq b$ es equivalente a decir que*

$$(t_1, \ldots, t_n) \leqslant_{lex} (s_1, \ldots, s_n),$$

donde t_k es el grado de trascendencia de $K(a_1, \ldots, a_k)$ sobre K, s_k es el grado de trascendencia de $K(b_1, \ldots, b_k)$ sobre K y $\leqslant_{lex}$ es el orden lexicográfico. Por lo tanto podemos utilizar las propiedades del orden lexicográfico para probar las propiedades del orden $\preceq$.

Vamos a ver que $\preceq$ es de verdad es un orden parcial, es decir que verifica las propiedades reflexiva, simétrica y transitiva.

1. Claramente, $a \preceq a$, puesto que $a = a$. Vemos que esta propiedad no se verifica para la relación $a \prec a$.

2. Si $a \preceq b$ y $b \preceq a$, veamos que tiene que ocurrir que $a = b$. En términos del orden lexicográfico tenemos que $(t_1, \ldots, t_n) \leq_{lex} (s_1, \ldots, s_n)$ y $(s_1, \ldots, s_n) \leq_{lex} (t_1, \ldots, t_n)$. Lo que significa que, o bien el primer elemento no nulo en $(t_1 - s_1, \ldots, t_n - s_n)$ es positivo y el primer elemento no nulo en $(s_1 - t_1, \ldots, s_n - t_n)$ es positivo, o bien son todos nulos. Como las dos primeras condiciones son incompatibles todos los elementos han de ser nulos y por lo tanto $(t_1, \ldots, t_n) = (s_1, \ldots, s_n)$. De aquí obtenemos que no se verifica $a \prec b$ y por tanto tiene que ser $a = b$.

3. Si $a \preceq b$ y $b \preceq c$, veamos que $a \preceq c$. Si se verifica una de los dos igualdades o ambas entonces se verificará que $a \preceq c$. Veamos el caso $a \prec b$ y $b \prec c$. En términos del orden lexicográfico $(t_1, \ldots, t_n) <_{lex} (s_1, \ldots, s_n)$ y $(s_1, \ldots, s_n) <_{lex} (r_1, \ldots, r_n)$. Supongamos que el primer término positivo no nulo en $(s_1 - t_1, \ldots, s_n - t_n)$ está en la posición k y el primer término positivo no nulo en $(r_1 - s_1, \ldots, r_n - s_n)$ está en la posición l. Si $k \leqslant l$ como $s_1 = t_1, \ldots, s_{k-1} = t_{k-1}$ y $t_k < s_k$ entonces el primer término no nulo en $(r_1 - t_1, \ldots, r_n - t_n)$ aparece en la posición k y además es positivo por lo que $(t_1, \ldots, t_n) <_{lex} (r_1, \ldots, r_n)$ y por tanto $a \prec c$. Si $l < k$ entonces como $s_1 = t_1, \ldots, s_l = t_l$ tendremos que el primer término no nulo en $(r_1 - t_1, \ldots, r_n - t_n)$ aparece en la posición l y es positivo. Por tanto $(t_1, \ldots, t_n) <_{lex} (r_1, \ldots, r_n)$ y $a \prec c$.

Vamos a ver ahora dos lemas fundamentales para la construcción y la demostración del algoritmo.

Lema 8. *Sea R una cadena regular en $K[x_1, \ldots, x_n]$ y $a, b \in RZ_n(R)$.*
Entonces:

$$a \sim b.$$

Demostración: Por la propia definición de cero regular de una cadena regular, vemos que el grado de trascendencia de dos ceros de una misma cadena es el mismo. □

Debido a este lema podemos definir las siguientes relaciones en cadenas regulares.

Definición 6.1.2. *Sean R y S dos cadenas regulares en $K[x_1, \ldots, x_n]$, y sea $a \in RZ_n(R)$, y $b \in RZ_n(S)$. Entonces $R \prec S$ si y solo si $a \prec b$ y $R \sim S$ si y solo si $a \sim b$.*

Lema 9. *No existen infinitas cadenas regulares R_1, R_2,... en $K[x_1, \ldots, x_n]$ tales que:*

$$R_1 \succ R_2 \succ \ldots$$

Demostración: Hay que demostrar que no existe una sucesión infinita de ceros regulares verificando que

$$(a_1, \ldots, a_n) \succ (b_1, \ldots, b_n) \succ \ldots$$

Demostraremos esto utilizando el orden lexicográfico, es decir demostraremos que no existe una sucesión infinita verificando

$$(t_1, \ldots, t_n) >_{lex} (s_1, \ldots, s_n) >_{lex} \ldots$$

Sabemos que el orden lexicográfico es un buen orden en $\mathbb{Z}_+^n$, es decir que todo subconjunto no vacío de $\mathbb{Z}_+^n$ posee un elemento minimal. Demostraremos el lema por contrarrecíproco, supongamos que existe una sucesión infinita de elementos con

$$(t_1, \ldots, t_n) >_{lex} (s_1, \ldots, s_n) >_{lex} \ldots$$

entonces habríamos encontrado un subconjunto de $\mathbb{Z}_+^n$ que no posee elemento minimal y por tanto el orden lexicográfico no sería un buen orden en $\mathbb{Z}_+^n$ lo que es una contradicción. □

Construiremos entonces el algoritmo **solve**$_n$, verificando las siguientes especificaciones:

Algoritmo solve$_n$:
Entrada:R, una cadena regular en $K[x_1, \ldots, x_{n-1}]$, y F un subconjunto de $K[x_1, \ldots, x_n]$.
Salida:O, un conjunto de cadenas regulares en $K[x_1, \ldots, x_n]$ tales que:

1. Para cada $R' \in O$:

$$RZ_{n-1}(R'_{n-1}) \subseteq RZ_{n-1}(R) \quad \textbf{o} \quad R'_{n-1} \prec R,$$

donde $R'_{n-1} = R' \cap K[x_1, \ldots, x_{n-1}]$.

2. Se tiene la inclusión:

$$Rep_n(R) \cap V_n(F) \subseteq \bigcup_{R' \in O} Rep_n(R') \subseteq V_n(F).$$

Tenemos que este algoritmo nos proporciona una solución para el problema que queremos resolver, debido a lo siguiente:

Teorema 6.1.1. *Sea F un subconjunto finito y no vacío de $K[x_1, \ldots, x_n]$ y $\{R_1, \ldots, R_l\} :=$ **solve**$_n(\emptyset, F)$. Entonces:*

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i).$$

Demostración: Ya hemos visto que $Rep_n(\emptyset) = \overline{K}^n$, de la especificación número 2 de **solve**$_n$, obtenemos que:

$$V_n(F) = \overline{K}^n \cap V_n(F) \subseteq \bigcup_{i=1}^{l} Rep_n(R_i) \subseteq V_n(F),$$

de donde se obtiene la igualdad. □

6.2. Construcción del algoritmo solve$_n$

Construiremos el algoritmo de forma inductiva:
Primero construimos el algoritmo **solve**$_n$ para $n = 1$. La entrada para este caso será una cadena en K y por definición la única cadena en K es la vacía, definimos pues el algoritmo como:

Algoritmo solve$_1$:
si gcd$(F) = 1$
entonces
$O := \emptyset$ (O es el conjunto vacío)
si no
$O := \{\{\mathbf{gcd}(F)\} - \{0\}\}$

Probaremos que verifica las especificaciones en la siguiente sección.
Construiremos ahora el algoritmo **solve**$_n$ para $n > 1$, en función del algoritmo **solve**$_{n-1}$ y del algoritmo **ggcd**$_n$:

Algoritmo solve$_n$:
solve$_n(R, F)$
$\{(S_1, g_1), \ldots, (S_l, g_l)\} := \mathbf{ggcd}_n(R, F)$
$J := \{i \in \{1, \ldots, l\} \mid g_i \neq 0\}$
$M := \bigcup_{j \in J} \mathbf{solve}_{n-1}(S_j \cap K[x_1, \ldots, x_{n-2}], S_j - K[x_1, \ldots, x_{n-2}] \cup \{lc_n(g_j)\})$
$O := \{S_i \mid i \in \{1, \ldots, l\},\ i \notin J\} \cup \{S_j \cup \{g_j\} \mid j \in J,\ g_j \notin K[x_1, \ldots, x_{n-1}]\} \cup \bigcup_{S \in M} \mathbf{solve}_n(S, F)$

Veamos ahora un ejemplo para ver como funciona este algoritmo:

Ejemplo 6.2.1. *Buscamos encontrar una representación mediante cadenas regulares de la variedad $V_2(\{x_2^2 - x_1, x_1x_2 + x_1^2\})$. Para ello utilizando el último teorema hemos de computar* ***solve***$_2(\emptyset, \{x_2^2 - x_1, x_1x_2 + x_1^2\})$.
$L :=$ ***ggcd***$_2(\emptyset, \{x_2^2 - x_1, x_1x_2 + x_1^2\})$
Como $|F - \{0\}| \geqslant 2$*:*
$f := x_1x_2 + x_1^2$
$F' := x_2^2 - x_1$
$M' :=$ ***common***$_1(\emptyset, x_1)$
ggcd$_1(\emptyset, \{x_1\}) := \{(\emptyset, x_1)\}$
Como $R - K = \emptyset$ *y* $x_1 \neq 0$
$O := \emptyset$ *(O es el conjunto vacío)*
$M' := \emptyset$ *(M' es el conjunto vacío)*
$M'' :=$ ***separate***$_1(\emptyset, x_1)$
ggcd$_1(\emptyset, \{x_1\}) := \{(\emptyset, x_1)\}$
Como $R - K = \emptyset$ *y* $x_1 \neq 0$
$O := \{\emptyset\}$ *(O es el conjunto compuesto por la cadena vacía)*
$M'' := \{\emptyset\}$ *(M'' es el conjunto compuesto por la cadena vacía)*
$f' := x_1x_2 + x_1^2 - x_1x_2 = x_1^2$
$F'' := \{prem_2(x_2^2 - x_1, x_1x_2 + x_1^2)\} = \{x_1^4 - x_1^3\}$
$O := \emptyset \cup$ ***ggcd***$_2(\emptyset, \{x_1^4 - x_1^3, x_1x_2 + x_1^2\}) =$ ***ggcd***$_2(\emptyset, \{x_1^4 - x_1^3, x_1x_2 + x_1^2\})$
Como $|F - \{0\}| \geqslant 2$*:*
$f := x_1^4 - x_1^3$
$F' := x_1x_2 + x_1^2$
$M' :=$ ***common***$_1(\emptyset, x_1^4 - x_1^3)$
ggcd$_1(\emptyset, \{x_1^4 - x_1^3\}) := \{(\emptyset, x_1^4 - x_3)\}$
Como $R - K = \emptyset$ *y* $x_1^4 - x_1^3 \neq 0$

$O := \emptyset$ *(O es el conjunto vacío)*
$M' := \emptyset$ *(M′ es el conjunto vacío)*
$M'' := \boldsymbol{separate}_1(\emptyset, x_1^4 - x_1^3)$
$\boldsymbol{ggcd}_1(\emptyset, \{x_1^4 - x_1^3\}) := \{(\emptyset, x_1^4 - x_1^3)\}$
Como $R - K = \emptyset$ *y* $x_1^4 - x_1^3 \neq 0$
$O := \{\emptyset\}$ *(O es el conjunto compuesto por la cadena vacía)*
$M'' := \{\emptyset\}$ *(M″ es el conjunto compuesto por la cadena vacía)*
$f' := x_1^4 - x_1^3 - (x_1^4 - x_1^3) = 0$
$F'' := \{prem_2(x_1x_2 + x_1^2, x_1^4 - x_1^3)\} = \{0\}$
$O := \emptyset \cup \boldsymbol{ggcd}_2(\emptyset, \{0, x_1^4 - x_1^3\}) = \boldsymbol{ggcd}_2(\emptyset, \{0, x_1^4 - x_1^3\})$
Como $|F - \{0\}| \ngeq 2$ *y* $lc(x^4 - x_1^3)(a) \neq 0$ *con* $a \in RZ_1(\emptyset) = (a)$
con a trascendente sobre K. Los puntos 0 *y* 1 *que es donde se*
anula $x_1^4 - x_1^3$ *son algebraicos.*
Como existe $f \neq 0$ *en F entonces:*
$O := \{(\emptyset, x_1^4 - x_1^3)\}$
$L := \{(\emptyset, x_1^4 - x_1^3)\}$
$J := \{1\}$
$M := \boldsymbol{solve}_1(\emptyset, \{x_1^4 - x_1^3\})$
Como $\boldsymbol{gcd}(\{x_1^4 - x_1^3\}) \neq 1$
$O := \{\{x_1^4 - x_1^3\}\}$
$M := \{\{x_1^4 - x_1^3\}\}$
$O := \emptyset \cup \emptyset \cup \boldsymbol{solve}_2(\{x_1^4 - x_1^3\}, \{x_2^2 - x_1, x_1x_2 + x_1^2\}) = \boldsymbol{solve}_2(\{x_1^4 - x_1^3\}, \{x_2^2 - x_1, x_1x_2 + x_1^2\})$

Tenemos que computar ahora $\boldsymbol{solve}_2(\{x_1^4 - x_1^3\}, \{x_2^2 - x_1, x_1x_2 + x_1^2\})$
$L := \boldsymbol{ggcd}_2(\{x_1^4 - x_1^3\}, \{x_2^2 - x_1, x_1x_2 + x_1^2\})$.
Esto lo hemos calculado en el ejemplo de la sección 4, así que tomamos de ahí el resultado.
$\{(S_1, g_1), (S_2, g_2)\} := \{(\{x_1\}, x_2^2 - x_1), (\{x_1 - 1\}, x_1x_2 + x_1^2)\}$
$J := \{1, 2\}$
$M := \boldsymbol{solve}_1(\emptyset, \{x_1\} \cup \{1\}) \cup \boldsymbol{solve}_1(\emptyset, \{x_1 - 1\} \cup \{x_1\})$
Como $\boldsymbol{gcd}(x_1, 1) = 1$ *y* $\boldsymbol{gcd}(x_1 - 1, x_1) = 1$
$\boldsymbol{solve}_1(\emptyset, \{x_1, 1\}) = \emptyset$
$\boldsymbol{solve}_1(\emptyset, \{x_1 - 1, x_1\}) = \emptyset$
$M := \emptyset$ *(M es el conjunto vacío)*
Como todo $j \in J$ *y* $g_j \notin K[x_1]$*:*
$O := \{\{x_1\} \cup \{x_2^2 - x_1\}\} \cup \{\{x_1 - 1\} \cup \{x_1x_2 + x_1^2\}\}$.
Por tanto $\boldsymbol{solve}_2(\emptyset, \{x_2^2 - x_1, x_1x_2 + x_1^2\}) = \{\{x_1, x_2^2 - x_1\}, \{x_1 - 1, x_1x_2 + x_1^2\}\}$
De aquí obtenemos que:

$$V_2(\{x_2^2 - x_1, x_1x_2 + x_1^2\}) = Rep_2(\{x_1, x_2^2 + x_1\}) \cup Rep_2(\{x_1 - 1, x_1x_2 + x_1^2\}).$$

6.3. Justificación de la terminación y corrección del algoritmo $\mathbf{solve}_n$

La demostración de la terminación y la corrección del algoritmo $\mathbf{solve}_n$ se hará de manera inductiva. Por tanto probaremos primero la terminación y la corrección del algoritmo para el caso $n = 1$.

El algoritmo es:
si $\mathbf{gcd}(F) = 1$
  entonces
    $O := \emptyset$ (O es el conjunto vacío)
si no
    $O := \{\{\mathbf{gcd}(F)\} - \{0\}\}$

El algoritmo termina como consecuencia de la terminación de **gcd**. Por las especificaciones del algoritmo **gcd** su salida es única salvo constante multiplicativa, por tanto, el caso $\mathbf{gcd}(F) = 1$ engloba cualquier salida que sea constante. El cual nos da el conjunto vacío que es una salida permitida. Si $\mathbf{gcd}(F) \neq 1$ entonces $\mathbf{gcd}(F) - 0$ es una cadena regular, pues el caso en que $\mathbf{gcd}(F) = 0$ obtenemos la cadena vacía, que es una cadena regular. Y si no obtenemos $\mathbf{gcd}(F) \notin K$ lo cual es una cadena regular porque solo hay un elemento en $\mathbf{gcd}(F) - K$ y $lc(\mathbf{gcd}(F))$ es una constante no nula y por tanto no se anula en $RZ_0(\emptyset)$.

Veamos la corrección del algoritmo, distinguiremos 3 casos:

Caso 1: Si $\mathbf{gcd}(F) = 1$, entonces $O := \emptyset$ (el conjunto vacío) y por tanto es trivial que se verifica la especificación 1 pues no hay elementos en O.

La especificación 2 se verifica pues $\bigcup_{R' \in O} Rep_n(R') = \emptyset$ y dado que por las propiedades de **gcd** si $\mathbf{gcd}(F) = 1$ entonces no hay ceros comunes a los polinomios en F y por lo tanto $V_1(F) = \emptyset$, con lo que se verifica la especificación 2.

Caso 2: Si $\mathbf{gcd}(F) = 0$, entonces $O := \{\emptyset\}$ (el conjunto compuesto por la cadena vacía). Dado que la entrada es $R = \emptyset$ y $R'_0 = \emptyset \cap K = \emptyset$ entonces se verifica que $RZ_1(R'_0) \subseteq RZ_1(R)$ con lo que se cumple la especificación 1.

Para la especificación 2, tenemos primero que $Rep_1(\emptyset) = \overline{K}$ y por tanto la condición se traduce en $V_n(F) = \bigcup_{R' \in O} Rep_1(R')$. Además como $O := \{\emptyset\}$ tenemos que $\bigcup_{R' \in O} Rep_1(R') = \overline{K}$, puesto que $\mathbf{gcd}(F) = 0$ si y solo si $F = \{0\}$, esto implica que todo punto de $\overline{K}$ pertenece a $V_1(F)$, con lo que tenemos lo buscado.

Caso 3: En caso el caso en que $\mathbf{gcd}(F) \notin K$, entonces $O = \{\mathbf{gcd}(F)\}$ por tanto $R'_0 = R' \cap K = \emptyset$ y por tanto $RZ_0(R'_0) \subseteq RZ_0(R)$ y se verifica la especificación 1.

Para la especificación 2, tenemos que $Rep_1(\emptyset) = \overline{K}$ y por tanto la condición se traduce en $V_1(F) = \bigcup_{R' \in O} Rep_1(R')$, o lo que es lo mismo $V_1(F) = Rep_1(\{\mathbf{gcd}(F)\})$. Lo cual se obtiene de la definición de Rep_1 y del hecho que los ceros comunes a un conjunto de polinomios coincide con los ceros del máximo común divisor de todos ellos.

6.3.1 Terminación del algoritmo $\mathbf{solve}_n$

Una vez probado el caso $n = 1$ supondremos que el algoritmo $\mathbf{solve}_{n-1}$ termina y verifica las especificaciones y probaremos la terminación y la corrección de $\mathbf{solve}_n$.

Sean R una cadena regular en $K[x_1, \ldots, x_{n-1}]$ y F un subconjunto de $K[x_1, \ldots, x_n]$ los argumentos de entrada. Si $M = \emptyset$ (el conjunto vacío), entonces el algoritmo termina, puesto que $\mathbf{ggcd}_n$ termina y no hay llamadas a más algoritmos.
Por tanto vamos a suponer que $M \neq \emptyset$. Lo primero que vamos a demostrar es que para todo $S \in M$

$$S \prec R,$$

siendo

$$M := \bigcup_{j \in J} \mathbf{solve}_{n-1}(S_j \cap K[x_1, \ldots, x_{n-2}], S_j - K[x_1, \ldots, x_{n-2}] \cup \{lc_n(g_j)\}).$$

Tomamos S un elemento arbitrario de M, es decir existirá un $j \in J$ tal que

$$S \in \mathbf{solve}_{n-1}(S_j \cap K[x_1, \ldots, x_{n-2}], S_j - K[x_1, \ldots, x_{n-2}] \cup \{lc_n(g_j)\}).$$

Basta demostrar que $a \prec b$ para cualesquiera $a \in RZ_{n-1}(S)$ y $b \in RZ_{n-1}(R)$,donde $a = (a_1, \ldots, a_{n-1})$ y $b = (b_1, \ldots, b_{n-1})$. Dado que por la especificación 1 de $\mathbf{ggcd}_n$, $RZ_{n-1}(R) = \bigcup_{i=1}^{l} RZ_{n-1}(S_i)$ tenemos que:

$$(b_1, \ldots, b_{n-1}) \in RZ_{n-1}(R). \tag{6.1}$$

Por la especificación 2 de $\mathbf{solve}_{n-1}$, tenemos que

$$Rep_{n-1}(S) \subseteq V_{n-1}(S_j - K[x_1, \ldots, x_{n-2}] \cup \{lc(g_j)).$$

Dado que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S)$ y debido a la definición de Rep_{n-1} tenemos que $(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(S)$. Por tanto

$$(a_1, \ldots, a_{n-1}) \in V_n(S_j - K[x_1, \ldots, x_{n-1}] \cup \{lc(g_j)\}),$$

y de aquí

$$lc_{n-1}(g_j)(a_1, \ldots, a_{n-1}) = 0. \tag{6.2}$$

Además tenemos por la especificación 2 de $\mathbf{solve}_{n-1}$ que:

$$RZ_{n-2}(S \cap K[x_1, \ldots, x_{n-2}]) \subseteq RZ_{n-2}(S_j \cap K[x_1, \ldots, x_{n-2}])$$

o

$$S \cap K[x_1, \ldots, x_{n-2}] \prec S_j \cap K[x_1, \ldots, x_{n-2}].$$

Supongamos primero que $S \cap K[x_1, \ldots, x_{n-2}] \prec S_j \cap K[x_1, \ldots, x_{n-2}]$. Entonces por definición de la relación $\prec$, tenemos que $S \prec S_j$. Como $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S)$ y

$(b_1, \ldots, b_{n-1}) \in RZ_{n-1}(S_j)$ y además también tenemos (6.1) obtenemos que $S \prec R$.

Asumiremos ahora entonces que:

$$RZ_{n-2}(S \cap K[x_1, \ldots, x_{n-2}]) \subseteq RZ_{n-2}(S_j \cap K[x_1, \ldots, x_{n-2}]).$$

Distinguiremos dos casos:

Caso 1: Existe un polinomio f en $S_j - K[x_1, \ldots, x_{n-2}]$
Por la especificación 2 de $\mathbf{solve}_{n-1}$ tenemos que

$$Rep_{n-1}(S) \subseteq V_{n-1}(f \cup \{lc(g_j)\}).$$

Como $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S)$ entonces por definición de $Rep_{n-1}(S)$,
$(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(S)$ y por tanto al estar contenido en $V_n(f \cup \{lc(g_j)\})$ tenemos
$f(a_1, \ldots, a_{n-1}) = 0$. Como

$$S_j = S_j \cap K[x_1, \ldots, x_{n-2}] \cup \{f\},$$

esta es una cadena regular y además $(a_1, \ldots, a_{n-2}) \in RZ_{n-2}(S_j \cap K[x_1, \ldots, x_{n-2}])$ tenemos que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$. Sabemos por la especificación 2a) de $\mathbf{ggcd}_n$ que
$lc_n(g_j)(a_1, \ldots, a_{n-1}) \neq 0$ para todo $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_j)$, lo que entra en contracción con (6.2). Por tanto este caso no es posible que se de.

Caso 2: Si $S_j - K[x_1, \ldots, x_{n-2}] = \emptyset$
Dado que $(a_1, \ldots, a_{n-2}) \in RZ_{n-2}(S_j \cap K[x_1, \ldots, x_{n-2}])$, entonces los ceros regulares de la cadena regular S_j tendrán la forma $(a_1, \ldots, a_{n-2}, a'_{n-1})$ donde a'_{n-1} es un elemento trascendente sobre $K(a_1, \ldots, a_{n-2})$. Dado que $(a_1, \ldots, a_{n-2}, a'_{n-1}) \in RZ_{n-1}(S_j)$ tenemos por la especificación 2a) de $\mathbf{ggcd}_n$ que

$$lc_n(g_j)(a_1, \ldots, a_{n-2}, a'_{n-1}) \neq 0.$$

Debido a esto deducimos que $lc_n(g_j)(a_1, \ldots, a_{n-2}, x_{n-1}) \neq 0$. Por esto y por (6.2) obtenemos que a_{n-1} es algebraico sobre $K(a_1, \ldots, a_{n-2})$. Por otro lado, dado que $(b_1, \ldots, b_{n-1}) \in RZ_{n-1}(S_j)$ por definición de cadena regular y dado que $S_j - K[x_1, \ldots, x_{n-2}] = \emptyset$, tenemos que b_{n-1} es trascendente sobre $K(b_1, \ldots, b_{n-2})$. Sabemos también que tanto $(a_1, \ldots, a_{n-2})$ como $(b_1, \ldots, b_{n-2})$ pertenecen a $RZ_{n-2}(S_j \cap K[x_1, \ldots, x_{n-2}]$. Por el lema 8 sabemos que $(a_1, \ldots, a_{n-2}) \sim (b_1, \ldots, b_{n-2})$. Por tanto como b_{n-1} es trascendente sobre $K(b_1, \ldots, b_{n-2})$ y a_{n-1} es algebraico sobre $K(a_1, \ldots, a_{n-2})$ podemos deducir que $(a_1, \ldots, a_{n-1}) \prec (b_1, \ldots, b_{n-1})$. Por tanto podemos concluir que $S \prec R$.

Probemos ahora la terminación del algoritmo, si suponemos que $\mathbf{solve}_n$ no terminase nunca entonces estaríamos generando una sucesión infinita $R, S, \ldots$ tal que $R \succ S \succ \ldots$ lo cual entra en contradicción con el lema 9 ya demostrado. Por tanto el algoritmo $\mathbf{solve}_n$ termina.

6.3.2 Justificación de la corrección del algoritmo $\mathbf{solve}_n$

Antes de probar la corrección del algoritmo se probarán dos lemas que se utilizarán en la demostración.

Lema 10. *Sea R una cadena regular en $K[x_1, \ldots, x_n]$. Si $(a_1, \ldots, a_n) \in Rep_n(R)$ entonces $(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(R_{n-1})$, donde*
$R_{n-1} = R \cap K[x_1, \ldots, x_{n-1}]$.

Demostración: Sea $(a_1, \ldots, a_n) \in Rep_n(R)$. Entonces por definición existirá $(b_1, \ldots, b_n) \in RZ_n(R)$ tal que $(a_1, \ldots, a_n) \in V$, donde V es una variedad irreducible de $\overline{K}^n$ que tiene a $(b_1, \ldots, b_n)$ como punto genérico. Por definición de cadena regular, $(b_1, \ldots, b_{n-1}) \in RZ_{n-1}(R_{n-1})$. Por definición de punto genérico, tenemos que $f(b_1, \ldots, b_n) = 0$ implica que $f(a_1, \ldots, a_n) = 0$ para todo polinomio $f \in K[x_1, \ldots, x_n]$. Entonces, en particular también pasa esto para polinomios en $K[x_1, \ldots, x_{n-1}]$, por tanto $f(b_1, \ldots, b_{n-1}) = 0$ implica $f(a_1, \ldots, a_{n-1}) = 0$ para todo $f \in K[x_1, \ldots, x_{n-1}]$. De aquí vemos que $(a_1, \ldots, a_{n-1})$ pertenece a la variedad irreducible en $\overline{K}^{n-1}$ con punto genérico $(b_1, \ldots, b_{n-1})$. Por tanto

$$(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(R_{n-1}).$$

□

Lema 11. *Sea V una variedad irreducible en $\overline{K}^{n-1}$ con $(b_1, \ldots, b_{n-1})$ como punto genérico, sea $(a_1, \ldots, a_n) \in \overline{K}^n$ tal que $(a_1, \ldots, a_{n-1}) \in V$, y sea h un polinomio en $K[x_1, \ldots, x_n]$ que verifique:*

$$lc(h)(b_1, \ldots, b_{n-1}) \neq 0, \quad lc(h)(a_1, \ldots, a_{n-1}) \neq 0, \quad h(a_1, \ldots, a_n) = 0.$$

Entonces existe un $b_n \in \overline{K}$ con $h(b_1, \ldots, b_n) = 0$ y si V' es la variedad irreducible en $\overline{K}^n$ con $(b_1, \ldots, b_n)$ como punto genérico, entonces $(a_1, \ldots, a_n) \in V'$.

Demostración: Como tenemos que $lc(h)(a_1, \ldots, a_{n-1}) \neq 0$ y $h(a_1, \ldots, a_n) = 0$, entonces $h \notin K[x_1, \ldots, x_{n-1}]$. Como $lc(h)(b_1, \ldots, b_{n-1}) \neq 0$ se sigue que existen un número finito de raíces $c_1, \ldots, c_k \in \overline{K}$ del polinomio en una variable $h(b_1, \ldots, b_{n-1}, x_n)$, recordemos en un dominio universal siempre van a existir estas raíces.
Tendremos entonces una variedad que es la generada por el polinomio $h(b_1, \ldots, b_{n-1}, x_n)$ en $K(b_1, \ldots, b_{n-1})[x_n]$, para la cual los puntos tendrán la forma $(b_1, \ldots, b_{n-1}, c_i)$. Llamaremos a esta variedad y vemos que esta se puede escribir como $V = \bigcup_{i=1}^{k} V_i$, donde V_i es la variedad irreducible en $\overline{K}^n$ con $(b_1, \ldots, b_{n-1}, c_i)$ como punto genérico. Veamos que $(a_1, \ldots, a_n) \in V$. Tomamos un polinomio cualquiera que pertenezca al ideal asociado a esta variedad, ese decir cualquier polinomio verificando que $f(b_1, \ldots, b_{n-1}, c_i) = 0$ para todo $i \in \{1, \ldots, k\}$. Notemos que el propio h verifica esto, pero en h la multiplicidad de las raíces podría no ser 1, por lo tanto claramente existirá un entero l de forma que $h(b_1, \ldots, b_{n-1}, x_n)$ divide a $f(b_1, \ldots, b_{n-1}, x_n)^l$.
Denotemos por r el pseudoresto y q el pseudocociente de la pseudodivisión de f^l entre h con respecto a la variable x_n. Dado que $h(b_1, \ldots, b_{n-1}, x_n)$ divide a $f(b_1, \ldots, b_{n-1}, x_n)^l$ y además $lc(h)(b_1, \ldots, b_{n-1}) \neq 0$ podemos aplicar el lema 7 y deducir que $r(b_1, \ldots, b_{n-1}, x_n) = 0$. Como $(b_1, \ldots, b_{n-1})$ es cero genérico de V, y $(a_1, \ldots, a_{n-1}) \in V$ entonces $r(a_1, \ldots, a_{n-1}, x_n) = 0$. De la definición de pseudodivisión, $lc(h)^d \cdot f^l = h \cdot q + r$, además sabemos que $lc(h)(a_1, \ldots, a_{n-1}) \neq 0$, $h(a_1, \ldots, a_n) = 0$ por hipótesis y $r(a_1, \ldots, a_n) = 0$ pues $r(a_1, \ldots, a_{n-1}, x_n) = 0$. Por todo esto ha de ser $f^l(a_1, \ldots, a_n) = 0$ y por tanto $f(a_1, \ldots, a_n) = 0$. Como f es un polinomio cualquiera del ideal asociado a la variedad con puntos de la forma $(b_1, \ldots, b_{n-1}, c_i)$, entonces $(a_1, \ldots, a_n) \in \mathbf{V}(\mathbf{I}(V))$. Ya hemos probado que para cualquier variedad $\mathbf{V}(\mathbf{I}(V)) = V$. Entonces $(a_1, \ldots, a_n) \in V$. Dado que $V = \bigcup_{i=1}^{k} V_i$, entonces $(a_1, \ldots, a_n) \in V_i$ para algún $i \in \{1, \ldots, n\}$. Por tanto existe $b_n \in \{c_1, \ldots, c_k\}$ tal que $(a_1, \ldots, a_n) \in V'$, donde V' es una variedad irreducible en $\overline{K}^n$ con $(b_1, \ldots, b_n)$ como punto genérico. □

Pasaremos ahora a probar la corrección del algoritmo mediante una inducción sobre el orden parcial $\prec$ en cadenas regulares. Sean R una cadena regular en $K[x_1, \ldots, x_{n-1}]$ y F un subconjunto de $K[x_1, \ldots, x_n]$ los argumentos de entrada. Lo primero que hay que ver es cual es el conjunto minimal con respecto al orden $\prec$, claramente es la cadena cuyos ceros regulares tienen grado de trascendencia 0, es decir que todas sus componentes son elementos algebraicos sobre K, lo que es equivalente a decir que R representa a una variedad 0-dimensional.

Por tanto comenzaremos probando la corrección del algoritmo en el caso en que la dimensión de $Rep_n(R)$ es 0.
En la demostración de la terminación vimos que $S \prec R$ para todo $S \in M$, dado que en nuestro caso esto no puede pasar pues R es minimal con respecto a $\prec$ tiene que ser $M = \emptyset$.
Entonces en este caso obtenemos que la salida será de la forma

$$O := \{S_i \mid i \in \{1, \ldots, l\},\ \ i \notin J\} \cup \{S_j \cup \{g_j\} \mid j \in J,\ \ g_j \notin K[x_1, \ldots, x_{n-1}]\}.$$

Esto son cadenas regulares pues por especificación de $\mathbf{ggcd}_n$, los S_i son cadenas regulares en $K[x_1, \ldots, x_{n-1}]$, además por la especificación 2a) de $\mathbf{ggcd}_n$ sabemos que $lc(g_j)(a) = 0$ para todo $a \in RZ_{n-1}(S_j)$ y por tanto $S_j \cup \{g_j\}$ es cadena regular.

Veamos que se verifica la especificación 1, probemos que:

$$RZ_{n-1}(R'_{n-1}) \subseteq RZ_{n-1}(R).$$

Sea $R' \in O$, debido a la forma de O sabemos que existe $i \in \{1, \ldots, l\}$ tal que

$$R'_{n-1} = S_i.$$

Por la especificación 1 de $\mathbf{ggcd}_n$ sabemos que $RZ_{n-1}(R) = \bigcup_{i=1}^{l} RZ_{n-1}(S_i)$ y por lo tanto se verifica que

$$RZ_{n-1}(R'_{n-1}) \subseteq RZ_{n-1}(R).$$

Demostraremos ahora la condición 2. Hay que ver que:

$$Rep_n(R) \cap V_n(F) \subseteq \bigcup_{R' \in O} Rep_n(R') \subseteq V_n(F).$$

Sea $(a_1, \ldots, a_n) \in Rep_n(R) \cap V_n(F)$. Por el lema 10, $(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(R)$. Dado que $Rep_{n-1}(R)$ es una variedad 0-dimensional hemos visto en el apartado de la dimensión que todos sus puntos son genéricos, por tanto $(a_1, \ldots, a_{n-1})$ es un punto genérico de una de las componentes irreducibles de $Rep_{n-1}(R)$. Por la definición de Rep_{n-1} tenemos que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(R)$. De aquí, por la especificación 1 de $\mathbf{ggcd}_n$, existe un $i \in \{1, \ldots, l\}$ con $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_i)$. Dado que S_i es una cadena en $K[x_1, \ldots, x_{n-1}]$ tenemos que entonces $(a_1, \ldots, a_n) \in Rep_n(S_i)$. Junto con que $(a_1, \ldots, a_n) \in V_n(F)$, tenemos que $(a_1, \ldots, a_n) \in Rep_n(R) \cap V_n(F)$. Por la especificación 3 de $\mathbf{ggcd}_n$ sabemos que g_i se anula en $Rep_n(S_i) \cap V_n(F)$, por lo tanto $g_i(a_1, \ldots, a_n) = 0$.

Si $g_i = 0$ entonces $g_i \in K[x_1, \ldots, x_{n-1}]$ y por tanto $S_i \in O$. De aquí obtenemos que

$$(a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep_n(R').$$

Si $g_i \neq 0$ entonces por la especificación 2a) de $\mathbf{ggcd}_n$, $lc(g_i)(a_1, \ldots, a_{n-1}) \neq 0$ y de aquí junto con que $g_i(a_1, \ldots, a_n) = 0$ se deduce que $g_i \notin K[x_1, \ldots, x_{n-1}]$. Por lo tanto $S_i \cup \{g_i\} \in O$ y además como S_i es una cadena de $K[x_1, \ldots, x_{n-1}]$ y g_i es un polinomio de $K[x_1, \ldots, x_n]$ por definición de cero regular de una cadena regular $(a_1, \ldots, a_n) \in RZ_n(S_i \cup \{g_i\})$. De aquí por la definición de Rep_{n-1} obtenemos que $(a_1, \ldots, a_n) \in Rep_n(S_i \cup \{g_i\})$. Por lo tanto

$$(a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep_n(R').$$

Probemos ahora la segunda contención. Sea $R' \in O$ y $(a_1, \ldots, a_n) \in Rep_n(R')$, ya hemos visto antes que como $M := \emptyset$, podemos elegir $i \in \{1, \ldots, l\}$ con $R'_{n-1} = S_i$. Por el lema 10, $(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(S_i)$. Por la especificación 1 de $\mathbf{ggcd}_n$ sabemos que $RZ_{n-1}(R) = \bigcup_{i=1}^{l} RZ_{n-1}(S_i)$, dado que la dimensión de $Rep_{n-1}(R)$ es 0, tenemos también que la dimensión de $Rep_{n-1}(S_i)$ es 0. Dado que todos los puntos de una variedad irreducible cero-dimensional son puntos genéricos y por la definición de Rep_{n-1} obtenemos que $(a_1, \ldots, a_{n-1}) \in RZ_{n-1}(S_i)$. Si $i \notin J$ entonces $g_i = 0$, si $i \in J$ entonces $(a_1, \ldots, a_n) \in Rep(S_i \cup \{g_i\})$. De cualquier manera $g_i(a_1, \ldots, a_n) = 0$. Dado que por especificación de $\mathbf{ggcd}_n$, $g_i(a_1, \ldots, a_{n-1}, x_n)$ es el máximo común divisor de los polinomios en $\{f(a_1, \ldots, a_{n-1}, x_n) \mid f \in F\}$, entonces como $(a_1, \ldots, a_n)$ anula al máximo común divisor del conjunto, entonces anulará también a todos los polinomios del conjunto y por lo tanto

$$(a_1, \ldots, a_n) \in V_n(F).$$

Con lo que se prueba el caso inicial.

Probemos ahora el caso general cuando R no es una cadena minimal con respecto a $\prec$. Veamos primero que O está compuesto por cadenas regulares. Dado que

$$O := \{S_i \mid i \in \{1, \ldots, l\},\ i \notin J\} \cup \{S_j \cup \{g_j\} \mid j \in J,\ g_j \notin K[x_1, \ldots, x_{n-1}]\} \cup \bigcup_{S \in M} \mathbf{solve}_n(S, F).$$

Ya hemos visto que los primeros son cadenas regulares por especificación de $\mathbf{ggcd}_n$. Para ver que los elementos de $\bigcup_{S \in M} \mathbf{solve}_n(S, F)$ son cadenas regulares recurrimos a la hipótesis de inducción pues ya hemos probado que $S \prec R$.

Veamos ahora que se verifica la primera especificación. Sea $R' \in O$.

Caso 1: Si existe $i \in \{1, \ldots, l\}$ tal que $R'_{n-1} = S_i$, es decir que R' pertenezca a los dos primeros conjuntos. Debido a la primera especificación de $\mathbf{ggcd}_n$ tenemos que $RZ_{n-1}(R) = \bigcup_{i=1}^{l} RZ_{n-1}(S_i)$, de lo que se deduce que $RZ_{n-1}(R'_{n-1}]) \subseteq RZ_{n-1}(R)$ con lo que se

verifica la primera especificación.

Caso 2: En el caso en que R' pertenezca al conjunto de salida de $\mathbf{solve}_n(S, F)$ para algún $S \in M$, como hemos probado ya que $S \prec R$, obtenemos de la hipótesis de inducción que $RZ_{n-1}(R'_{n-1}) \subseteq\in RZ_{n-1}(S)$ o $R'_{n-1} \prec S$. Si $R'_{n-1} \prec S$ dado que $S \prec R$ tenemos que $R'_{n-1} \prec R$. Si $RZ_{n-1}(R'_{n-1}) \subseteq\in RZ_{n-1}(S)$ entonces los ceros regulares de R'_{n-1} tienen los mismos grados de trascendencia que los de S y por tanto dado que $S \prec R$ obtenemos que $R'_{n-1} \prec R$. Con lo que verifica la especificación 1.

Probemos ahora que se verifica que:

$$Rep_n(R) \cap V_n(F) \subseteq \bigcup_{R' \in O} Rep_n(R') \subseteq V_n(F).$$

Debido a la especificación 1 de $\mathbf{ggcd}_n$ tenemos que $RZ_{n-1}(R) = \bigcup_{i=1}^{l} RZ_{n-1}(S_i)$ como todas son cadenas regulares en $K[x_1, \ldots, x_{n-1}]$ podemos extender esta igualdad por la definición de cero regular a dimensión n y tenemos que $RZ_n(R) = \bigcup_{i=1}^{l} RZ_n(S_i)$. Ahora de la definición de $Rep_n(R)$ obtenemos que $Rep_n(R) = \bigcup\{V \mid V$ es una variedad irreducible en $\overline{K}^n$ con un punto genérico en $RZ_n(R)\}$ por la expresión de los ceros regulares de antes obtenemos que:

$$Rep_n(R) = \bigcup \bigcup_{i=1}^{l} \{V \mid V \textit{ es variedad irreducible en } \overline{K}^n \textit{ con un punto genérico en } RZ_n(S_i)\}$$

intercambiando las uniones obtenemos:

$$Rep_n(R) = \bigcup_{i=1}^{l} Rep_n(S_i).$$

Sea $(a_1, \ldots, a_n) \in Rep_n(R) \cap V_n(F)$. Entonces por lo anterior existirá un $i \in \{1, \ldots, l\}$ tal que $(a_1, \ldots, a_n) \in Rep_n(S_i)$. Por la especificación 3 de $\mathbf{ggcd}_n$ como $(a_1, \ldots, a_n) \in Rep_n(S_i) \cap V_n(F)$ tenemos que

$$g_i(a_1, \ldots, a_n) = 0.$$

Distinguiremos tres casos:

Caso 1: Si $g_i = 0$ entonces $g_i \in K[x_1, \ldots, x_{n-1}]$ y por la construcción de $\mathbf{solve}_n$ tenemos que $S_i \in O$. Como $(a_1, \ldots, a_n) \in Rep_n(S_i)$ obtenemos que

$$(a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep_n(R').$$

Caso 2: Si $g_i \neq 0$ y $lc(g_i)(a_1, \ldots, a_{n-1}) \neq 0$.
Dado que $(a_1, \ldots, a_n) \in Rep_n(S_i)$, obtenemos del lema 10 que $(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(S_i)$. Por tanto existe una variedad irreducible V con $(b_1, \ldots, b_{n-1}) \in RZ_{n-1}(S_i)$ como punto genérico y tal que $(a_1, \ldots, a_{n-1}) \in V$. Dado que $lc(g_i)(a_1, \ldots, a_{n-1}) \neq 0$ tiene que ser $lc(g_i)(b_1, \ldots, b_{n-1}) \neq 0$ por definición de punto genérico. Por tanto se verifican todas las hipótesis para aplicar el lema 11

y por lo tanto obtenemos que existe un cero b_n de $g_i(b_1, \ldots, b_{n-1}, x_n)$ tal que $(a_1, \ldots, a_n) \in V'$, donde V' es la variedad irreducible con $(b_1, \ldots, b_n)$ como punto genérico.

Como $(b_1, \ldots, b_{n-1}) \in RZ_{n-1}(S_i)$, entonces $(b_1, \ldots, b_n) \in RZ_n(S_i \cup \{g_i\})$. Dado que $lc(g_i)(a_1, \ldots, a_{n-1}) \neq 0$ y $g_i(a_1, \ldots, a_n) = 0$ entonces $g_i \notin K[x_1, \ldots, x_{n-1}]$. Se sigue por construcción de $\mathbf{solve}_n$, que $S_i \cup \{g_i\} \in O$. Como $(a_1, \ldots, a_n)$ pertenece a la variedad irreducible con $(b_1, \ldots, b_n)$ como punto genérico, por la definición de Rep_n y el hecho de que $(b_1, \ldots, b_n) \in RZ_n(S_i \cup \{g_i\})$ entonces $(a_1, \ldots, a_n) \in Rep_n(S_i \cup \{g_i\})$ y por tanto

$$(a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep_n(R').$$

Caso 3: Si $g_i \neq 0$ y $lc(g_i)(a_1, \ldots, a_{n-1}) = 0$.
Dado que $(a_1, \ldots, a_{n-1})$ es un elemento de $Rep_{n-1}(S_i)$ tenemos también que

$$(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(S_i \cap K[x_1, \ldots, x_{n-2}]),$$

(se reduce el número de polinomios que describen la cadena regular por tanto hay menos restricciones y hay más elementos en la variedad). Además por la definición de cero regular $(a_1, \ldots, a_{n-1})$ anula al único elemento de $S_i - K[x_1, \ldots, x_{n-2}]$, si existiera, y por hipótesis anula también a $lc(g_i)$. Por lo tanto $(a_1, \ldots, a_{n-1}) \in V(S_i - K[x_1, \ldots, x_{n-2}] \cup \{lc_n(g_i)\})$, por la especificación 2 de $\mathbf{solve}_{n-1}$ existe un $S \in M$ con $(a_1, \ldots, a_{n-1}) \in Rep_{n-1}(S)$ y de aquí $(a_1, \ldots, a_n) \in Rep_n(S)$. Además ya sabemos que $(a_1, \ldots, a_n) \in V_n(F)$. Como ya hemos visto que $S \prec R$ podemos aplicar la hipótesis de inducción sobre $\mathbf{solve}_n(S, F)$ y obtenemos que

$$(a_1, \ldots, a_n) \in \bigcup_{\overline{R} \in \overline{O}} Rep_n(\overline{R}),$$

donde $\overline{O}$ es el conjunto salida de $\mathbf{solve}_n(S, F)$. Como por construcción $\overline{O}$ es un elemento de O entonces tenemos que

$$(a_1, \ldots, a_n) \in \bigcup_{R' \in O} Rep_n(R').$$

Con lo que hemos probado que:

$$Rep_n(R) \cap V_n(F) \subseteq \bigcup_{R' \in O} Rep_n(R').$$

Probemos ahora la otra contención, sea $R' \in O$, $(a_1, \ldots, a_n) \in Rep_n(R')$, y $(b_1, \ldots, b_n) \in RZ_n(R')$ tal que $(a_1, \ldots, a_n) \in V$, donde V es la variedad irreducible en $\overline{K}^n$ con $(b_1, \ldots, b_n)$ como punto genérico. Si existe un $S \in M$ tal que R' es un elemento del conjunto de salida de $\mathbf{solve}_n(S, F)$, podemos aplicar la hipótesis de inducción para deducir que $(a_1, \ldots, a_n) \in V_n(F)$.

Si no ocurre esto entonces existe un $i \in \{1, \ldots, l\}$ tal que $R'_{n-1} = S_i$. De aquí se obtiene por la definición de cero regular que $(b_1, \ldots, b_{n-1}) \in RZ_{n-1}(S_i)$. Veamos que $g_i(a_1, \ldots, a_n) = 0$ tanto si R' es de la forma S_i como si es de la forma $S_i \cup \{g_i\}$, en el primer

caso por la construcción del algoritmo $g_i = 0$ y por tanto $g_i(b_1, \ldots, b_n) = 0$. Si $R' = S_i \cup \{g_i\}$ entonces para que se verifique la definición de cero regular de una cadena regular tiene que ser también $g_i(b_1, \ldots, b_n) = 0$. Puesto que $g_i(b_1, \ldots, b_{n-1}, x_n)$ es el máximo común divisor de los polinomios de $\{f(b_1, \ldots, b_{n-1}, x_n) \mid f \in F\}$, entonces si $(b_1, \ldots, b_n)$ anula al máximo común divisor también anulará a todos los polinomios del conjunto F, por tanto tenemos que

$$(b_1, \ldots, b_n) \in V_n(F).$$

De aquí obtenemos, puesto que $(a_1, \ldots, a_n)$ pertenece a la variedad irreducible con $(b_1, \ldots, b_n)$ como punto genérico que $(a_1, \ldots, a_n) \in V_n(F)$. Con lo que se demuestra:

$$\bigcup_{R' \in O} Rep_n(R') \subseteq V_n(F).$$

Con lo que queda demostrada la especificación y con ello se termina la prueba de la corrección del algoritmo.

Capítulo 7

Aplicaciones de los algoritmos

Una vez que hemos encontrado un algoritmo que resuelve el problema de encontrar un conjunto de cadenas regulares $M = \{R_1, \ldots, R_l\}$ de forma que dado un conjunto $F = \{f_1, \ldots, f_k\}$ se verifique:

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i).$$

Vamos a ver qué posibles aplicaciones puede tener el encontrar esta representación mediante cadenas regulares.
Antes de nada vamos a probar que:

$$\bigcup_{i=1}^{l} Rep_n(R_i) = \emptyset \Leftrightarrow M = \emptyset. \tag{7.1}$$

Por definición de $Rep_n(R_i)$ tenemos que probar que

$$\bigcup_{i=1}^{l} \left(\bigcup_{V \in AIV_n(R_i)} V \right) = \emptyset \Leftrightarrow M = \emptyset,$$

pero la parte de la izquierda es vacía si y solamente si $AIV_n(R_i) = \emptyset \ \forall i = 1, \ldots, l$. Dado que todo punto es punto genérico de una variedad irreducible $AIV_n(R_i) = \emptyset \ \forall i = 1, \ldots, l$ si y solo $RZ_n(R_i) = \emptyset \ \forall i = 1, \ldots, l$. Y por la definición de cero regular el conjunto de ceros regulares es vacío si y solo si $R_i = \emptyset \ \forall i = 1, \ldots, l$ y esto ocurre si y solo si $M = \emptyset$.

Veamos las distintas aplicaciones del algoritmo:

7.1. Calcular la dimensión de una variedad y de un ideal

Teorema 7.1.1. *Sea R una cadena regular en $K[x_1, \ldots, x_n]$. Entonces $Rep_n(R)$ se descompone en variedades todas ellas de dimensión $n - |R|$ y por tanto*

$$dim(Rep_n(R)) = n - |R|$$

Demostración: Por definición,

$$Rep_n(R) = \bigcup_{V \in AIV_n(R)} V.$$

Sea $V \in AIV_n(R)$ y $(a_1, \ldots, a_n) \in RZ_n(R)$ un punto genérico de V. Si utilizamos la definición de $RZ_n(R)$, vemos que se añade un elemento trascendente cuando no hay ningún polinomio que dependa de la última variable, por tanto vamos a añadir n menos el número de polinomios en la cadena regular es decir, $n - |R|$. Y por ello todas las variedades tienen dimensión $n - |R|$. Utilizando que una variedad arbitraria descompone en variedades irreducibles y que su dimensión es la dimensión de la variedad con dimensión más grande dentro de estas obtenemos que:

$$dim(Rep_n(R)) = n - |R|$$

□

De la fórmula (7.1) y del teorema anterior obtenemos que:

$$dim(V(F)) = -1 \Leftrightarrow M = \emptyset \tag{7.2}$$

$$dim(V(F)) = n - min(|R_1|, \ldots, |R_l|) \Leftrightarrow M \neq \emptyset \tag{7.3}$$

Dado que el ideal $\mathcal{A} = (F)$, tiene la misma dimensión que $V(F)$ podemos usar lo anterior para determinar la dimensión de $\mathcal{A}$.

7.2. Resolver sistemas de ecuaciones algebraicas

Lo primero de todo, podemos decidir si el sistema

$$f_1 = 0, \ldots, f_k = 0$$

tiene ninguna, finitas, o infinitas soluciones: es consecuencia de (7.2) y (7.3) que

1. el sistema no tiene soluciones $\Leftrightarrow M = \emptyset$
2. el sistema tiene finitas soluciones $\Leftrightarrow M \neq \emptyset$ y $|R_i| = n \ \ \forall i \in \{1, \ldots, l\}$
3. el sistema tiene infinitas soluciones $\Leftrightarrow$ existe un $R \in M$ con $|R| < n$

Tenemos la representación de una variedad en términos de cadenas regulares,

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i).$$

Para todo $i \in \{1, \ldots, l\}$, $RZ_n(R_i)$ es el subconjunto de $Rep_n(R_i)$ que contiene a aquellos elementos que son punto genérico de una de las variedades irreducibles asociadas a R_i. Sabemos que si $Rep_n(R_i)$ tiene finitos elementos entonces las variedades irreducibles que lo componen tendrán también finitos elementos y por ello serán cero-dimensionales y su ideal asociado también por lo tanto por el teorema 2.4.2 todos los puntos son genéricos y tendremos que

$$Rep_n(R_i) = RZ_n(R_i).$$

Cada uno de los conjuntos $RZ_n(R_1), \ldots, RZ_n(R_l)$ se puede calcular por sustitución.

En el caso en que la variedad no sea cero-dimensional el cálculo de $RZ_n(R_i)$ nos proporcionará todos los puntos genéricos de la variedad, por lo tanto a partir de ellos podremos describir la variedad.

Ejemplo 7.2.1. *Consideramos el siguiente sistema de ecuaciones:*

$$f_1 := x_1 + x_2 + x_3 + x_4,$$

$$f_2 := x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1,$$

$$f_3 := x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2,$$

$$f_4 := x_1x_2x_3x_4 - 1 \ .$$

Supongamos que hemos calculado la representación mediante un número finito de cadenas regulares de la variedad $V_4(\{f_1, f_2, f_3, f_4\})$. Tenemos que que la variedad se representa por una sola cadena regular, es decir:

$$V_4(\{f_1, f_2, f_3, f_4\}) = Rep_4(R), \ \ donde \ \ R := \{x_1^2x_2^2 - 1, x_3 + x_1, x_4 + x_2\}.$$

Calculemos la dimensión, vimos que $dim(V(F)) = n - min(|R_1|, \ldots, |R_l|)$ y en este caso solo hay una cadena de dimensión 3 y la dimension total es 4, obtenemos que la dimensión de la variedad es 1. Calcularemos $RZ_4(R)$, iremos calculando $RZ_1(R)$,$RZ_2(R)$,$RZ_3(R)$ y $RZ_4(R)$. Para ello aplicaremos la definición. Sabemos que $RZ_1(R) = \{a | a \in \overline{\mathbb{Q}} \ trascendente \ sobre \ \mathbb{Q}\}$, esto se debe a que no hay polinomios solo en la variable x_1. Tenemos que

$$R \cap K[x_1, x_2] = \{x_1^2x_2^2 - 1\}.$$

Por tanto
$RZ_2(\{x_1^2x_2^2 - 1\}) = \{(a, 1/a) | a \in \overline{\mathbb{Q}} \ trascendente \ sobre \ \mathbb{Q}\}$
$\cup\{(a, -1/a) | a \in \overline{\mathbb{Q}} \ trascendente \ sobre \ \mathbb{Q}\},$
esto se debe a la definición de cero regular y a que $x_1^2x_2^2 - 1 = (x_1x_2 - 1)(x_1x_2 + 1)$, ahora calculamos $RZ_3(R \cap K[x_1, \ldots, x_3])$, como tenemos que esta intersección añade el polinomio $x_3 + x_1$ tenemos que

$$RZ_3(\{x_1^2x_2^2 - 1, x_3 + x_1\}) = \{(a, 1/a, -a) | a \in \overline{\mathbb{Q}} \ trascendente \ sobre \ \mathbb{Q}\}$$

$$\cup\{(a, -1/a, -a) | a \in \overline{\mathbb{Q}} \ trascendente \ sobre \ \mathbb{Q}\}.$$

Ahora calculamos $RZ_4(R)$ como añadimos el polinomio $x_4 + x_2$ tenemos que:

$$RZ_4(R) = \{(a, 1/a, -a, -1/a) | a \in \overline{\mathbb{Q}} \ trascendente \ sobre \ \mathbb{Q}\}$$

$$\cup\{(a, -1/a, -a, -1/a) | a \in \overline{\mathbb{Q}} \ trascendente \ sobre \ \mathbb{Q}\}.$$

Con esto se obtienen los ceros genéricos de dos variedades irreducibles, a partir de ellos se obtendrá la descripción de la variedad al completo en este caso por ejemplo obtenemos

$$V_4(\{f_1, f_2, f_3, f_4\} = \{(a, 1/a, -a, -1/a), \ \ a \in \overline{\mathbb{Q}}\} \cup \{(a, -1/a, -a, -1/a), \ \ a \in \overline{\mathbb{Q}}\}$$

7.3. Pertenencia a un radical

Al igual que en apartados anteriores tenemos:

$$V_n(F) = \bigcup_{i=1}^{l} Rep_n(R_i).$$

Utilizando el algoritmo $\mathbf{separate}_n$ podemos decidir la pertenencia al radical de un polinomio g. Sea $I = (F)$, sea $J = \sqrt{I}$ y sea $g \in K[x_1, \ldots, x_n]$ un polinomio. Por el Teorema de los ceros de Hilbert, tenemos que $g \in J$ si y solo si $g \in \mathbf{I}(\mathbf{V}(F))$. Es decir que g se anule en $\mathbf{V}(F)$. Veamos que g se anula en $\mathbf{V}(F)$ si y solo si para todo $i \in \{1, \ldots, l\}$, $\mathbf{separate}_n(R_i, g_i) = \emptyset$. Tenemos que g se anula en $V(F) = \bigcup_{i=1}^{l} Rep(R_i)$ si y solo si se anula en $Rep_n(R_i)$ para todo $i \in \{1, \ldots, l\}$. Por definición de punto genérico esto pasa si y solo si g se anula en el punto genérico y por por definición de Rep_n se anulará si y solo si se anula para todo $a \in RZ_n(R_i)$. Por especificación de $\mathbf{separate}_n$, $g(a) = 0$ para todo $a \in RZ_n(R_i)$ si y solo si $\mathbf{separate}_n(R_i, g) = \emptyset$ para todo $i \in \{1, \ldots, l\}$.

Bibliografía

[1] M. Kalkbrener, *A generalized Euclidean algorithm for computing triangular representations of algebraic varieties*, Journal of Symbolic Computation 15, 143-167, 1993.

[2] B. L. van der Waerden, *Modern Algebra Volume I*, segunda edición , 1949.

[3] B. L. van der Waerden, *Modern Algebra Volume II*, quinta edición, 1967.

[4] D. Cox, J. Little y D. O'Shea, *Ideals, Varieties and Algorithms*, tercera edición, 2006.

[5] R. Mines, F. Richman y W. Ruitenburg, *A Course in Constructive Algebra*, 1988.

[6] P. M. Cohn, MA, PhD, FRS, *Basic Algebra*, 2003

[7] P. Aubry, D. Lazard y M. Moreno Maza, *On the Theories of Triangular Sets*, 1999

[8] F. Boulier, F. Lemaire, A. Poteaux y M. Moreno Maza, *An equivalence theorem for regular differential chains*, Journal of Symbolic Computation 93, 34-55, 2019

[9] C. Chen y M. Moreno Maza, *Algorithms for Computing Triangular Decompositions of Polynomial Systems*, 2011

[10] *http://www.regularchains.org/index.html*