USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Resolvendo ecuacións alxébricas con autovalores e autovectores

Guillermo Portela Vázquez

2022/2023

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Resolvendo ecuacións alxébricas con autovalores e autovectores

Guillermo Portela Vázquez

Setembro, 2023

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: Resolvendo ecuacións alxébricas con autovalores e autovectores
Breve descrición do contido
O obxectivo deste TFG é atopar as solucións dun sistema de ecuacións polinómicas $f_1 = f_2 = \cdots = f_s = 0$ sobre o corpo dos números complexos $\mathbb{C}$, cando o sistema só ten un número finito de solucións. Neste caso, a álxebra $A = \mathbb{C}[x_1, \ldots, x_n]/I$, onde $I = \langle f_1, f_2, \ldots, f_s \rangle$, é un espazo vectorial de dimensión finita sobre $\mathbb{C}$. A idea é aproveitar a estrutura de A para avaliar un polinomio arbitrario f nos puntos da variedade $V(I)$; en particular, a avaliación dos polinomios $f = x_i$ dá as coordenadas dos puntos. Os valores de f en $V(I)$ resultan ser autovalores de certas aplicacións lineais en A. Analizaranse técnicas para calcular estes autovalores e mostrarase que os correspondentes autovectores conteñen información útil sobre as solucións.
Bibliografía
D. A. Cox, J. Little, D. O' Shea, *Using Algebraic Geometry*, 2 ed., Springer, 2005.
Recomendacións (non vinculantes)
É recomendable cursar a materia optativa "Álxebra, Números e Xeometría".

Índice general

Resumen

Este trabajo se enmarca dentro de los métodos computacionales para resolver sistemas de ecuaciones polinómicas en varias variables que surgen a partir de 1965. El principal objetivo es dar herramientas para determinar si, dado un sistema de ecuaciones polinómicas en varias variables en el cuerpo de los números complejos, el conjunto de puntos que conforman su solución es finito. De serlo, aprovechar los cálculos hechos hasta ese punto; buscar autovalores y autovectores de ciertas aplicaciones y, con todo ello, intentar encontrar las coordenadas de dichos puntos. También se hace un pequeño recorrido acerca de distintos conceptos teóricos que envuelven al problema en general como relaciones entre variedades e ideales. Al mismo tiempo nos ayudamos de la herramienta informática SAGE para realizar ejemplos concretos de dichas ideas y procedimientos que se desarrollan a lo largo del documento como pueden ser división de polinomios; calcular bases de Gröbner; tablas de multiplicar del Álgebra involucrada en el proceso y resolver un par de sistemas de ecuaciones polinómicas. Finalmente se comentan pequeñas complicaciones que pueden surgir y formas de intentar evitarlas.

Abstract

This piece of work is framed within the computational methods concieved to solve polynomial equations on multiple variables that arose since 1965. The main objective is to provide mechanisms to determine, given a system of polynomial equations on multiple variables over the complex field, whether the set of solutions is finite or not. If it happens to be finite then take advantage from the calculations done up to that point; find eigenvalues and eigenvectors of certain applications and use all that information on trying to determine the coordinates of the aforementioned points. In addition we will explore theoretical concepts that surround the problem, such as relations between varieties and ideals. At the same time we will use the informatic tool SAGE to work on concrete examples of

named ideas and procedures that are developed throughout the document such as polynomial division; Gröbner basis computations; Multiplication tables of the algebra involved in the process and solving a couple of systems of polynomial equations. Finally we make a commentary upon little complications that might arise and ways to avoid them.

Introducción

Resolver distintos tipos de sistemas de ecuaciones constituye uno de los mayores paradigmas de las matemáticas. Estos surgen en cualquiera de sus disciplinas y su utilidad es casi incuestionable. En este documento se trabaja sobre un tipo concreto de ellas, las ecuaciones polinómicas en varias variables, las cuales son un ejemplo del fuerte vínculo entre la geometría y el álgebra.

La introducción de las bases de Gröbner en 1965 gracias a Bruno Buchberger [1] supuso un gran avance para trabajar con ciertas álgebras estrechamente relacionadas con las soluciones de un sistema polinómico de ecuaciones, permitiendo realizar divisiones de polinomios sin ambigüedades y, además, al mismo tiempo Buchberger proporcionó un algoritmo que permitía calcular dichas bases. Gracias a esto, se han podido desarrollar computacionalmente distintos métodos como el método de eliminación, por resultantes, por autovalores o por autovectores. En el presente trabajo exploramos estos dos últimos. El objetivo principal será resolver aquellos sistemas de ecuaciones polinómicas en los cuales el conjunto de puntos que los solucionan es finito, encontrando relaciones entre las coordenadas de los puntos buscados, los autovalores de ciertas aplicaciones lineales y los autovectores de otras, ayudandonos de la herramienta informática SAGE durante el proceso. Sin embargo, también se pretenden exponer los distintos conceptos y estructuras teóricas que subyacen al problema de partida y que también son usados en otros ámbitos del álgebra.

Estructuralmente, este trabajo está dividido en 5 capítulos. En el primero, se recuerdan brevemente ciertos conceptos sobre polinomios vistos en la asignatura Estructuras Algebraicas, profundizando especialmente en el los conceptos de ideal de un anillo, el anillo de polinomios y el radical de un ideal. Además se proporciona un algoritmo para realizar divisiones de polinomios en varias variables. En el segundo capitulo, se introducen los conceptos de bases de Gröbner, su utilidad, un algoritmo para calcularlas a mano e instrucciones para calcularlas con SAGE. También en este segundo capítulo se habla de las variedades afines, mostrando algunos resultados sobre cuestiones conjuntistas acerca de ellas y evidenciando que el conjunto de puntos que queremos encontrar se trata de una variedad afín. En el tercer capítulo, se dan herramientas para trabajar sobre el álgebra obtenida al cocientar el

anillo de polinomios por un ideal dado. Tales herramientas son las que permiten decidir si el sistema de ecuaciones tiene o no una cantidad finita de soluciones. En el cuarto, se explica y demuestra el método de resolución por autovalores además de resolver un ejemplo a modo ilustrativo. Por último en el quinto se expone el método de resolución por autovectores, el cual, en muchos de los casos, supone una mejora computacional respecto al método por autovalores. En este capítulo se resuelve de nuevo un ejemplo y además se expone como ambos métodos se pueden usar coordinadamente para resolver casos más problemáticos.

Capítulo 1

CONOCIMIENTOS PREVIOS SOBRE EL ANILLO DE POLINOMIOS

1.1. Ideales, radical de un ideal e ideales de eliminación

Se recuerda que, dado un cuerpo $\mathbb{K}$ y unas variables $\{x_1, x_2, \ldots, x_n\}$, el conjunto de los polinomios con coeficientes en $\mathbb{K}$ en esas variables forma un anillo que denotaremos por $\mathbb{K}[x_1, x_2, \ldots, x_n]$.

Definición 1.1. (Grado total de un monomio)

Dado un monomio $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ que denotaremos, cuando no haya riesgo de confusión, por x^α donde $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$ es el vector de exponentes del monomio. Llamaremos grado total de x^α a $\alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Ejemplo 1.2. Consideremos $\mathbb{K} = \mathbb{Q}$ y $n = 3$. Sea $x^\alpha = x_1^5 x_2^0 x_3^{140} = x_1^5 x_3^{140}$ se tiene que el grado total de x^α es $5 + 0 + 140 = 145$.

Nos preguntamos cómo son los ideales del anillo $\mathbb{K}[x_1, x_2, \ldots, x_n]$.

Supongamos que tenemos un conjunto de polinomios $A = \{P_1, P_2, P_3 \ldots\}$, no necesariamente finito. Para que A sea un ideal debe verificar las siguientes condiciones:

1. Dados $P, Q \in A$ entonces $P + Q \in A$.

2. Dados $P \in A, S \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ entonces $SP \in A$.

Por otra parte, dada una cantidad finita de r polinomios $f_1, f_2, \ldots, f_r$, consideramos el conjunto $\langle f_1, f_2, \ldots, f_r\rangle = \{p_1f_1 + p_2f_2 + \cdots + p_rf_r : p_i \in \mathbb{K}[x_1, x_2, \ldots, x_n], i = 1, \ldots, r\}$. Se tiene que $\langle f_1, f_2, \ldots, f_r\rangle$ cumple las condiciones para ser un ideal.

Demostración. Se tiene que:

- $P, Q \in \langle f_1, f_2, \ldots, f_r\rangle \iff [P = p_1f_1 + p_2f_2 + \cdots + p_rf_r, Q = q_1f_1 + q_2f_2 + \cdots + q_rf_r]$ de donde $P + Q = p_1f_1 + p_2f_2 + \cdots + p_rf_r + q_1f_1 + q_2f_2 + \cdots + q_rf_r = f_1(p_1 + q_1) + f_2(p_2 + q_2) + \cdots + f_r(p_r + q_r) = \widehat{p_1}f_1 + \widehat{p_2}f_2 + \cdots + \widehat{p_r}f_r \in \langle f_1, f_2, \ldots, f_r\rangle$ donde $\widehat{p_i} = (p_i + q_i), i = 1, \ldots, r$. Por lo que se cumple la primera condición.
- Sea ahora $P \in \langle f_1, f_2, \ldots, f_r\rangle, P = p_1f_1 + p_2f_2 + \cdots + p_rf_r$ y S un polinomio cualquiera de $\mathbb{K}[x_1, x_2, \ldots, x_n]$ se tiene que $SP = Sp_1f_1 + Sp_2f_2 + \cdots + Sp_rf_r = \widehat{p_1}f_1 + \widehat{p_2}f_2 + \cdots + \widehat{p_r}f_r \in \langle f_1, f_2, \ldots, f_r\rangle$ donde $\widehat{p_i} = Sp_i,\ i = 1, \ldots, r$. Por lo que se cumple también la segunda.

□

Por este motivo diremos que $\langle f_1, f_2, \ldots, f_r\rangle$ es el ideal generado por los polinomios $f_1, f_2, \ldots, f_r$, o equivalentemente que $\{f_1, f_2, \ldots, f_r\}$ es un conjunto generador del ideal $I = \langle f_1, f_2, \ldots, f_r\rangle$.
Es natural preguntarse si ocurre el recíproco, es decir ¿para todo ideal I de $\mathbb{K}[x_1, x_2, \ldots, x_n]$ existe un conjunto de polinomios $\{f_1^I, f_2^I, \ldots, f_r^I\}$ tal que $I = \langle f_1^I, f_2^I, \ldots, f_r^I\rangle$? La respuesta es afirmativa y la proporciona uno de los teoremas más importantes sobre el anillo de polinomios en varias variables.

Teorema 1.3. *(De la base de Hilbert)*
Todo ideal $I \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ admite un conjunto finito generador.

La prueba de este resultado se proporcionará una vez introducidos los ordenes monomiales y el algoritmo de división.

Observación 1.4. Nótese que el resultado anterior sería trivial para anillos de polinomios sobre una variable pues ya sabemos que estos son Dominios de Ideales Principales (DIP). Sin embargo $\mathbb{K}[x_1, x_2, \ldots, x_n]$ no es DIP, pues el ideal $I = \langle x_1, \ldots, x_n\rangle$ no admite un elemento generador.

Ahora procedemos a construir dos nuevos tipos de ideales en $\mathbb{K}[x_1, x_2, \ldots, x_n]$ a partir de otro dado.

Definición 1.5. Dado un ideal $I \in \mathbb{K}[x_1, x_2, \ldots, x_n]$, definimos el radical de I, $\sqrt{I}$, como $\sqrt{I} := \{P \in \mathbb{K}[x_1, x_2, \ldots, x_n] : \exists n_0 \in \mathbb{N}, P^{n_0} \in I\}$.

Proposición 1.6. *El radical de un ideal I es también un ideal de $\mathbb{K}[x_1, x_2, \ldots, x_n]$, y claramente $I \subset \sqrt{I}$.*

Demostración. Comprobar la segunda condición de ideal es muy sencillo. Sea $P \in \sqrt{I}$, sea $n_0 \in \mathbb{N}$ tal que $P^{n_0} \in I$ y sea $S \in \mathbb{K}[x_1, x_2, \ldots, x_n]$, se tiene que $(SP)^{n_0} = S^{n_0}P^{n_0} \in I$. La primera condición es un poco más delicada pero de idea sencilla. Sean $P, Q \in \sqrt{I}$ y sean $n_p, n_q \in \mathbb{N}$ tales que $P^{n_p}, Q^{n_q} \in I$. Basta fijarse en que los sumandos del binomio $(P+Q)^{n_p+n_q-1}$ son todos de la forma $\alpha P^r Q^s$ donde α es un coeficiente perteneciente a la fila $n_p + n_q$-ésima del triangulo de Pascal, y como $r + s = n_p + n_q - 1$ entonces $r \geqslant n_p$ o $s \geqslant n_q$ por lo que $(P+Q)^{n_p+n_q-1}$ es una suma de elementos en el ideal I y por tanto está en I.

□

Definición 1.7. Un ideal I se le llama ideal radical si cumple $I = \sqrt{I}$.

Definición 1.8. Dado un ideal $I \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ se define el l-ésimo ideal de eliminación de I como $I_l := I \cap \mathbb{K}[x_{l+1}, x_{l+2}, \ldots, x_n]$ donde $l \in \mathbb{N}, l \geqslant 1$, que es claramente un ideal por ser intersección de ideales.

1.2. División de polinomios

Una vez visto el algoritmo de división de polinomios en una variable queremos extenderlo para polinomios en $\mathbb{K}[x_1, \ldots, x_n]$. Para ello tenemos que encontrar alguna forma de ordenar los distintos monomios que tiene un polinomio. Este orden va a tomar un papel parecido al que toma el grado en la división en una variable.

Definición 1.9. Una relación $>$ definida en el conjunto de monomios de $\mathbb{K}[x_1, x_2, \ldots, x_n]$ se llama orden monomial si verifica:

1. La relación $>$ es un orden total en $\mathbb{K}[x_1, x_2, \ldots, x_n]$. Es decir, dados dos monomios x^α, x^β cualesquiera siempre podemos decidir cual de las 3 siguientes opciones se verifica:
   - $x^\alpha > x^\beta$
   - $x^\beta > x^\alpha$
   - $x^\alpha = x^\beta$.
2. El conjunto $\mathbb{K}[x_1, x_2, \ldots, x_n]$ con el orden $>$ es un conjunto bien ordenado. Es decir, todo subconjunto no vacío de monomios tiene un elemento mínimo.

3. $x^\alpha > x^\beta \Longrightarrow x^\gamma x^\alpha > x^\gamma x^\beta \ \forall x^\gamma \in \mathbb{K}[x_1, x_2, \ldots, x_n]$.

Es fácil verificar que el único orden monomial posible en $\mathbb{K}[x]$ es el dado por el grado, lo cual ayuda a comprender el orden monomial como una posible extensión del concepto de grado de un monomio distinto al del grado total. Notar que el grado total no es un orden total en $\mathbb{K}[x_1, x_2, \ldots, x_n]$.

1.2.1. Algunos órdenes monomiales clásicos

Cuando se trabaja en varias variables surgen distintos órdenes monomiales y cada uno tiene ventajas y defectos. Veamos tres de los más usados.

Definición 1.10. (Orden Lexicográfico)
Decimos que $x^\alpha > x^\beta$ en orden lexicográfico si $\alpha - \beta \in \mathbb{Z}^n$ tiene su primer coeficiente no nulo por la izquierda positivo, y lo denotamos por $x^\alpha >_{lex} x^\beta$.

Definición 1.11. (Orden Graduado Lexicográfico) Decimos que $x^\alpha >_{grlex} x^\beta$ si el grado total de x^α es mayor que el de x^β o, de tener el mismo grado total, si $x^\alpha >_{lex} x^\beta$.

Definición 1.12. (Orden Reverso Graduado Lexicográfico)
Decimos que $x^\alpha >_{grevlex} x^\beta$ si el grado total de x^α es mayor que el de x^β o, de tener el mismo grado total, si $\alpha - \beta \in \mathbb{Z}^n$ tiene su primer coeficiente no nulo por la derecha negativo.

Ejemplo 1.13. $x_1 >_{lex} x_2^2$ pero $x_2^2 >_{grlex} x_1$. Por otra parte $x_1^3 x_3^3 >_{lex} x_2^6$ pero $x_2^6 >_{grevlex} x_1^3 x_3^3$.

Definición 1.14. Dado un polinomio $f = \sum_{i=0}^{n} c_i x_i^{\alpha_i}$ y un orden monomial $>$ definimos el término líder de f, que en inglés suelen denotar con $lt(f)$, como el elemento $c_j x^{\alpha_j}$ donde x^{α_j} es el mayor monomio de f en el orden monomial dado.

Definición 1.15. Dado un ideal I y un orden $>$ definimos el ideal "líderes de I", que denotamos por $\langle lt(I) \rangle$ o $\langle lt(I) \rangle_>$ si no está claro al orden escogido, como el ideal generado por el conjunto $\{lt(f) : f \in I\}$.

Una vez vistas estas definiciones procedemos a explicar cómo dividir polinomios en $\mathbb{K}[x_1, x_2, \ldots, x_n]$ a través de un ejemplo. Aún así, puede demostrarse que el procedimiento funciona para cualquier caso planteado en las siguientes condiciones.

- Objetivo del algoritmo de la división en $\mathbb{K}[x_1, x_2, \ldots, x_n]$.
  Queremos dividir el polinomio $f \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ por un conjunto de s polinomios $G = \{g_1, g_2, \ldots, g_s\}$ de forma que f quede expresado del siguiente modo:

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_s g_s + r \tag{1.1}$$

  Donde los q_i con $i \in \{1, \ldots, s\}$ y r son también polinomios en $\mathbb{K}[x_1, x_2, \ldots, x_n]$ y además ningún monomio de r es divisible por ningún $lt(g_i), i \in \{1, \ldots, s\}$.

Es fácil ver la similitud de esta expresión respecto a la proporcionada por el algoritmo de división para polinomios de una variable. Al dividir entre varios polinomios, en vez de uno surgen varios cocientes q_i. Por otra parte, el resto r pasa de verificar una condición sobre el grado a verificar una de divisibilidad.

1.2.2. Ejemplo del algoritmo

En este ejemplo vamos a considerar $f = x^2y + xy^2 + y^2, G = \{g_1, g_2\}$ donde $g_1 = xy - 1,\ g_2 = y^2 - 1$ y el orden considerado será el lexicográfico $>_{lex}$.
La idea de partida es igual que dividiendo polinomios en una variable: ordenamos en función del grado (ahora orden monomial) y buscamos múltiplos del cociente (ahora múltiplos de g_1 o múltiplos de g_2) de forma que nos permita reducir el orden de $lt\,(f)$.
Tanto $lt\,(g_1) = xy$ como $lt\,(g_2) = y^2$ dividen a $lt\,(f) = x^2y$. En esta situación empezamos dividiendo siguiendo el orden en el que se nos presenta G, es decir, empezamos a dividir usando g_1. Después comentaremos que ocurre si cambiamos el orden.

	x^2y	$+xy^2$		$+y^2$
xg_1	x^2y		$-x$	
		xy^2	$+x$	$+y^2$

En este punto volvemos a poder dividir $lt\left(xy^2 - x + y^2\right) = xy^2$ con cualquiera de los polinomios de G, así que seguimos con la regla de usar g_1.

	xy^2	x	y^2	
yg_1	xy^2			$-y$
		x	$+y^2$	$+y$

Ahora $lt\left(x+y^2+y\right) = x$ no es divisible por $lt\left(g_1\right) = xy$ ni por $lt\left(g_2\right) = y^2$, sin embargo, $lt(g_2)$ divide a uno de los monomios de $x+y^2+y$ por lo que el algoritmo no ha acabado aún. Realizando este último paso:

	x	$+y^2$	$+y$	
g_2		y^2		-1
	x		$+y$	$+1$

Vemos que ya no se puede avanzar y por tanto el algoritmo concluye y obtuvimos la expresión $f = (x+y)g_1 + (1)\, g_2 + x + y + 1$ donde el resto, al que normalmente llamaremos $\overline{f}^G$ o forma normal de f modulo G, es $x+y+1$.

Observación 1.16.

- Visto este ejemplo es fácil entender como se implementaría el algoritmo en otro caso cualquiera. A partir de ahora para realizar estas divisiones se hará uso de la herramienta SAGE.

- ¿Qué ocurre si en vez de empezar a dividir por g_1 hubiéramos empezado a dividir por g_2? Llegaríamos a la siguiente expresión: $f = (x+1)\, g_2 + xg_1 + 2x + 1$ donde, esta vez, $\overline{f}^G = 2x+1$. Es decir, a diferencia del caso en una variable, el algoritmo no proporciona una expresión única a cada problema. Esto es un defecto grave del algoritmo en varias variables pues, el principal uso que nos gustaría darle es decidir si $f \in \langle f_1, f_2, \ldots, f_r\rangle$ y claramente si $\overline{f}^{\{f_1, f_2, \ldots, f_r\}} = 0$ entonces se cumple que $f \in \langle f_1, f_2, \ldots, f_r\rangle$. Sin embargo sean $f = x_1^2 + \frac{1}{2}x_2^2x_3 - x_3 - 1$, $G = \{g_1, g_2\}$ con $g_1 = x_1^2 + x_3^2 - 1$, $g_2 = x_1^2 + x_2^2 + (x_3-1)^2 - 4$ y $I = \langle G\rangle$ se tiene que, usando $>_{lex}$ $\overline{f}^G = \frac{1}{2}x_2^2x_3 - x_3 - x_3^2 \neq 0$ ¡Pero $f \in I$! pues $f = \left(-\frac{1}{2}x_3 + 1\right) g_1 + \frac{1}{2}x_3 g_2$.

La no unicidad de restos supone, por ahora, un obstáculo. Las técnicas para sortearlo se introducen en el siguiente capítulo.

Para acabar este capítulo, veamos la demostración del teorema de la base de Hilbert, pues había quedado pendiente. Para ello necesitamos antes algún que otro resultado previo.

Definición 1.17. Un ideal I se dice monomial si existe un conjunto $B \subset \mathbb{N}^n$ no necesariamente finito de forma que que todo polinomio $f \in I$ es una suma finita de la forma $\sum_{\alpha} h_\alpha x^\alpha$, donde $h_\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ y $\alpha \in B$. Si en este punto diésemos por cierto el teorema de la base de Hilbert, que I sea un ideal monomial significaría que $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_k}\rangle$.

Proposición 1.18. *Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal y $>$ un orden monomial, entonces se verifica:*

1. *$\langle lt(I)\rangle$ es un ideal monomial.*

2. *Existen $g_1, \ldots, g_s \in I$ verificando $\langle lt(I)\rangle = \langle lt(g_1), \ldots, lt(g_s)\rangle$.*

Probar esta proposición requiere previamente el enunciado y demostración del llamado lema de Dickson. Este se puede encontrar en [2] capítulo 2, sección 4, página 69. Mientras que la demostración de la proposición recién enunciada se encuentra en [2] capítulo 2, sección 5, páginas 73-74.

Ahora sí pasamos a la demostración prometida.

Demostración. (del teorema de la base de Hilbert) Sea I un ideal no nulo, usando la proposición 1.18 tenemos que existen $G = \{g_1, \ldots, g_s\} \subset I$ tales que $\langle lt(I)\rangle = \langle lt(g_1), \ldots, (g_s)\rangle$ veamos que $I = \langle g_1, \ldots, g_s\rangle$. Por un lado como $g_1, \ldots, g_s \in I$ e I es un ideal $\langle g_1, \ldots, g_s\rangle \subset I$, para ver $I \subset \langle g_1, \ldots, g_s\rangle$ consideremos $f \in I$ y veamos que $f \in \langle g_1, \ldots, g_s\rangle$. En efecto, si dividimos f entre G tendremos:

$$f = a_1 g_1 + \cdots + a_s g_s + r.$$

Al despejar r de esa expresión vemos que es una suma de elementos en I, por tanto $r \in I$, pero ello implica $lt(r) \in \langle I\rangle = \langle g_1, \ldots, g_s\rangle$ lo que, por como funciona el algoritmo de división, implica $r = 0$, de forma que:

$$f = a_1 g_1 + \cdots + a_s g_s + 0 \in \langle g_1, \ldots, g_s\rangle.$$

□

Capítulo 2

BASES DE GRÖBNER Y VARIEDADES AFINES

2.1. Bases de Gröbner

Tal y como vimos en el anterior capítulo, al efectuar el algoritmo de la división de un polinomio entre un conjunto G de polinomios puede darse la mala situación de proporcionar un resto distinto de cero y, sin embargo, el polinomio que hemos dividido pertenecer a $\langle G \rangle$. Si encontrásemos una forma de conseguir que si $f \in \langle G \rangle$ el algoritmo de la división proporcione un resto nulo, entonces al considerar el anillo de polinomios $\mathbb{K}[x_1, \ldots,]$ y un ideal $I = \langle G \rangle$ podremos decir con total certeza cuándo un polinomio en el anillo cociente

$$\frac{\mathbb{K}[x_1, \ldots, x_n]}{I}$$

pertenece a la clase del 0. La forma de conseguirlo es construir una base del ideal de la forma adecuada.

Definición 2.1. (Base de Gröbner)
Dados un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ y un orden monomial $>$ en $\mathbb{K}[x_1, \ldots, x_n]$, definimos una base de Gröbner de I respecto al orden $>$ como una colección finita de polinomios $G = \{g_1, \ldots, g_s\}$, tales que $\forall f \in I,\ lt(f)$ es divisible por $lt(g_i)$ para algún i.

La existencia de al menos una base de Gröbner para cada ideal I se tiene por los argumentos dados en la demostración del teorema de la base de Hilbert. A continuación, veamos como construir una base de Gröbner.

Definición 2.2. Sean $F = \{f, g\}$ con $f, g \in \mathbb{K}[x_1, \ldots, x_n]$, $lt(f) = cx^{\alpha}$, $lt(g) = dx^{\beta}$ y

$x^\gamma = mcm\left(x^\alpha, x^\beta\right)$, entonces definimos el S-polinomio de f y g como:

$$S(f,g) = \frac{x^\gamma}{lt(f)}f - \frac{x^\gamma}{lt(g)}g$$

que cumple $S(f,g) \in \langle f, g\rangle$.

- (Criterio de Buchberger) $G = \{g_1, \ldots, g_s\} \in I$ es una base de Gröbner de $I \iff \overline{S(g_i, g_j)}^G = 0$, $\forall i \neq j$, con $i, j \in \{1, \ldots s\}$.
- (Algoritmo de Buchberger) Sea $F = \{f_1, \ldots, f_s\}$ tal que $I = \langle F\rangle$, vamos a ampliar reiteradamente un conjunto G' hasta que sea base de Gröbner. Primeramente, $G' = F$ y en cada paso calculamos $\overline{S(p,q)}^{G'}$ $\forall p \neq q$ con $p, q \in G'$. Si $\overline{S(p,q)}^{G'} \neq 0$ entonces añadimos $\overline{S(p,q)}^{G'}$ a G' hasta que, en algún paso, $\overline{S(p,q)}^{G'} = 0$ $\forall p, q \in G'$, en cuyo caso habremos acabado y nuestra base es G'.

Observación 2.3. (Deficiencias del algoritmo)

1. Notar que el algoritmo empieza con una colección de s elementos y acaba con una base de t elementos con $t \geqslant s$. En este sentido "ser base" implica ser un conjunto de generadores pero ya no tiene garantizado ser minimal (hay conjuntos generadores con menos elementos).

2. El algoritmo descrito es un proceso muy rudimentario y poco eficiente para obtener una base de Gröbner de un ideal dado y se detalla por si se da el terrible caso de tener que calcular una a mano. Las herramientas informáticas tienen implementados algoritmos mucho más eficientes y sofisticados para realizar esa tarea.

Definición 2.4. Una base de Gröbner reducida de un ideal I es una base de Gröbner G de dicho ideal donde, dado $\forall p, q \in G$, con $p \neq q$, se tiene que si x^α es monomio de p, entonces $x^\alpha \notin \langle lt(q)\rangle$ y, además, $\forall p \in G$, con $lt(p) = cx^\alpha$ se tiene que $c = 1$ [1].

Enumeramos aquí dos propiedades muy atractivas de las bases de Gröbner reducidas. Dado un orden monomial $>$ en $\mathbb{K}[x_1, \ldots, x_n]$.

1. Si $f \in I$, con I ideal de $\mathbb{K}[x_1, \ldots, x_n]$ y $G = \{g_1, \ldots, g_t\}$ siendo G base de Gröbner reducida de I en el orden $>$ entonces $\overline{f}^G = 0$. Esta propiedad ya la poseen las bases de Gröbner en general. Esto supone haber encontrado la solución al problema que puntualizábamos al principio del capítulo.

[1] Para [3] una base mónica de Gröbner solo necesita cumplir la primera condición mencionada. Si cumple las dos la llaman base mónica de Gröbner, sin embargo en la mayor parte de la literatura siguen la notación expresada aquí

2. Para todo ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, existe una única base de Gröbner reducida de I para el orden $>$.

Veamos qué instrucciones realizar en SAGE para obtener una base de Gröbner reducida. En este ejemplo vamos a calcular la base de Gröbner reducida del ideal $J = \langle xy - 1, y^2 - 1 \rangle$ en $>_{lex}$. Para ello introducimos en una hoja de cálculo los siguientes comandos:

```
R.<x,y>=PolynomialRing(QQ,order="lex")
f1=x*y-1
f2=y^2-1
J=Ideal([f1,f2])
G=J.groebner_basis()
G
[x - y, y^2 - 1]
```

Obteniendo de resultado: $\left[x - y, y^2 - 1\right]$.

Observación 2.5. Cambiar el orden monomial con el que se trabaja produce distintas bases de Gröbner reducidas de un mismo ideal, y distintos órdenes tienen distintas propiedades. En concreto usar el orden lexicográfico suele eliminar variables (por ejemplo en la calculada arriba el segundo polinomio de la base está en $\mathbb{Q}[y]$) y el orden $>_{grevlex}$ tiende a minimizar el número de cuentas necesarias.

Una observación hecha previamente mencionaba que una base de Gröbner podía no ser un conjunto generador minimal. El siguiente ejemplo ilustra esa posibilidad.

Ejemplo 2.6. Si introducimos las siguientes lineas en SAGE:

```
P.<x,y,z,t>=PolynomialRing(QQ,order="lex")
f1=x^5*t^3*z-y^4*x+t;f2=t^6-x^2+4;f3=y-x*t;f4=x*y^2*z*t-32*y*z
I=Ideal([f1,f2,f3,f4])
F=I.groebner_basis()
F
```

SAGE nos devuelve:

```
[x^2 - t^6 - 4,
x*t + 128*z*t^7 + 1024*z*t^5 + 512*z*t - t^22 - 12*t^16 - 48*t^10 - 64*t^4,
y + 128*z*t^7 + 1024*z*t^5 + 512*z*t - t^22 - 12*t^16 - 48*t^10 - 64*t^4,
z^2*t - 2*z*t^2 + 1/33554432*t^43 + 5/8388608*t^37 + 5/1048576*t^31
+ 5/262144*t^25 + 5/131072*t^19 + 1/32768*t^13 - 1/33554432*t^7,
```

```
z*t^9 + 4*z*t^3 - 32*z*t,t^45 + 24*t^39 - 32*t^37 + 240*t^33 - 640*t^31
+ 1280*t^27 - 5120*t^25 + 3840*t^21 - 20480*t^19
+ 6144*t^15 - 40960*t^13 + 4095*t^9 - 32768*t^7 - 4*t^3 + 32*t]
```

Que se trata de un conjunto con 5 polinomios (cada coma denota el final de un polinomio), mientras que el conjunto generador de partida estaba formado solo por 4. Además se puede observar el efecto mencionado sobre el orden lexicográfico, pues a partir del segundo polinomio de la base se va reduciendo el número de variables involucradas en cada elemento.

2.2. Variedades Afines

Notar que cada polinomio $f \in \mathbb{K}[x_1, \ldots, x_n]$ con $f = \sum_{\alpha} c_\alpha x^\alpha$, $\alpha \in \mathbb{Z}^n$ y $c_\alpha \in \mathbb{K}$ define una función $f : \mathbb{K}^n \to \mathbb{K}$ que a cada punto $(a_1, \ldots, a_n)$ del espacio afín $\mathbb{K}^n$ le asigna el valor resultante de hacer la sustitución $x_i = a_i$ en la expresión de f. Una ecuación polinómica será una ecuación de la forma $f = 0$, donde $f \in \mathbb{K}[x_1, \ldots, x_n]$.

Definición 2.7. (Variedad afín)
Se le llama variedad afín al conjunto de puntos que satisfacen simultáneamente un sistema de ecuaciones polinómicas:

$$f_1(x_1, \ldots, x_n) = 0$$
$$f_2(x_1, \ldots, x_n) = 0$$
$$\vdots$$
$$f_s(x_1, \ldots, x_n) = 0.$$

A dicha variedad afín la denotaremos como $V(f_1, \ldots, f_s)$.

Uno de los elementos más estudiados por la geometría son los puntos del espacio afín $\mathbb{R}^n, n \geqslant 1$ que satisfacen una ecuación polinómica. Por ejemplo, si en $n = 3$ consideramos la ecuación $x^2 + y^2 + z^2 - 9 = 0$, los puntos que la satisfacen son los de una esfera de radio 3. Siguiendo entonces la definición de variedad afín tenemos que los puntos de una esfera forman una variedad afín (donde el sistema de ecuaciones polinómicas esta formado por una sola ecuación). Sin embargo, este trabajo se va a centrar únicamente en aquellas variedades afines que tengan un conjunto finito de puntos.

Proposición 2.8. *Se verifica que:*

1. *La unión finita de variedades afines es una variedad afín.*
2. *La intersección finita de variedades afines es una variedad afín.*

3. Todo conjunto finito de $\mathbb{K}^n$ es una variedad afín.

Demostración. Comprobar (1) es muy fácil. Sean $V = V(f_1, \dots, f_s)$, $W = V(g_1, \dots, g_t)$ dos variedades afines, si $a = (a_1, \dots a_n) \in V \cap W \Longrightarrow f_i(a) = 0 = g_j(a)\ \forall i \in \{1, \dots s\}$, $j \in \{1, \dots t\}$ y por tanto $V \cap W = V(f_1, \dots, f_s, g_1, \dots, g_t)$.

Para probar (2) veamos que $V \cup W = V(f_i g_j : i \in \{1, \dots s\}, j \in \{1, \dots t\})$. Primeramente, si $a \in \mathbb{K}^n$ verifica $f_i(a) = 0$ para un cierto subíndice i, entonces $f_i g_j(a) = f_i(a) g_j(a) = 0 g_j(a) = 0,\ \ \forall j \in (1, \dots t)$ y por tanto $V \subset V(f_i, g_j)$. Análogamente se ve que $W \subset V(f_i g_j)$ y por tanto $V \cup W \subset V(f_i g_j)$. Para probar el otro contenido supongamos $a \in V(f_i g_j)$. Si $a \in V$ entonces ya tenemos que $a \in V \cup W$ pero si $a \notin V$ entonces existe i_0 tal que $f_{i_0}(a) \neq 0$ pero como $f_{i_0} g_j(a) = 0\ \ \forall j \in 1, \dots, t$ y $a \in V(f_i g_j)$. Se tiene entonces que $g_j(a) = 0\ \ \forall j \in 1, \dots, t \Longrightarrow a \in W$, por tanto $a \in V \cup W$.

Para probar (3) solo hay que tener en cuenta que una recta es una variedad afín. Sea $A = \{a_1, \dots a_p\}$ un conjunto de p puntos en $\mathbb{K}^n$ y sean r_{a_1}, s_{a_1} dos rectas que se intersecan únicamente en el punto a_1 tenemos que, por la propiedad (1) $V_{a_1} = V(r_{a_1}, s_{a_1})$ es una variedad afín por ser intersección finita de variedades afines, $a_1 \in V_{a_1}$ y además es el único punto de esa variedad. Análogamente construimos V_{a_i} con $i \in \{2, \dots p\}$. Por la propiedad (2) tenemos que $A = \bigcup_{i=1}^{p} V_{a_i}$ es una variedad afín. □

¿Qué relaciones hay entre la variedad $V(F) = V(f_1, f_2, \dots, f_s)$ y el ideal $\langle F \rangle = \langle f_1, f_2, \dots, f_s \rangle$? Es fácil ver que si $a \in V(F)$ entonces $\forall g \in \langle F \rangle$. Por lo tanto, se tiene que $g = g_1 f_1 + \cdots + g_s f_s \Rightarrow g(a) = g_1 f_1(a) + \cdots + g_s f_s(a) = g_1 0 + \cdots + g_s 0 = 0$. Utilizando reiteradas veces esta idea se tiene también que, si $\langle f_1, \dots, f_s \rangle$ y $\langle g_1, \dots, g_t \rangle$ son dos bases del mismo ideal I entonces $V(F) = V(f_1, \dots, f_s) = V(g_1, \dots, g_t) = V(G)$, pues cada $g_i = g_{i_1} f_1 + \cdots + g_{i_s} f_s$ y así si $a \in V(f_1, \dots, f_s), g \in V(G) \Longrightarrow g(a) = q_1 g_1(a) + \cdots + q_t g_t(a) = q_1 (g_{1_1} f_1(a) + \cdots + g_{1_s} f_s(a)) + \cdots + q_t (g_{t_1} f_1(a) + \cdots + g_{t_s} f_s(a)) = 0$.
Es decir, si V está definido por los polinomios $f_1, \dots, f_s$, entonces $V = V(\langle f_1, \dots, f_s \rangle)$. Esto, junto a que todo ideal I es de la forma $I = \langle f_1, \dots, f_s \rangle$, nos permite pensar que una variedad afín está determinada por un ideal en $\mathbb{K}[x_1, \dots, x_n]$ y la denotaremos, cuando conozcamos dicho ideal I, por $V = V(I)$.

Una vez visto que un ideal define una variedad. Veamos como una variedad en $\mathbb{K}^n$ también define un ideal en $\mathbb{K}[x_1, \dots, x_n]$.

Definición 2.9. Si $V \subset \mathbb{K}^n$ es una variedad afín entonces definimos el ideal de la variedad $I(V)$ como el siguiente conjunto.

$$I(V) = \{f \in \mathbb{K}[x_1, \dots, x_n] : f(a) = 0,\ \forall a \in V\}.$$

Se tiene que ese conjunto es, en efecto, un ideal pues:
Por un lado, si $f_1, f_2 \in V(I) \Longrightarrow (f_1 + f_2)(a) = f_1(a) + f_2(a) = 0 \Longrightarrow f_1 + f_2 \in V(I)$.
Por otro, si $f \in V(I), p \in \mathbb{K}[x_1, \ldots, x_n] \Longrightarrow p(a) f(a) = 0 \Longrightarrow pf \in V(I)$.

Observación 2.10. En lo que sigue, dados un ideal $\widehat{I}$ y una variedad $\widehat{V}$, van a surgir cuestiones que involucran a las variedades $V\left(\widehat{I}\right)$, $V\left(I\left(\widehat{V}\right)\right)$ y a los ideales $I\left(\widehat{V}\right)$, $I\left(V\left(\widehat{I}\right)\right)$. Sin embargo, a menudo se van a denotar simplemente a los ideales con I y a las variedades con V pero hay que tener cuidado de no confundirse. Cuando digamos $I(V(I))$ el ideal es solo la I de dentro de los paréntesis, mientras que la I que hay fuera de ellos denota la aplicación:

$$\begin{aligned} I : Variedades &\longrightarrow Ideales \\ V &\longmapsto I(V) \end{aligned}$$

Del mismo modo, cuando hablemos de $V(I(V))$ la variedad será solo la "V" de dentro de los paréntesis, mientras el V de fuera de ellos denota la aplicación:

$$\begin{aligned} V : Ideales &\longrightarrow Variedades \\ I &\longmapsto V(I) \end{aligned}$$

Comenzamos a ver resultados con un sencillo lema.

Lema 2.11. *Sea V una variedad y $f \in \mathbb{K}[x_1, \ldots, x_n]$, entonces* $[\exists\, m \in \mathbb{N} : f^m \in I(V)] \Longleftrightarrow f \in I(V)$.

Demostración. ($\Leftarrow$) es trivial.

($\Rightarrow$) sea $x \in V$ y f tal que $f(x)^m = 0$ si $f(x) \neq 0 \Longrightarrow K$ no es dominio de integridad pero K es un cuerpo por tanto llegamos a contradicción. □

Una conclusión inmediata de este lema es que para toda variedad V se cumple que $I(V)$ es un ideal radical; además deja claro que $\sqrt{I} \subset I(V(I))$. El resultado llamado Teorema fuerte de los ceros de Hilbert nos dice que si $\mathbb{K}$ es un cuerpo algebraicamente cerrado (como lo es $\mathbb{C}$) entonces se tiene el otro contenido. Para poder demostrarlo necesitamos un par de teoremas previos.

Teorema 2.12. *(Teorema débil de los ceros de Hilbert)*
Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado e $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal verificando que $V(I) = \emptyset$ entonces $1 \in I \Longleftrightarrow I = \mathbb{K}[x_1, \ldots, x_n]$.
Una demostración extensa de este teorema se puede encontrar en [2] capítulo 4 sección 1 páginas 168–169. Otra demostración más sencilla se encuentra en [4] capítulo 11 página 242.

Teorema 2.13. *(Teorema de los ceros de Hilbert)*
Si $\mathbb{K}$ *es un cuerpo algebraicamente cerrado y* $f \in \mathbb{K}[x_1, \ldots, x_n]$ *verifica que* $f \in I(V(f_1, \ldots, f_s))$ *para* $f_1, \ldots, f_s$ *dados, entonces existe* m *tal que* $f^m \in \langle f_1, \ldots, f_s \rangle$.
Enunciar esto expresando $I = \langle f_1, \ldots, f_s \rangle$ *significa que* $\forall f \in I(V(I)), \exists m$ *tal que* $f^m \in I$.

Demostración. Sea $f \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $f(a) = 0 \quad \forall a \in V(I)$ donde, recordemos, $I = \langle f_1, \ldots, f_s \rangle$. Queremos ver que existe m verificando $f^m \in I$. Para ello recurrimos a un curioso truco. Construimos el siguiente ideal:

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

Donde los $f_1, \ldots, f_s, f$ son los polinomios del enunciado. Veamos que $V\left(\widetilde{I}\right) = \emptyset$.
Consideremos un punto cualquiera $p \in \mathbb{K}^{n+1}$ con $p = (a_1, \ldots, a_n, a_{n+1})$. Se dá una de las dos opciones siguientes:

- $(a_1, \ldots, a_n) \in V(I)$.
- $(a_1, \ldots, a_n) \notin V(I)$.

En el primer caso tenemos por hipótesis que $f(p) = 0$ y, por tanto, al evaluar el polinomio $(1 - yf) \in \widetilde{I}$ en el punto p obtenemos:

$$(1 - yf)(p) = 1 - a_{n+1} f(a_1, \ldots, a_n) = 1 - a_{n+1} 0 = 1 \neq 0.$$

Por tanto $p \notin V\left(\widetilde{I}\right)$. En el segundo caso si $(a_1, \ldots, a_n) \notin V(I)$ entonces para algún polinomio $f_i,\ i \in \{1, \ldots, s\}$ se cumple que $f_i(a_1, \ldots, a_n) \neq 0$, y basta pensar en f_i como un polinomio en $n+1$ variables donde no se ve involucrada la última, teniendo así que $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$. Obteniendo de nuevo que $p \notin V\left(\widetilde{I}\right)$.

Aplicando ahora el teorema débil de los ceros de Hilbert en el ideal $\widetilde{I}$ tenemos que $1 \in \widetilde{I}$, con lo cual podemos expresar:

$$1 = q(x_1, \ldots, x_n, y)(1 - yf) + \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i. \tag{2.1}$$

Ahora podemos evaluar $y = 1/f$ y anular el sumando multiplicado por $q(x_1, \ldots, x_n, y)$ para obtener

$$1 = \sum_{i=1}^{s} p_i\left(x_1, \ldots, x_n, \frac{1}{f}\right) f_i. \tag{2.2}$$

Ahora basta con multiplicar en ambos lados por f^m con m suficientemente alto para despejar las f de los denominadores en la expresión a la derecha de la igualdad. De esta forma obtendremos:

$$f^m = \sum_{i=1}^{s} A_i f_i \tag{2.3}$$

Lo cual prueba el resultado. □

Teorema 2.14. *(Teorema fuerte de los ceros de Hilbert o Nullstellensatz fuerte)*
Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado entones para todo ideal I, se tiene $I(V(I)) = \sqrt{I}$.

Demostración. Como ya se ha comentado anteriormente, solo falta ver que $I(V(I)) \subset \sqrt{I}$. Supongamos que $f \in I(V(I))$ ¿Qué significa eso? que $f(a) = 0 \; \forall a \in V(I)$. Ahora, usando el teorema 2.13 tenemos que existe m tal que $f^m \in I$ que, por definición de radical de un ideal, implica $f \in \sqrt{I}$. □

Una consecuencia inmediata del teorema de los ceros de Hilbert es que, si $\mathbb{K}$ es un cuerpo algebraicamente cerrado e I es un ideal radical (que, recordemos, significa $\sqrt{I} = I$), entonces está claro que $I(V(I)) = I$. En este punto uno podría aventurarse a buscar condiciones bajo las cuales se tiene que $V(I(V)) = V$. La buena noticia es que no hace falta imponer ninguna, sin embargo para demostrarlo necesitamos pasar por el siguiente teorema importante.

Teorema 2.15. *(Correspondencia Ideal-Variedad, parte 1)*
Las aplicaciones

$$V : Ideales \longrightarrow Variedades \qquad I : Variedades \longrightarrow Ideales$$
$$I \longmapsto V(I) \qquad V \longmapsto I(V)$$

Invierten la inclusión. Es decir verifican que

1. $V_1 \subset V_2 \implies I(V_1) \supset I(V_2)$
2. $I_1 \subset I_2 \implies V(I_1) \supset V(I_2)$

Demostración. Para la segunda afirmación vamos a suponer el caso no trivial donde del lado izquierdo se dan los contenidos pero no la igualdad. Notar que si $I_1 = I_2$ ya se ha visto que $V(I_1) = V(I_2)$. Si bien también se cumple que $V_1 = V_2 \implies I(V_1) = I(V_2)$, no va a ser necesario hacer uso de ello.
Empezamos demostrando la segunda afirmación. Sean I_1, I_2 ideales verificando $I_1 \subsetneq I_2$, entonces $\exists h \in I_2$ tal que $h \notin I_1$. Por definición de $V(I_1)$, $V(I_2)$ tenemos que si $a \in V(I_2)$ entonces a verifica todas las condiciones para pertenecer a $V(I_1)$ y, al menos, la condición $h(a) = 0$ a mayores, por tanto $a \in V(I_1)$.
Ahora la primera afirmación sea $V_1 \subset V_2$ si $h \in I(V_2)$ entonces $h(a) = 0 \;\; \forall a \in V_2 \implies h(a) = 0 \;\; \forall a \in V_1$.

□

Ahora sí estamos en condiciones de demostrar el resultado que estaba pendiente.

Proposición 2.16. *$V(I(V)) = V$ para toda variedad V.*

Demostración. Empezamos demostrando $V \subset V(I(V))$. Sea $a \in V$, se tiene que $\forall f \in I(V)$, $f(a) = 0$ lo que implica, por definición, que $a \in V(I(V))$.
Demostremos ahora $V(I(V)) \subset V$. Si denotamos $V = V(f_1, \ldots, f_s)$, por definición de ideal de una variedad $f_1, \ldots, f_s \in I(V)$. Además $I(V)$ es un ideal, por tanto $\langle f_1, \ldots, f_s \rangle \subset I(V)$, es decir el ideal que genera la variedad $V(I(V))$ es mayor o igual que el ideal que genera V. Ahora usando que $I_1 \subset I_2 \Longrightarrow V(I_1) \supset V(I_2)$ tenemos el resultado deseado. □

Terminamos el capítulo con una versión del teorema de correspondencia entre variedades e ideales cuando los ideales involucrados son ideales radicales.

Teorema 2.17. *(Correspondencia Ideal-Variedad, parte 2)*
En las condiciones del teorema 2.15, si $\mathbb{K}$ es un cuerpo algebraicamente cerrado, se tiene que las aplicaciones:

$$V : Ideales\ \ radicales \longrightarrow Variedades \qquad I : Variedades \longrightarrow Ideales\ \ radicales$$
$$I \longmapsto V(I) \qquad V \longmapsto I(V)$$

Además de invertir la inclusión son también biyectivas.

Demostración. Es consecuencia de utilizar que $I(V)$ es un ideal radical y que, como $\mathbb{K}$ es algebraicamente cerrado, $I(V(I)) = I$, $V(I(V)) = V$. □

Capítulo 3

ÁLGEBRAS DE DIMENSIÓN FINITA

Este trabajo pretende desarrollar un método para encontrar los puntos de una variedad afín en $V \subset \mathbb{C}^n$, donde $V = V(f_1, \ldots, f_s)$ para $f_i \in \mathbb{C}[x_1, \ldots, x_n]$, $\forall i \in \{1, \ldots s\}$ cuando V es una cantidad finita de puntos. A lo largo de este capítulo se introducirán algunas herramientas que se usan en dicho método y, además, se mostrará un criterio para decidir si V es realmente un conjunto finito.

Introducido el concepto de base de Gröbner reducida podemos continuar con el estudio de la división de polinomios. Recordemos que si $f \in \mathbb{K}[x_1, \ldots, x_n]$ y $G = \langle g_1, \ldots, g_s \rangle$ es una base de Gröbner reducida del ideal I, entonces:

$$f = f_1 g_1 + \cdots + f_s g_s \ + \overline{f}^G \text{ con } \ f_i \in \mathbb{K}[x_1, \ldots, x_n] \ , \forall i \in \{1, \ldots s\} \, ,$$

donde $\overline{f}^G = \sum_{i=1}^{r} c_i x^{\alpha_i}$ con $c_i \in \mathbb{K}$ y $c_i x^{\alpha_i} \notin \langle lt(G) \rangle$, $\forall i$. Además, sabemos que $\overline{f}^G = 0 \iff f \in I$, lo cual implica que $\overline{f}^G = \overline{h}^G \iff f - g \in I$.

Si pensamos en términos del anillo cociente $\dfrac{\mathbb{K}[x_1, \ldots, x_n]}{I}$, esta última observación nos indica que podemos tomar como representante de $[f] \in \dfrac{\mathbb{K}[x_1, \ldots, x_n]}{I}$ al elemento $\overline{f}^G$. Ahora, para ver como se comportan la suma y producto de elementos en el anillo cociente, nos basta con ver como se comportan sobre el conjunto de formas normales módulo G, siendo G la base de Gröbner reducida de I.

Dados dos polinomios f y h, veamos como son las formas normales de $f + h$ y de fh. La suma de dos restos es también un resto $\overline{f + h}^G = \overline{f}^G + \overline{h}^G$. Esto se puede ver fácilmente expresando la división de f y de h módulo G.

Sin embargo, el producto de restos no es necesariamente un resto. Esto se ve en un ejemplo: supongamos $I = \langle x^2, y^2 \rangle$. Con orden lexicográfico $G = \{x^2, y^2\}$ es su base reducida de Gröbner y sea f tal que $\overline{f}^G = x$ en ese caso $\overline{f}^G \overline{f}^G = x^2$ que no es un resto, es por ello que $\overline{fh}^G = \overline{\overline{f}^G \overline{h}^G}^G$.

Así, considerando la correspondencia:

$$\overline{f}^g \longleftrightarrow [f] .$$

Podemos encontrar los representantes de la suma y producto de clases en el espacio cociente mediante:

$$\overline{f}^G + \overline{h}^G \longleftrightarrow [f] + [h] \tag{3.1}$$

$$\overline{\overline{f}^G \overline{h}^G}^G \longleftrightarrow [f]\,[h] \tag{3.2}$$

Definición 3.1. En el anillo cociente $\dfrac{\mathbb{K}[x_1, \ldots, x_n]}{I}$ podemos sumar elementos y multiplicar por las constantes $\{[c] : c \in \mathbb{K}\}$. Por ello, el anillo tiene también estructura de espacio vectorial sobre $\mathbb{K}$. A los anillos con estructura de espacio vectorial los llamaremos "álgebras" y de ahora en adelante también escribiremos $\dfrac{\mathbb{K}[x_1, \ldots, x_n]}{I}$ como A.

Proposición 3.2. *El conjunto de monomios* $B = \{[x^\alpha] : x^\alpha \notin \langle lt(I) \rangle\}$ *es una base de* A.

Demostración. Es claro que se trata de un conjunto generador pues toda forma normal es una combinación de elementos de B. Para ver que son linealmente independientes procedemos por reducción al absurdo y suponemos que:

$$[c_1]\,[x^{\alpha_1}] + \cdots + [c_k]\,[x^{\alpha_k}] = 0$$

lo que implica $[c_1]\,[x^{\alpha_1}] = -[c_2]\,[x^{\alpha_2}] - \cdots - [c_k]\,[x^{\alpha_k}]$ lo cual contradice la unicidad de formas normales.

□

Queremos aprovecharnos de esta base para simplificar el proceso de encontrar un representante para $[f]\,[h]$ que es el más complicado de obtener. Como la multiplicación en A es distributiva nos llega con saber como funciona la multiplicación en elementos de la base B. Veamos un ejemplo.

Ejemplo 3.3. sea $I = \langle x^2 + 3/2xy + 1/2y^2 - 3/2x - 3/2y, xy^2 - x, y^3 - y \rangle$ con $G = \{x^2 + 3/2xy + 1/2y^2 - 3/2x - 3/2y, xy^2 - x, y^3 - y\}$ base de Gröbner reducida de I. En el orden $>_{grevlex}$ tenemos que la base de A es $B = \{1, x, y, xy, y^2\}$. Ahora usaremos los

mismos comandos de SAGE empleados para encontrar una base de Gröbner. Luego calcularemos, usando repetidas veces el comando *reduce*, podemos rellenar la siguiente tabla de multiplicar:

.	1	x	y	xy	y^2
1	1	x	y	xy	y^2
x	x	γ_1	xy	γ_2	x
y	y	xy	y^2	x	y
xy	xy	γ_2	x	γ_1	xy
y^2	y^2	x	y	xy	y^2

Tabla 3.1: Tabla de multiplicar de A

Donde

$$\gamma_1 = -3/2xy - 1/2y^2 + 3/2x + 3/2y$$
$$\gamma_2 = 3/2xy + 3/2y^2 - 3/2x - 1/2y.$$

En cada casilla de la tabla se ha calculado el resto módulo G del producto del monomio fila y columna.

Enunciamos ahora el teorema que nos da el criterio para decidir la finitud de V.

Teorema 3.4. *(Teorema de finitud)*
Sea $\mathbb{K}$ un cuerpo contenido en $\mathbb{C}$ y sea un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Las siguientes afirmaciones son equivalentes:

1. *El álgebra $A = \dfrac{\mathbb{K}[x_1, \ldots, x_n]}{I}$ tiene dimensión finita al pensarla como espacio vectorial sobre $\mathbb{K}$.*
2. *La variedad $V(I) \subset \mathbb{C}^n$ es un conjunto finito de puntos.*
3. *Si G es una base de Gröbner de I, entonces para cada variable x_i existe algún exponente mínimo m_{x_i} tal que $x_i^{m_i} = lt(g_i)$ para algún $g_i \in G$.*

Si un ideal verifica las condiciones de alguna de las afirmaciones entonces se le llama ideal cero-dimensional.
Revisando el ejemplo 2.6 se observa que la base obtenida no tiene un polinomio cuyo término principal sea de la forma z^r. Por tanto, en virtud de este teorema, el álgebra subyacente no tiene dimensión finita.

Queremos mostrar un teorema más en el capítulo pero va a necesitar un lema previo [3] página 43.

Lema 3.5. *Sea $S = \{p_1, \ldots, p_m\}$ un conjunto finito de puntos en $\mathbb{C}^n$, entonces existe una colección $\{g_1, \ldots, g_m\}$ de polinomios verificando:*

$$g_i(p_j) = \begin{cases} 0 & si\ i \neq j \\ 1 & si\ i = j \end{cases} \tag{3.3}$$

La construcción de estos polinomios se puede entender como una generalización de la construcción del polinomio interpolador de Lagrange.

Teorema 3.6. *Sea I un ideal cero-dimensional en $\mathbb{C}[x_1, \ldots, x_n]$ y consideremos el álgebra $A = \dfrac{\mathbb{C}[x_1, \ldots, x_n]}{I}$. Se verifica que la dimensión de A es mayor o igual que la cantidad de puntos en $V(I) = \{p_1, \ldots, p_m\}$. Además, la igualdad se da si y solo si I es un ideal radical.*

Demostración. Consideremos la aplicación $\varphi : \mathbb{C}[x_1, \ldots, x_n] \longrightarrow \mathbb{C}^m$ tal que $\varphi([f]) = (f(p_1), \ldots, f(p_m))$. Veamos primeramente que φ está bien definida.
Sean f, h tales que $[f] = [h]$, entonces se tiene:

$$\left.\begin{array}{l} h(p_i) - f(p_i) \quad \in I \\ p_i \in V(I) \end{array}\right\} \Longrightarrow (h(p_i) - f(p_i)) = 0.$$

Además, gracias a la definición 3.1, φ es una aplicación lineal, por lo que podemos usar bien argumentos sobre dimensiones.
Para probar que $\dim_{\mathbb{C}} A \geqslant \#V(I)$ nos llega con ver que φ es una aplicación sobreyectiva. Sea $a = (a_1, \ldots, a_m)$ un punto cualquiera de $\mathbb{C}^m$, usando la colección de polinomios garantizada por el lema previo sobre los puntos $\{p_1, \ldots, p_m\}$ tenemos que, tomando $f = \sum_{i=1}^{m} a_i g_i$, se verifica que $\varphi[f] = a$.
Sea ahora I un ideal radical y sea $[f]$ tal que $f(p_i) = 0 \quad \forall i \in \{1, \ldots, m\}$, es decir, $[f] \in ker(\varphi)$. Entonces, por definición de ideal de una variedad, tenemos que $f \in I(V(I))$. Además, por el teorema de los ceros de Hilbert $I(V(I)) = \sqrt{I} = I$. Por tanto φ es en este caso también inyectiva y por tanto un isomorfismo. Lo que prueba $dim_{\mathbb{C}} A = \#V(I)$.
Supongamos ahora que φ es un isomorfismo y lleguemos a que $I = \sqrt{I}$. Sea $f \in \sqrt{I} \Longrightarrow f \in I(V(I))$, tenemos que $f(p_i) = 0$, $\forall i$ y como φ isomorfismo $[f] = [0] \Longrightarrow f \in I$.

□

Capítulo 4

RESOLVER ECUACIONES MEDIANTE AUTOVALORES

4.1. Desarrollo teórico

Después de todas las adecuadas introducciones, llegamos al capítulo principal del trabajo. Como ya se dijo antes, aquí intentaremos encontrar los puntos de una variedad afín generada por un ideal cero-dimensional. Van a aparecer varias aplicaciones y construcciones creadas sobre otras recién definidas. Por ello, es mejor ir con pies de plomo y pararse cada vez que surgen confusiones para pensar de donde a donde parte cada aplicación que vaya apareciendo. Sin más preámbulos introducimos la primera, m_f, que podríamos vagamente llamarla la aplicación "multiplicar por $[f]$ en el álgebra" y vendría definida por:

$$\begin{aligned} m_f : A &\longrightarrow A \\ [h] &\longmapsto [fh] \end{aligned}$$

Donde, recordemos, el anillo cociente $\dfrac{\mathbb{K}[x_1, \ldots, x_n]}{I}$ pensado como un espacio vectorial con la multiplicación por constantes, era lo que llamábamos un álgebra y lo denotábamos por A.

4.1.1. Un adelanto de lo que está por venir

Veamos una motivación del desarrollo que realizaremos más adelante a través del caso concreto de trabajar en el anillo de polinomios en una variable $\mathbb{K}[x]$.

Definición 4.1. Sea $p(x) = x^n + a_{n_1}x^{n_1} + \cdots + a_1 x + a_0$ un polinomio mónico en $\mathbb{K}[x]$, definimos la matriz compañera[1] de p como:

$$A_p = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a_2 \\ 0 & 0 & 1 & \cdots & 0 & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix} \tag{4.1}$$

Consideremos el Álgebra $\dfrac{\mathbb{K}[x]}{(p)}$. Utilizando la proposición 3.2 para este caso, obtenemos que una base del Álgebra es $B = \{1, x, \ldots, x^{n-1}\}$. Es fácil ver que, si consideramos $m_f = m_x$ y pensamos en la matriz asociada a m_x en la base B, vemos que se trata de la matriz A_p. Pero ahora bien la matriz A_p tiene la siguiente propiedad:

Proposición 4.2. *El polinomio característico de A_p es el propio p.*

Demostración. Basta desarrollar el determinante de la ecuación característica por la última columna para obtener el resultado. □

Por tanto las raices del polinomio $p \in \mathbb{K}[x]$ coinciden con los autovalores de la matriz A_p y, por tanto, tendríamos el problema resuelto. En este capítulo se construye una generalización de este procedimiento para resolver esta situación en varias variables.

Proposición 4.3. *Se verifica que:*

1. *m_f es un endomorfismo de espacios vectoriales.*
2. *$m_f = m_h \iff f - h \in I \iff [f] = [h]$.*
3. *$m_{f_1+f_2} = m_{f_1} + m_{f_2}$.*
4. *$m_{fh} = m_f \circ m_h$ donde $\circ$ denota composición de aplicaciones lineales (como I es cero dimensional, A tiene dimensión finita como espacio vectorial y se puede entender $\circ$ como producto de sus matrices asociadas respecto a cierta base. Más detalles sobre esto después de la demostración).*

[1] Muchos libros sobre este tema definen la matriz compañera de p como la matriz traspuesta a la definida en este documento.

Demostración. (1) se verifica, pues como A es un anillo la multiplicación es distributiva sobre la suma y por tanto:

$$m_f\left(c_1\left[h_1\right]+c_2\left[h_2\right]\right)=\left[f\right]\left(c_1\left[h_1\right]+c_2\left[h_2\right]\right)=c_1\left[f\right]\left[h_1\right]+c_2\left[f\right]\left[h_2\right]$$

$$=c_1m_f\left(\left[h_1\right]\right)+c_2m_f\left(\left[h_2\right]\right).$$

(2) La segunda flecha doble se verifica, pues se trata de lo que define las clases en el anillo. Falta ver $[f]=[h]\Longleftrightarrow m_f=m_h$.
($\Longleftarrow$) $[f]=[f]\,[1]=m_f\,[1]=m_h\,[1]=[h]\,[1]=[h]$. ($\Longrightarrow$) trivial.
(3) y (4) se prueban de forma similar a (1).
(3) $m_{f_1+f_2}\left(\left[h\right]\right)=\left[f_1+f_2\right]\left[h\right]=\left[f_1h\right]+\left[f_2h\right]=m_{f_1}\left[h\right]+m_{f_2}\left[h\right]$.
(4) $m_{fh}\left[l\right]=\left[fhl\right]=\left[f\right]\left[hl\right]=m_f\left(m_h\left(l\right)\right)$.

□

Observación 4.4. Los apartados (3) y (4) de esta proposición implican que la aplicación:

$$\begin{aligned} m:\mathbb{K}\left[x_1,\ldots,x_n\right] &\longrightarrow M_{d\times d}\left(\mathbb{K}\right)\\ f &\longmapsto m_f\end{aligned}$$

Es un homomorfismo de anillos cuyo núcleo es I. Usando ahora el primer teorema de isomorfía de anillos, tenemos que la aplicación:

$$\begin{aligned} m:A &\longrightarrow M_{d\times d}\left(\mathbb{K}\right)\\ \left[f\right] &\longmapsto m_f\end{aligned}$$

Es inyectiva.

Como ya se dijo en el enunciado de la proposición, al estar trabajando por un álgebra generada por un ideal cero-dimensional, el álgebra tendrá dimensión finita sobre $\mathbb{K}$ y podremos representar la aplicación m_f mediante su matriz respecto a una base. En concreto, nos va a interesar usar la base de monomios $\{x^\alpha:\ x^\alpha\notin\langle lt\left(I\right)\rangle\}$ definida en el capítulo 3. De ese capítulo vamos a recuperar también el ejemplo 3.3 que, recordemos, trabajaba en el ideal I que tiene por base de Gröbner reducida:

$$G=\left\{x^2+3/2xy+1/2y^2-3/2x-3/2y,xy^2-x,y^3-y\right\}.$$

Recordamos también que una base del álgebra $A=\frac{\mathbb{K}[x_1,\ldots,x_n]}{\langle G\rangle}$ era $B=\left\{1,x,y,xy,y^2\right\}$. Utilizando la tabla 3.1 de multiplicar de A, es fácil obtener la matriz asociada a m_f para cualquier f, incluso se pueden hacer las cuentas a mano para algunos casos sencillos gracias a que, por la proposición 4.3 (2), tenemos que $m_f=m_{\overline{f}^G}$ y si f es una suma de varios

monomios en A, entonces por la proposición 4.3(3) basta con calcular la matriz de cada uno de los sumandos. Calculemos pues la matriz asociada a m_{xy-y^2} como ejemplo ilustrativo. Como ya se ha indicado, podemos calcular simplemente m_{xy} y $-m_{y^2}$ y luego sumarlas. De este modo:

$$m_{xy} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & -3/2 & 1 & 3/2 & 0 \\ 0 & -1/2 & 0 & 3/2 & 0 \\ 1 & 3/2 & 0 & -3/2 & 1 \\ 0 & 3/2 & 0 & -1/2 & 0 \end{pmatrix} \quad m_{y^2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

De donde:

$$m_{xy-y^2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & -5/2 & 1 & 3/2 & 0 \\ 0 & -1/2 & -1 & 3/2 & 0 \\ 0 & 3/2 & 0 & -5/2 & 0 \\ -1 & 3/2 & 0 & -1/2 & -1 \end{pmatrix}.$$

Hasta ahora la mayor parte de los resultados referían a un cuerpo $\mathbb{K}$ sin especificar cual. A partir de este punto vamos a centrarnos en el caso $\mathbb{K} = \mathbb{C}$ que es donde vamos a obtener el resultado final. Por tanto, a partir de ahora el anillo de polinomios pasa a ser $\mathbb{C}[x_1, \ldots, x_n]$. En el, consideremos los polinomios $f_1, \ldots, f_n$ tales que $f_i = x_i$. Por el teorema 3.4 de finitud tenemos que $\forall i \in \{1, \ldots, n\}$ $\exists m_i$ tal que $[f_i]^{m_i} \in I \iff [f_i]^{m_i} = 0$ lo que implica que el conjunto $\left\{1, [f_i], [f_i]^2, \ldots, [f_i]^{m_i}\right\}$ es linealmente dependiente y por tanto existe una combinación lineal:

$$\sum_{j=0}^{m_i} c_j f_i^j = 0 \iff \sum_{j=0}^{m_i} c_j f_i^j \in I. \tag{4.2}$$

Donde no todos los c_j son nulos. Esa estructura del sumatorio evoca de nuevo a un polinomio en la "variable f" que nos conduce a considerar la siguiente construcción:

Dado $\rho(t) = \sum_{i=0}^{m} p_i t^i \in \mathbb{C}[t]$ un polinomio en una variable y $f = \sum_{j=0}^{k} c_j x^{\alpha_j} \in \mathbb{C}[x_1, \ldots, x_n]$, entonces $\rho(f) = \sum_{i=0}^{m} p_i \left(\sum_{j=0}^{k} c_j x^{\alpha_j}\right)^i = \sum_{i=0}^{m} p_i f^i$ es a su vez un elemento de $\mathbb{C}[x_1, \ldots, x_n]$. Del mismo modo podemos considerar evaluar el polinomio $\rho(t)$ en la matriz m_f consiguiendo otra matriz $\rho(m_f) = \sum_{i=0}^{m} p_i (m_f)$ y está claro que las matrices

$m_{\rho(f)}$ y $\rho(m_f)$ son la misma. Quizá ayuda a comprender esta construcción pensar que es algo parecido a como, en las asignaturas de análisis, se llega al concepto de exponencial de una matriz, pero en este caso con una cantidad finita de sumas.

Retomando el resultado (4.2) lo que ocurría ahí era que $\rho([f]) = [0]$ o, lo que es lo mismo, la matriz $\rho(m_f)$ es nula.

Proposición 4.5. *Sea $[f] \in A$. El conjunto de polinomios $\Theta_{[f]} = \{\rho \in \mathbb{C}[t] : \rho([f]) = 0\}$ forma un ideal de $\mathbb{C}[t]$. Expresado en matrices tenemos, similarmente, que dada M matriz cuadrada de orden d, el conjunto de polinomios $\Theta_M = \{\rho \in \mathbb{C}[t] : \rho(M) = 0\}$ es un ideal de $\mathbb{C}[t]$. Además, claramente si $M = m_f$ entonces $\Theta_{[f]} = \Theta_M$.*

Demostración. Sean $\rho_1, \rho_2 \in \Theta$, $q(t) \in \mathbb{C}[x_1, \ldots, x_n]$ entonces $(\rho_1 + \rho_2)(M) = \rho_1(M) + \rho_2(M) = 0$, $(qp)\rho_1 = 0$. □

Llegados a este punto, podemos extraer resultados valiosos de la situación pues hemos encontrado un ideal en $\mathbb{C}[t]$ que se trata de un dominio de ideales principales y por tanto sabemos que:

1. Existe ρ_M el generador mínimo mónico del ideal I_M llamado polinomio mínimo de la matriz M.
2. si $\rho \in \Theta_M$ entonces $\rho_M | \rho$.
3. por el teorema del Cayley-Hamilton ρ_M divide al polinomio característico de M.
4. las raíces de ρ_M son los autovalores de M.

Mostramos en breve el más importante teorema del trabajo y que relaciona las nuevas construcciones de este capítulo con los puntos de la variedad afín $V(I)$. En la demostración van a surgir el autovector asociado a un autovalor de la matriz m_f y es importante entender que si m_f es una matriz que representa, en la base de los monomios $\{x^\alpha : x^\alpha \notin \langle lt(G)\rangle\}$, a una aplicación lineal de A en A, entonces un autovector de dicha matriz es, en terminos de A, una clase de equivalencia.

Teorema 4.6. *Sean $f \in \mathbb{C}[x_1, \ldots, x_n]$ y ρ_f el polinomio mínimo de m_f en $A = \dfrac{\mathbb{C}[x_1, \ldots, x_n]}{I}$. Si $\lambda \in \mathbb{C}$ entonces equivalen:*

1. *λ es una raíz de la ecuación $\rho_f(t) = 0$.*
2. *λ es un autovalor de la matriz m_f.*
3. *λ es el valor de f en algún punto de $V(I)$.*

Demostración. (1) $\iff$ (2) es un resultado conocido de álgebra lineal.

(2) $\implies$ (3) Por reducción al absurdo. Sea λ un autovalor de m_f y sea $[w_\lambda] \neq 0$ un autovector asociado suyo. Supongamos que λ no es un valor de f evaluada en $V(I) = \{p_1, \ldots, p_m\}$ entonces $f(p_i) \neq \lambda \ \ \forall i \in \{1, \ldots, m\}$. Construimos la aplicación $g = f - \lambda$ que verifica $g(p_i) \neq 0, \ \ \forall p_i \in V(I)$. Gracias a la expresión (3.3), existen m polinomios $\{g_1, \ldots, g_m\}$ tales que:

$$g_i(p_j) = \begin{cases} 0 & si\ i \neq j \\ 1 & si\ i = j \end{cases}$$

Construimos con ellos el polinomio $g'(p) = \sum_{i=1}^{m} c_i g_i(p)$ donde $c_i = \dfrac{1}{g(p_i)}$. Se tiene que $g'(p_i) = c_i = \dfrac{1}{g(p_i)}$ y, por tanto, $g(p_i)\, g'(p_i) = 1 \ \ \forall p_i \in V(I)$. Esto implica que $1 - gg' \in I(V(I))$. Usando el teorema de los ceros de Hilbert tenemos que $(1 - gg')^l \in I$ para algún $l \geqslant 1$. Si analizamos como es la expansión del binomio vemos que es $(1 - gg')^l = 1^l - 1^{l-1} lgg' + \dfrac{l(l+1)}{2} 1^{l-2} g^2 g'^2 - \ldots$, donde, en la expresión de la izquierda, todos los sumandos a partir del segundo (incluido) tienen a g como factor común. Gracias a ello, podemos expresar $(1 - gg')^l$ como $1 - \widetilde{g}g$ donde $\widetilde{g} \in \mathbb{C}[x_1, \ldots, x_n]$. Como $1 - \widetilde{g}g = (1 - gg')^l \in I$ tenemos que $[g]\,[\widetilde{g}] = [1]$, es decir, $[g]$ es una unidad del anillo A. Pero recordemos que, por ser λ autovalor con autovector $[w_\lambda]$, se cumple que $[f - \lambda]\,[w_\lambda] = [g]\,[w_\lambda] = 0$ pero eso es una contradicción pues al multiplicar por $[\widetilde{g}]$ llegamos a $[w_\lambda] = 0$.

(3) $\implies$ (1) sea $\lambda = f(p)$ para algún $p \in V(I)$, como $\rho_f(m_f) = 0$ por la proposición 4.5 tenemos que $\rho_f([f]) = [0] \iff \rho_f([f]) \in I$ es decir $\rho_f(\lambda) = \rho_f(f(p_i)) = 0$

□

De este teorema se sigue un corolario que marca el camino a seguir para obtener las coordenadas de los puntos de $V(I)$.

Corolario 4.7. *Sea I un ideal cero dimensional de $\mathbb{C}$, entonces los m autovalores de la matriz asociada a la aplicación m_{x_i} en A son los valores de la i-ésima coordenada de los distintos m puntos de la variedad $V(I)$. Además, evaluando $\rho_{x_i}(t)$ en $t = x_i$ obtenemos el generador mónico del ideal $I \cap \mathbb{C}[x_i]$.*

Ahora podríamos recuperar de la asignatura Análisis Numérico Matricial los métodos de la potencia y la potencia inversa para resolver problemas de este tipo siempre que las matrices que surjan en el proceso tengan autovalor dominante. O de la asignatura Cálculo Numérico en una Variable métodos para encontrar raíces de ecuaciones para encontrar las del polinomio ρ_f. Se puede realizar un análisis para ver que este resultado proporciona un algoritmo mejor para resolver el problema que otros métodos como el de eliminación

explorado en [3] capítulo 2 sección 1. De hecho un refinamiento del método visto en este capítulo permite resolver el problema con solo encontrar los autovalores de una matriz asociada a una cierta aplicación $m_{c_1x_1+\cdots+c_nx_n}$ en lugar de n aplicaciones diferentes. Esta mejora se estudia en el siguiente capítulo donde se le saca información a los autovectores de la matriz m_f.

4.1.2. Resolvamos un ejemplo

Utilizando los conocimientos desarrollados hasta este punto y usando SAGE vamos a encontrar los puntos de la variedad $V = V(I)$ donde $I = \langle x - y^2 - z^2, y^2 - z, z^2 - 1\rangle$.

```
P.<x,y,z>=PolynomialRing(QQ,order='lex')
```

Trabajaremos, en este caso, con el orden lexicográfico.

```
f1=x-y^2-z^2;f2=y^2-z;f3=z^2-1;
```

```
J=Ideal([f1,f2,f3])
```

```
G=J.groebner_basis();G
```

```
[x - z - 1, y^2 - z, z^2 - 1]
```

```
J.normal_basis()
```

```
[y*z, z, y, 1]
```

Hasta aquí hemos declarado el ideal J; Calculado su base de Gröbner reducida G y calculado también una base B del Álgebra $\dfrac{\mathbb{C}[x,y,z]}{J}$ y vemos que esta tiene 4 elementos, ordenándolos de menor a mayor en el orden lexicográfico tenemos $B = \{1, z, y, yz\}$. En este punto ya sabemos que el número de puntos de la variedad es 4.

```
(x).reduce(G)
```

```
z + 1
```

```
(z*x).reduce(G)
```

```
z + 1
```

```
(y*x).reduce(G)
```

```
y*z + y
```

```
(y*z*x).reduce(G)
```

```
y*z + y
```

En estas líneas hemos encontrado las formas normales de los elementos de la base B multiplicados todos ellos por la variable x para obtener la matriz m_x.

```
Mx=matrix(QQ\
,[[1,1,0,0],[1,1,0,0],[0,0,1,1],[0,0,1,1]])
show(Mx)
```

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

```
Mx.eigenvalues()
```

```
[2, 2, 0, 0]
```

Ahora sabemos los valores de las coordenadas x. Procedemos a repetir el proceso para las otras dos variables.

```
(y^2).reduce(G)
```

```
z
```

```
(y^2*z).reduce(G)
```

```
1
```

No necesitamos buscar las formas normales de y ni de yz pues ya son elementos de B. Se da una situación similar al calcular algunas coordenadas z.

```
My=matrix(QQ\
,[[0,0,0,1],[0,0,1,0],[1,0,0,0],[0,1,0,0]]);
show(My)
```

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

```
My.eigenvalues()
```

```
[1, -1, -1*I, 1*I]
```

```
(z^2).reduce(G)
```

```
1
```

```
(y*z^2).reduce(G)
```

```
y
```

```
Mz=matrix(QQ\
,[[0,1,0,0],[1,0,0,0],[0,0,0,1],[0,0,1,0]])
show(Mz)
```

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

```
Mz.eigenvalues()
```

```
[1, 1, -1, -1]
```

De esta forma sabemos que las coordenadas x son $[2, 2, 0, 0]$ las y son $[1, -1, -i, i]$ y por ultimo las z son $[1, 1, -1, -1]$. Se puede comprobar que los puntos $p_1 = (2, 1, 1)$, $p_2 = (2, -1, 1)$, $p_3 = (0, -i, -1)$ y $p_4 = (0, i, -1)$ verifican las ecuaciones que definen el ideal y por tanto son la solución buscada.

Capítulo 5

POR ÚLTIMO, LOS AUTOVECTORES AÚN TIENEN ALGO QUE DECIR

5.1. Teoría previa

Vamos a detallar como podemos sacarle partido a los autovectores para mejorar la eficiencia del método explorado en el capítulo anterior. Tradicionalmente, cuando en álgebra lineal se habla de los autovectores de una matriz M, se refiere a los vectores columna $v \neq 0$ que cumplen:

$$Mv = \lambda v. \tag{5.1}$$

Sin embargo, existen dos tipos de autovectores, los vectores que verifican (5.1) se les llama autovectores a la derecha. Es conocido que la matriz traspuesta M^T tiene los mismos autovalores que M. Por tanto, existen unos vectores columna v' tales que $M^T v' = \lambda v'$. Ahora, tomando traspuestas a ambos lados, llegamos a:

$$\left(M^T v'\right)^t = \left(\lambda v'\right)^t \Longrightarrow \left(v'\right)^t M = \lambda \left(v'\right)^t \Longleftrightarrow wM = \lambda w. \tag{5.2}$$

Donde $w = (v')^t$. Esos w son vectores fila a los que llamamos autovectores por la izquierda. Es fácil encontrar la relación entre los autovectores a la izquierda y los autovectores a la derecha si suponemos que M es una matriz diagonalizable. Recordando la descomposición aprendida de álgebra lineal tenemos que, si P es la matriz que tiene por columnas a los autovectores de M. Entonces se verifica:

$$M = PDP^{-1}. \tag{5.3}$$

Multiplicando ahora a la izquierda por P^{-1} tenemos:

$$P^{-1}M = DP^{-1}. \tag{5.4}$$

Para que esta expresión sea cierta, la matriz P^{-1} tiene que ser la matriz cuyas filas son los autovectores de la matriz M^T. Pues, trasponiendo a ambos lados la expresión (5.4) obtenemos $M^T \left(P^{-1}\right)^T = \left(P^{-1}\right)^T D$. Ahora multiplicando por P^T a la derecha llegamos a $M^T = \left(P^{-1}\right)^T DP^T$. De esta manera hemos llegado a la descomposición diagonal de M^T y la matriz $\left(P^{-1}\right)^T$ tiene por columnas a los autovectores de M^T.

Supongamos ahora que trabajamos en un ideal radical. Por tanto, en virtud del teorema 3.6, $dim_{\mathbb{C}} A = \#V(I) = \#\{p_1, \dots p_m\} = m$, y sea entonces $B = \{[x^{\alpha_1}], \dots, [x^{\alpha_m}]\}$ la base monomial que consideraremos del álgebra A.

Proposición 5.1. *Sea $f \in \mathbb{C}[x_1, \dots, x_n]$ escogido de forma que $f(p_i) \neq f(p_j)$, $\forall p_i, p_j \in V(I)$. Entonces los autovectores a la izquierda de la matriz m_f tienen dimensión 1 y son de la forma $\mu(p^{\alpha_1}, \dots, p^{\alpha_m})$ con p recorriendo $V(I)$ y $f(p) = \mu \in \mathbb{C}$.*

Demostración. Realizaremos esta demostración por coordenadas en la base B. Por tanto expresemos $m_f = m_{ij}$ con $i, j \in \{1, \dots, m\}$.

Por definición de m_f tenemos que:

$$[x^{\alpha_j} f] = m_f [x^{\alpha_j}]. \tag{5.5}$$

Fijarse ahora que como $[x^{\alpha_j}] \in B$ tenemos que $[x^{\alpha_j}]$, expresado en la base B, es de la forma $(0, \dots, 0, 1, 0, \dots, 0,)^t$ donde toma el valor 1 únicamente en la componente j-ésima. Por tanto al expresar en coordenadas $m_f [x^{\alpha_j}]$ tenemos:

$$m_f [x^{\alpha_j}] = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1j} & \cdots & m_{1m} \\ m_{21} & m_{22} & \cdots & m_{2j} & \cdots & m_{2m} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ m_{j1} & m_{j2} & \cdots & m_{jj} & \cdots & m_{jm} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ m_{m1} & m_{m2} & \cdots & m_{mj} & \cdots & m_{mm} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} m_{1j} \\ m_{2j} \\ \vdots \\ m_{jj} \\ \vdots \\ m_{mj} \end{pmatrix}. \tag{5.6}$$

Pero ahora si queremos expresar $(m_{1j}, \dots, m_{jj}, \dots, m_{mj})^t$ como una suma de vectores de B, tenemos:

$$\begin{pmatrix} m_{1j} \\ m_{2j} \\ \vdots \\ m_{mj} \end{pmatrix} = m_{1j} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + m_{2j} \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + m_{mj} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = m_{1j} [x^{\alpha_1}] + m_{2j} [x^{\alpha_2}] + \cdots + m_{mj} [x^{\alpha_m}]. \tag{5.7}$$

Juntando todo lo visto hasta aquí obtenemos la expresión:

$$[x^{\alpha_j} f] = \sum_{i=1}^{m} m_{ij} [x^{\alpha_i}] \tag{5.8}$$

A continuación evaluamos (5.8) en $p \in V(I)$ y tenemos:

$$p^{\alpha_j} f(p) = \sum_{i=1}^{m} m_{ij} p^{\alpha_i} = \sum_{i=1}^{m} p^{\alpha_i} m_{ij} \tag{5.9}$$

Notar ahora que en la expresión $(p^{\alpha_1}, \ldots, p^{\alpha_m}) \begin{pmatrix} m_{11} & \cdots & m_{1m} \\ \vdots & \ddots & \vdots \\ m_{m1} & \cdots & m_{mm} \end{pmatrix} = (w_1, \ldots, w_m)$ cada w_j es de la forma $w_j = \sum_{i=1}^{m} p^{\alpha_i} m_{ij}$, que coincide con la igualdad a la derecha en la expresión (5.9) por lo que, finalmente, juntando todo tenemos:

$$(p^{\alpha_1}, \ldots, p^{\alpha_m}) \begin{pmatrix} m_{11} & \cdots & m_{1m} \\ \vdots & \ddots & \vdots \\ m_{m1} & \cdots & m_{mm} \end{pmatrix} = \left(\sum_{i=1}^{m} p^{\alpha_i} m_{i1}, \ldots, \sum_{i=1}^{m} p^{\alpha_i} m_{im} \right) \tag{5.10}$$

$$= \left(p^{\alpha_1} f(p), \ldots, p^{\alpha_m} f(p)\right) = f(p) \left(p^{\alpha_1}, \ldots, p^{\alpha_m}\right)$$

Por último gracias a la proposición 3.2 y que A es de dimensión finita se verifica que $\alpha(j) = (0, \ldots, 0) \in \mathbb{N}^n$ para algún $j \in \{1, \ldots, m\}$ y por tanto $(p^{\alpha_1}, \ldots, p^{\alpha_m})$ es no nulo. Esto, junto a (5.10), nos garantiza que $(p^{\alpha_1}, \ldots, p^{\alpha_m})$ es un autovector derecho de m_f con autovalor asociado $f(p)$. Además como $f(p_i) \neq f(p_j)$ si $i \neq j$ con $i, j \in \{1, \ldots, m\}$ m_f tiene m autovalores distintos y por tanto sus autovectores, tanto a la izquierda como a la derecha, son todos de dimensión 1. □

Veamos como aprovechar esta proposición para encontrar los puntos de $V(I)$ usando únicamente una función polinómica f como se adelantaba al final del capítulo anterior.

5.2. Construcción del método

Consideremos un orden monomial $>$ y un ideal radical cero dimensional I. Construyamos una base de Gröbner reducida G de I y además una base monomial B del Álgebra $\frac{\mathbb{C}[x_1,\ldots,x_n]}{I}$. Sea ahora $f = c_1 x_1 + \cdots + c_n x_n$, $c_i \in \mathbb{Z}$, $\forall i \in \{1, \ldots, n\}$ elegida con la esperanza de verificar $f(p_i) \neq f(p_j)$ $\forall i \neq j$ calculamos la matriz m_f respecto a la base

B y usando métodos numéricos calculamos un autovalor λ y su correspondiente autovector a la izquierda v_λ. Por la proposición 5.1 sabemos que $v_\lambda = \mu\left(p^{\alpha_1}, \ldots, p^{\alpha_m}\right)$ para algún $\mu \neq 0$ constante. Por la tercera afirmación del teorema 3.4 de finitud se verifica que $\forall i \in \{1, \ldots, n\} \quad \exists m_i \geqslant 1$ tal que $x_i^m = lt\left(g_i\right)$ para algún $g_i \in G$ distingamos según los casos donde $m_i > 1$ de los que $m = 1$. Expresemos $P = (a_1, \ldots, a_n)$, de esta forma $v_\lambda = \mu\left((a_1, \ldots, a_n)^{\alpha_1}, \ldots, (a_1, \ldots, a_n)^{\alpha_m}\right)$.

- Si $m_i > 1$ entonces $x_i^1 \neq lt\left(g_j\right), \quad \forall g_j \in G$. Esto implica que $[x_i] \in B$ y por tanto existe un $\alpha(k), \ k \in \{1, \ldots, m\}$ que tiene un 1 en la componente i-ésima y todas las demás nulas por lo cual una de las componentes de v_λ es μa_i.
  Por otra parte $[1] \in B$ y por tanto μ es, también, una de las componentes de v_λ.
  Juntando estas dos cosas podemos encontrar las coordenadas i-ésimas, si $m_i > 1$, de los puntos $p \in V(I)$.

- El caso $m_i = 1$ necesita hacerse tras realizar los casos $m_j > 1$.

  Consideremos los dos siguientes conjuntos:
  $\Upsilon := \{x_i : \ i \in \{1, \ldots, n\}, m_i = 1 \}$, $\Lambda_i := \{j \in \{1, \ldots, n\} : x_i > x_j \text{ en } >\}$

  Como la variable x_i no aparece en la base monomial B, tenemos que recurrir a la base de Gröbner G. Si $g \in G$ es tal que $lt(g) = x_i$ entonces está claro que g es de la forma:

$$g = x_i + \sum_{j \in \Lambda_i} c_j x_j^{\alpha_j}. \tag{5.11}$$

  Por tanto si evaluamos la expresión (5.11) de g en p (donde recordemos $g(p) = 0$ pues $g \in I, p \in V(I)$) obtenemos:

$$0 = a_i + \sum_{j \in \Lambda_i} c_j a_j^{\alpha_j}. \tag{5.12}$$

  Ahora lo que hacemos es considerar el elemento mínimo de Υ, $x_{i_{min}}$ en el orden $>$. Se verifica que $j \in \Lambda_{i_{min}} \Longrightarrow x_j \notin \Upsilon$. Sea $g \in G$ tal que $lt(g) = x_{i_{min}}$ en ese caso usando (5.12) tenemos que $a_{i_{min}} = -\sum_{j \in \Lambda_i} c_j a_j^{\alpha_j}$ pero como conocemos ya todos los a_j por el paso anterior obtenemos el valor de $a_{i_{min}}$. Continuando este proceso cogiendo cada vez la variable más baja en el orden $>$ dentro de las variables que aún no hemos resuelto completamos el problema.

5.2.1. Recuperando el ejemplo del anterior capítulo

Usemos el método recién mostrado para resolver el ejemplo 4.1.2 visto en el capítulo anterior. Por suerte, al considerar $f(x, y, z) = x + y + z$ se verifica que $f(p_i) \neq f(p_j)$ si

$p_i \neq p_j \quad i,j \in \{1,2,3,4\}$ (esto lo sabemos porque ya tenemos la solución). Por linealidad tenemos que:

$$m_f = m_x + m_y + m_z = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

Recordemos que la base del álgebra $\frac{\mathbb{C}[x,y,z]}{J}$ era $B = \{1, z, y, yz\}$, por tanto la variable x tendrá que ser tratada después de las otras.
Ahora volviendo a recurrir a SAGE:

```
Mf=matrix(QQ\
,[[1,2,0,1],[2,1,1,0],[1,0,1,2],[0,1,2,1]]);
```

```
Mf.eigenspaces_left()
```

```
[
(4, Vector space of degree 4 and dimension 1 over Rational Field
User basis matrix:
[1 1 1 1]),
(2, Vector space of degree 4 and dimension 1 over Rational Field
User basis matrix:
[ 1  1 -1 -1]),
(-1 - 1*I, Vector space of degree 4 and dimension 1 over Algebraic Field
User basis matrix:
[   1   -1 -1*I  1*I]),
(-1 + 1*I, Vector space of degree 4 and dimension 1 over Algebraic Field
User basis matrix:
[   1   -1  1*I -1*I])
]
```

Con esto ya tenemos la información necesaria. Sabemos que cada autovector contiene información sobre la segunda y tercera coordenada de un punto concreto de la variedad. Llamemos a estos autovectores:

$$v_1 = (1,1,1,1) \qquad v_2 = (1,1,-1,-1)$$
$$v_3 = (1,-1,-i,i) \qquad v_4 = (1,-1,i,-i)\,.$$

Ahora usando la proposición 5.1 y analizando la base B sabemos que cada vector v_i y su punto asociado $p_i = (a_{1_i}, a_{2_i}, a_{3_i})$ $i \in \{1,2,3,4\}$ verifican:

$$v_i = (v_{i_1}, v_{i_2}, v_{1_3}, v_{i_4}) = \mu_i \left((a_{1_i}, a_{2_i}, a_{3_i})^{\alpha_1}, \ldots, (a_{1_i}, a_{2_i}, a_{3_i})^{\alpha_4}\right). \tag{5.13}$$

Como $\alpha_1, \ldots, \alpha_4$ son los dados por la base B, es decir, $\alpha_1 = (0,0,0)$, $\alpha_2 = (0,0,1)$, $\alpha_3 = (0,1,0)$, $\alpha_4 = (0,1,1)$, la expresión (5.13) se reduce a:

$$v_i = \mu_i\,(1, a_{i_3}, a_{i_2}, a_{i_2}a_{i_3})\,. \tag{5.14}$$

Ahora tendríamos que dividir la segunda y tercera componente de cada v_i por μ_i para obtener, respectivamente, la tercera y la segunda coordenada del punto p_i. Pero, como SAGE saca automáticamente factor común de los autovectores, la primera componente de los vectores que obtengamos repitiendo este proceso será siempre 1. Es decir, sabemos que $\mu_i = 1$ $\forall i$ y por tanto la segunda componente de cada vector es la coordenada z de su correspondiente punto y la tercera componente nos da la coordenada z. En resumen, hasta ahora sabemos:

$$p_1 = (a_{1_1}, 1, 1)\,,\ p_2 = (a_{2_1}, -1, 1)\,,\ p_3 = (a_{3_1}, -i, -1)\,,\ p_4 = (a_{4_1}, i, -1)$$

Por último, queda determinar las coordenadas x de los 4 puntos. Como se explica en el método, nos valemos de la base de Gröbner del ideal para encontrarlas. Recordemos que en el ejemplo del tema 4 obtuvimos la base de Gröbner usando SAGE con las líneas:

```
G=J.groebner_basis();G
```

```
[x - z - 1, y^2 - z, z^2 - 1]
```

Nos valemos, evidentemente, del primer polinomio de esa base $x - z - 1$ sabiendo que al evaluarlo en todo punto del ideal este tiene que dar cero. Por tanto:

$$a_{1_1} - 1 - 1 = 0 \Longrightarrow a_{1_1} = 2 \qquad a_{2_1} - 1 - 1 = 0 \Longrightarrow a_{2_1} = 2,$$
$$a_{3_1} - (-1) - 1 = 0 \Longrightarrow a_{3_1} = 0 \qquad a_{4_1} - (-1) - 1 = 0 \Longrightarrow a_{4_1} = 0$$

Recopilando todo obtenemos:

$$p_1 = (2,1,1) \qquad p_2 = (2,-1,1)$$
$$p_3 = (0,-i,-1) \qquad p_4 = (0,i,-1)$$

Que es el mismo resultado que habíamos obtenido en el tema 4.

5.3. Casos patológicos y posibles complicaciones

Como hemos trabajado en este capítulo suponiendo que el ideal era radical. Por la proposición 3.6 puede que algún punto con cierta multiplicidad se haya tratado como un punto simple. Para evitar esto y reconocer puntos múltiples, si los hay, conviene analizar si el álgebra dada por el ideal de partida tiene la misma dimensión que la obtenida al trabajar con el ideal radical. En caso de ser dimensiones distintas analizar si alguna coordenada es distinta en todos los puntos del conjunto de puntos obtenido. Si se da ese caso para la variable x_i obtendríamos los autovalores de la matriz m_{x_i} y analizar cuales se repiten para obtener las multiplicidades. El siguiente resultado versa sobre este tema y se pone aquí por una cuestión de completitud.

Proposición 5.2. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado, $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal cero dimensional. Dado $f \in \mathbb{K}[x_1, \ldots, x_n]$ se tiene que:*

$$det(m_f - \lambda Id) = (-1)^d \prod_{p \in V(I)} (\lambda - f(p))^{m(p)}. \tag{5.15}$$

Donde d es la dimensión del álgebra y $m(p)$ es la multiplicidad del punto p.

Veamos un ejemplo donde esto es relevante.

Ejemplo 5.3. Consideremos el ideal $I \subset \mathbb{C}[x, y]$ generado por los polinomios $f_1 = y^2 - 3$, $f_2 = 6y - x^3 + 9x$ y procedamos a buscar los puntos de $V(I)$ con SAGE:

```
p.<x,y>=PolynomialRing(QQ,order="lex")\
;
```

```
r.<t>=PolynomialRing(QQ)
```

```
E.<a>=QQ.extension(t^2-3)
```

En esta línea hemos construido la extensión $\mathbb{Q}(\sqrt{3})$.

```
f1=y^2-3;f2=6*y-x^3+9*x
```

```
J=Ideal(f1,f2)
```

```
Jr=J.radical();Jr
```

```
Ideal (x^2 - x*y - 6, x*y^2 - 3*x) of Multivariate Polynomial Ring
in x, y over Rational Field
```

```
Ja=J.normal_basis();Ja
```

```
[x^2*y, x*y, y, x^2, x, 1]
```

Aquí vemos que $V(I)$ tiene 6 puntos.

```
Jrnp=Jr.normal_basis();Jrnp
```

```
[x*y, y, x, 1]
```

Sin embargo, al considerar la base que nos proporciona el ideal radical, vemos que solo tiene 4 puntos.

```
Jrn=[1,y,x,x*y]
```

Aquí simplemente hemos reordenado los términos de la base.

```
fv=x-y
```

Esta es la función con la que esperamos conseguir $f(p_i) \neq f(p_j)$.

```
Jrg=Jr.groebner_basis()
```

```
Mant=[(fv*j).reduce(Jrg) for j in Jrn\
];Mant
```

```
[x - y, x*y - 3, 6, 6*y]
```

```
Mfv=matrix(E\
,[[0,-3,6,0],[-1,0,0,6],[1,0,0,0],[0,1,0,0]])
```

```
Mfv.eigenspaces_left()
```

```
[(2*a, Vector space of degree 4 and dimension 1
over Number Field in a with defining polynomial t^2 - 3
User basis matrix: [ 1 -a  a -3]),
(a, Vector space of degree 4 and dimension 1
over Number Field in a with defining polynomial t^2 - 3
User basis matrix: [  1   a 2*a   6]),
(-a, Vector space of degree 4 and dimension 1
over Number Field in a with defining polynomial t^2 - 3
User basis matrix: [   1   -a -2*a    6]),
(-2*a, Vector space of degree 4 and dimension 1
over Number Field in a with defining polynomial t^2 - 3
User basis matrix: [ 1  a -a -3])]
```

En el resultado mostrado, a denota $\sqrt{3}$. Procedemos como antes para encontrar los 4 puntos. La base monomial es $\{1, y, x, xy\}$ y por tanto $\alpha_1 = (0,0), \alpha_2 = (0,1), \alpha_3 = (1,0)$ y $\alpha_4 = (1,1)$. Ya sabíamos que $\mu_i = 1$ para los 4 vectores y, entonces, la segunda componente de cada vector nos dará la coordenada y de su punto correspondiente, mientras que la tercera componente nos da la coordenada x. Los vectores obtenidos son:

$$v_1 = \left(1, -\sqrt{3}, \sqrt{3}, -3\right) \qquad v_2 = \left(1, \sqrt{3}, 2\sqrt{3}, 6\right)$$

$$v_3 = \left(1, -\sqrt{3}, -2\sqrt{3}, 6\right) \qquad v_4 = \left(1, \sqrt{3}, -\sqrt{3}, -3\right).$$

De donde rápidamente obtenemos los puntos buscados, que son:

$$p_1 = \left(\sqrt{3}, -\sqrt{3}\right) \quad p_2 = \left(2\sqrt{3}, \sqrt{3}\right) \quad p_3 = \left(-2\sqrt{3}, -\sqrt{3}\right) \quad p_4 = \left(-\sqrt{3}, \sqrt{3}\right).$$

Ahora falta dirimir cuales de ellos son de multiplicidad mayor que 1. Observamos que los puntos tienen distinta coordenada x entre ellos. Por tanto recurrimos a calcular los autovalores de m_x:

```
Jg=J.groebner_basis()
```

```
                        Mint=[(x*j).reduce(Jg) for j in Jn];\
  Mint
```

```
[x, x*y, x^2, x^2*y, 9*x + 6*y, 9*x*y + 18]
```

```
                        Mx=matrix(E\
  ,[[0,0,0,0,0,18],[0,0,0,0,6,0],[1,0,0,0,9,0]
                        \
  ,[0,1,0,0,0,9],[0,0,1,0,0,0],[0,0,0,1,0,0]])
```

```
                        Mx.eigenvalues()
```

```
[2*a, -2*a, a, a, -a, -a]
```

Observamos con esto que las coordenadas x que se repiten son $\sqrt{3}$ y $-\sqrt{3}$. Por tanto, $m(p_1) = m(p_4) = 2$.

Otra complicación que puede surgir se da cuando f, a pesar de conseguir que $f(p_i) \neq f(p_j)\ \forall p_i, p_j \in V(I)\,,\ p_i \neq p_j$, hace que m_f no sea diagonalizable. Para proceder en esta situación basta probar con distintas funciones.

Bibliografía

[1] B. Buchberger, An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal, *Journal of Symbolic Computation, 41* p 475-511. 2006.

[2] D. A. Cox, J. Little, D. O' Shea, *Ideals, Varieties and Algorithms* 2 ed., Springer, 2004

[3] D. A. Cox, J. Little, D. O' Shea, *Using Algebraic Geometry*, 2 ed., Springer, 2005.

[4] A. L. Gorodentsev, *Algebra II*, 1 ed., Springer, 2017.