Universidad Nacional Autónoma de México

Facultad de Ciencias

CONJUNTOS SEMI-ALGEBRAICOS REALES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A:

MÓNICA DE NOVA VÁZQUEZ

DIRECTOR DE TESIS:

DRA. ADRIANA ORTIZ RODRÍGUEZ

2009

Hoja de Datos del Jurado

1. Datos del alumno
   De Nova
   Vázquez
   Mónica
   57 31 85 56
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Matemáticas
   302254655

2. Datos del tutor
   Dra
   Adriana
   Ortiz
   Rodríguez

3. Datos del sinodal 1
   Dr
   Alberto León
   Kushner
   Shnur

4. Datos del sinodal 2
   Dr
   Héctor
   Méndez
   Lango

5. Datos del sinodal 3
   Dra
   Laura
   Ortíz
   Bobadilla

6. Datos del sinodal 4
   Dr
   Ernesto
   Rosales
   González

7. Datos del trabajo escrito
   Conjuntos Semi-algebraicos Reales
   105 p
   2009

¡Oh matemáticas severas!

Con ayuda de vuestra leche fortificante, mi inteligencia se ha desarrollado rápidamente, adquiriendo proporciones enormes en medio de la estupenda claridad que entregáis como regalo a todos aquellos que os aman con amor sincero...

-Conde de Lautréamont

A Rocío Lizeth,

que algún día tus pasos te lleven

al camino de las matemáticas

A Dios

Gracias señor por permitirme llegar a
este momento tan importante de mi vida.

A mis padres

Gracias *mamá* por todo tu tiempo, tu inmenso cariño,
incondicional apoyo y tierno cuidado para mi.
Papá, gracias por enseñarme a defender lo que pienso
y lo que soy, y por todo tu cariño.

A mis hermanos y cuñado

Rocío gracias por ser mi ejemplo, mi guía y mi
hermana consentida; *Arturo*, por ser ejemplo de
disciplina en el ámbito científico y *Enrique*,
las palabras sobran, gracias por estar, por ser mi
cómplice de vida y mi mejor amigo.
Jorge, gracias por tu apoyo, algunas veces directo
otras indirecto y por aguantar a esta familia.

A mi asesora y sinodales

Dra. Adriana Ortiz, gracias por tus enseñanzas en cada
una de las materias que me impartiste y tus amables asesorías,
de no ser por ti esta tesis no habría visto la luz.
Gracias a cada uno de mis sinodales por el tiempo
tomado para este trabajo.

A la Universidad Nacional Autónoma de México

Gracias a esta noble institución educativa y en especial
a la Facultad de Ciencias por forjar mi pensamiento
matemático. Agradezco también el apoyo económico
otorgado del proyecto IN102009-PAPIIT.

A mis amigos

Cynthia, gracias por tu apoyo y cariño siempre,
y sobre todo, por tener palabras de aliento para mi;
Gabys y Rob, por acompañarme en este andar por
la universidad, convirtiéndose en mis grandes amigos;
Aldo, por las buenas charlas matemáticas, la respuesta
está en π. *Miriam y Mary Carmen* (mis dos amargas),
por sus charlas que siempre me devuelven la calma
cuando siento perder el camino. De manera muy especial
a *Jesusin, Liz, Victor y Guadalupe*.

Agradezco también a cada uno de mis profesores
y a las personas que han pasado por mi vida, de cada una
he aprendido y gracias a ello hoy estoy aquí.

Índice general

Introducción

La Geometría siempre estuvo presente en cada uno de los semestres de mi vida universitaria y aunque en aquellos inicios desconocía el tema a desarrollar en una tesis nunca dude que hablaría sobre geometría.

Estudiar conjuntos semi-algebraicos reales surge a partir de mi encuentro con las curvas algebraicas tratadas en un Seminario de Geometría; fue en ese momento que descubrí que dos ramas de la matemática podían unirse de manera muy estrecha: la geometría y el álgebra. Esta unión no puede más que tener consecuencias bastante interesantes.

Sin embargo, para desarrollar toda la teoría referente a estos conjuntos, necesitamos recordar algunas definiciones y propiedades relacionadas con la teoría de anillos, teoría de conjuntos, topología y por supuesto, con los anillos de polinomios. Es por ello, que el primer capítulo de este trabajo está dedicado a establecer estas definiciones, esto es, el primer capítulo se convierte así en los preliminares de lo que se desarrollará en los siguientes capítulos.

En primer lugar, un conjunto algebraico es un conjunto que puede ser descrito a partir de un número finito de polinomios, precisamente, los conjuntos algebraicos son los ceros de dichos polinomios. En cambio, los conjuntos semi-algebraicos reales, ya no

sólo son los ceros de polinomios, sino que incluyen regiones descritas por desigualdades de polinomios. De esta manera, todo conjunto algebraico es semi-algebraico. Esta particularidad fue la que me condujo a esta estructura de trabajo. Me ha sido más sencillo trabajar primero con los conjuntos algebraicos y sus propiedades para posteriormente generalizar a los conjuntos semi-algebraicos.

Siendo así, el capítulo 2 está dedicado a los conjuntos algebraicos y algunas de sus propiedades. Este capítulo tiene objetivos particulares - como que cualquier ideal en un anillo de polinomios tiene una base finita que lo genera o como se puede describir al ideal - sin embargo, lo desarrollado en éste fijará bases para abordar la teoría del último capítulo.

Alfred Harnack plantea en 1876 que cualquier curva algebraica en el plano proyectivo real tiene un número finito de componentes conexas, incluso exhibe una cota superior. Y al hacer ejemplos de conjuntos algebraicos y semi-algebraicos reales en dimensiones pequeñas, como 2 ó 3, pareciera que estos conjuntos tienen un número finito de componentes conexas.

Así, la pregunta que surge a raíz de este importante teorema y un tanto de la intuición que se percibe en estas dimensiones es:

> *¿Todo conjunto semi-algebraico real tiene un número finito de componentes conexas?*

Y de ésta se derivan otras, por ejemplo: si resultara que, efectivamente cualquier conjunto semi-algebraico tiene un número finito de componentes conexas, entonces ¿cómo son estas componentes, es decir, son también conjuntos semi-algebraicos? ¿se pueden describir estas componentes conexas?

La respuesta a esta pregunta es positiva; es el primer teorema de estructura de los conjuntos semi-algebraicos reales. En la primera parte del capítulo 3, se desarrollan algunas propiedades de los conjuntos semi-algebraicos reales. La parte central del capítulo 3 está enfocada a mostrar este primer teorema de estructura. Dicho resultado es el objetivo principal de este trabajo. Todas las definiciones y resultados se desarrollarán con el fin de llegar al objetivo.

El capítulo 3, aunque es el más pesado, en el sentido teórico (pues utiliza resultados abordados durante todo el trabajo), resulta ser claro.

El trabajo culmina mostrando que las componentes de los conjuntos semi-algebraicos son también conjuntos semi-algebraicos. Se concluye dando algunos ejemplos de conjuntos semi-algebraicos reales.

Capítulo 1

Preliminares

En este capítulo se darán una serie de definiciones que pertenecen a ciertas ramas de la matemática, debido a que los conceptos referentes a conjuntos semi-algebraicos, que se verán en los siguientes capítulos, se basan en estas definiciones.

La primera sección de este capítulo es referente a la teoría de grupos y de anillos, ya que algunos resultados del segundo capítulo están estrechamente ligados con éstas. Se hará mención de algunos teoremas que se requerirán para estudiar los conjuntos semi-algebraicos, sin embargo, estos teoremas no serán demostrados pues no atañen de manera directa al tema en cuestión y por otro lado, son demostraciones que se estudian en cursos escolares o bien, se pueden encontrar en la bibliografía referente al *álgebra moderna* [4] y [6]. Así, la parte correspondiente a establecer las definiciones de grupo y anillo, así como algunas propiedades que pueden cumplir, mencionando algunos ejemplos se dan con el único propósito de aclarar dichos conceptos.

La segunda parte, teniendo ya el previo estudio de la definición de anillo, está dedicada a establecer la definición de anillo de polinomios (pues los conjuntos semi-algebraicos están definidos por polinomios).

La tercera sección trata sobre órdenes en anillos. En mayor medida, la última sección, es referente a espacios topológicos.

1.1. Grupos y anillos

Una *operación binaria* $*$ *en un conjunto*, es una regla que asigna a cada par ordenado de elementos de un conjunto, algún elemento del conjunto, es decir, en un conjunto X, una operación binaria es una función $* : X \times X \longrightarrow X$.

Un ejemplo de una operación binaria es definir $* : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ tal que $a * b = a$. Así, $2 * 11 = 2$; $10 * -2 = 10$ y $3 * 3 = 3$.

Este concepto nos permite definir lo que es un grupo.

Definición 1.1 Un *grupo* $\langle G, * \rangle$ es un conjunto G, junto con una operación binaria $*$ en G, tal que se satisfacen los siguientes axiomas:

1. La operación binaria $* : G \times G \longrightarrow G$ es asociativa.

2. Existe un elemento e en G tal que $e * x = x * e = x$ para toda $x \in G$ (este elemento e es llamado un *elemento identidad* para $*$ en G).

3. Para cada a en G, existe un elemento a' en G tal que $a' * a = a * a' = e$ (el elemento a' es llamado un *inverso de a respecto de* $*$).

Un grupo $\langle G, * \rangle$ es *abeliano* si su operación binaria $*$ es conmutativa.

Como ejemplo de un grupo abeliano tenemos a $\langle \mathbb{Z}, + \rangle$, donde su elemento neutro es el cero. Sin embargo, no todos los grupos son abelianos, por ejemplo, si tomamos el conjunto de las matrices de 2×2 con coeficientes en $\mathbb{R}$ y determinante distinto de cero, el cual se denota de la siguiente manera

$$GL_2(\mathbb{R}) := \{A \in M_{2\times 2}(\mathbb{R}) \mid det(A) \neq 0\},$$

con la operación binaria producto (multiplicación de matrices) y elemento neutro la matriz identidad, es un grupo no abeliano.

Definición 1.2 Un *anillo* $\langle A, +, \cdot \rangle$ es un conjunto A junto con dos operaciones binarias $+, \cdot : A \times A \longrightarrow A$, que llamamos *suma* y *multiplicación* respectivamente, definidas en A tales que satisfacen los siguientes axiomas:

1. $\langle A, + \rangle$ es un grupo abeliano.

2. La multiplicación es asociativa.

3. Para todas las $a, b, c \in A$, se cumple tanto la ley distributiva izquierda como la ley distributiva derecha, es decir

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

Hay varios tipos de anillo según las propiedades que tenga. Así, un anillo en donde la multiplicación es conmutativa es un *anillo conmutativo*. Un anillo $\langle A, +, \cdot \rangle$ con identidad multiplicativa 1 tal que $1 \cdot x = x \cdot 1 = x$ para toda $x \in A$ es un *anillo con unitario*.

Un *elemento unitario* es una identidad multiplicativa en un anillo y un *inverso multiplicativo* de un elemento a en un anillo $\langle A, +, \cdot \rangle$ con unitario 1 es un elemento $a^{-1} \in A$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Si $\langle A, +, \cdot \rangle$ es un anillo con unitario, entonces un elemento u en A es una *unidad de* A si tiene un inverso multiplicativo en A. Con esto, se define otro tipo de anillo; si todo elemento distinto del neutro aditivo en A es una unidad, entonces $\langle A, +, \cdot \rangle$ es un *semi campo* o *anillo con división*. Por último, un *campo* K es un anillo conmutativo con división.

El ejemplo más sencillo de un semi campo en el cual no se cumple la propiedad conmutativa del producto es el anillo de los cuaterniones de Hamilton, el cual se representa

de la siguiente manera

$$\mathbb{H} = \{a_1 + a_2 i + a_3 j + a_4 k = (a_1, a_2, a_3, a_4) \mid a_1, a_2, a_3, a_4 \in \mathbb{R}\},$$

donde $1 = (1,0,0,0)$, $i = (0,1,0,0)$, $j = (0,0,1,0)$ y $k = (0,0,0,1)$. La suma se define componente a componente y para definir el producto comenzamos definiendo $1 \cdot a = a \cdot 1 = a$, $\forall\ a \in \mathbb{H}$, $i^2 = j^2 = k^2 = -1$ y $i \cdot j = k$, $j \cdot k = i$, $k \cdot i = j$, $j \cdot i = -k$, $k \cdot j = -i$ y $i \cdot k = -j$. Así, se puede definir el producto como sigue

$$\begin{aligned}(a_1 + a_2 i + a_3 j + a_4 k) \cdot (b_1 + b_2 i + b_3 j + b_4 k) &= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + \\ &+ (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) i + \\ &+ (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) j + \\ &+ (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) k.\end{aligned}$$

Los elementos de un anillo pueden cumplir propiedades interesantes, derivando así más tipos de anillos. Si a y b son dos elementos distintos del neutro aditivo del anillo $\langle A, +, \cdot \rangle$ tales que $a \cdot b = 0$, entonces a y b son *divisores de 0*. En paticular, a es un *divisor izquierdo de 0* y b es un *divisor derecho de 0*. Este concepto de los divisores nos lleva a definir dominio entero: $\langle A, +, \cdot \rangle$ es un *dominio entero* si es un anillo conmutativo con unitario que no contiene divisores de 0.

El anillo $\langle \mathbb{Z}, +, \cdot \rangle$ es un dominio entero, ya que no tiene divisores de 0, es decir, si $a \cdot b = 0$ entonces $a = 0$ o $b = 0$. De hecho, si p es primo entonces $\langle \mathbb{Z}_p, +, \cdot \rangle$ es dominio entero. Por otro lado, $\langle \mathbb{Z}_{12}, +, \cdot \rangle$ no es dominio entero porque 2, 3, 4, 6, 8, 9 y 10 son divisores de 0.

De hecho, es sencillo probar que todo campo es un dominio entero y que todo dominio entero finito es un campo.

Para un dominio entero D y $a, b \in D$, decimos que a *divide* b (o a *es un factor de* b) si existe $c \in D$ tal que $b = ac$. Además, dos elementos $a, b \in D$ son *asociados en* D si $a = bu$, donde u es una unidad de D.

Por último, enunciaremos una definición de un dominio que resulta ser muy importante.

Definición 1.3 Un dominio entero D es un *dominio de factorización única* (DFU), si se satisfacen las siguientes condiciones:

1. Todo elemento de D que no sea ni cero ni unidad, se puede factorizar en un número finito de irreducibles.

2. Si $p_1, \ldots, p_r$ y $q_1, \ldots, q_s$ son dos factorizaciones en irreducibles del mismo elemento de D, entonces $r = s$ y los q_j pueden renumerarse de manera que p_i y q_i sean asociados.

Una consecuencia importante y que nos interesa es que si D es un DFU, entonces $D[x]$ es un DFU. Y por lo tanto, si K es un campo entonces $K[x_1, \ldots, x_n]$ es un DFU.

1.2. Anillo de polinomios

Sea A un anillo. Un *polinomio* $f(x)$ *con coeficientes en* A e indeterminada x es una suma formal infinita

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots$$

donde $a_i \in A$ para todo $i \geq 0$, $a_i = 0$ para todos, excepto un número finito de valores i. Las a_i son los *coeficientes de* $f(x)$. Si para alguna $i > 0$ es cierto que $a_i \neq 0$, el mayor de dichos valores i es el *grado de* $f(x)$ (denotado por $gra(f)$). De no existir dicha $i > 0$, entonces $f(x)$ es de *grado cero*.

La suma y multiplicación de polinomios con coeficientes en un anillo A están definidas de la siguiente manera: si

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_n x^n + \ldots \\ g(x) &= b_0 + b_1 x + \ldots + b_n x^n + \ldots \end{aligned}$$

entonces, para el *polinomio suma*, tenemos

$$f(x) + g(x) := c_0 + c_1x + \ldots + c_nx^n + \ldots$$

donde $c_n = a_n + b_n$ para toda $n \geq 0$ y, para el *polinomio multiplicación*, tenemos

$$f(x)g(x) := d_0 + d_1x + \ldots + d_nx^n + \ldots$$

donde $d_n = \sum_{i=0}^{n} a_i b_{n-i}$. Es claro que, de nuevo, c_i y d_i ambas son cero para todos, salvo un número finito de valores i, así que estas operaciones son cerradas en el conjunto de todos los polinomios con coeficientes en A.

A continuación se enunciará un teorema importante sobre los anillos de polinomios, el cual se utilizará en demostraciones posteriores.

Teorema 1.1 *El conjunto $A[x]$ de todos los polinomios en una indeterminada x con coeficientes en un anillo A, es un anillo bajo la suma y multiplicación polinomial. Si A es conmutativo, entonces, lo es $A[x]$ y si A tiene unitario 1, entonces 1 también es unitario en $A[x]$.*

Si A es un anillo y x y y son indeterminadas, podemos formar el anillo $(A[x])[y]$, esto es, el anillo de polinomios en y cuyos coeficientes son polinomios en x. Además $(A[x])[y]$ es naturalmente isomorfo a $(A[y])[x]$. Identificaremos estos anillos mediante este isomorfismo natural y lo consideraremos el anillo $A[x, y]$, *el anillo de polinomios en dos indeterminadas x y y con coeficientes en A*. Se define de manera análoga el *anillo $A[x_1, \ldots, x_n]$ de polinomios en n indeterminadas x_i con coeficientes en A*.

Además, si D es un dominio entero, entonces también lo es $D[x]$. En particular, si K es un campo, entonces $K[x]$ es un dominio entero. En el tercer capítulo se utilizarán en mayor medida resultados sobre el anillo de polinomios, donde el anillo es campo.

Teorema 1.2 (Algoritmo de la división) *Sean*

$$\begin{aligned} f(x) &= a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0 \\ g(x) &= b_mx^m + b_{m-1}x^{m-1} + \ldots + b_0, \end{aligned}$$

dos elementos de $K[x]$, donde K es campo, con a_n y b_m ambos elementos distintos del cero de K. Entonces, existen polinomios únicos $q(x)$ y $r(x)$ en $K[x]$ tales que $f(x) = g(x)q(x) + r(x)$, donde el grado de $r(x)$ es menor que el grado de $g(x)$.

Este teorema tiene una consecuencia importante y que utilizaremos en todo el trabajo. Recordemos que una *raíz* o *cero* en K de un polinomio $f(x)$ es un elemento $a \in K$ tal que $f(a) = 0$. Notemos que la definición es la misma si hablamos de un anillo de polinomios en varias variables.

Corolario 1.1 *Un polinomio distinto de cero en $K[x]$ de grado n puede tener a lo más n raíces en un campo K.*

Además, si K es un campo, decimos que K es *algebraicamente cerrado* si todo polinomio no constante $f \in K[x]$ en una variable, tiene al menos una raíz en K.

Tenemos que $\mathbb{R}$ es un ejemplo de un campo que no es algebraicamente cerrado, pues el polinomio $f(x) = x^2 + 1$ no tiene sus raíces en $\mathbb{R}$. Mientras que $\mathbb{C}$ sí es un campo algebraicamente cerrado, de hecho, tenemos el *Teorema Fundamental del Álgebra*, el cual dice que todo polinomio en una variable, con coeficientes en los complejos y de grado mayor que cero tiene al menos una raíz en $\mathbb{C}$. Como consecuencia de este teorema, tenemos otro que resulta importante.

Teorema 1.3 (de factorización) *Sea $f(x) \in \mathbb{C}[x]$ de grado $n > 0$. Entonces existen n números complejos, $\alpha_1, \alpha_2, \ldots, \alpha_n$, no necesariamente diferentes dos a dos, y un complejo c tales que*

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

Además, esta factorización es única.

Observación 1.1 *Sea $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$, $c \neq 0$ y $n > 0$. Entonces a es raíz de $f(x)$ si y sólo si $a = \alpha_i$ para alguna i.*

Esta observación da lugar a la noción de multiplicidad de una raíz. Es decir, se dice que *a es una raíz de multiplicidad m de* $f(x)$ si hay precisamente m índices i para los cuales $a = \alpha_i$.

Decimos que un polinomio no constante $f \in K[x]$ es *irreducible sobre* K o es un *polinomio irreducible en* $K[x]$ si f no puede expresarse como producto de dos polinomios $g(x)$ y $h(x)$ en $K[x]$, ambos de grado menor que el grado de $f(x)$ y de grado mayor o igual que 1.

Definición 1.4 Sean $p, q \in K[x]$ polinomios no nulos. Decimos que $r \in K[x]$ es un *máximo común divisor de* p *y* q si

1. r divide tanto a p como a q.

2. Si $f \in K[x]$ tal que f divide a p y q, entonces f divide a r.

Y lo denotamos por $MCD(p, q)$.

El algoritmo de la división nos permite encontrar el máximo común divisor de dos polinomios. De hecho, se puede mostrar que como $K[x]$ es un DFU, entonces cualesquiera $p, q \in K[x]$ tienen un máximo común divisor: factorizando p y q en irreducibles.

En el caso del campo de los complejos tenemos una importante relación entre las raíces de un polinomio y sus derivadas. Si $f(x) = a_0 + a_1x + \ldots + a_nx^n$, con $a_i \in \mathbb{C}$, definimos la *derivada* $f'(x)$ de $f(x)$ como

$$f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}.$$

Para $n \geq 1$ definimos la $n+1$-*ésima derivada*, $f^{(n+1)}(x)$, como la derivada de la n-ésima derivada. Y con estas definiciones podemos establecer el siguiente teorema.

Teorema 1.4 *Sea* $f \in \mathbb{C}[x]$ *de grado* $n > 0$ *y sea* m *un entero positivo. Entonces,* a *es raíz de multiplicidad* m *de* f *si y sólo si se cumplen las condiciones siguientes:*

a) $f(a) = f'(a) = \ldots = f^{(m-1)}(a) = 0$.

b) $f^{(m)}(a) \neq 0$.

Convenimos que $f^{(0)}(x) = f(x)$. *En el caso* $m = 1$, *la condición a) se reduce a* $f(a) = 0$.

1.3. Órdenes

En el capítulo 2 se abordará el concepto de orden monomial y su relación con los conjuntos algebraicos, por ello, es necesario establecer la definición de orden, así como los tipos de órdenes.

Tenemos que un conjunto R es una *relación (binaria)* si todo elemento de R es un par ordenado, es decir, si para todo $z \in R$, existen $x \in A$ y $y \in B$ (donde A y B son conjuntos) tales que $z = (x, y)$. Si $R \subseteq A \times B$ diremos que R *es una relación de* A *en* B, *o entre* A *y* B, y si $R \subseteq A \times A$ diremos simplemente que R *es una relación en* A. Denotamos por xRy cuando x *está en relación* R *con* y.

Si R es una relación en A tenemos que:

1. R es llamada *reflexiva en* A si para todo $a \in A$, aRa.
2. R es llamada *simétrica en* A si para todo $a, b \in A$, aRb implica bRa.
3. R es llamada *transitiva en* A si para todo $a, b, c \in A$, aRb y bRc implica aRc.
4. R es llamada *antisimétrica en* A si para todo $a, b \in A$, aRb y bRa implica $a = b$.
5. R es llamada *asimétrica en* A si para todo $a, b \in A$, aRb implica que no ocurre bRa.

Así, una relación R se llama *de equivalencia en* A, si es reflexiva, simétrica y transitiva en A. Generalmente una relación de equivalencia se denota por $\equiv, \cong, \approx$ o $\sim$. Si $\sim$ es una relación de equivalencia y $a \in A$, entonces la *clase de equivalencia de* a se define como el siguiente conjunto:

$$[a] := \{x \in A \mid x \sim a\}.$$

Con estos conceptos, podemos establecer la definición de *orden*.

Definición 1.5 Una relación R en A, que es reflexiva, antisimétrica y transitiva se llama *orden (parcial)* en A. Al par (A, R) se le llama *conjunto (parcialmente) ordenado*.

A aRb se le puede leer como "a es menor o igual que b" o "b es mayor o igual que a". Así, todo elemento de A es menor (mayor) o igual a sí mismo. Generalmente se usan los símbolos $\leq, \preceq, \ll$, para denotar órdenes.

Definición 1.6 Una relación R en A es un *orden estricto*, si es asimétrica y transitiva.

Además, dados $a, b \in A$ y $\leq$ un orden en A, decimos que a y b son *comparables en el orden* $\leq$ (o que son $\leq$-*comparables*) si

$$a \leq b \text{ o } b \leq a.$$

Decimos que a y b son $\leq$-*incomparables* si no son $\leq$-comparables. Similarmente se definen para un orden estricto $<$ las nociones de $<$-comparables y $<$-incomparables.

Definición 1.7 Un orden $\leq$ (o $<$) es llamado *lineal* o *total* si cualesquiera dos elementos de A son comparables. El par $(A, \leq)$ es entonces llamado *conjunto linealmente* o *totalmente ordenado*.

Definición 1.8 Sea $\leq$ un orden en A y sea $B \subseteq A$.

1. $b \in B$ es el *elemento mínimo de* B en el orden $\leq$ si para todo $x \in B$, $b \leq x$.

2. $b \in B$ es el *elemento máximo de* B en el orden $\leq$ si para todo $x \in B$, $x \leq b$.

El siguiente tipo de conjunto totalmente ordenado es muy importante.

Definición 1.9 Un conjunto parcialmente ordenado $(W, \leq)$ se llama *bien ordenado* si cada subconjunto no vacío $B \subseteq W$ tiene elemento mínimo. En este caso al orden $\leq$ se le llama *buen orden*.

1.4. Topología

En el tercer capítulo se utilizan de manera constante conceptos de espacios topológicos, así como el de topología cociente y algunos otros relacionados con éstos.

Recordemos que para cualquier conjunto X existe un conjunto S tal que $A \in S$ si y sólo si $A \subseteq X$. Puesto que el conjunto S está unívocamente determinado, llamamos al conjunto S de todos los subconjuntos de X, el *conjunto potencia* de X y lo denotamos por $\mathcal{P}(X)$.

Definición 1.10 Una *topología* sobre un conjunto X es una familia $\tau \subset \mathcal{P}(X)$ tal que verifica los siguientes axiomas:

1. $\emptyset, X \in \tau$.
2. Si $\{A_i\}_{i \in I} \subset \tau$, entonces $\bigcup_{i \in I} A_i \in \tau$.
3. Si $A, B \in \tau$, entonces $A \cap B \in \tau$.

Los elementos de τ se llaman *abiertos* y el par (X, τ) se llama *espacio topológico*.

Un subconjunto $V \subset X$ es una *vecindad* de un punto x en (X, τ), si existe un abierto $U \in \tau$ tal que $x \in U \subset V$. La familia $\mathcal{N}_x$ de todas las vecindades de x se llama *sistema de vecindades* de x.

En (X, τ), una familia $\beta \subset \tau$ es una *base* de τ, si para todo $U \in \tau$ y para cada $x \in U$, existe $B \in \beta$, tal que $x \in B \subset U$. Los elementos de β se llaman *abiertos básicos*.

Definición 1.11 Sea $f : (X, \tau_X) \longrightarrow (Y, \tau_Y)$ una función entre dos espacios topológicos, donde τ_X es la topología sobre X y τ_Y es la topología sobre Y. Se dice que f es *continua* en a, si para toda vecindad $M \in \mathcal{N}_{f(a)}$, existe $N \in \mathcal{N}_a$, tal que $f(N) \subset M$. Una función es *continua en* A si lo es en cada punto de A.

La siguiente proposición nos ayuda a identificar funciones continuas de una manera más sencilla que siguiendo la definición. La demostración no se dará, pues puede encontrarse en cualquier libro de *topología general* [10].

Proposición 1.1 *Sea $f : (X, \tau_X) \longrightarrow (Y, \tau_Y)$ una función entre dos espacios topológicos. La función f es continua si y sólo si para todo básico β en Y, $f^{-1}(\beta) \in \tau_X$.*

Definición 1.12 Una aplicación $f : (X, \tau_X) \longrightarrow (Y, \tau_Y)$ es un *homeomorfismo*, si f es biyectiva, continua y con inversa f^{-1} continua. Decimos que (X, τ_X) es *homeomorfo* a (Y, τ_Y).

Si $f : (X, \tau_X) \longrightarrow Y$ es una aplicación, entonces definimos la siguiente familia

$$\tau^f = \{B \subseteq Y \mid f^{-1}(B) \in \tau\}.$$

Se puede demostrar fácilmente que τ^f es una topología en Y, de hecho, es llamada la *topología coinducida* en Y. También, es sencillo ver que $f : (X, \tau_X) \longrightarrow (Y, \tau^f)$ es continua.

Esta forma de construir topologías forma el camino para definir un tipo importante de topología y con la cual se va a trabajar más adelante.

Consideramos (X, τ) un espacio topológico y $\sim$ una relación de equivalencia. Denotaremos por $X/\sim$ el conjunto de todas las clases de equivalencia, esto es

$$X/\sim := \{[x] \mid x \in X\}.$$

La función $\pi : X \longrightarrow X/\sim$ definida por $\pi(x) = [x]$, denominada *proyección cociente* coinduce una topología en $X/\sim$. El espacio así definido recibe el nombre de *espacio cociente* y la topología coinducida se llama *topología cociente*. U es abierto en $X/\sim$ si y sólo si $\pi^{-1}(U) \in \tau$.

Como trabajaremos en mayor medida con espacios normados, definiremos cuales son éstos y sus topologías.

Sea X un conjunto no vacío. Una función $d : X \times X \longrightarrow \mathbb{R}$ es llamada una *métrica* en X si satisface:

1. $d(x, y) \geq 0$ para todas $x, y \in X$.

2. $d(x, y) = 0$ si y sólo si $x = y$.

3. $d(x, y) = d(y, x)$ para todas $x, y \in X$.

4. $d(x, y) \leq d(x, z) + d(z, y)$ para todas $x, y, z \in X$.

Así, si d es una métrica en X, para cualquier punto $p \in X$ y cualquier número real $\delta > 0$, podemos definir el conjunto de puntos de distancia a lo más δ de p, es decir,

$$S(p, \delta) := \{x \in X \mid d(p, x) < \delta\}.$$

A $S(p, \delta)$ le llamamos *bola abierta* con centro p y radio δ.

Definición 1.13 Sea d una métrica en un conjunto no vacío X. La topología τ en X generada por la familia de bolas abiertas en X es llamada la *topología métrica* (o la topología *inducida* por la métrica d). Más aún, el conjunto X junto con la topología τ inducida por la métrica d es llamado un *espacio métrico* y es denotado por (X, d).

Para establecer la definición de espacio normado, necesitamos conocer la definición de espacio vectorial.

Definición 1.14 Un *espacio vectorial* V sobre un campo F es un conjunto de elementos en el que están definidas dos operaciones binarias, llamadas *suma vectorial* y *producto por un escalar*, que satisfacen lo siguiente:

1. $x + y = y + x$, para todas $x, y \in V$.

2. $(x + y) + z = x + (y + z)$, para todas $x, y, z \in V$.

3. Existe un elemento 0 en V tal que $0 + x = x + 0 = x$ para toda $x \in V$.

4. Si $x \in V$ existe un elemento $-x \in V$ tal que $x + (-x) = (-x) + x = 0$.

5. $1x = x$ con $1 \in F$ y para todo $x \in V$.

6. $a(bx) = (ab)x$ para todas $a, b \in F$ y $x \in V$.

7. $a(x+y) = ax + ay$ y $(a+b)x = ax + bx$ para todas $a, b \in F$ y $x, y \in V$.

De esta manera, un espacio vectorial X se llama *espacio normado* cuando a cada $x \in X$ se le asigna un número real no negativo $||x||$, llamado *norma* de x, de manera que

1. $||x|| \geq 0$ para todo $x \in X$ y $||x|| = 0$ si $x = 0$.

2. $||ax|| = |a|||x||$ si $x \in X$ y a es un escalar.

3. $||x + y|| \leq ||x|| + ||y||$ para cualesquiera $x, y \in X$.

Si X es un espacio normado, la función d definida por $d(v, w) = ||v - w||$ donde $v, w \in X$, es una métrica, llamada *métrica inducida* en X. Así, cada espacio normado con la métrica inducida es un espacio métrico y de ahí que sea también un espacio topológico.

Un ejemplo de un espacio normado es $\mathbb{C}^n$, por medio de la métrica euclídea usual, es decir, si $z = (z_1, \ldots, z_n) \in \mathbb{C}^n$ entonces $||z|| = (|z_1|^2 + \ldots + |z_n|^2)^{1/2}$. Se pueden definir otras normas en $\mathbb{C}^n$, por ejemplo

$$||z|| = |z_1| + \ldots + |z_n| \qquad \text{ó} \qquad ||z|| = max\{|z_i| \mid 1 \leq i \leq n\}.$$

Estas normas corresponden a diferentes métricas en $\mathbb{C}^n$ (con $n > 1$) pero se puede ver que inducen la misma topología sobre $\mathbb{C}^n$.

De hecho, podemos identificar $\mathbb{C}^n$ con $\mathbb{R}^{2n}$ y resulta que la métrica de $\mathbb{C}^n$ es la métrica euclídea usual en $\mathbb{R}^{2n}$. Por tanto, la topología de $\mathbb{C}^n$ es exactamente la topología euclídea de $\mathbb{R}^{2n}$.

Podemos establecer la definición de continuidad entre espacios métricos, es decir, si (X, d) y (Y, d^*) son espacios métricos, entonces una función f de X a Y es continua en $p \in X$ si para cada $\epsilon > 0$ existe una $\delta > 0$ tal que si $d(p, x) < \delta$ entonces

$$d^*(f(p), f(x)) < \epsilon.$$

En el capítulo 3 utilizaremos un teorema que relaciona espacios compactos con espacios de Hausdorff, por lo que necesitamos tales definiciones.

Un espacio topológico X es un *espacio de Hausdorff* o *espacio* T_2 si y sólo si para cualesquiera $a, b \in X$, $a \neq b$, existen conjuntos abiertos A, B tales que $a \in A$, $b \in B$ y $A \cap B = \emptyset$.

Lema 1.1 *Todo espacio métrico* (X, d) *es Hausdorff.*

Prueba. Sean $a, b \in X$ puntos distintos, entonces $d(a, b) = \epsilon > 0$. Consideramos las bolas abiertas $A = S(a, \frac{1}{3}\epsilon)$ y $B = S(b, \frac{1}{3}\epsilon)$. Supongamos que existe $p \in A \cap B$, es decir, $d(a, p) < \frac{1}{3}\epsilon$ y $d(b, p) < \frac{1}{3}\epsilon$. Por la desigualdad del triángulo tenemos

$$d(a, b) \leq d(a, p) + d(b, p) < \frac{2}{3}\epsilon.$$

Lo cual es una contradicción. Por lo tanto, $A \cap B = \emptyset$, es decir, (X, d) es Hausdorff. ■

Por este lema podemos afirmar que tanto $\mathbb{R}^n$ como $\mathbb{C}^n$ son espacios de Hausdorff.

Definición 1.15 Se dice que un conjunto K es *compacto* si siempre que está contenido en la unión de una colección $\mathcal{G} = \{G_i\}$ de conjuntos abiertos, también está contenido en la unión de algún número finito de conjuntos en $\mathcal{G}$.

Identificar conjuntos compactos en $\mathbb{R}^n$, resulta sencillo gracias al teorema de Heine-Borel, el cual daremos a continuación, no así la demostración pues no interviene directamente en este trabajo.

Teorema 1.5 (de Heine-Borel) *Un subconjunto de* $\mathbb{R}^n$ *es compacto si y sólo si es cerrado y acotado.*

Si definimos lo que es un *punto de acumulación* en un conjunto, respecto a una sucesión de un conjunto, es decir, si S es un conjunto y $\{x_n\}$ una sucesión en S, a es *punto de acumulación* de $\{x_n\}$ si para toda $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que $\forall\ n \geq N$, $||x_n - a|| < \epsilon$. Así, podemos establecer que un conjunto de S es *compacto* si cada

sucesión de elementos del conjunto tiene un punto de acumulación en S. Es sencillo ver que a partir de esta definición, se cumple el siguiente teorema.

Teorema 1.6 *Un conjunto de $\mathbb{C}^n$ es compacto si y sólo si es cerrado y acotado.*

Existen algunas propiedades de compactos y funciones continuas que nos interesan.

Proposición 1.2 *Sea $f : (X, \tau_X) \longrightarrow (Y, \tau_Y)$ función continua. Si $K \subset X$ es compacto, entonces $f(K) \subset Y$ es compacto.*

Enunciaremos un teorema que relaciona espacios compactos y espacios de Hausdorff que usaremos en el capítulo 3.

Teorema 1.7 *Sea f una función biyectiva continua de un espacio compacto X a un espacio de Hausdorff Y. Entonces, X y $f(X)$ son homeomorfos.*

Por último, se dice que un subconjunto $D \subseteq \mathbb{R}^n$ es *inconexo* si existen dos conjuntos abiertos A, B tales que $A \cap D$ y $B \cap D$ son ajenos, no vacíos y su unión es D. Así, un subconjunto que no es inconexo se dice que es *conexo*.

Como ejemplo tenemos que la totalidad de $\mathbb{R}^p$ es conexo, mientras que el subconjunto $\mathbb{N} \subseteq \mathbb{R}$ es inconexo.

Si x, y son dos puntos en $\mathbb{R}^n$, entonces *una curva poligonal* que une a x con y es un conjunto P que se obtiene de la unión de un número finito de segmentos de línea ordenados $(L_1, L_2, \ldots, L_s)$ en $\mathbb{R}^n$, tales que el segmento de línea L_1 tiene como puntos terminales x y z_1; el segemento de línea L_2 tiene como puntos terminales z_1 y z_2; $\ldots$; y el segmento de línea tiene como puntos terminales z_{s-1} y y.

Teorema 1.8 *Sea G un conjunto abierto en $\mathbb{R}^p$. G es conexo si y sólo si cualquier par de puntos x, y en G se puede unir por medio segmentos paralelos a algún eje que caen enteramente en G.*

Teorema 1.9 *Sea $f : A \subseteq \mathbb{R}^p \longrightarrow \mathbb{R}^q$ una función, si $H \subseteq A$ es un conjunto conexo en $\mathbb{R}^p$ y f es continua en H, entonces $f(H)$ es conexo en $\mathbb{R}^q$.*

Capítulo 2

Conjuntos Algebraicos en $\mathbb{K}^n$

En este capítulo se presentarán algunas propiedades elementales de los conjuntos algebraicos, así como algunos ejemplos de conjuntos algebraicos en dimensiones pequeñas. Los conjuntos algebraicos son un caso especial de los conjuntos semi-algebraicos y resulta más sencillo estudiar primero éstos y algunas de sus propiedades; así se podrá generalizar de manera un tanto más natural. Para el desarrollo de este capítulo se estudió en mayor medida el libro *Ideals, varieties, and algorithms* [5].

Al tratar con estructuras de anillo es inevitable estudiar ideales y cómo se relacionan con los conjuntos algebraicos; y como se puede obtener una base para cualquier ideal en un anillo de polinomios. De hecho, esto es el punto concluyente de la segunda parte del capítulo, el denominado *Teorema de la Base de Hilbert*.

La tercera parte del capítulo trata sobre conjuntos algebraicos irreducibles y su relación con los ideales primos. Se muestra que cualquier conjunto algebraico se puede escribir como la unión finita de conjuntos algebraicos irreducibles. La parte concluyente de este capítulo son los teoremas "Nullstellensatz".

2.1. Definiciones y propiedades

Para poder definir un conjunto algebraico, denotaremos a $\mathbb{K}$ como el campo de los números reales o el campo de los números complejos. Así definimos el espacio afín $\mathbb{K}^n$,

$$\mathbb{K}^n = \{(k_1, \ldots, k_n) | \, k_i \in \mathbb{K}\}.$$

Definición 2.1 Sean $f_1, \ldots, f_k \in \mathbb{K}[x_1, \ldots, x_n]$. Un conjunto V de $\mathbb{K}^n$ es un *conjunto algebraico definido por* $f_1, \ldots, f_k$ si satisface:

$$V = \mathbf{V}(f_1, \ldots, f_k) := \{x \in \mathbb{K}^n | \, f_i(x) = 0 \text{ para toda } 1 \leq i \leq k\}.$$

En la definición estamos suponiendo que el conjunto de polinomios que definen a V es finito ya que posteriormente se mostrará que cualquier subconjunto $J \subseteq \mathbb{K}[x_1, \ldots, x_n]$ es generado por un número finito de polinomios.

Vamos a dar algunos ejemplos de conjuntos algebraicos en $\mathbb{R}$, $\mathbb{R}^2$ y $\mathbb{R}^3$ indicando qué objetos son geométricamente. En $\mathbb{R}$ tenemos el siguiente conjunto algebraico

$$V = \{x \in \mathbb{R} \mid f(x) = x^3 - 2x^2 - 13x - 10 = 0\},$$

el cual es una unión de puntos: la unión de las raíces del polinomio f. Es decir, $V = \{-2, -1, 5\}$. De hecho, cualquier conjunto algebraico en $\mathbb{R}$ distinto del vacío es la unión finita de puntos, esto es porque cada polinomio en $\mathbb{R}[x]$ de grado m tiene a lo más m raíces reales.

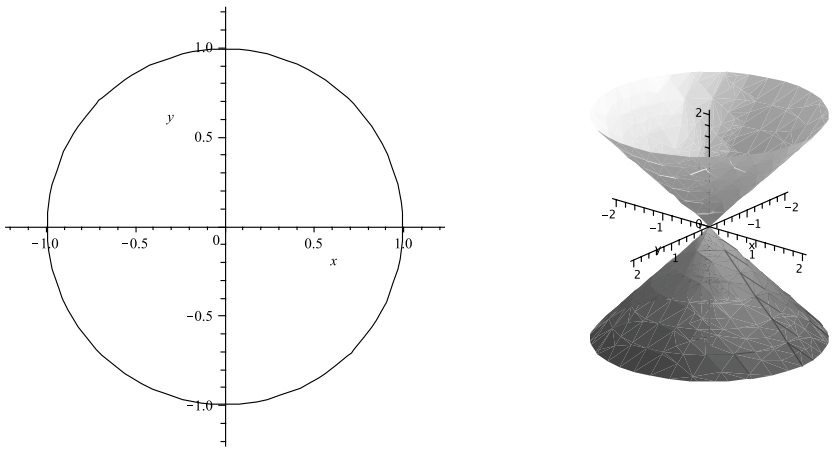
Para $\mathbb{R}^2$ un conjunto algebraico es el siguiente

$$W = \{(x, y) \in \mathbb{R}^2 \mid f(x, y) = x^2 + y^2 - 1 = 0\},$$

el cual se trata de una circunferencia con centro en el origen de radio 1 (Figura 2.1: *a)*). De hecho, las secciones cónicas (circunferencias, elipses, parábolas e hipérbolas) son ejemplos de conjuntos algebraicos en el plano.

En $\mathbb{R}^3$ tenemos el conjunto algebraico

$$X = \{(x, y, z) \in \mathbb{R}^3 \mid f(x, y, z) = z^2 - x^2 - y^2 = 0\}.$$



a) Circunferencia b) Cono

Figura 2.1: Representación geométrica de conjuntos algebraicos en $\mathbb{R}^2$ y $\mathbb{R}^3$

Geométricamente, el conjunto X es un cono cuyo eje es el eje z (Figura 2.1: *b)*).

Observación 2.1 *Cualquier conjunto algebraico real V (es decir $V \subseteq \mathbb{R}^n$) puede ser representado por un sólo polinomio, es decir, si $V = \mathbf{V}(f_1, \ldots, f_k)$, entonces tomamos $f = f_1^2 + \ldots + f_k^2$ y así $V = \mathbf{V}(f)$*

Prueba. $\boxed{\subseteq}$ Sea $x \in V \Rightarrow f_i(x) = 0 \ \ \forall\, i \in \{1, \ldots, k\}$, así $f_i^2(x) = 0 \ \ \forall\, i \in \{1, \ldots, k\}$, entonces $0 = f_1^2(x) + \ldots + f_k^2(x) = f(x)$, de este modo $x \in \mathbf{V}(f)$. Lo cual implica que

$$V \subseteq \mathbf{V}(f) \ldots\ldots (\alpha).$$

$\boxed{\supseteq}$ Sea $x \in \mathbf{V}(f) \Rightarrow f(x) = 0$. Así $f_1^2(x) + \ldots + f_k^2(x) = 0$ pero $f_i^2(x) \in \mathbb{R} \ \ \forall\, i \in \{1, \ldots, k\}$. Entonces $f_i^2(x) = 0 \ \ \forall\, i \in \{1, \ldots, k\}$, así tenemos que $f_i(x) = 0 \ \ \forall\, i \in \{1, \ldots, k\}$, es decir, $x \in V$, lo cual implica que

$$\mathbf{V}(f) \subseteq V \ldots\ldots (\beta).$$

De (α) y (β) se concluye que $V = \mathbf{V}(f)$ ■

A partir de dos conjuntos algebraicos se pueden construir nuevos conjuntos algebraicos, el siguiente lema establece una forma de hacerlo.

Lema 2.1 *Si $V, W \subset \mathbb{K}^n$ son conjuntos algebraicos, entonces $V \cup W$ y $V \cap W$ también lo son en $\mathbb{K}^n$.*

Prueba. Como V y W son conjuntos algebraicos entonces tenemos que $V = \mathbf{V}(f_1, \ldots, f_k)$ y $W = \mathbf{V}(g_1, \ldots, g_s)$ para algunos $f_1, \ldots, f_k, g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$. Se demostrará que $V \cap W = A$ donde $A = \mathbf{V}(f_1, \ldots, f_k, g_1, \ldots, g_s)$ y que $V \cup W = B$ donde $B = \mathbf{V}(f_i g_j \mid 1 \leq i \leq k,\, 1 \leq j \leq s)$.

$\boxed{(i)}$ Sea $x \in V \cap W \iff x \in V$ y $x \in W \iff f_i(x) = 0,\ \forall\, i \in \{1, \ldots, k\}$ y $g_j(x) = 0,\ \forall\, j \in \{1, \ldots, s\} \iff x \in A$. Así, $V \cap W = A$. Por lo tanto, $V \cap W$ es un conjunto algebraico.

$\boxed{(ii)}$ Sea $x \in V \cup W \iff x \in V$ ó $x \in W \iff f_i(x) = 0,\ \forall\, i \in \{1, \ldots, k\}$ ó $g_j(x) = 0,\ \forall\, j \in \{1, \ldots, s\} \iff f_i g_j(x) = f_i(x) g_j(x) = 0$ tal que $1 \leq i \leq k$, $1 \leq j \leq s \iff x \in B$. Así, $V \cup W = B$. Por lo tanto, $V \cup W$ es un conjunto algebraico. ■

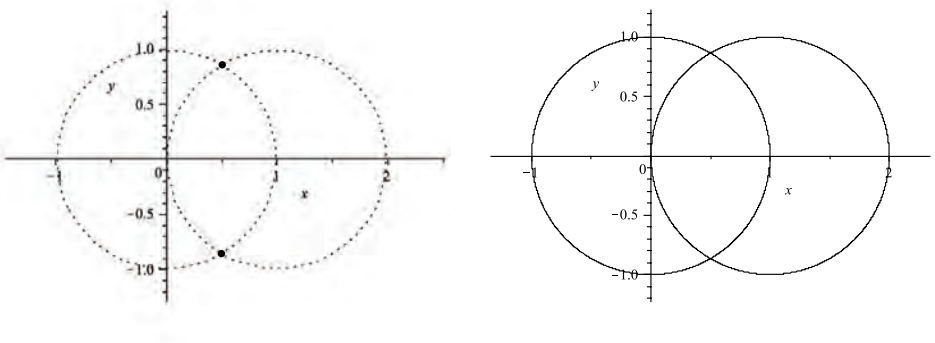
Por ejemplo, si se tienen $V, W \subset \mathbb{R}^2$ conjuntos algebraicos, representados de la siguiente manera

$$\begin{aligned} V &= \{(x, y) \in \mathbb{R}^2 \mid f_1(x, y) = x^2 + y^2 - 1 = 0\}, \\ W &= \{(x, y) \in \mathbb{R}^2 \mid f_2(x, y) = (x - 1)^2 + y^2 - 1 = 0\}. \end{aligned}$$

Geométricamente, V es la circunferencia con centro en el origen y radio 1, mientras que W es la circunferencia del mismo radio pero con centro en $(1, 0)$. Así, se pueden construir los conjuntos algebraicos

$$\begin{aligned} V \cap W &= \{(x, y) \in \mathbb{R}^2 \mid f_1(x, y) = f_2(x, y) = 0\}, \\ V \cup W &= \{(x, y) \in \mathbb{R}^2 \mid f_1(x, y) \cdot f_2(x, y) = 0\}. \end{aligned}$$

El primero está formado por los puntos que satisfacen tanto f_1 como f_2, de hecho, $V \cap W = \{(1/2, \sqrt{3}/2), (1/2, -\sqrt{3}/2)\}$, los cuales son los puntos de intersección de las circunferencias (Figura 2.2 *a)*). Mientras que $V \cup W$ son los puntos de ambas circunferencias ya que son los puntos de $\mathbb{R}^2$ tales que se anula f_1 ó f_2 (Figura 2.2 *b)*).



a) $V \cap W$ b) $V \cup W$

Figura 2.2: Intersección y unión de conjuntos algebraicos en $\mathbb{R}^2$

Otra manera de construir conjuntos algebraicos es a partir de ideales del anillo de polinomios con el que se esté trabajado; para ello, se establece la siguiente definición.

Definición 2.2 Un subconjuto $I \subset \mathbb{K}[x_1, \ldots, x_n]$ es un *ideal* si se satisface:

(i) $0 \in I$.

(ii) Si $f, g \in I$, entonces $f + g \in I$.

(iii) Si $f \in I$ y $h \in \mathbb{K}[x_1, \ldots, x_n]$, entonces $hf \in I$.

Observación 2.2 *Si $I, J \subset \mathbb{K}[x_1, \ldots, x_n]$ son ideales entonces $I \cap J$ también es ideal en $\mathbb{K}[x_1, \ldots, x_n]$*

Prueba. $\boxed{(i)}$ Notemos que $0 \in I \cap J$ ya que $0 \in I$ y $0 \in J$, por ser ideales.
$\boxed{(ii)}$ Sean $f, g \in I \cap J$, esto implica que $f, g \in I$ y $f, g \in J$, como I y J son ideales entonces $f + g \in I$ y $f + g \in J$. Por lo tanto $f + g \in I \cap J$.
$\boxed{(iii)}$ Sea $f \in I \cap J$ y $h \in \mathbb{K}[x_1, \ldots, x_n]$, entonces $f \in I$ y $f \in J$. Como ambos son ideales, entonces $hf \in I$ y $hf \in J$. Por lo tanto. $hf \in I \cap J$.
De *(i), (ii)* y *(iii)* concluimos que $I \cap J \subset \mathbb{K}[x_1, \ldots, x_n]$ es un ideal. ■

Un ideal con el que se estará trabajando en adelante es el generado por un número finito de polinomios, el cual definimos de la siguiente manera.

Definición 2.3 Sean $f_1, \ldots, f_s$ polinomios en $\mathbb{K}[x_1, \ldots, x_n]$. El *conjunto generado por* $f_1, \ldots, f_s$, denotado por $\langle f_1, \ldots, f_s \rangle$, se define como:

$$\langle f_1, \ldots, f_s \rangle := \left\{ \sum_{i=1}^{s} h_i f_i \,\middle|\, h_1, \ldots, h_s \text{ son polinomios cualesquiera en } \mathbb{K}[x_1, \ldots, x_n] \right\}.$$

Esto es, es el conjunto formado por las sumas finitas de la forma $\sum h_i f_i$ con $h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$.

Lema 2.2 *Si $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, entonces $\langle f_1, \ldots, f_s \rangle$ es un ideal en $\mathbb{K}[x_1, \ldots, x_n]$.*

Prueba. $\boxed{(i)}$ Tenemos que $0 \in \langle f_1, \ldots, f_s \rangle$ ya que $0 = \sum_{i=1}^{s} 0 \cdot f_i$.
$\boxed{(ii)}$ Supongamos que$f, g \in \langle f_1, \ldots, f_s \rangle$, esto es, $f = \sum_{i=1}^{s} p_i f_i$ y $g = \sum_{i=1}^{s} q_i f_i$. Entonces

$$f + g = \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i = \sum_{i=1}^{s} (p_i + q_i) f_i.$$

Así, $f + g \in \langle f_1, \ldots, f_s \rangle$.
$\boxed{(iii)}$ Supongamos que $f \in \langle f_1, \ldots, f_s \rangle$, esto es, $f = \sum_{i=1}^{s} p_i f_i$ y sea $h \in \mathbb{K}[x_1, \ldots, x_n]$. Entonces

$$hf = h\left(\sum_{i=1}^{s} p_i f_i \right) = \sum_{i=1}^{s} (hp_i) f_i.$$

Así, $hf \in \langle f_1, \ldots, f_s \rangle$
Por lo tanto $\langle f_1, \ldots, f_s \rangle$ es un ideal en $\mathbb{K}[x_1, \ldots, x_n]$ ■

Derivado de esta definición y este lema, decimos que un ideal I es *finitamente generado* si existen $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ tales que $I = \langle f_1, \ldots, f_s \rangle$, y decimos que $f_1, \ldots, f_s$ son una *base* de I.

Así, a partir de un ideal en el anillo de polinomios se puede construir un conjunto algebraico.

Definición 2.4 Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ ideal. Se define el siguiente conjunto:

$$\mathbf{V}(I) := \{x \in \mathbb{K}^n |\, f(x) = 0, \ \forall f \in I\}$$

Lema 2.3 *Dicho conjunto satisface lo siguiente:*

(i) *Sea* $0 \in \mathbb{K}[x_1, \ldots, x_n]$. *Entonces* $\mathbf{V}(0) = \mathbb{K}^n$ *y* $\mathbf{V}(\mathbb{K}[x_1, \ldots, x_n]) = \emptyset$.

(ii) *Sean* $I, J \subset \mathbb{K}[x_1, \ldots, x_n]$ *ideales. Si* $I \subset J$ *entonces* $\mathbf{V}(J) \subset \mathbf{V}(I)$.

(iii) *Sean* $J_1, J_2 \subset \mathbb{K}[x_1, \ldots, x_n]$ *ideales. Entonces* $\mathbf{V}(J_1 \cap J_2) = \mathbf{V}(J_1) \cup \mathbf{V}(J_2)$.

(iv) *Sea* Λ *un conjunto y sea* $J_\lambda \in \mathbb{K}[x_1, \ldots, x_n]$ *tal que* J_λ *es ideal finitamente generado,* $\forall \lambda \in \Lambda$. *Entonces* $\mathbf{V}\left(\sum_{\lambda\in\Lambda} J_\lambda\right) = \bigcap_{\lambda\in\Lambda} \mathbf{V}(J_\lambda)$, *donde*

$$\sum_{\lambda\in\Lambda} J_\lambda := \left\{ f \in \mathbb{K}[x_1, \ldots, x_n] \;\middle|\; f = \sum_{\lambda\in\Lambda} \left(\sum_{f_{i_\lambda}\in J_\lambda} h_{i_\lambda f_{i_\lambda}} \right) \right\}.$$

Prueba. $\boxed{(i)}$ Por hipótesis $I = 0$ entonces $\mathbf{V}(0) = \{x \in \mathbb{K}^n |\, 0(x) = 0\}$ pero $\{x \in \mathbb{K}^n |\, 0(x) = 0\} = \mathbb{K}^n$. Por lo tanto, $\mathbf{V}(0) = \mathbb{K}^n$.

Luego, supongamos que $\mathbf{V}(\mathbb{K}[x_1, \ldots, x_n]) \neq \emptyset$, es decir, existe $x_0 \in \mathbb{K}^n$ tal que $f(x_0) = 0, \ \forall f \in \mathbb{K}[x_1, \ldots, x_n]$. Como $\mathbb{K}$ es campo, entonces $\mathbb{K}[x_1, \ldots, x_n]$ tiene unitario. Así, tomando $f(x) \equiv 1$ el elemento unitario, tenemos que en particular $f(x_0) = 1$, lo cual es una contradicción. Por lo tanto, $\mathbf{V}(\mathbb{K}[x_1, \ldots, x_n]) = \emptyset$.

$\boxed{(ii)}$ Sea $x \in \mathbf{V}(J) \Rightarrow f(x) = 0, \ \forall f \in J$. Como $I \subset J$ por hipótesis, entonces, en particular, $f(x) = 0, \ \forall f \in I$. Por lo tanto, $x \in \mathbf{V}(I)$, es decir, $\mathbf{V}(J) \subset \mathbf{V}(I)$.

$\boxed{(iii)}$ Sea $x \in \mathbf{V}(J_1 \cap J_2)$, entonces $f(x) = 0, \ \forall f \in (J_1 \cap J_2)$. Supongamos que $x \notin \big(\mathbf{V}(J_1) \cup \mathbf{V}(J_2)\big) \Rightarrow x \notin \mathbf{V}(J_1)$ y $x \notin \mathbf{V}(J_2)$. Esto es, $\exists\, f_1 \in J_1$ tal que $f_1(x) \neq 0$ y $\exists\, f_2 \in J_2$ tal que $f_2(x) \neq 0$. Como J_1 y J_2 son ideales entonces $f_1 f_2 \in J_1$ y $f_1 f_2 \in J_2$, lo cual implica $f_1 f_2 \in (J_1 \cap J_2)$ pero $f_1 f_2(x) \neq 0$ ya que $\mathbb{K}[x_1, \ldots, x_n]$ es dominio entero. Entonces $x \notin \mathbf{V}(J_1 \cap J_2)$ lo cual es una contradicción. Así, $x \in \big(\mathbf{V}(J_1) \cup \mathbf{V}(J_2)\big)$. Por lo tanto,

$$\mathbf{V}(J_1 \cap J_2) \subseteq \mathbf{V}(J_1) \cup \mathbf{V}(J_2) \ldots\ldots (\alpha)$$

Sea $x \in \big(\mathbf{V}(J_1) \cup \mathbf{V}(J_2)\big)$, entonces $f(x) = 0,\ \forall\, f \in J_1$ ó $g(x) = 0,\ \forall\, g \in J_2$. Supongamos que $x \notin \mathbf{V}(J_1 \cap J_2)$. Esto es, $\exists\, h \in J_1 \cap J_2$ tal que $h(x) \neq 0$. Como $h \in J_1$ y $h \in J_2$ entonces por hipótesis, $h(x) = 0$, lo cual es una contradicción. Así, $x \in \mathbf{V}(J_1 \cap J_2)$. Por lo tanto,

$$\mathbf{V}(J_1) \cup \mathbf{V}(J_2) \subseteq \mathbf{V}(J_1 \cap J_2) \ldots\ldots (\beta)$$

De (α) y (β) concluimos que $\mathbf{V}(J_1 \cap J_2) = \mathbf{V}(J_1) \cup \mathbf{V}(J_2)$.

$\boxed{(iv)}$ Sea $x \in \mathbf{V}\Big(\sum_{\lambda\in\Lambda} J_\lambda\Big)$ entonces $f(x) = 0,\ \forall\, f \in \big(\sum_{\lambda\in\Lambda} J_\lambda\big)$. Demostraremos que $x \in \mathbf{V}(J_\lambda)\ \forall\ \lambda \in \Lambda$.

Sea $\lambda_0 \in \Lambda$ y elegimos una $f \in J_{\lambda_0}$ arbitraria. Por definición cualquier elemento de $\sum_{\lambda\in\Lambda} J_\lambda$ es de la forma $\sum_{\lambda\in\Lambda}\big(\sum_{f_{i_\lambda}\in J_\lambda} h_{i_\lambda} f_{i_\lambda}\big)$. Tomando $h_{i_\lambda} \equiv 0,\ \ \forall\, \lambda \neq \lambda_0$ obtenemos $f \in J_{\lambda_0}$, es decir, $f \in \sum_{\lambda\in\Lambda} J_\lambda$ y así, por hipótesis $f(x) = 0$. Como f fue arbitraria, entonces $f(x) = 0,\ \ \forall f \in J_{\lambda_0}$ lo cual implica que $x \in \mathbf{V}(J_{\lambda_0})$ pero λ_0 también fue arbitraria, entonces, $x \in \mathbf{V}(J_\lambda),\ \ \forall\lambda \in \Lambda$, es decir, $x \in \bigcap_{\lambda\in\Lambda} \mathbf{V}(J_\lambda)$. Por lo tanto,

$$\mathbf{V}\Big(\sum_{\lambda\in\Lambda} J_\lambda\Big) \subseteq \bigcap_{\lambda\in\Lambda} \mathbf{V}(J_\lambda) \ldots\ldots (\gamma)$$

Sea $x \in \bigcap_{\lambda\in\Lambda} \mathbf{V}(J_\lambda)$, es decir, $x \in \mathbf{V}(J_\lambda),\ \ \forall\, \lambda \in \Lambda$, esto es,

$$f(x) = 0,\ \ \forall\, f \in J_\lambda\ \ y\ \ \forall\, \lambda \in \Lambda \ldots\ldots (\star)$$

Elegimos $f \in \sum_{\lambda\in\Lambda} J_\lambda$, es decir, f es de la forma $\sum_{\lambda\in\Lambda}\big(\sum_{f_{i_\lambda}\in J_\lambda} h_{i_\lambda} f_{i_\lambda}\big)$. Así,

$$f(x) = \sum_{\lambda\in\Lambda}\Bigg(\sum_{f_{i_\lambda}\in J_\lambda} h_{i_\lambda}(x) f_{i_\lambda}(x)\Bigg).$$

Pero $f_{i_\lambda}(x) = 0$ por $(\star)$, lo cual implica que $f(x) = 0$, es decir, $x \in \mathbf{V}\Big(\sum_{\lambda\in\Lambda} J_\lambda\Big)$. Por lo tanto,

$$\bigcap_{\lambda\in\Lambda} \mathbf{V}(J_\lambda) \subseteq \mathbf{V}\Big(\sum_{\lambda\in\Lambda} J_\lambda\Big) \ldots\ldots (\delta)$$

De (γ) y (δ) se concluye que $\mathbf{V}\left(\sum_{\lambda\in\Lambda} J_\lambda\right) = \bigcap_{\lambda\in\Lambda} \mathbf{V}(J_\lambda)$ ■

Por ejemplo si $I = \langle x^2-4, y^2-1\rangle \subset \mathbb{R}[x,y]$. Tenemos que $0 \in I$ ya que $0 = 0(x^2-4) + 0(y^2-1)$; luego, si $f, g \in I$, es decir, $f = h_1(x^2-4) + h_2(y^2-1)$ y $g = k_1(x^2-4) + k_2(y^2-1)$ con $h_1, h_2, k_1, k_2 \in \mathbb{R}[x,y]$, entonces

$$f+g = h_1(x^2-4)+h_2(y^2-1)+k_1(x^2-4)+k_2(y^2-1) = (h_1+k_1)(x^2-4)+(h_2+k_2)(y^2-1),$$

es decir, $f+g \in I$. Si $f \in I$, esto es $f = h_1(x^2-4) + h_2(y^2-1)$ con $h_1, h_2 \in \mathbb{R}[x,y]$, y $g \in \mathbb{R}[x,y]$ entonces

$$gf = g[h_1(x^2-4) + h_2(y^2-1)] = gh_1(x^2-4) + gh_2(y^2-1),$$

es decir, $gf \in I$; estos tres puntos implican que I es un ideal en $\mathbb{R}[x,y]$. Con la definición anterior tenemos que $\mathbf{V}(I) = \{(2,1),(2,-1),(-2,1),(-2,-1)\}$, que son los puntos donde x^2-4 y y^2-1 se anulan; y por tanto, cualquier polinomio en I.

En este ejemplo se puede observar que $\mathbf{V}(I) = \mathbf{V}(x^2-4, y^2-1)$, planteando así la pregunta de si esta idea puede generalizarse. El siguiente lema la responde.

Lema 2.4 *Sea $V = \mathbf{V}(f_1,\ldots,f_k) \subset \mathbb{K}^n$ un conjunto algebraico. Si $I = \langle f_1,\ldots,f_k\rangle$ entonces $\mathbf{V}(I) = V$.*

Prueba. $\boxed{\subseteq}$ Sea $x \in \mathbf{V}(I)$ entonces $f(x) = 0,\ \forall\, f \in I$, es decir, $f_i(x) = 0,\ \forall\, i \in \{1,\ldots,k\}$. Así, $x \in V$, lo cual implica que $\mathbf{V}(I) \subseteq V$.

$\boxed{\supseteq}$ Sea $x \in V$. Entonces, por definición $f_i(x) = 0,\ \forall\, i \in \{1,\ldots,k\}$. Elegimos $f \in I$ arbitrario, así f es de la forma $f = \sum_{i=1}^k h_i f_i$. Evaluando tenemos

$$f(x) = \sum_{i=1}^{k} h_i(x) f_i(x) = \sum_{i=1}^{k} h_i(x)\cdot 0 = 0.$$

Por lo tanto, $V \subseteq \mathbf{V}(I)$

De ambas contenciones concluimos que $\mathbf{V}(I) = V$ ■

Proposición 2.1 *Si $f_1, \ldots, f_s$ y $g_1, \ldots, g_t$ son bases del mismo ideal en $\mathbb{K}[x_1, \ldots, x_n]$, de modo que $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, entonces $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.*

Prueba. Sea $I = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, entonces, por el lema anterior tenemos que $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$ y $\mathbf{V}(I) = \mathbf{V}(g_1, \ldots, g_t)$. Por lo tanto, $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$. ■

Si trabajamos con el anillo de polinomios en una variable podemos describir todos sus ideales.

Proposición 2.2 *Cada ideal de $\mathbb{K}[x]$ puede ser escrito en la forma $\langle f \rangle$ para alguna $f \in \mathbb{K}[x]$. Además, f es único salvo multiplicación por una constante no cero en $\mathbb{K}$.*

Prueba. Sea $I \subset \mathbb{K}[x]$ ideal. Si $I = \{0\}$, entonces tomamos el polinomio cero y por lo tanto, $I = \langle 0 \rangle$.

Si $I \neq \{0\}$, entonces podemos tomar un polinomio f no cero de grado mínimo contenido en I. Vamos a demostrar que $I = \langle f \rangle$.

$\boxed{\subseteq}$ Tenemos que $\langle f \rangle \subseteq I$ ya que I es ideal.

$\boxed{\supseteq}$ Elegimos $g \in I$ arbitraria. Por el algoritmo de la división sabemos que $g = hf + r$, donde $r = 0$ ó $gra(r) < gra(f)$. Como I es ideal entonces $hf \in I$, pero $r = g - hf$ y por tanto $r \in I$. Si r fuera no cero entonces $gra(r) < gra(f)$ lo cual es una contradicción ya que f es de grado mínimo en I. Por lo tanto $r = 0$ y $g = hf$, lo cual implica que $g \in \langle f \rangle$. Por lo tanto $I = \langle f \rangle$

Para demostrar la unicidad supongamos que $\langle f \rangle = I = \langle g \rangle$, entonces $f \in \langle g \rangle$, lo cual dice que $f = hg$ para algún polinomio h, así, $gra(f) = gra(h) + gra(g)$, es decir, $gra(f) \geq gra(g)$. Analogamente $g \in \langle f \rangle$ y así $g = qf$, donde $gra(g) = gra(q) + gra(f)$, esto es, $gra(g) \geq gra(f)$. Por lo tanto $gra(f) = gra(g)$, esto implica que $gra(h) = 0$ y así h es una constante no cero. ■

Así como podemos construir conjuntos algebraicos a partir de un ideal, se puede construir un ideal a partir de un conjunto algebraico dado.

Definición 2.5 Sea $V \subset \mathbb{K}^n$ un conjunto no vacío. Se define el siguiente conjunto:

$$\mathbf{I}(V) := \{f \in \mathbb{K}[x_1, \ldots, x_n] | \, f(x) = 0, \ \forall \, x \in V\}.$$

Lema 2.5 *Si $W \subset \mathbb{K}^n$ es un conjunto no vacío, entonces $\mathbf{I}(W) \subset \mathbb{K}[x_1, \ldots, x_n]$ es un ideal, llamado el ideal de W.*

Prueba. Tenemos que $0 \in \mathbf{I}(W)$ ya que $0(x) = 0, \ \forall \, x \in \mathbb{K}^n$; en particular para todo $x \in W$. Ahora, supongamos que $f, g \in \mathbf{I}(W)$ y $h \in \mathbb{K}[x_1, \ldots, x_n]$. Sea x un punto cualquiera en W, entonces

$$(f+g)(x) = f(x) + g(x) = 0 + 0 = 0, \ \text{ lo cual implica que } (f+g) \in \mathbf{I}(W),$$

$$(hf)(x) = h(x)f(x) = h(x)0 = 0, \ \text{ lo cual implica que } hf \in \mathbf{I}(W).$$

Por lo tanto, $\mathbf{I}(W)$ es ideal. ■

La pregunta natural que surge a raíz de esta manera de construir un ideal es cómo se relacionan un ideal dado y el ideal del conjunto algebraico definido por éste. El siguiente lema nos contesta tal interrogante.

Lema 2.6 *Si $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, entonces $\langle f_1, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$. Hay casos en que la igualdad no se realiza.*

Prueba. Sea $f \in \langle f_1, \ldots, f_s \rangle$, entonces $f = \sum_{i=1}^{s} h_i f_i$, para algunos polinomios $h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$. Sea $x \in \mathbf{V}(f_1, \ldots, f_s)$, demostraremos que $f(x) = 0$. Notemos que $f_i(x) = 0$, ya que $x \in \mathbf{V}(f_1, \ldots, f_s)$, para toda $1 \leq i \leq s$. Entonces

$$f(x) = \sum_{i=1}^{s} h_i f_i(x) = \sum_{i=1}^{s} h_i(x) \cdot 0 = 0.$$

Así, $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$. Por lo tanto, $\langle f_1, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$.
Se demostrará que la inclusión $\langle x^2, y^2 \rangle \subset \mathbf{I}(\mathbf{V}(x^2, y^2))$ no es una igualdad. Primero tenemos que $\mathbf{V}(x^2, y^2) = \{(0,0)\}$ y los polinomios que se anulan en (0,0) son de la forma $h_1 x + h_2 y$. Así, $\mathbf{I}(\mathbf{V}(x^2, y^2)) = \langle x, y \rangle$ pero el polinomio $x \notin \langle x^2, y^2 \rangle$ ya que los

polinomios de la forma $h_1(x,y)x^2 + h_2(x,y)y^2$ tienen monomios de grado al menos 2. Por lo tanto la inclusión es propia. ■

Por último, las siguientes proposiciones establecen relaciones importantes de estos ideales con conjuntos algebraicos.

Proposición 2.3 *Sean V y W conjuntos algebraicos en $\mathbb{K}^n$. Entonces:*

(i) $V \subset W$ *si y sólo si* $\mathbf{I}(V) \supset \mathbf{I}(W)$.

(ii) $V = W$ *si y sólo si* $\mathbf{I}(V) = \mathbf{I}(W)$.

Prueba. $\boxed{(i)}$ $\boxed{\Rightarrow}$ Supongamos que $V \subset W$. Sea $f \in \mathbf{I}(W) \Rightarrow f(x) = 0\ \forall x \in W$. En particular, $f(x) = 0\ \forall x \in V$. Así, $f \in \mathbf{I}(V)$. Por lo tanto, $\mathbf{I}(W) \subset \mathbf{I}(V)$.
$\boxed{\Leftarrow}$ Ahora supongamos que $\mathbf{I}(W) \subset \mathbf{I}(V)$. Sea $x \in V \Rightarrow f(x) = 0\ \forall f \in \mathbf{I}(V)$. En particular $f(x) = 0\ \forall f \in \mathbf{I}(W)$, lo cual implica que $x \in W$ (ya que los polinomios que describen al conjunto algebraico W están en $\mathbf{I}(W)$). Por lo tanto, $V \subset W$.
$\boxed{(ii)}$ $V = W \iff V \subset W$ y $V \supset W \iff$ (por i) $\mathbf{I}(V) \supset \mathbf{I}(W)$ y $\mathbf{I}(V) \subset \mathbf{I}(W) \iff \mathbf{I}(V) = \mathbf{I}(W)$. ■

Proposición 2.4 *Sea $X \subseteq \mathbb{K}^n$ cualquier conjunto y $J \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal. Entonces:*

(i) $X \subseteq \mathbf{V}\big(\mathbf{I}(X)\big)$. *La igualdad se da si y sólo si X es algebraico.*

(ii) $J \subseteq \mathbf{I}\big(\mathbf{V}(J)\big)$.

Prueba. $\boxed{(i)}$ Sea $p \in X$. Como $\mathbf{I}(X) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \,|\, f(q) = 0\ \ \forall\, q \in X\}$ entonces $f(p) = 0,\ \ \forall\, f \in \mathbf{I}(X)$. Así, $p \in \mathbf{V}\big(\mathbf{I}(X)\big)$. Por lo tanto $X \subseteq \mathbf{V}\big(\mathbf{I}(X)\big)$.
Ahora supongamos que $X = \mathbf{V}\big(\mathbf{I}(X)\big)$ entonces, X es algebraico ya que está dado por los ceros de los polinomios en $\mathbf{I}(X)$.
Supongamos que X es un conjunto algebraico, entonces $X = \mathbf{V}(f_1, \ldots, f_k)$. Así, tomamos $J = \langle f_1, \ldots, f_k \rangle$, el cual es un ideal y por el lema 2.4 tenemos que $X = \mathbf{V}(J)$.

Sabemos que $J = \langle f_1, \ldots, f_k \rangle \subseteq \mathbf{I}(X)$. Entonces, por el lema 2.3 (ii) tenemos que $\mathbf{V}\big(\mathbf{I}(X)\big) \subseteq \mathbf{V}(J)$. Como $\mathbf{V}(J) = X$, entonces, $\mathbf{V}\big(\mathbf{I}(X)\big) \subseteq X$; además, ya sabíamos que $X \subseteq \mathbf{V}\big(\mathbf{I}(X)\big)$ (por la primer parte de (i)). Por lo tanto, $X = \mathbf{V}\big(\mathbf{I}(X)\big)$.
$\boxed{(ii)}$ Sea $f \in J$ y sea $p \in \mathbf{V}(J)$ arbitraria. Entonces, $g(p) = 0, \ \forall\, g \in J$; en particular para f, es decir, $f(p) = 0$. Como p fue arbitraria, entonces $f(p) = 0, \ \forall\, p \in \mathbf{V}(J)$, esto es, $f \in \mathbf{I}\big(\mathbf{V}(J)\big)$. Por lo tanto, $J \subseteq \mathbf{I}\big(\mathbf{V}(J)\big)$. ■

2.2. Bases de Groebner

Después de estudiar ideales y bases generadoras, la interrogante que surge es si cualquier ideal tiene una base generadora. Esta pregunta es respondida por el *Teorema de la base de Hilbert*, pero para poder abordarlo es necesario conocer las definiciones de cierto tipo de orden, estrechamente relacionado con el anillo de polinomios.

Definición 2.6 Un *orden monomial* en $\mathbb{K}[x_1, \ldots, x_n]$ es una relación $>$ en $\mathbb{Z}^n_{\geq 0}$, es decir, es una relación en el conjunto de monomios $x^\alpha, \ \alpha \in \mathbb{Z}^n_{\geq 0}$ que satisface:

(i) $>$ es un orden total (o lineal) en $\mathbb{Z}^n_{\geq 0}$.

(ii) Si $\alpha > \beta$ y $\gamma \in \mathbb{Z}^n_{\geq 0}$, entonces $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ es un buen orden en $\mathbb{Z}^n_{\geq 0}$.

En algunas ocasiones resulta un poco complicado determinar si una relación es buen orden en $\mathbb{Z}^n_{\geq 0}$ a partir de la definición. Para resolver este problema, se utiliza en mayor medida el siguiente lema.

Lema 2.7 *Una relación $>$ en $\mathbb{Z}^n_{\geq 0}$ es un buen orden si y sólo si cada secuencia estrictamente decreciente en $\mathbb{Z}^n_{\geq 0}$*

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots$$

termina eventualmente.

Prueba. Se probará por contrapuesta, es decir, $>$ no es un buen orden si y sólo si existe una secuencia infinita estrictamente decreciente en $\mathbb{Z}^n_{\geq 0}$.
$\boxed{\Rightarrow}$ Como $>$ no es un buen orden, entonces existe un subconjunto $S \subset \mathbb{Z}^n_{\geq 0}$ no vacío, tal que no tiene elemento mínimo. Así, podemos elegir $\alpha(1) \in S$. Como éste no es elemento mínimo entonces existe $\alpha(2) \in S$ tal que $\alpha(1) > \alpha(2)$. Como $\alpha(2)$ no es elemento mínimo, entonces existe $\alpha(3) \in S$ tal que $\alpha(2) > \alpha(3)$. Continuando de este modo, obtenemos una secuencia infinita estrictamente decreciente:

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

$\boxed{\Leftarrow}$ Sea $S = \{\alpha(1), \alpha(2), \alpha(3), \dots\}$ una secuencia infinita estrictamente decreciente en $\mathbb{Z}^n_{\geq 0}$. Así, S es no vacío y $S \subset \mathbb{Z}^n_{\geq 0}$ sin elemento mínimo. Por lo tanto, $\mathbb{Z}^n_{\geq 0}$ no es un buen orden. ■

A continuación, explicaremos dos ejemplos de órdenes monomiales en $\mathbb{Z}^n_{\geq 0}$.

Definición 2.7 (Orden Lexicográfico) Sean $\alpha = (\alpha_1, \dots, \alpha_n)$ y $\beta = (\beta_1, \dots, \beta_n)$ en $\mathbb{Z}^n_{\geq 0}$. Decimos que α *es mayor que* β *en orden lexicográfico* y denotado por $\alpha >_{lex} \beta$ si, en el vector diferencia $\alpha - \beta \in \mathbb{Z}^n$, la primera entrada no cero es positiva. Escribiremos $x^\alpha >_{lex} x^\beta$ si $\alpha >_{lex} \beta$.

Proposición 2.5 *El orden lex (lexicográfico) en* $\mathbb{Z}^n_{\geq 0}$ *es un orden monomial en* $\mathbb{K}[x_1, \dots, x_n]$.

Prueba. $\boxed{(i)}$ Sea $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ tales que $\alpha \neq \beta$, esto implica que $\alpha_i \neq \beta_i$ para alguna $i \in \{1, \dots, n\}$. Sea j el índice de la primera entrada en la que difieren α y β. Como $\alpha_j, \beta_j \in \mathbb{Z}_{\geq 0}$ y $\mathbb{Z}_{\geq 0}$ es un orden total entonces $\alpha_j > \beta_j$ ó $\alpha_j < \beta_j$.
Si $\alpha_j > \beta_j$ entonces $\alpha_j - \beta_j > 0$, y así en el vector $\alpha - \beta \in \mathbb{Z}^n$ la primera entrada no cero es positiva. Por lo tanto, $\alpha >_{lex} \beta$.
Si $\alpha_j < \beta_j$ entonces $0 < \beta_j - \alpha_j$, y así en el vector $\beta - \alpha \in \mathbb{Z}^n$ la primera entrada no cero es positiva. Por lo tanto, $\beta >_{lex} \alpha$.

De esta manera, cualesquiera dos elementos distintos en $\mathbb{Z}^n_{\geq 0}$ son comparables. Por lo tanto, $>_{lex}$ es un orden total.

$\boxed{(ii)}$ Sean $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ tales que $\alpha >_{lex} \beta$ y sea $\gamma \in \mathbb{Z}^n_{\geq 0}$. Tenemos que la primera entrada no cero en el vector $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ es positiva, digamos que $\alpha_k - \beta_k > 0$. Pero además, tenemos que $\alpha + \gamma = (\alpha_1 + \gamma_1, \ldots, \alpha_n - \gamma_n)$ y $\beta + \gamma = (\beta_1 + \gamma_1, \ldots, \beta_n + \gamma_n)$. De esta manera

$$\begin{aligned}(\alpha + \gamma) - (\beta + \gamma) &= \Big(\alpha_1 + \gamma_1 - (\beta_1 + \gamma_1), \ldots, \alpha_n + \gamma_n - (\beta_n + \gamma_n)\Big) \\ &= (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n) \\ &= \alpha - \beta,\end{aligned}$$

en el cual, la primera entrada no cero es $\alpha_k - \beta_k$, y la cual es positiva. Por lo tanto, $\alpha + \gamma >_{lex} \beta + \gamma$.

$\boxed{(iii)}$ Supongamos que $>_{lex}$ no es un buen orden. Entonces existe una sucesión infinita estrictamente decreciente, digamos $\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \ldots$ con $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Consideramos la primera entrada de cada $\alpha(i)$. Dichas entradas forman una secuencia no creciente, es decir $\alpha(1)_1 \geq \alpha(2)_1 \geq \alpha(3)_1 \geq \ldots$ (ya que si $\alpha(i)_1 < \alpha(j)_1$ para alguna $i < j$ entonces $0 < \alpha(j)_1 - \alpha(i)_1$; lo cual implica que $\alpha(j) >_{lex} \alpha(i)$ con $i < j$. Pero esto contradice la hipótesis). Como $\mathbb{Z}_{\geq 0}$ está bien ordenado entonces $\alpha(1)_1 \geq \alpha(2)_1 \geq \alpha(3)_1 \geq \ldots$ debe terminar eventualmente, es decir, existe $k \in \mathbb{Z}_{\geq 0}$ tal que todas las $\alpha(i)_1$ con $i \geq k$ son iguales. Ahora consideramos la segunda entrada de $\alpha(i)$, para $i \geq k$. Éstas forman una secuencia no creciente $\alpha(k)_2 \geq \alpha(k+1)_2 \geq \alpha(k+2)_2 \geq \ldots$ (el argumento es el mismo que el de las $\alpha(i)_1$) y como $\mathbb{Z}_{\geq 0}$ está bien ordenado, debe terminar eventualmente. Siguiendo de esta manera, hasta abarcar todas las entradas, va existir $l \in \mathbb{Z}_{\geq 0}$ tal que $\alpha(l), \alpha(l+1), \ldots$ son iguales. En particular $\alpha(l) = \alpha(l+1)$, lo cual contradice que la secuencia sea estrictamente decreciente.

De (i), (ii) y (iii) concluimos que $>_{lex}$ es un orden monomial. ■

Definición 2.8 (Orden Lexicográfico Graduado) Sean $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Decimos que

α es mayor que β respecto al orden lexicográfico graduado y denotado por $\alpha >_{grlex} \beta$ si

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \qquad \text{ó} \qquad |\alpha| = |\beta| \;\; y \;\; \alpha >_{lex} \beta.$$

Proposición 2.6 *El orden lexicográfico graduado en $\mathbb{Z}_{\geq 0}^n$ es un orden monomial en $\mathbb{K}[x_1, \ldots, x_n]$.*

Prueba. $\boxed{(i)}$ Sean $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ tales que $\alpha \neq \beta$, esto implica que $\alpha_i \neq \beta_i$ para alguna $i \in \{1, \ldots, n\}$.

Caso 1: $|\alpha| = |\beta|$. Como el orden lexicográfico es un orden total, entonces, pasa que $\alpha >_{lex} \beta$ ó $\beta >_{lex} \alpha$. Por lo tanto, $\alpha >_{grlex} \beta$ ó $\beta >_{grlex} \alpha$.

Caso 2: $|\alpha| \neq |\beta|$. Sabemos que $|\alpha|, |\beta| \in \mathbb{Z}_{\geq 0}$ y $\mathbb{Z}_{\geq 0}$ es un orden total, entonces, $|\alpha| > |\beta|$ ó $|\beta| > |\alpha|$. Por lo tanto, $\alpha >_{grlex} \beta$ ó $\beta >_{grlex} \alpha$.

Cualquiera que sea el caso, dos elementos distintos de $\mathbb{Z}_{\geq 0}^n$ son comparables. Por lo tanto, el orden lexicográfico graduado es un orden total.

$\boxed{(ii)}$ Sean $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ tales que $\alpha >_{grlex} \beta$ y sea $\gamma \in \mathbb{Z}_{\geq 0}^n$. Como $\alpha >_{grlex} \beta$ entonces $|\alpha| > |\beta|$ ó $|\alpha| = |\beta|$ y $\alpha >_{lex} \beta$.

Caso 1: $|\alpha| > |\beta|$. Tenemos que

$$\begin{aligned} |\alpha + \gamma| &= \sum_{i=1}^{n} (\alpha_i + \gamma_i) = \sum_{i=1}^{n} \alpha_i + \sum_{i=1}^{n} \gamma_i \\ &= |\alpha| + |\gamma| > |\beta| + |\gamma| \\ &= \sum_{i=1}^{n} \beta_i + \sum_{i=1}^{n} \gamma_i = \sum_{i=1}^{n} (\beta_i + \gamma_i) = |\beta + \gamma|. \end{aligned}$$

Por lo tanto, $\alpha + \gamma >_{grlex} \beta + \gamma$.

Caso 2: $|\alpha| = |\beta|$ y $\alpha >_{lex} \beta$. Así, tenemos que $|\alpha + \gamma| = |\beta + \gamma|$. Como $\gamma \in \mathbb{Z}_{\geq 0}^n$ y el orden lexicográfico es un orden monomial, entonces $\alpha + \gamma >_{lex} \beta + \gamma$. Por lo tanto, $\alpha + \gamma >_{lex} \beta + \gamma$.

$\boxed{(iii)}$ Supongamos que el orden lexicográfico graduado no es un buen orden. Entonces, existe una secuencia infinita estrictamente decreciente, digamos

$$\alpha(1) >_{grlex} \alpha(2) >_{grlex} \alpha(3) >_{grlex} \ldots \text{ con } \alpha(i) \in \mathbb{Z}_{\geq 0}^n.$$

Observación: No puede ocurrir que $|\alpha(1)| = |\alpha(2)| = |\alpha(3)| = \ldots$ porque entonces habría una secuencia infinita estrictamente decreciente $\alpha(1) >_{lex} \alpha(2) >_{lex} \ldots$, lo cual es una contradicción pues el orden lexicográfico es un buen orden. De hecho, sólo un número finito de elementos de la secuencia pueden tener norma igual.
Así, sea $\alpha(i)$ un elemento de la secuencia tal que $|\alpha(i)| > |\alpha(j)|$ con $i < j$. Si ocurre que $|\alpha(j+1)| = |\alpha(j+2)| = \ldots = |\alpha(k)|$, entonces tomamos $\alpha(k+1)$, el cual existe porque la secuencia es infinita. Así, tenemos que $|\alpha(i)| > |\alpha(j)| > |\alpha(k+1)|$. Continuando de este modo, construimos una secuencia infinita estrictamente decreciente, lo cual es una contradicción porque son elementos de $\mathbb{Z}_{\geq 0}$ y éste es bien ordenado. Por lo tanto, el orden lexicográfico graduado es un buen orden. De (i), (ii) y (iii) concluimos que el orden lexicográfico graduado es un orden monomial. ■

Las siguientes definiciones y el lema nos ayudarán a entender de mejor manera un tipo de ideal que nos interesa fuertemente.

Definición 2.9 Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio no cero en $\mathbb{K}[x_1, \ldots, x_n]$ y sea $>$ un orden monomial.

1. El *multigrado* de f es

$$multigra(f) := max\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\},$$

   (el máximo es tomado con respecto a $>$).

2. El *coeficiente principal* de f es

$$\text{LC}(f) := a_{multigra(f)} \in \mathbb{K}.$$

3. El *monomio principal* de f es

$$\text{LM}(f) := x^{multigra(f)},$$

   (con coeficiente 1).

4. El *término principal* de f es

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

Lema 2.8 *Sean $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ polinomios no cero. Entonces:*

(i) $multigra(fg) = multigra(f) + multigra(g)$.

(ii) Si $f + g \neq 0$, entonces $multigra(f + g) \leq max\{multigra(f), multigra(g)\}$. Si, además, $multigra(f) \neq multigra(g)$, entonces ocurre la igualdad.

Prueba. Como f y g son polinomios en $\mathbb{K}[x_1, \ldots, x_n]$, entonces $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ y $g = \sum_{\beta \in B} b_\beta x^\beta$ con $A, B \subset \mathbb{Z}^n_{\geq 0}$. Y sean $\alpha_0 = multigra(f)$ y $\beta_0 = multigra(g)$. Por definición tenemos que $\alpha_0 > \alpha \ \ \forall\, \alpha \in A$ y $\beta_0 > \beta \ \ \forall\, \beta \in B$.

$\boxed{(i)}$ Tenemos que $fg = \sum_{\alpha+\beta} a_\alpha b_\beta x^{\alpha+\beta}$. Como $>$ es orden monomial entonces

$$\alpha_0 + \beta_0 > \alpha + \beta_0, \ \ \forall\, \alpha \qquad y \qquad \alpha + \beta_0 > \alpha + \beta, \ \ \forall\, \beta.$$

Esto implica que $\alpha_0 + \beta_0 > \alpha + \beta \ \ \forall\, \alpha + \beta$. Así, $\alpha_0 + \beta_0 = multigra(fg)$. Por lo tanto, $multigra(fg) = multigra(f) + multigra(g)$.

$\boxed{(ii)}$ Tenemos que $f + g = \sum_{\alpha \in A \setminus B} a_\alpha x^\alpha + \sum_{\beta \in B \setminus A} b_\beta x^\beta + \sum_{\gamma \in A \cap B} (a_\gamma + b_\gamma) x^\gamma$.

Caso 1: $\alpha_0 = \beta_0$. Tenemos dos casos: $a_{\alpha_0} + b_{\beta_0} = 0$ ó $a_{\alpha_0} + b_{\beta_0} \neq 0$.

Si $a_{\alpha_0} + b_{\beta_0} = 0$ entonces $multigra(f + g) < multigra(f) = multigra(g)$.

Si $a_{\alpha_0} + b_{\beta_0} \neq 0$ entonces $multigra(f + g) = multigra(f) = multigra(g)$.

Por lo tanto, $multigra(f + g) \leq max\{multigra(f), multigra(g)\}$.

Caso 2: $\alpha_0 \neq \beta_0$. Como $>$ es orden monomial, entonces $\alpha_0 > \beta_0$ ó $\beta_0 > \alpha_0$.

Si $\alpha_0 > \beta_0$ entonces $\alpha_0 > \alpha, \ \ \forall\, \alpha \in A$ y $\alpha_0 > \beta_0 > \beta, \ \ \forall \beta \in B$. Esto implica que $\alpha_0 = multigra(f + g)$.

Si $\beta_0 > \alpha_0$, entonces $\beta_0 > \beta, \ \ \forall\, \beta \in B$ y $\beta_0 > \alpha_0 > \alpha, \ \ \forall \alpha \in A$. Esto implica que $\beta_0 = multigra(f + g)$.

Por lo tanto, $multigra(f + g) \leq max\{multigra(f), multigra(g)\}$ y si $multigra(f) \neq multigra(g)$, entonces ocurre la igualdad. ■

Gracias a estos conceptos se puede definir un ideal en el anillo de polinomios relacionado con un orden monomial.

Definición 2.10 Un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ es un *ideal monomial* si existe un subconjunto $A \subset \mathbb{Z}^n_{\geq 0}$ (posiblemente infinito) tal que I consiste de todos los polinomios los cuales son sumas finitas de la forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, donde $h_\alpha \in \mathbb{K}[x_1, \ldots, x_n]$. En este caso, escribimos $I = \langle x^\alpha \,|\, \alpha \in A \rangle$.

El siguiente lema establece cómo son los monomios que pertenecen a un ideal dado, de este modo, nos es más sencillo visualizar el ideal.

Lema 2.9 *Sea $I = \langle x^\alpha \,|\, \alpha \in A \rangle$ un ideal monomial. Entonces un monomio x^β pertenece a I si y sólo si x^β es divisible por x^α para alguna $\alpha \in A$.*

Prueba. $\boxed{\Rightarrow}$ Como $x^\beta \in I$, esto implica que $x^\beta = \sum_{\alpha \in A} h_\alpha x^\alpha$, esto es, $\sum_{\alpha \in A} h_\alpha x^\alpha - x^\beta = 0$. Como I es ideal, entonces, $\sum_{\alpha \in A} h_\alpha x^\alpha - x^\beta \in I$. Tenemos que cada término de $\sum_{\alpha \in A} h_\alpha x^\alpha$ es divisible por algún x^α, entonces x^β también es divisible por algún x^α.
$\boxed{\Leftarrow}$ Tenemos que x^β es divisible por x^α, para alguna $\alpha \in A$. Entonces, $x^\beta = x^\gamma x^\alpha$ con $x^\gamma \in \mathbb{K}[x_1, \ldots, x_n]$. Por definición de I, $x^\beta \in I$. ■

Observemos que x^β es divisible por x^α exactamente cuando $x^\beta = x^\alpha \cdot x^\gamma$, para alguna $\gamma \in \mathbb{Z}^n_{\geq 0}$. Esto es equivalente a $\beta = \alpha + \gamma$. De este modo

$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma \mid \gamma \in \mathbb{Z}^n_{\geq 0}\}$$

consiste de los exponentes de todos los monomios divisibles por x^α.

Así, un ejemplo de ideal monomial está dado de la siguiente manera: si

$$A = \{(1,4), (2,3), (4,1)\} \subset \mathbb{Z}^2_{\geq 0},$$

entonces, $I = \langle xy^4, x^2y^3, x^4y \rangle$. Así, los exponentes de los monomios en I forman el conjunto

$$((1,4) + \mathbb{Z}^2_{\geq 0}) \cup ((2,3) + \mathbb{Z}^2_{\geq 0}) \cup ((4,1) + \mathbb{Z}^2_{\geq 0}).$$

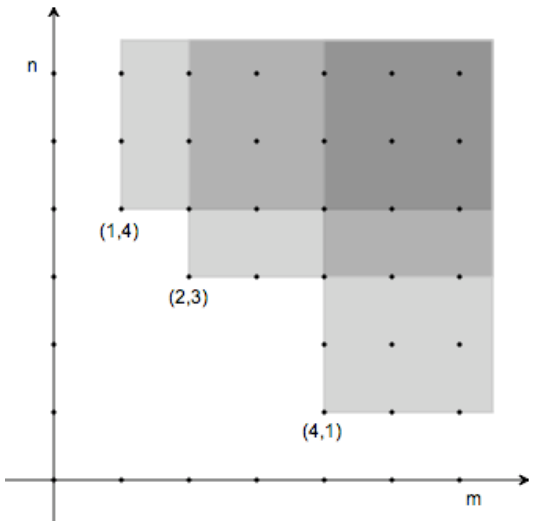


Figura 2.3: $(m, n) \longleftrightarrow x^m y^n$

Podemos visualizar este conjunto como la unión de puntos enteros en tres copias trasladadas del primer cuadrante del plano (ver Figura 2.3).

El siguiente lema nos dice cómo identificar cuando un polinomio pertenece al ideal monomial.

Lema 2.10 *Sea I un ideal monomial, y sea $f \in \mathbb{K}[x_1, \ldots, x_n]$. Entonces los siguientes son equivalentes:*

(i) $f \in I$.

(ii) Cada término de f pertenece a I.

(iii) f es una combinación $\mathbb{K}$-lineal de monomios en I, es decir, f es una combinación lineal de monomios en I con coeficientes en $\mathbb{K}$.

Prueba. $\boxed{(i) \Rightarrow (iii)}$ Como $f \in I$, entonces, $f = \sum_{\alpha \in A} h_\alpha x^\alpha$. Si desarrollamos cada h_α como una combinación lineal de monomios, tenemos por el lema 2.9 que cada término va a pertenecer a I. Por lo tanto, f es una combinación $\mathbb{K}$-lineal de monomios en I.

$\boxed{(iii) \Rightarrow (ii)}$ Como f es una combinación $\mathbb{K}$-lineal de monomios en I, entonces, $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ con $a_\alpha \in \mathbb{K} \ \ \forall\, \alpha \in A$. Por lo tanto, cada término de f pertenece a I.
$\boxed{(ii) \Rightarrow (i)}$ Por hipótesis tenemos que cada término de f pertenece a I. Como I es ideal, entonces la suma de los términos está en I, la cual es precisamente f. Por lo tanto, $f \in I$. ■

Como una consecuencia inmediata de este lema tenemos el siguiente corolario, el cual establece cuándo dos ideales monomiales son iguales.

Corolario 2.1 *Dos ideales monomiales son iguales si y sólo si contienen los mismos monomios.*

Prueba. $\boxed{\Rightarrow}$ Sean $I, J \subset \mathbb{K}[x_1, \ldots, x_n]$ ideales monomiales tales que $I = J$. Entonces, $x^\alpha \in I \iff x^\alpha \in J$. Por lo tanto, tienen los mismos monomios.
$\boxed{\Leftarrow}$ Sean $I, J \subset \mathbb{K}[x_1, \ldots, x_n]$ ideales monomiales tales que contienen los mismos monomios.
Sea $f \in I$, entonces, por el lema 2.10 f es una combinación $\mathbb{K}$-lineal de los monomios de I, los cuales están en J, es decir, f es una combinación $\mathbb{K}$-lineal de los monomios de J. Así por el lema 2.10, $f \in J$. Lo cual implica que $I \subseteq J$.
Sea $g \in J$, de manera análoga (por el lema 2.10 y por hipótesis) tenemos que $g \in I$. Lo cual implica que $J \subseteq I$. Por lo tanto, $I = J$. ■

El siguiente teorema es muy importante ya que muestra que todo ideal monomial tiene una base finita. Y nos ayudará a demostrar que cualquier ideal tiene una base finita.

Teorema 2.1 (Lema de Dickson) *Todo ideal monomial* $I = \langle x^\alpha \mid \alpha \in A \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ *puede ser escrito de la forma* $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, *donde* $\alpha(1), \ldots, \alpha(s) \in A$. *En particular,* I *tiene una base finita.*

Prueba. La demostración se hará por inducción sobre el número de variables en el anillo de polinomios.

Si $n = 1$, es decir, si el anillo de polinomios es $\mathbb{K}[x_1]$, entonces I es generado por los monomios x_1^α, donde $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Como $\mathbb{Z}_{\geq 0}$ está bien ordenado entonces A tiene un elemento mínimo. Así, sea β dicho elemento mínimo, es decir, $\beta \leq \alpha \ \ \forall\, \alpha \in A$. De esta manera, x_1^β divide a todos los elementos x_1^α de I. Por lo tanto, $I = \langle x_1^\beta \rangle$.

Hipótesis de inducción: Supongamos que $n > 1$ y que el teorema es cierto para $n - 1$. Tenemos que $\mathbb{K}[x_1, \ldots, x_{n-1}, y]$ es un anillo de polinomios con n variables y sus monomios son de la forma $x^\alpha y^m$, donde $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ y $m \in \mathbb{Z}_{\geq 0}$.

Supongamos que $I \subset \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ es un ideal monomial. Consideremos $J \subset \mathbb{K}[x_1, \ldots, x_{n-1}]$ el ideal generado por los monomios x^α tales que $x^\alpha y^m \in I$ con $m \geq 0$. Como $J \subset \mathbb{K}[x_1, \ldots, x_{n-1}]$ es un ideal monomial, entonces por la hipótesis de inducción, hay un número finito de monomios x^α que generan J, así, $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. De esta manera, para cada $i \in \{1, \ldots, s\}$, se tiene por definición de J, $x^{\alpha(i)} y^{m_i} \in I$ para alguna $m_i \geq 0$. Por otro lado notemos que existe $m \geq 0$ tal que $m \geq m_i \ \ \forall\ i \in \{1, \ldots, s\}$.

Entonces para cada k entre 0 y $m - 1$, consideramos el ideal $J_k \subset \mathbb{K}[x_1, \ldots, x_{n-1}]$ generado por los monomios x^β tales que $x^\beta y^k \in I$. Por hipótesis de inducción, $J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)} \rangle$.

Afirmación: I es generado por los monomios de la siguiente lista

$$\begin{aligned}
\text{de } J &: x^{\alpha(1)} y^m, \ldots, x^{\alpha(s)} y^m \\
\text{de } J_0 &: x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)} \\
\text{de } J_1 &: x^{\alpha_1(1)} y, \ldots, x^{\alpha_1(s_1)} y \\
&\vdots \\
\text{de } J_{m-1} &: x^{\alpha_{m-1}(1)} y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1}.
\end{aligned}$$

Es decir, queremos demostrar que

$$\begin{aligned}
I = \langle & x^{\alpha(1)} y^m, \ldots, x^{\alpha(s)} y^m, x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)}, x^{\alpha_1(1)} y, \ldots, x^{\alpha_1(s_1)} y, \ldots, \\
& x^{\alpha_{m-1}(1)} y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1} \rangle.
\end{aligned}$$

Denotemos por N el ideal generado por los monomios de la lista.

Sea $x^\alpha y^p$ cualquier monomio en I.

Caso 1: $p \geq m$, entonces $x^\alpha y^p$ es divisible por alguna $x^{\alpha(i)}y^m$ por construcción de J. Así por el lema 2.9, $x^\alpha y^p \in N$.

Caso 2: $p \leq m$, entonces $x^\alpha y^p$ es divisible por alguna $x^{\alpha_p(i)}y^p$ por construcción de J_p. Así, por el lema 2.9, $x^\alpha y^p \in N$. Por lo tanto, en cualquier caso los monomios de I están contenidos en N.

Además, cada $x^{\alpha_i(j)}y^{m_i} \in I$ por construcción. Por lo tanto, los monomios de N están contenidos en I, es decir, I y N tienen los mismos monomios. Así, por el corolario 2.1, tenemos que $I = N$, es decir, I tiene una base finita. ■

Tomamos nuevamente el ejemplo antes dado de ideal monomial, donde

$$I = \langle xy^4, x^2y^3, x^4y \rangle.$$

Así, tenemos que $J = \langle x \rangle \subset \mathbb{K}[x]$ (se puede ver en la Figura 2.3), luego, como $xy^4 \in I$, entonces $m = 4$. Finalmente, obtenemos los ideales J_k, con $0 \leq k \leq 3 = m - 1$, generados por los monomios que contienen a y^k:

$$\begin{aligned} J_0 &= \{0\} \\ J_1 &= J_2 = \langle x^4 \rangle \\ J_3 &= \langle x^2 \rangle. \end{aligned}$$

Determinar los J_k es sencillo con ayuda de la gráfica de los exponentes (Figura 2.3). Y así, por la demostración obtenemos que $I = \langle xy^4, x^4y, x^4y^2, x^2y^3 \rangle$.

Una consecuencia del lema de Dikson es el siguiente corolario que trata sobre buenos órdenes en $\mathbb{Z}^n_{\geq 0}$.

Corolario 2.2 *Sea $>$ una relación en $\mathbb{Z}^n_{\geq 0}$ que satisface:*

(i) $>$ es un orden total en $\mathbb{Z}^n_{\geq 0}$.

(ii) Si $\alpha > \beta$ *y* $\gamma \in \mathbb{Z}^n_{\geq 0}$, *entonces* $\alpha + \gamma > \beta + \gamma$.

Entonces $>$ *es buen orden si y sólo si* $\alpha \geq 0$ *para toda* $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Prueba. $\boxed{\Rightarrow}$ Como $>$ es buen orden, entonces, $\mathbb{Z}^n_{\geq 0}$ tiene elemento mínimo, digamos α_0. Así, $\alpha_0 \leq \alpha, \quad \forall\, \alpha \in \mathbb{Z}^n_{\geq 0}$.

Supongamos que $\alpha_0 < 0$, entonces, por (ii), $\alpha_0 + \alpha_0 < \alpha_0 + 0$, es decir, $2\alpha_0 < \alpha_0$. Pero $2\alpha_0 \in \mathbb{Z}^n_{\geq 0}$, lo cual es una contradicción porque α_0 es elemento mínimo. Esto implica que $\alpha_0 \geq 0$. Por lo tanto, $\alpha \geq 0 \ \ \forall\ \alpha \in \mathbb{Z}^n_{\geq 0}$.

$\boxed{\Leftarrow}$ Supongamos que $\alpha \geq 0 \ \ \forall\ \alpha \in \mathbb{Z}^n_{\geq 0}$. Sea $A \subset \mathbb{Z}^n_{\geq 0}$ no vacío y tenemos que $I = \langle x^\alpha \mid \alpha \in A\rangle$ es un ideal monomial. Por el lema de Dickson, I tiene una base finita, es decir, $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$ ordenado de tal manera que $\alpha(1) < \alpha(2) < \ldots < \alpha(s)$.

Afirmación: $\alpha(1)$ es el elemento mínimo de A.

Sea $\alpha \in A$. Entonces $x^\alpha \in I$. Por el lema 2.9, x^α es divisible por alguna $x^{\alpha(i)}$, es decir, $\alpha = \alpha(i) + \gamma$ para alguna $\gamma \in \mathbb{Z}^n_{\geq 0}$ y $\gamma \geq 0$. Entonces, por hipótesis y de (ii) tenemos que

$$\alpha = \alpha(i) + \gamma \geq \alpha(i) + 0 = \alpha(i) \geq \alpha(1).$$

Lo cual implica que $\alpha(1)$ es el elemento mínimo de A.

Como A fue cualquier subconjunto no vacío de $\mathbb{Z}^n_{\geq 0}$, entonces $>$ es buen orden. ■

Definición 2.11 Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal distinto de $\{0\}$.

(i) Denotamos por $\text{LT}(I)$ al conjunto de términos principales de I. Esto es,

$$\text{LT}(I) = \{cx^\alpha \mid \text{existe } f \in I \text{ con } \text{LT}(f) = cx^\alpha\}.$$

(ii) Denotamos por $\langle \text{LT}(I)\rangle$ al ideal generado por los elementos de $\text{LT}(I)$.

Esta definición y la siguiente proposición son las que utilizaremos para demostrar el teorema de la base de Hilbert, el cual es el objetivo de esta sección.

Proposición 2.7 *Sea* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *un ideal.*

(i) $\langle \text{LT}(I) \rangle$ *es un ideal monomial.*

(ii) Existen $g_1, \ldots, g_s \in I$ *tales que* $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$.

Prueba. $\boxed{(i)}$ Los monomios principales $\text{LM}(g)$ de elementos $g \in I \setminus \{0\}$ generan al ideal monomial $\langle \text{LM}(g) \mid g \in I \setminus \{0\} \rangle$. Pero, sabemos que $\text{LM}(g)$ y $\text{LT}(g)$ difieren por una constante no cero.

Afirmación: $\langle \text{LM}(g) \mid g \in I \setminus \{0\} \rangle = \langle \text{LT}(I) \rangle$.

Sea $x^\alpha \in \langle \text{LM}(g) \mid g \in I \setminus \{0\} \rangle$ un monomio arbitrario. Sabemos que $cx^\alpha \in \text{LT}(I)$ con $c \in \mathbb{K}$. Así, $cx^\alpha \in \langle \text{LT}(I) \rangle$. Entonces x^α es divisible por cx^α. Por el lema 2.9 tenemos que $x^\alpha \in \langle \text{LT}(I) \rangle$.

Sea $cx^\alpha \in \langle \text{LT}(I) \rangle$ un monomio arbitrario. Entonces cx^α es divisible por x^α. Por el lema 2.9 tenemos que $cx^\alpha \in \langle \text{LM}(g) \mid g \in I \setminus \{0\} \rangle$. De esta manera, $\langle \text{LM}(g) \mid g \in I \setminus \{0\} \rangle$ y $\langle \text{LT}(I) \rangle$ contienen los mismos monomios. Entonces, por el corolario 2.1, $\langle \text{LM}(g) \mid g \in I \setminus \{0\} \rangle = \langle \text{LT}(I) \rangle$. Por lo tanto, $\langle \text{LT}(I) \rangle$ es un ideal monomial.

$\boxed{(ii)}$ Por lo anterior, tenemos que $\langle \text{LT}(I) \rangle$ es generado por los monomios $\text{LM}(g)$ para $g \in I \setminus \{0\}$. Así, por el lema de Dickson, tenemos que $\langle \text{LT}(I) \rangle = \langle \text{LM}(g_1), \ldots, \text{LM}(g_s) \rangle$. Como $\text{LM}(g_i)$ difiere de $\text{LT}(g_i)$ por una constante no cero, entonces $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$. Por lo tanto, existen $g_1, \ldots, g_s \in I$ tales que $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$. ■

Teorema 2.2 (Teorema de la Base de Hilbert) *Cada ideal* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *tiene un conjunto generador finito. Esto es,* $I = \langle g_1, \ldots, g_s \rangle$ *para algunos* $g_1, \ldots, g_s \in I$.

Prueba. Si $I = \{0\}$ entonces el conjunto generador es $\langle 0 \rangle$, el cual es finito.

Si I contiene al menos un polinomio no cero, entonces un conjunto generador para I puede ser construido como sigue: por la proposición 2.6 existen $g_1, \ldots, g_s \in I$ tales que $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$.

Afirmación: $I = \langle g_1, \ldots, g_s \rangle$.

$\boxed{\subseteq}$ Sea $f \in I$ cualquier polinomio. Si aplicamos el algoritmo de la división, es decir, dividir f por $g_1, \ldots, g_s$ obtenemos que $f = a_1 g_1 + \ldots + a_s g_s + r$, donde cada término en r

no es divisible por ningún $\text{LT}(g_1), \ldots, \text{LT}(g_s)$. Esto implica que $r = f - a_1g_1 - \ldots - a_sg_s \in I$ ya que $f, a_1g_1 + \ldots + a_sg_s \in I$.

Si $r \neq 0$ entonces $\text{LT}(r) \in \langle \text{LT}(I) \rangle$. Así, por el lema 2.9, $\text{LT}(r)$ debe ser divisible por algún $\text{LT}(g_i)$, lo cual es una contradicción.

De esta manera, $r = 0$. Así, $f = a_1g_1 + \ldots + a_sg_s \in \langle g_1, \ldots, g_s \rangle$, lo cual prueba que $I \subseteq \langle g_1, \ldots, g_s \rangle$.

$\boxed{\supseteq}$ $\langle g_1, \ldots, g_s \rangle \subseteq I$ ya que $g_i \in I$ para toda $i \in \{1, \ldots, s\}$ e I es ideal. Por lo tanto, $I = \langle g_1, \ldots, g_s \rangle$. ■

Hemos demostrado que cualquier ideal tiene un conjunto generador finito, sin embargo, existe un tipo de bases que son derivadas de este teorema.

Definición 2.12 Fijamos un orden monomial. Un subconjunto finito $G = \{g_1, \ldots, g_s\}$ de un ideal I es llamado una *base de Groebner (o base estándar) de* I si

$$\langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle = \langle \text{LT}(I) \rangle.$$

Corolario 2.3 *Considere un orden monomial. Entonces cada ideal* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *distinto de* $\{0\}$ *tiene una base de Groebner. Más aún, cualquier base de Groebner de un ideal* I *es una base de* I.

Prueba. Dado un ideal no cero, el conjunto $G = \{g_1, \ldots, g_s\}$ construido en la prueba de teorema 2.2 es una base de Groebner por definición. Como $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$ entonces por el mismo argumento que en el teorema 2.2, $I = \langle g_1, \ldots, g_s \rangle$, lo cual implica que G es una base de I. ■

Por último, daremos una demostración de la Condición de la Cadena Ascendente.

Teorema 2.3 (Condición de la Cadena Ascendente) *Sea*

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

una cadena ascendente de ideales en $\mathbb{K}[x_1, \ldots, x_n]$. *Entonces existe un número natural* $N \geq 1$ *tal que*

$$I_N = I_{N+1} = I_{N+2} = \ldots$$

Prueba. Dada la cadena ascendente $I_1 \subset I_2 \subset I_3 \subset \ldots$ consideremos el conjunto $I = \bigcup_{i=1}^{\infty} I_i$. Es fácil demostrar que I es un ideal en $\mathbb{K}[x_1, \ldots, x_n]$.
Así, por el teorema de la base de Hilbert, el ideal I debe tener un conjunto generador finito, es decir, $I = \langle f_1, \ldots, f_s \rangle$. Notemos que cada generador está contenido en un I_j, esto es, $f_i \in I_{j_i}$ para algún j_i con $i = 1, \ldots, s$. Definimos $N = max(j_i)$. Por la definición de cadena ascendente, tenemos que $f_i \in I_N \ \forall\, i$. Así, tenemos que

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \ldots \subset I.$$

Como resultado de esto, obtenemos que la cadena ascendente se estabiliza con I_N. ■

2.3. Conjuntos algebraicos irreducibles e ideales primos

Los conjuntos algebraicos irreducibles son un tipo importante de los conjuntos algebraicos, de hecho, el objetivo de esta sección es mostrar que cualquier conjunto algebraico puede escribirse como una unión finita de conjuntos algebraicos irreducibles.

Definición 2.13 Un conjunto algebraico $V \subset \mathbb{K}^n$ es *irreducible* si siempre que V es escrito en la forma $V = V_1 \cup V_2$, donde V_1 y V_2 son conjuntos algebraicos, entonces, $V_1 = V$ ó $V_2 = V$.

Un ejemplo de un conjunto algebraico irreducible es $V = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 0\}$, el cual es el origen del plano. Es irreducible porque no puede escribirse de la forma $V = V_1 \cup V_2$, con V_1 y V_2 conjuntos algebraicos distintos de V.

Por el contrario, $W = \{(x, y) \in \mathbb{R}^2 \mid (x^2 + y^2 - 1)(y - x) = 0\}$ no es irreducible ya que si $W_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 - 1 = 0\}$ y $W_2 = \{(x, y) \in \mathbb{R}^2 \mid y - x = 0\}$, entonces, $W = W_1 \cup W_2$, donde $W \neq W_1$ y $W \neq W_2$.

Estos ejemplos nos hacen pensar si existe alguna relación entre los conjuntos algebraicos irreducibles y los polinomios irreducibles. La respuesta es que no existe nin-

guna relación, es decir, que el conjunto algebraico sea irreducible no implica que el polinomio que lo describe sea irreducible. Tampoco ocurre que si el polinomio que lo describe es irreducible entonces el conjunto algebraico es irreducible. El ejemplo $V = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 0\}$ es el origen en el plano y es descrito también por el polinomio $(x^2+y^2)(x^2+1)$, el cual no es irreducible. Por otra parte, observamos que el polinomio $f(x, y) = y^2 + x^2(x-1)^2$ es irreducible pero $U = \{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\}$ no es irreducible. Veamos porqué. Geométricamente, U consiste de los puntos $(0, 0)$ y $(1, 0)$. De este modo definimos $U_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 0\}$ y $U_2 = \{(x, y) \in \mathbb{R}^2 \mid (x-1)^2 + y^2 = 0\}$, entonces $U = U_1 \cup U_2$, donde $U \neq U_1$ y $U \neq U_2$.

Decidir si un conjunto algebraico es irreducible o no, basándonos únicamente en la definición, es una tarea complicada, sin embargo, existe una manera más sencilla de saberlo. Para ello es necesario definir cierto tipo de ideal.

Definición 2.14 Un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ es *primo* si siempre que $fg \in I$, entonces $f \in I$ ó $g \in I$.

Como ejemplo tenemos $I = \langle x \rangle \subset \mathbb{R}[x]$, el cual es un ideal primo ya que si $fg \in I$ y suponemos que $f \notin I$ y $g \notin I$, entonces ambos polinomios tienen un termino que no es divisible por x, es decir, un termino independiente. Esto implica que fg tiene un termino independiente, es decir, $fg \notin I$, lo cual es una contradicción. Por lo tanto, $f \in I$ ó $g \in I$.

Por el contrario, $J = \langle x^2 \rangle \subset \mathbb{R}[x]$ no es un ideal primo, ya que si $f(x) = 2x$ y $g(x) = x$, tenemos que $fg(x) = 2x^2 \in J$ pero $f \notin J$ y $g \notin J$.

La siguiente proposición establece la relación que existe entre conjuntos algebraicos irreducibles y el tipo de su ideal.

Proposición 2.8 *Sea $V \subset \mathbb{K}^n$ un conjunto algebraico. Entonces V es irreducible si y sólo si $\mathbf{I}(V)$ es un ideal primo.*

Prueba. La prueba se realizará por contrapuesta, es decir, se demostrará que V no es irreducible si y sólo si $\mathbf{I}(V)$ no es ideal primo.

Tenemos que V no es irreducible $\iff$ $V = V_1 \cup V_2$, para algunos V_1, V_2 conjuntos algebraicos tales que $V \neq V_1$ y $V \neq V_2$ $\iff$ $V_1 \subsetneq V$, $V_2 \subsetneq V$ y $V_1 \cup V_2 = V$ $\iff$ $\mathbf{I}(V_1) \supsetneq \mathbf{I}(V)$ y $\mathbf{I}(V_2) \supsetneq \mathbf{I}(V)$ (porque si fueran iguales entonces los conjuntos algebraicos serían iguales) $\iff$ existen $f \in \mathbf{I}(V_1)$ y $g \in \mathbf{I}(V_2)$ tales que $f, g \notin \mathbf{I}(V)$ y $fg \in \mathbf{I}(V)$ (ya que si $x \in V$ entonces $x \in V_1$ ó $x \in V_2$ y así $fg(x) = f(x)g(x) = 0$) $\iff$ $\mathbf{I}(V)$ no es ideal primo. Por lo tanto, V es irreducible si y sólo si $\mathbf{I}(V)$ es ideal primo. ■

Así como tenemos una condición de cadena ascendente para ideales, tenemos una condición de cadena descendente para conjuntos algebraicos.

Proposición 2.9 (Condición de la Cadena Descendente) *Cualquier cadena descendente de conjuntos algebraicos*

$$V_1 \supset V_2 \supset V_3 \supset \dots$$

en $\mathbb{K}^n$ debe estabilizarse, esto es, existe un entero positivo N tal que $V_N = V_{N+1} = V_{N+2} = \dots$

Prueba. Como $V_1 \supset V_2 \supset V_3 \supset \dots$ entonces por la proposición 2.3 tenemos que $\mathbf{I}(V_1) \subset \mathbf{I}(V_2) \subset \mathbf{I}(V_3) \subset \dots$, es decir, tenemos una cadena ascendente de ideales. Por el teorema 2.3 existe un entero positivo N tal que $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \dots$. Además tenemos que $\mathbf{V}(\mathbf{I}(V)) = V$ para cualquier conjunto algebraico (por la proposición 2.4). Por lo tanto, $V_N = V_{N+1} = \dots$ ■

Esta condición nos ayuda a demostrar el siguiente teorema que es el objetivo principal de esta sección.

Teorema 2.4 *Sea $V \subset \mathbb{K}^n$ un conjunto algebraico. Entonces, V puede ser escrito como una unión finita*

$$V = V_1 \cup V_2 \cup \dots \cup V_m,$$

donde cada V_i es un conjunto algebraico irreducible.

Prueba. Supongamos que V es un conjunto algebraico que no puede escribirse como una unión finita de irreducibles. Entonces V es no irreducible (ya que si lo fuera, entonces él mismo sería la unión finita de irreducibles). Esto es, $V = V_1 \cup V_1'$, donde $V \neq V_1$ y $V \neq V_1'$ y V_1, V_1' conjuntos algebraicos. Más aún, al menos uno no debe ser unión finita de conjuntos algebraicos irreducibles pues si los dos fueran entonces V sería unión finita de conjuntos algebraicos irreducibles. Decimos que V_1 no es una unión finita de conjuntos algebraicos irreducibles. Por el mismo argumento para V, podemos escribir $V_1 = V_2 \cup V_2'$ donde $V_1 \neq V_2$ y $V_1 \neq V_2'$; con al menos uno que no es una unión finita de conjuntos algebraicos irreducibles, digamos V_2. Continuando en este sentido, damos una secuencia infinita de conjuntos algebraicos

$$V \supset V_1 \supset V_2 \supset \dots$$

con $V \neq V_1 \neq V_2 \neq \dots$ lo cual contradice la proposición 2.9. ■

2.4. Teorema de los ceros de Hilbert

En esta sección lo que buscamos es describir la correspondencia entre los ideales y los conjuntos algebraicos. Para ello, trataremos tres importantes teoremas, que son los denominados "Nullstellensatz". Tal palabra es formada por las palabras alemanas Null (= cero), Stellen (= lugares), Satz (= teorema).

Sin embargo, antes de poder probar estos teoremas, necesitamos definiciones y ciertas propiedades de éstas.

Definición 2.15 Dado $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{K}[x_1, \dots, x_n]$, el *l-ésimo ideal de eliminación* I_l es el ideal de $\mathbb{K}[x_{l+1}, \dots, x_n]$ definido por

$$I_l = I \cap \mathbb{K}[x_{l+1}, \dots, x_n]$$

Enunciaremos el siguiente teorema pues nos será necesario más adelante, sin embargo, la prueba no la explicaremos pues abarca conceptos que no hemos visto en este

trabajo y que no nos atañen de manera directa.

Teorema 2.5 (Teorema de Extensión) *Sea $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ y sea I_1 el primer ideal de eliminación de I. Para cada $1 \leq i \leq s$, f_i es de la forma*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \textit{términos en los que } x_1 \textit{ tiene grado} < N_i,$$

donde $N_i \geq 0$ y $g_i \in \mathbb{C}[x_2, \ldots, x_n]$ es no cero. Supongamos que tenemos una solución parcial $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. Si $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$, entonces existe $a_1 \in \mathbb{C}$ tal que $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Corolario 2.4 *Sea $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$, y asumimos que para alguna i, f_i es de la forma*

$$f_i = cx_1^N + \textit{términos en los que } x_1 \textit{ tiene grado} < N,$$

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

Prueba. Sea $g_i = c \neq 0$ entonces $\mathbf{V}(g_1, \ldots, g_s) = \emptyset$, así $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$ para todas las soluciones parciales y por el Teorema de Extensión existe $a_1 \in \mathbb{C}$ tal que $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$. ■

Vamos a establecer la definición de la proyección de un conjunto algebraico. Supongamos que tenemos $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{C}^n$. Para eliminar las primeras l variables $x_1, \ldots, x_l$, consideraremos la *aplicación proyección*

$$\pi_l : \mathbb{C}^n \to \mathbb{C}^{n-l}$$

el cual manda $(a_1 \ldots, a_n)$ a $(a_{l+1}, \ldots, a_n)$. Si aplicamos π_l a $V \subset \mathbb{C}^n$, entonces obtenemos $\pi_l(V) \subset \mathbb{C}^{n-l}$. Podemos relacionar $\pi_1(V)$ con el l-ésimo ideal de eliminación como sigue.

Lema 2.11 *Sea $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ y $I_l = \langle f_1, \ldots, f_s \rangle \cap \mathbb{C}[x_{l+1}, \ldots, x_n]$ el l-ésimo ideal de eliminación. Entonces, en $\mathbb{C}^{n-l}$, tenemos*

$$\pi_l(V) \subset \mathbf{V}(I_l).$$

Prueba. Elegimos $f \in I_l$ arbitrario. Si $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$ entonces f se anula en $(a_1, \ldots, a_n)$ ya que $f \in \langle f_1, \ldots, f_s \rangle$. Como f sólo está desarrollado en las variables $x_{l+1}, \ldots, x_n$ entonces podemos escribir

$$f(a_{l+1}, \ldots, a_n) = f(\pi(a_1 \ldots, a_n)) = 0$$

Esto muestra que f se anula en todo punto de $\pi_l(V)$ y como f fue arbitrario entonces se tiene que $\pi_l(V) \subset \mathbf{V}(I_l)$. ■

El primer ideal de eliminación posee ciertas propiedades importantes, es por ello que enunciamos el siguiente teorema y posteriormente, un corolario inmediato.

Teorema 2.6 *Dado $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{C}^n$, sean g_i como en el Teorema de Extensión. Si I_1 es el primer ideal de eliminación de $\langle f_1, \ldots, f_s \rangle$, entonces tenemos la igualdad en $\mathbb{C}^{n-1}$*

$$\mathbf{V}(I_1) = \pi_1(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)),$$

donde $\pi_1 : \mathbb{C}^n \to \mathbb{C}^{n-1}$ es la proyección sobre las últimas $n-1$ componentes.

Prueba. $\boxed{\subseteq}$ Sea $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. Por el lema 2.11 tenemos que $\pi_1(V) \subset \mathbf{V}(I_1)$ entonces $(a_2, \ldots, a_n) \in \pi_1(V)$ ó $(a_2, \ldots, a_n) \notin \pi_1(V)$.
Si $(a_2, \ldots, a_n) \in \pi_1(V)$ entonces $(a_2, \ldots, a_n) \in \pi_1(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1))$.
Si $(a_2, \ldots, a_n) \notin \pi_1(V)$ entonces para todo $a \in \mathbb{C}$ se tiene que $(a, a_2, \ldots, a_n) \notin \mathbf{V}(f_1, \ldots, f_s)$ y se puede afirmar que $(a_2, \ldots, a_n) \in \mathbf{V}(g_1, \ldots, g_s)$ (si no fuera así podríamos aplicar el Teorema de Extensión y se llegaría a una contradicción). De esta manera $(a_2, \ldots, a_n) \in \pi_1(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1))$. Por lo tanto, $\mathbf{V}(I_1) \subseteq \pi_1(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1))$.
$\boxed{\supseteq}$ Sea $(a_2, \ldots, a_n) \in \pi_1(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1))$.

Si $(a_2, \ldots, a_n) \in \pi_1(V)$, por el lema 2.11 se tiene que $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$.
Si $(a_2, \ldots, a_n) \in \mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)$entonces $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. Por lo tanto, $\mathbf{V}(I_1) \supseteq \pi_1(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1))$.
De ambas contenciones tenemos lo que se quería probar. ■

Corolario 2.5 *Sea $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{C}^n$, y asumimos que para alguna i, f_i es de la forma*

$$f_i = cx_1^N + \textit{términos en los que } x_1 \textit{ tiene grado} < N,$$

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

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

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

Prueba. Tenemos por el Teorema 2.6 que $\mathbf{V}(I_1) = \pi_1(V) \cup (\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1))$, pero para i tenemos que $g_i = c \neq 0$, entonces $\mathbf{V}(g_1, \ldots, g_s) = \emptyset$, de esta manera $\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1) = \emptyset$ y por lo tanto $\mathbf{V}(I_1) = \pi_1(V)$ ■

Recordando la defínción de campo algebraicamente cerrado que establecimos en el capítulo 1, podemos enunciar una observación que nos será útil en la demostración del siguiente teorema.

Observación 2.3 *Todo campo algebraicamente cerrado tiene una infinidad de elementos.*

Prueba. Sea $\mathbb{K}$ un campo algebraicamente cerrado. Supongamos que $\mathbb{K}$ tiene un número finito de elementos, es decir, $\mathbb{K} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Por otro lado, proponemos el polinomio

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) + 1 = \prod_{i=1}^{n} (x - \alpha_i) + 1.$$

Así, tenemos que $f \in \mathbb{K}[x]$ porque $0, 1 \in \mathbb{K}$ ($\mathbb{K}$ es campo), además, f es un polinomio no constante en una variable.

Como $\mathbb{K}$ es algebraicamente cerrado entonces, existe $x \in \mathbb{K}$ tal que $f(x) = 0$, es decir, $x = \alpha_i$, para alguna i. Con esto, tenemos que $\prod_{i=1}^{n}(x - \alpha_i) = 0$, entonces $f(x) = 1$, es decir, $1 = 0$, lo cual es una contradicción.
Por lo tanto, $\mathbb{K}$ tiene una infinidad de elementos. ■

Ahora, ya podemos enunciar nuestro primer teorema importante de esta sección. A partir de ciertas condiciones podemos establecer cómo es nuestro ideal.

Teorema 2.7 (Débil Nullstellensatz) *Sea $\mathbb{K}$ un campo algebraicamente cerrado y sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal tal que $\mathbf{V}(I) = \emptyset$. Entonces $I = \mathbb{K}[x_1, \ldots, x_n]$.*

Prueba. La idea de la demostración radica en probar que $1 \in I$, ya que así $f \cdot 1 \in I$, $\forall\ f \in \mathbb{K}[x_1, \ldots, x_n]$ (por ser ideal), pero $f \cdot 1 = f$ y entonces se tendría lo que se quiere. La prueba se hará por inducción sobre el número de variables.
Si $n = 1$ y tomamos $I \subset \mathbb{K}[x]$ ideal tal que $\mathbf{V}(I) = \emptyset$. Sabemos, por la proposición 2.2 que $I = \langle f \rangle$ para algún $f \in \mathbb{K}[x]$, entonces $\mathbf{V}(I) = \{a \in \mathbb{K} \mid f(a) = 0\}$. Como $\mathbb{K}$ es algebraicamente cerrado entonces f es constante no cero y así $f^{-1} \in \mathbb{K}$, además $1 = f^{-1} \cdot f$ pero $f^{-1} \cdot f \in I$ (por ser ideal). Por lo tanto, $1 \in I$.
Hipótesis de inducción: Supongamos que el teorema se cumple para un anillo de polinomios de $n - 1$ variables.
Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal tal que $\mathbf{V}(I) = \emptyset$. Por el Teorema de la Base de Hilbert sabemos que $I = \langle f_1, \ldots, f_s \rangle$ con $f_i \in \mathbb{K}[x_1, \ldots, x_n]$. Podemos asumir que f_1 no es constante ya que si lo fuera tendría que ser distinto de cero (si fuera cero entonces $\mathbf{V}(I) \neq \emptyset$) y entonces ya habríamos terminado, pues $1 \in I$.
Así, supongamos que f_1 tiene grado $N \geq 1$. Ahora, consideramos el siguiente cambio lineal de coordenadas:

$$\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2\tilde{x}_1 \\ &\vdots \end{aligned}$$

$$x_n = \tilde{x}_n + a_n\tilde{x}_1$$

donde las a_i son constantes en $\mathbb{K}$ que serán determinadas. Primero, sustituyendo tenemos que f_1 tiene la forma

$$\begin{aligned} f_1(x_1,\ldots,x_n) &= f_1(\tilde{x}_1, \tilde{x}_2 + a_2\tilde{x}_1, \ldots, \tilde{x}_n + a_n\tilde{x}_1) \\ &= c(a_2,\ldots,a_n)\tilde{x}_1^N + \text{términos en los que } \tilde{x}_1 \text{ tiene grado} < N \end{aligned}$$

y $c(a_2,\ldots,a_n)$ debe ser una expresión polinomial no cero ya que f_1 es de grado N. Como $\mathbb{K}$ es algebraicamente cerrado es infinito, así, existen $(a_2,\ldots,a_n)$ tal que $c(a_2,\ldots,a_n) \neq 0$. Con esta elección bajo tal cambio lineal de coordenadas cada polinomio $f \in \mathbb{K}[x_1,\ldots,x_n]$ es enviado a un polinomio $\tilde{f} \in \mathbb{K}[\tilde{x}_1,\ldots,\tilde{x}_n]$.
Afirmación: $\widetilde{I} = \{\tilde{f} : f \in I\}$ es un ideal en $\mathbb{K}[\tilde{x}_1,\ldots,\tilde{x}_n]$.

> Tenemos que $0 \in \widetilde{I}$ ya que $0 \in I$. Luego, sean $\tilde{f}, \tilde{g} \in \widetilde{I}$, así existen $f, g \in I$, como es ideal entonces $f + g \in I$ y bajo el cambio de coordenadas tenemos que $\tilde{f} + \tilde{g} \in \widetilde{I}$. Por último, sea $h \in \mathbb{K}[\tilde{x}_1,\ldots,\tilde{x}_n]$ y $\tilde{f} \in \widetilde{I}$, entonces existen $h \in \mathbb{K}[x_1,\ldots,x_n]$ y $f \in I$, como es ideal entonces $hf \in I$ y bajo el cambio de coordenadas entonces $\tilde{h}\tilde{f} \in \widetilde{I}$. Por lo tanto, la afirmación está probada.

Observemos que $\mathbf{V}(\widetilde{I}) = \emptyset$ ya que si las ecuaciones transformadas tuvieran solución entonces las originales también tendrían. Además, si mostramos que $1 \in \widetilde{I}$, entonces $1 \in I$ (ya que las constantes no son afectadas por la operación $\tilde{}$).
Tenemos que $f_1 \in I$ se transforma en $\tilde{f}_1 \in \widetilde{I}$, con la propiedad

$$\tilde{f}_1(\tilde{x}_1,\ldots,\tilde{x}_n) = c(a_2,\ldots,a_n)\tilde{x}_1^N + \text{términos en los que } \tilde{x}_1 \text{ tiene grado} < N,$$

donde $c(a_2,\ldots,a_n) \neq 0$. Sea $\pi_1 : \mathbb{K}^n \to \mathbb{K}^{n-1}$ la proyección en las últimas $n-1$ componentes. Así, $\widetilde{I}_1 = \widetilde{I} \cap [\tilde{x}_2,\ldots,\tilde{x}_n]$ y por el corolario 2.5 tenemos que $\mathbf{V}(\widetilde{I}_1) = \pi_1(\mathbf{V}(\widetilde{I}))$. Esto implica que $\mathbf{V}(\widetilde{I}_1) = \pi_1(\mathbf{V}(\widetilde{I})) = \pi_1(\emptyset) = \emptyset$. Por la hipótesis de inducción $\widetilde{I}_1 = \mathbb{K}[\tilde{x}_2,\ldots,\tilde{x}_n]$, lo cual implica $1 \in \widetilde{I}_1 \subset \widetilde{I}$, y la prueba está completa. ■

El segundo teorema importante relaciona el ideal de un conjunto algebraico con el ideal que lo genera.

Teorema 2.8 (Nullstellensatz de Hilbert) *Sea $\mathbb{K}$ un campo algebraicamente cerrado. Si $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ son tales que $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, entonces existe un entero $m \geq 1$ tal que*

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

Prueba. Se demostrará que si $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ entonces existe un entero $m \geq 1$ tal que

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

donde los A_i son polinomios en $\mathbb{K}[x_1, \ldots, x_n]$.
Consideremos el siguiente ideal

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

(la prueba de ser ideal de $\mathbb{K}[x_1 \ldots, x_n, y]$ es similar a la hecha en el lema 2.2). Se verá que $\mathbf{V}(\widetilde{I}) = \emptyset$.
Sea $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{K}^{n+1}$, entonces se tienen sólo dos casos, que $(a_1, \ldots, a_n)$ sea un cero común de $f_1, \ldots, f_s$ o que no lo sea.
Caso 1: Si es un cero en común de $f_1, \ldots, f_s$ entonces $f(a_1, \ldots, a_n) = 0$ porque $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$. Así, el polinomio $1 - yf$ toma el valor $1 - a_{n+1} f(a_1, \ldots, a_n) = 1 \neq 0$ en el punto $(a_1, \ldots, a_n, a_{n+1})$, lo cual implica que $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\widetilde{I})$.
Caso 2: Como $(a_1, \ldots, a_n)$ no es un cero común, entonces para alguna i $(1 \leq i \leq s)$, pasa que $f_i(a_1, \ldots, a_n) \neq 0$. Podemos ver a f_i como una función de $n + 1$ variables que no depende de la última, así $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$, lo cual implica que $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\widetilde{I})$.
Como $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{K}^{n+1}$ fue arbitrario, se puede concluir que $\mathbf{V}(\widetilde{I}) = \emptyset$.

Ya que se cumplen las hipótesis del Teorema Débil Nullstellensatz, podemos afirmar que $\widetilde{I} = \mathbb{K}[x_1, \ldots, x_n, y]$, en particular $1 \in \widetilde{I}$, es decir

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

para algunos polinomios $p_i, q \in \mathbb{K}[x_1, \ldots, x_n, y]$. Si consideramos $y = 1/f(x_1, \ldots, x_n)$, entonces

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

Al multiplicar ambos lados por f^m, donde m es suficientemente grande para eliminar todos los denominadores, tenemos que

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

para algunos polinomios $A_i \in \mathbb{K}[x_1, \ldots, x_n]$. ■

Y por último, antes de enunciar el teorema fuerte, necesitamos una definición.

Definición 2.16 Sea $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal. El *radical de* I, denotado por $\sqrt{I}$, es el conjunto

$$\sqrt{I} := \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f^m \in I \text{ para algún entero } m \geq 1\}$$

Teorema 2.9 (Fuerte Nullstellensatz) *Sea* $\mathbb{K}$ *un campo algebraicamente cerrado. Si* I *es un ideal de* $\mathbb{K}[x_1, \ldots, x_n]$*, entonces*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$$

Prueba. $\boxed{\subseteq}$ Sea $f \in \mathbf{I}(\mathbf{V}(I))$ arbitrario, entonces f se anula en $\mathbf{V}(I)$. Por el Teorema Nullstellensatz de Hilbert existe un entero $m \geq 1$ tal que $f^m \in I$ pero esto significa que $f \in \sqrt{I}$. Como f fue arbitrario, concluimos que $\mathbf{I}(\mathbf{V}(I)) \subseteq \sqrt{I}$.

$\boxed{\supseteq}$ Sea $f \in \sqrt{I}$ arbitrario, entonces $f^m \in I$ para algún entero $m \geq 1$, por definición f^m se anula en $\mathbf{V}(I)$ y esto implica que f se anula en $\mathbf{V}(I)$, es decir, $f \in \mathbf{I}(\mathbf{V}(I))$. Como f fue arbitrario, concluimos que $\mathbf{I}(\mathbf{V}(I)) \supseteq \sqrt{I}$ ■

Capítulo 3

Conjuntos Semi-algebraicos Reales

Con lo desarrollado en el capítulo 2 podemos abordar los conjuntos semi-algebraicos reales de manera más natural. Para el desarrollo de este capítulo se consultó el libro *Real algebraic and semi-algebraic sets* [2].

En la primera sección establecemos la definición de estos conjuntos así como algunas de sus propiedades más importantes, tomando en cuenta que todos estos resultados nos serán de gran ayuda para desmostrar el primer teorema de estructura de los conjuntos semi-algebraicos reales.

En la segunda sección, estudiaremos resultantes y subresultantes. Pareciera que ésto no tiene mucha relación con los conjuntos semi-algebraicos pero las propiedades que determinan los subresultantes servirán para demostrar el primer teorema de estructura.

Al igual que la segunda, la tercera sección tampoco guarda relación con los conjuntos semi-algebraicos a primera vista, sin embargo, el último corolario de esa sección, que trata sobre la continuidad de las raíces reales de un polinomio dado, es muy importante para establecer el teorema final.

Por último, en la cuarta sección se demostrará el primer teorema de estructura, el cual dice que todo conjunto semi-algebraico en $\mathbb{R}^n$ tiene un número finito de componentes y cada una de ellas es un conjunto semi-algebraico.

3.1. Definiciones y propiedades

Mientras que los conjuntos algebraicos son los ceros de polinomios, los conjuntos semi-algebraicos son regiones determinadas por polinomios, la definición es la siguiente.

Definición 3.1 Un subconjunto V de $\mathbb{R}^n$ es llamado *semi-algebraico* si admite alguna representación de la forma

$$V := \bigcup_{i=1}^{s} \bigcap_{j=1}^{r_i} \{x \in \mathbb{R}^n \mid P_{i,j}(x) \ \delta_{ij} \ 0\}$$

donde, para cada $i = 1, \ldots, s$ y $j = 1, \ldots, r_i$,

1. $\delta_{ij} \in \{>, =, <\}$;

2. $P_{i,j} \in \mathbb{R}[x_1, \ldots, x_n]$.

En los conjuntos algebraicos, observamos que la intersección finita o la unión de dos conjuntos algebraicos, continua siendo algebraico. La siguiente proposición es la generalización de este resultado.

Proposición 3.1 *Si $A_1, \ldots, A_m$ son conjuntos semi-algebraicos en $\mathbb{R}^n$ entonces $\bigcup_{i=1}^{m} A_i$ y $\bigcap_{i=1}^{m} A_i$ también lo son.*

Prueba. Como $A_1, \ldots, A_m$ son conjuntos semi-algebraicos entonces pueden ser representados de la forma

$$A_1 \ = \ \bigcup_{i=1}^{s_1} \bigcap_{j=1}^{r_i} \{x \in \mathbb{R}^n \mid P^1_{i,j}(x) \ \delta_{ij} \ 0\}$$

$$\begin{aligned} A_2 &= \bigcup_{i=1}^{s_2}\bigcap_{j=1}^{r_i}\{x\in\mathbb{R}^n \mid P^2_{i,j}(x)\ \delta_{ij}\ 0\} \\ &\vdots \\ A_m &= \bigcup_{i=1}^{s_m}\bigcap_{j=1}^{r_i}\{x\in\mathbb{R}^n \mid P^m_{i,j}(x)\ \delta_{ij}\ 0\}. \end{aligned}$$

De esta manera tenemos que

$$\begin{aligned} \bigcup_{i=1}^{m} A_i &= \Big(\bigcup_{i=1}^{s_1}\bigcap_{j=1}^{r_i}\{x\in\mathbb{R}^n \mid P^1_{i,j}(x)\ \delta_{ij}\ 0\}\Big)\cup\ldots\cup\Big(\bigcup_{i=1}^{s_m}\bigcap_{j=1}^{r_i}\{x\in\mathbb{R}^n \mid P^m_{i,j}(x)\ \delta_{ij}\ 0\}\Big) \\ &= \bigcup_{i=1}^{t}\bigcap_{j=1}^{r_i}\{x\in\mathbb{R}^n \mid Q^i_{i,j}(x)\ \delta_{ij}\ 0\} \end{aligned}$$

donde $t = s_1 + \ldots + s_m$ y

$$Q^i_{i,j} = \begin{cases} P^1_{i,j} & \text{si } 1 \le i \le s_1 \\ P^2_{i-s_1,j} & \text{si } s_1+1 \le i \le s_1+s_2 \\ \vdots & \\ P^m_{i-(s_1+\ldots+s_{m-1}),j} & \text{si } s_1+\ldots+s_{m-1}+1 \le i \le s_1+\ldots+s_m \end{cases}$$

Por lo tanto, $\bigcup_{i=1}^{m} A_i$ es un conjunto semi-algebraico.

Luego, tenemos que

$$\bigcap_{i=1}^{m} A_i = \Big(\bigcup_{i=1}^{s_1}\bigcap_{j=1}^{r_{i_1}}\{x\in\mathbb{R}^n \mid P^1_{i,j}(x)\ \delta_{ij}\ 0\}\Big)\cap\ldots\cap\Big(\bigcup_{i=1}^{s_m}\bigcap_{j=1}^{r_{i_m}}\{x\in\mathbb{R}^n \mid P^m_{i,j}(x)\ \delta_{ij}\ 0\}\Big).$$

Denotemos por

$$A_{k,i} = \bigcap_{j=1}^{r_{i_k}}\{x\in\mathbb{R}^n \mid P^k_{i,j}(x)\ \delta_{ij}\ 0\},\ \text{ es decir, }\ A_k = \bigcup_{i=1}^{s_k} A_{k,i}.$$

De esta manera

$$\bigcap_{i=1}^{m} A_i = \bigcup\{A_{1,i_1}\cap A_{2,i_2}\cap\ldots\cap A_{m,i_m} \mid (i_1,\ldots,i_m)\in R_1\times R_2\times\ldots\times R_m\},$$

donde $R_i = \{1,2,\ldots,s_i\}$. Pero $A_{1,i_1}\cap A_{2,i_2}\cap\ldots\cap A_{m,i_m}$ es semi-algebraico para cualquier $(i_1,\ldots,i_m)\in R_1\times R_2\times\ldots\times R_m$, ya que se pueden escribir en la forma como dice la

definición. Esto es, la intersección de A_{r,i_r} con $A_{r+1,i_{r+1}}$ es un conjunto semi-algebraico. Por la primera parte de la demostración, tenemos que $\bigcap_{i=1}^{m} A_i$ es semi-algebraico. ■

Como el campo de los números complejos carece de un orden, no tiene sentido hablar de conjuntos semi-algebraicos en un anillo de polinomios con coeficientes en los complejos, sin embargo, podemos definir otro tipo de conjuntos que guardan relación con los conjuntos semi-algebraicos.

Definición 3.2 Un subconjunto $V \subseteq \mathbb{C}^n$ es llamado *construíble* si existen polinomios $P_{i,j} \in \mathbb{C}[x_1, \ldots, x_n]$ $(i = 1, \ldots, s;\ \ j = 1, \ldots, r_i)$ tales que

$$V = \bigcup_{i=1}^{s} \bigcap_{j=1}^{r_i} \{x \in \mathbb{C}^n \mid P_{i,j}(x)\ \delta_{ij}\ 0\},$$

donde $\delta_{ij} \in \{=, \neq\}$.

Observación 3.1 *Identificando $\mathbb{R}^n$ con la parte "real" de $\mathbb{C}^n$, para cualquier conjunto construíble V, se sigue que*

$$V_{\mathbf{R}} := \{(x_1, \ldots, x_n) \in V \mid \textit{la parte imaginaria de } x_i \textit{ es cero}\}$$

es semi-algebraico en $\mathbb{R}^n$.

Prueba. Tenemos que $V_{\mathbf{R}} = V \cap \mathbb{R}^n$ ya que si $\bar{x} \in V_{\mathbf{R}}$ entonces la parte imaginaria de cada entrada es cero, así $\bar{x} \in \mathbb{R}^n$, esto implica que $\bar{x} \in V \cap \mathbb{R}^n$. Y si $\bar{x} \in V \cap \mathbb{R}^n$ entonces la parte imaginara de cada entrada debe ser cero, esto implica que $\bar{x} \in V_{\mathbf{R}}$. Ahora bien, como V es construíble entonces existen polinomios $P_{i,j} \in \mathbb{C}[x_1, \ldots, x_n]$ $(i = 1, \ldots, s;\ \ j = 1, \ldots, r_i)$ tales que

$$V = \bigcup_{i=1}^{s} \bigcap_{j=1}^{r_i} \{x \in \mathbb{C}^n \mid P_{i,j}(x)\ \delta_{ij}\ 0\},$$

donde $\delta_{ij} \in \{=, \neq\}$. Se denota $V_i = \bigcap_{j=1}^{r_i} \{x \in \mathbb{C}^n \mid P_{i,j}(x)\ \delta_{ij}\ 0\}$, así $V = \bigcup_{i=1}^{s} V_i$ y por lo tanto $V_{\mathbf{R}} = \left(\bigcup_{i=1}^{s} V_i\right) \cap \mathbb{R}^n = \bigcup_{i=1}^{s} (V_i \cap \mathbb{R}^n)$.

Demostraremos que cada $V_i \cap \mathbb{R}^n$ es semi-algebraico. Elegimos un V_i arbitrario. Así, $V_i = \bigcap_{j=1}^{r_i}\{x \in \mathbb{C}^n \mid P_{i,j}(x)\ \delta_{ij}\ 0\}$. Reordenamos los polinomios de tal modo que

$$V_i = \{x \in \mathbb{C}^n \mid P_{i,1}(x), P_{i,2}(x), \ldots, P_{i,l}(x) = 0, P_{i,l+1}(x), \ldots, P_{i,r_1}(x) \neq 0\}.$$

Como cada $P_{i,j}$ es un polinomio con coeficientes en los complejos, de grado $m \geq 0$, en n variables, entonces

$$P_{i,j}(x) = a_0 + a_1 x + \ldots + a_m x^m,$$

donde $a_k \in \mathbb{C}$ para toda $0 \leq k \leq m$, y $x = (x_1, \ldots, x_n)$. Así, $a_k = b_k + ic_k$ y entonces podemos escribir al polinomio de la siguiente manera

$$P_{i,j}(x) = (b_0 + b_1 + \ldots + b_m x^m) + i(c_0 + c_1 x + \ldots + c_m x^m).$$

Es decir, cada polinomio se puede escribir en dos partes, la parte real y la parte imaginaria. Denotamos $R_{i,j_1}(x) = b_0 + b_1 x + \ldots + b_m x^m$ y $R_{i,j_2}(x) = c_0 + c_1 x + \ldots + c_m x^m$, y $R_{i,j_1}, R_{i,j_2} \in \mathbb{R}[x_1, \ldots, x_n]$. Definimos los siguientes conjuntos:

$$\begin{array}{ll} Q_1(x) = R_{i,1_1}(x), & Q_{l+1}(x) = R_{i,1_2}(x), \\ Q_2(x) = R_{i,2_1}(x), & Q_{l+2}(x) = R_{i,2_2}(x), \\ \vdots & \vdots \\ Q_l(x) = R_{i,l_1}(x), & Q_{2l}(x) = R_{i,l_2}(x), \end{array}$$

y

$$\begin{aligned} Q_{2l+1}(x) &= R_{i,(l+1)_1} \cdot R_{i,(l+1)_2}(x), \\ &\vdots \\ Q_{2l+(r_i-l)}(x) &= R_{i,r_{1_1}} \cdot R_{i,r_{i_2}}(x). \end{aligned}$$

Afirmación:

$$V_i \cap \mathbb{R}^n = \bigcup_{k=1}^{3(ri-l)} \bigcap_{j=1}^{2l+(r_i-l)} \{x \in \mathbb{R}^n \mid Q_{k,j}(x)\ \delta_{kj}\ 0\},$$

donde $Q_{k,j}(x) = Q_j(x)$, δ_{kj} ="=" si $1 \leq j \leq 2l$ y para toda k; $\delta_{kj} \in \{>, =, <\}$ si $2l + 1 \leq j \leq 2l + (r_i - l)$ (es decir, depende de la permutación que se trate). Además,

si $Q_{k,j}(a) = 0$ para alguna $a \in \mathbb{R}^n$ y $2l+1 \leq j \leq 2l+(r_i - l)$, entonces $R_{i,j_1}(a) = 0$ ó $R_{i,j_2}(a) = 0$, pero no ambos.

$\boxed{\subseteq}$ Sea $a \in V_i \cap \mathbb{R}^n$, esto es, $Im(a) = 0$, $P_{i,j}(a) = 0 \ \forall \ 1 \leq j \leq l$ y $P_{i,j}(a) \neq 0 \ \forall \ l+1 \leq j \leq r_i$. Para $1 \leq j \leq l$, tenemos que $R_{i,j_1}(a) = 0$ y $R_{i,j_2}(a) = 0$ ya que $P_{i,j}(a) = 0$, esto implica que $Q_{k,j}(a) = 0$ para cada $1 \leq j \leq 2l$ y para toda k. Para $l+1 \leq j \leq r_i$, tenemos que $R_{i,j_1}(a) \neq 0$ ó $R_{i,j_2} \neq 0$ o ambos son distintos de cero, entonces $Q_{k,j}(a) = 0$ ó $Q_{k,j} < 0$ ó $Q_{k,j} > 0$. Así, existe $k \in \{1, \ldots, 3r - l\}$ un ordenamiento tal que $a \in \bigcap_{j=1}^{r_i} \{x \in \mathbb{R}^n \mid Q_{k,j}(x) \ \delta_{kj} \ 0\}$.

$\boxed{\supseteq}$ Sea $a \in \bigcup_{k=1}^{3(ri-l)} \bigcap_{j=1}^{2l+(r_i-l)} \{x \in \mathbb{R}^n \mid Q_{k,j}(x) \ \delta_{kj} \ 0\}$, es decir,

$$a \in \bigcap_{j=1}^{2l+(r_i-l)} \{x \in \mathbb{R}^n \mid Q_{k,j}(x) \ \delta_{kj} \ 0\},$$

para alguna k. Esto es, $Q_{k,j}(x) = 0$ para toda $1 \leq j \leq 2l$. Así, $P_{i,j}(a) = 0$ para toda $1 \leq j \leq l$. Para los valores entre $2l+1$ y $l + r_i$, tales que $Q_{k,j}(a) = 0$, tenemos que $R_{i,j_1}(a) = 0$ ó $R_{i,j_2}(a) = 0$, pero no ambos, así $P_{i,j}(a) \neq 0$. Para los valores entre $2l+1$ y $l + r_i$ tales que $Q_{k,j}(a) < 0$ ó $Q_{k,j}(a) > 0$, entonces $R_{i,j_1}(a) \neq 0$ ó $R_{i,j_2}(a) \neq 0$. Así, $P_{i,j}(a) \neq 0$. Por lo tanto, $a \in V_i \cap \mathbb{R}^n$.

Así, cada $V_i \cap \mathbb{R}^n$ es semi-algebraico y por la proposición 3.1, V es semi-algebraico. ■

Observemos que cada conjunto semi-algebraico V en $\mathbb{R}^n$ tiene una representación tal que $\delta_{i,j} \in \{=, >\}$. Esto es así porque por ejemplo, $\{P \leq 0\} = \{-P \geq 0\}$ y $\{P \geq 0\} = \{P = 0\} \cup \{P > 0\}$.

Así como los conjuntos algebraicos no vacíos de $\mathbb{R}$ se pueden describir como la unión finita de puntos, también se pueden describir los conjuntos semi-algebraicos de $\mathbb{R}$.

Observación 3.2 *Los conjuntos semi-algebraicos no vacíos de $\mathbb{R}$ son los dados por una unión finita de puntos e intervalos (acotados y no acotados).*

Prueba. Sea $V \subset \mathbb{R}$ cualquier subconjunto semi-algebraico de $\mathbb{R}$, entonces

$$V = \bigcup_{i=1}^{s} \bigcap_{j=1}^{r_i} \{a \in \mathbb{R} \mid P_{i,j}(a) \ \delta_{ij} \ 0\},$$

donde $\delta_{ij} \in \{>, =\}$ y $P_{i,j} \in \mathbb{R}[x]$.

Afirmación: cada $\{a \in \mathbb{R} \mid P_{i,j}(a) \ \delta_{ij} \ 0\}$ es la unión finita de intervalos o puntos.

> Si δ_{ij} ="=", entonces el conjunto son las raíces del polinomio, así, es la unión de puntos, los cuales son un número finito ya que el polinomio puede tener a lo más el número de su grado de raíces reales.
>
> Si δ_{ij} =">", entonces, en el conjunto no se incluyen las raíces. Como el polinomio está en $\mathbb{R}[x]$ entonces es un polinomio irreducible de grado a lo más 2, o puede escribirse como producto de polinomios de grado 1 ó 2. Así, el conjunto es la unión de intervalos (acotados o no, dependiendo de los polinomios de grado 1 ó 2). Son un número finito debido al grado del polinomio.

Como cada conjunto de esta manera es unión finita de puntos o intervalos, entonces la intersección finita de conjuntos de este tipo también es unión finita de intervalos o puntos y así la unión finita de estas intersecciones. ■

Recordemos que si $f : A \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^m$ es una función, se define *la gráfica de* f como $Gr(f) := \{(x, f(x)) \in \mathbb{R}^n \times \mathbb{R}^m \mid x \in A\}$.

Definición 3.3 Sea $X \subseteq \mathbb{R}^n$ y $Y \subseteq \mathbb{R}^m$ conjuntos semi-algebraicos. Una función $f : X \longrightarrow Y$ es llamada *semi-algebraica* si la gráfica de f es un conjunto semi-algebraico en $\mathbb{R}^{n+m}$.

Proposición 3.2 *Sea $p : \mathbb{R}^n \times \mathbb{R}^m \longrightarrow \mathbb{R}^m$ la proyección natural. Sea V un conjunto semi-algebraico en $\mathbb{R}^{n+m}$, entonces $p(V)$ es semi-algebraico.*

Por ejemplo, $V = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 - 1 = 0\}$ es un conjunto semi-algebraico, en particular es algebraico. Su proyección sobre el eje X a lo largo del eje Y es $p(V) =$

$\{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$. Es semi-algebraico porque se representa de la siguiente manera

$$P(V) = \{x \in \mathbb{R} \mid x + 1 > 0\} \cap \{x \in \mathbb{R} \mid x - 1 < 0\}.$$

Observemos que este ejemplo muestra que la proyección de un conjunto algebraico no necesariamente es un conjunto algebraico.

Proposición 3.3 *Sea $f : A \longrightarrow B$ una función semi-algebraica. Si $S \subset A$ es semi-algebraico, entonces su imagen $f(S)$ es semi-algebraico. Si $T \subset B$ es semi-algebraico, entonces su imagen inversa $f^{-1}(T)$ es semi-algebraico.*

Prueba. Tenemos que $f(S) = \{f(x) \in B \mid x \in S\}$. Por otro lado, $S \times B$ es semi-algebraico, ya que S y B son semi-algebraicos (de hecho, los puntos en $S \times B$ pueden ser representados por los polinomios que describen a S pensados como polinomios en $n + m$ variables, donde sólo dependen de las primeras n variables; y también por los polinomios que representan a B pensados como polinomios de $n + m$ variables que sólo dependen de las últimas m variables). Así, $(S \times B) \cap Gr(f)$ es semi-algebraico. Tenemos que mediante la proyección $p : A \times B \longrightarrow B$, $p[(S \times B) \cap Gr(f)] = f(S)$. Por la proposición 3.2, $f(S)$ es semi-algebraico.
Ahora bien, tenemos que $f^{-1}(T) = \{x \in A \mid f(x) \in T\}$. Análogamente a la prueba anterior, $(A \times T) \cap Gr(f)$ es semi-algebraico. Mediante la proyección $p' : A \times B \longrightarrow A$, tenemos que $p'[(A \times T) \cap Gr(f)] = f^{-1}(T)$. Por lo tanto, $f^{-1}(T)$ es semi-algebraico. ■

3.2. Resultantes y subresultantes

En esta sección trabajaremos con polinomios en una variable. Las definiciones, resultados y observaciones que estableceremos serán utilizadas de manera importante en la última sección de este capítulo.

Definición 3.4 Sean $P = a_0 + a_1x + \ldots + a_px^p$ y $Q = b_0 + b_1x + \ldots + b_qx^q$ dos polinomios en $\mathbb{K}[x]$. El *resultante* $R(P, Q)$ es un elemento en $\mathbb{K}$ definido como el determinante de la siguiente matriz $M(P, Q)$ de $(p + q) \times (p + q)$ (llamada *"Matriz de Sylvester"*):

$$M(P,Q) = \begin{matrix} q \\ \\ \\ \\ p \\ \\ \\ \\ \end{matrix} \begin{pmatrix} a_0 & a_1 & \cdots & a_{q-1} & \cdots & a_{p-1} & a_p & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & & \cdots & & & a_p & & \vdots \\ \vdots & & \ddots & & & & & & \ddots & 0 \\ 0 & \cdots & 0 & a_0 & \cdots & & & \cdots & & a_p \\ b_0 & \cdots & & \cdots & b_q & 0 & \cdots & & \cdots & 0 \\ 0 & b_0 & & \cdots & & b_q & 0 & \cdots & & \vdots \\ \vdots & & \ddots & & & & \ddots & & & 0 \\ 0 & \cdots & & \cdots & & & b_0 & \cdots & \cdots & b_q \end{pmatrix}$$

Observación 3.3 *Sean $d, p, q \in \mathbb{N}$, sea j un entero tal que $0 \leq j \leq min(p, q)$, y sea $P_d(\mathbb{K})$ el conjunto de polinomios de grado menor o igual a d con coeficientes en el campo $\mathbb{K}$. Consideramos $\psi_j : P_{q-1-j}(\mathbb{K}) \times P_{p-1-j}(\mathbb{K}) \longrightarrow P_{p+q-1-j}(\mathbb{K})$ una función lineal definida por $\psi_j(U, V) = UP + VQ$. Entonces, si escribimos U y V como vectores, esto es, $U = (u_0, \ldots, u_{q-1-j})$ y $V = (v_0, \ldots, v_{p-1-j})$, tenemos que*

$$\begin{aligned} UP + VQ &= (a_0 + a_1x + \ldots + a_px^p)(u_0 + \ldots + u_{q-j-1}x^{q-j-1}) + \\ &\quad +(b_0 + b_1x + \ldots + b_qx^q)(v_0 + \ldots + v_{p-j-1}x^{p-j-1}) \\ &= (a_0u_0 + b_0v_0) + (a_0u_1 + a_1u_0 + b_0v_1 + b_1v_0)x + \ldots + \\ &\quad +(a_pu_{q-j-1} + b_qv_{p-j-1})x^{p+q-j-1}. \end{aligned}$$

Los coeficientes de este polinomio se escriben en forma matricial como

$$\begin{pmatrix} u_0 & u_1 & \ldots & u_{q-j-1} & v_0 & v_1 & \ldots & v_{p-j-1} \end{pmatrix} \cdot \overline{M}(P, Q),$$

donde $\overline{M}(P, Q)$ es una matriz de $(p + q - 2j)$ renglones[1] y $(p + q - j)$ columnas[2]. De hecho, $M(P, Q)$ es justamente la matriz de la función ψ_0.

Prueba. La función es lineal, ya que si elegimos $(U, V), (U', V') \in P_{q-1-j}(\mathbb{K}) \times P_{p-1-j}(\mathbb{K})$ y $c \in \mathbb{K}$, tenemos que

$$\begin{aligned} \psi_j(c(U, V) + (U', V')) &= \psi_j((cU + U', cV + V')) = (cU + U')P + (cV + V')Q \\ &= c(UP + VQ) + U'P + V'Q = c\psi_j(U, V) + \psi_j(U', V'). \end{aligned}$$

[1]El número de renglones es igual a $(gra(U) + 1) + (gra(V) + 1)$.

[2]El número de columnas es igual a $1 + max\{gra(PU), gra(QV)\}$.

Luego, para ver que $M(P,Q)$ es la matriz de la función ψ_0, observamos que una base de $P_{q-1}(\mathbb{K}) \times P_{p-1}(\mathbb{K})$ es

$$\begin{array}{cc} e_1 = (1,0), & e_{q+1} = (0,1), \\ e_2 = (x,0), & e_{q+2} = (0,x), \\ \vdots & \vdots \\ e_q = (x^{q-1},0), & e_{q+p} = (0,x^{p-1}), \end{array}$$

y así tenemos que

$$\begin{aligned} \psi_0(e_1) &= P = a_0 + a_1x + \ldots + a_px^p, \\ \psi_0(e_2) &= xP = a_0x + a_1x^2 + \ldots + a_px^{p+1}, \\ &\vdots \\ \psi_0(e_q) &= x^{q-1}P = a_0x^{q-1} + a_1x^q + \ldots + a_px^{p+q-1}, \\ \psi_0(e_{q+1}) &= Q = b_0 + b_1x + \ldots + b_qx^q, \\ \psi_0(e_{q+2}) &= xQ = b_0x + b_1x^2 + \ldots + b_qx^{q+1}, \\ &\vdots \\ \psi_0(e_{q+p}) &= x^{p-1}Q = b_0x^{p-1} + b_1x^p + \ldots + b_qx^{q+p-1}. \end{aligned}$$

Así, justo la matriz de esta transformación es $M(P,Q)$. ■

Observación 3.4 *Sean $P, Q \in \mathbb{K}[x]$ polinomios de grado p y q respectivamente. Entonces, P y Q tienen un factor común no constante si y sólo si existen polinomios $H, G \in \mathbb{K}[x]$ tales que $gra(H) < p$, $gra(G) < q$ y $PG = HQ$.*

Prueba. $\boxed{\Rightarrow}$ Supongamos que P y Q tienen un factor común no constante, es decir, existe $F \in \mathbb{K}[x]$ tal que

$$\begin{aligned} P &= F\widetilde{P} \quad \text{con} \quad gra(\widetilde{P}) < p, \\ Q &= F\widetilde{Q} \quad \text{con} \quad gra(\widetilde{Q}) < q. \end{aligned}$$

Así, tenemos que $\widetilde{P}Q = \widetilde{P}F\widetilde{Q} = P\widetilde{Q}$. De esta manera, tomamos $H = \widetilde{P}$ y $G = \widetilde{Q}$ y se cumple lo que queríamos demostrar.

$\boxed{\Leftarrow}$ Supongamos que existen $H, G \in \mathbb{K}[x]$ polinomios tales que $gra(H) < p$, $gra(G) < q$ y $PG = HQ$. Factorizamos P y G en irreducibles, es decir, $P = P_1^{r_1} \dots P_k^{r_k}$ y $G = G_1^{u_1} \dots G_s^{u_s}$. Así $PG = P_1^{r_1} \dots P_k^{r_k} G_1^{u_1} \dots G_s^{u_s} = HQ$. Como P_i es irreducible, entonces P_i divide a H o divide a Q. Si suponemos que ninguna P_i divide a Q, entonces, obtenemos que P divide a H y eso quiere decir que $gra(H) \geq gra(P) = p$, lo cual es una contradición. Esto implica que P_i divide a Q para alguna i, por lo tanto P y Q tienen un factor común. ■

Proposición 3.4 *P y Q polinomios en $\mathbb{K}[x]$ de grado p y q respectivamente, tienen un factor común no constante en $\mathbb{K}[x]$ si y sólo si $R(P, Q) = 0$.*

Prueba. Tenemos que P y Q tienen un factor común no trivial, por la observación anterior esto ocurre si y sólo si existen $H, G \in \mathbb{K}[x]$ tales que $gra(H) < p$, $gra(G) < q$ y $PG = HQ$. Podemos expresar $H(x) = c_0 + c_1x + \ldots + c_{p-1}x^{p-1}$ y $G(x) = d_0 + d_1x + \ldots + d_{q-1}x^{q-1}$. Luego, $PG = HQ$ si y sólo si

$$\begin{aligned}
& (a_0 + a_1x + \ldots + a_px^p)(d_0 + d_1x + \ldots + d_{q-1}x^{q-1}) = \\
= \;& (c_0 + c_1x + \ldots + c_{p-1}x^{p-1})(b_0 + b_1x + \ldots + b_qx^q) \\
\Rightarrow \;& a_0d_0 + (a_0d_1 + a_1d_0)x + (a_0d_2 + a_1d_1 + a_2d_1)x^2 + \ldots + a_pd_{q-1}x^{p+q-1} = \\
= \;& c_0b_0 + (c_0b_1 + c_1b_0)x + \ldots + c_{p-1}b_qx^{p+q-1}.
\end{aligned}$$

Asociando los términos semejantes tenemos

$$\begin{aligned}
a_0d_0 - c_0b_0 &= 0 \\
a_0d_1 + a_1d_0 - c_0b_1 - c_1b_0 &= 0 \\
&\vdots \\
a_pd_{q-2} + a_{p-1}d_{q-1} - c_{q-1}b_q - c_{p-1}b_{q-1} &= 0 \\
a_pd_{q-1} - c_{p-1}b_q &= 0.
\end{aligned}$$

Este sistema lineal de ecuaciones se puede ver en forma matricial de la siguiente manera

$$\begin{pmatrix} d_0 & d_1 & \dots & d_{q-1} & -c_0 & -c_1 & \dots & -c_{p-1} \end{pmatrix} \cdot M(P,Q) = 0.$$

Por resultados de álgebra lineal, sabemos que el sistema tiene una solución no trivial si y sólo si $det(M(P,Q)) = 0$. Así $R(P,Q) = 0$. Por lo tanto, P y Q tienen un factor común no trivial si y sólo si $R(P,Q) = 0$ ■

Dados P y Q polinomios en $\mathbb{K}[x]$ de grado p y q respectivamente, M la "matriz de Sylvester" de P y Q, podemos definir una submatriz. Es decir, para $0 \leq j \leq min(p,q)$, definimos M_j como la submatriz $(p+q-2j) \times (p+q-j)$ de M obtenida al eliminar de M

- las últimas j columnas,
- los renglones con índices desde $(q-j+1)$ hasta q,
- los últimos j renglones.

$$\overbrace{\phantom{\begin{matrix}a_0 & \cdots & & a_p & 0 & \cdots & 0\end{matrix}}}^{p+q-j}$$

$$\left.\begin{matrix}\\\\\\\end{matrix}\right\{ q-j$$

$$\left.\begin{matrix}\\\\\\\end{matrix}\right\{ p-j$$

$$\begin{bmatrix} a_0 & \cdots & & a_p & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & & \vdots \\ \vdots & & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & a_0 & \cdots & & a_p \\ b_0 & \cdots & & b_q & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & & \vdots \\ \vdots & & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & b_0 & \cdots & & b_q \end{bmatrix} = M_j$$

Además, sea $r_{j,i}$ $(0 \leq i \leq j)$ el determinante de la submatriz $(p+q-2j) \times (p+q-2j)$ de M_j, formada por

- las últimas $p+q-2j-1$ columnas de M_j (y serán las últimas de la nueva matriz),
- la columna con índice i de M_j,

- todos los renglones de M_j.

Definidos así esta submatriz y determinante, podemos establecer la definición de subresultante y una proposición que nos será de gran ayuda en la última sección.

Definición 3.5 Sean P y Q polinomios en $\mathbb{K}[x]$ de grado p y q respectivamente

a) $r_j(P,Q) = r_{j,j}$ es el *j-ésimo subresultante de P y Q* (en particular, $r_0(P,Q) = R(P,Q)$, el resultante).

b) El polinomio $D_j(x) = r_{j,0} + r_{j,1}x + \ldots + r_{j,j}x^j$ es el *j-ésimo subMCD* de P y Q.

Proposición 3.5 *Con la notación anterior, las siguientes afirmaciones son equivalentes (para* $0 \leq j \leq min(p,q)$*):*

a_j) *P y Q tienen al menos* $j+1$ *raíces comunes (contadas con multiplicidad) en la cerradura algebraica de* $\mathbb{K}$.

b_j) $gra(MCD(P,Q)) \geq j+1$.

c_j) $r_0(P,Q) = r_1(P,Q) = \ldots = r_j(P,Q) = 0$.

Prueba. $\boxed{a_j) \Rightarrow b_j)}$ Como $\mathbb{K} = \mathbb{R}$ ó $\mathbb{K} = \mathbb{C}$, entonces tenemos dos casos.
Caso 1: Supongamos que $\mathbb{K} = \mathbb{C}$. Como $\mathbb{C}$ es algebraicamente cerrado, entonces coincide con su cerradura algebraica. Como P y Q tienen al menos $j+1$ raíces comunes en $\mathbb{C}[x]$ (sean $c_1, c_2, \ldots, c_{j+1}$ las raíces comunes), entonces $P = (x-c_1)(x-c_2)\ldots(x-c_{j+1})\widetilde{P}$ y $Q = (x-c_1)(x-c_2)\ldots(x-c_{j+1})\widetilde{Q}$. De este modo, $(x-c_1)(x-c_2)\ldots(x-c_{j+1})$ divide al máximo común divisor de P y Q. Por lo tanto, $gra(MCD(P,Q)) \geq j+1$.
Caso 2: Supongamos que $\mathbb{K} = \mathbb{R}$, entonces, su cerradura algebraica es $\mathbb{C}$. Por otro lado, observamos que si $a \in \mathbb{C}$ es raíz de un polinomio entonces también lo es su conjugado y $(x-a)(x-\tilde{a}) \in \mathbb{R}[x]$ y es de grado 2. Como P y Q tienen al menos $j+1$ raíces comunes en $\mathbb{C}$ (digamos $c_1, c_2, \ldots, c_{j+1}$ las raíces comunes), entonces $P = (x-c_1)(x-c_2)\ldots(x-c_{j+1})\widetilde{P}$ y $Q = (x-c_1)(x-c_2)\ldots(x-c_{j+1})\widetilde{Q}$ (ordenándolas de

tal modo que si $c_i \in \mathbb{C}$ entonces $c_{i+1} = \tilde{c}_i$). De este modo, $(x-c_1)(x-c_2)\ldots(x-c_{j+1})$ divide al máximo común divisor de P y Q. Por lo tanto, $gra(MCD(P,Q)) \geq j+1$.

$\boxed{b_j) \Rightarrow a_j)}$ Como el grado del máximo común divisor es al menos $j+1$, entonces tiene al menos $j+1$ raíces en la cerradura algebraica de $\mathbb{K}$. Así, P y Q tienen al menos $j+1$ raíces comunes en la cerradura algebraica de $\mathbb{K}$.

$\boxed{b_j) \Rightarrow c_j)}$ La prueba se realizará por inducción sobre j. Para $j = 0$, tenemos por hipótesis que $gra(MCD) \geq 1$, esto implica que P y Q tienen un factor común no constante. Por la proposición 3.4, $R(P,Q) = 0$ y justamente $R(P,Q) = r_0(P,Q)$.

Hipótesis de inducción para $j-1$: Supongamos que si $gra(MCD(P,Q)) \geq j$, entonces $r_0(P,Q) = \ldots = r_{j-1}(P,Q) = 0$.

Ahora supongamos que $gra(MCD(P,Q)) = s \geq j+1$, como $j+1 > j$, por hipótesis de inducción, tenemos que $r_0(P,Q) = \ldots = r_{j-1}(P,Q) = 0$. Falta demostrar que $r_j(P,Q) = 0$. Digamos que $G = MCD(P,Q)$, entonces $P = GF$ y $Q = GH$, donde F y H son polinomios de grado $p-s \leq p-j-1$ y $q-s \leq q-j-1$, respectivamente. De esa manera, tenemos que $HP = QF$. Por otro lado, podemos expresar a F y H de la siguiente manera

$$\begin{aligned} F &= c_0 + c_1x + \ldots + c_{p-j-1}x^{p-j-1} \\ H &= d_0 + d_1x + \ldots + d_{q-j-1}x^{q-j-1}. \end{aligned}$$

Como $HP = QF$, tenemos que

$$\begin{aligned} & (d_0 + d_1x + \ldots + d_{q-j-1}x^{q-j-1})(a_0 + a_1x + \ldots + a_px^p) = \\ = \;& (b_0 + b_1x + \ldots + b_qx^q)(c_0 + c_1x + \ldots + c_{p-j-1}x^{p-j-1}) \\ \Rightarrow \;& d_0a_0 + (d_0a_1 + d_1a_0)x + \ldots + d_{q-j-1}a_px^{p+q-j-1} = \\ = \;& b_0c_0 + (b_0c_1 + b_1c_0)x + \ldots + b_qc_{p-j-1}x^{p+q-j-1}. \end{aligned}$$

Asociando términos semejantes e igualando al polinomio cero tenemos

$$d_0a_0 - b_0c_0 = 0$$

$$\begin{aligned} d_0a_1 + d_1a_0 - b_0c_1 - b_1c_0 &= 0 \\ &\vdots \\ d_{q-j-1}a_p - b_qc_{p-j-1} &= 0, \end{aligned}$$

entonces este último sistema lineal $(*)$ se escribe en forma matricial de la siguiente manera

$$\begin{pmatrix} d_0 & d_1 & \dots & d_{q-j-1} & -c_0 & -c_1 & \dots & -c_{p-j-1} \end{pmatrix} \cdot M_j = 0.$$

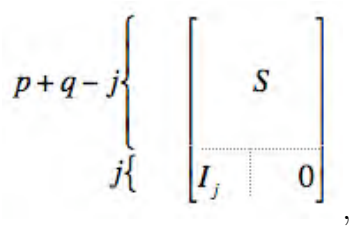
Tenemos que el rango de M_j es menor o igual que $p+q-2j$ porque es una matriz de $(p+q-2j) \times (p+q-j)$. De este modo, $(*)$ es equivalente a un sistema de $p+q-2j$ variables $(d_0, \dots, d_{q-j-1}, c_0, \dots, c_{p-j-1})$ y $p+q-2j$ ecuaciones. Como $(*)$ tiene solución no trivial, entonces el nuevo sistema también tiene solución no trivial. Esto implica que el rango de M_j es estrictamente menor que $p+q-2j$. Así, $r_j(P,Q) = 0$ ya que es una submatriz de $(p+q-2j) \times (p+q-2j)$ de M_j.

$\boxed{c_j) \Rightarrow b_j)}$ Esta prueba también se realizará por inducción sobre j. Si $j = 0$, tenemos que $0 = r_0(P,Q) = R(P,Q)$. Por la proposición 3.4, esto ocurre si y sólo si P y Q tienen un factor común no constante, esto implica que $gra(MCD(P,Q)) \geq 1$. Por lo tanto, se cumple lo que se quería probar.

Hipótesis de inducción: Supongamos que $r_0(P,Q) = r_1(P,Q) = \ldots = r_{j-1}(P,Q) = 0$ y $gra(MCD(P,Q)) \geq j$.

Supongamos que $r_0(P,Q) = r_1(P,Q) = \ldots = r_j(P,Q) = 0$, entonces, por hipótesis de inducción ocurre que $gra(MCD(P,Q)) \geq j$. Esto implica que P y Q tienen al menos j raíces comunes en la cerradura algebraica de $\mathbb{K}$.

Por otro lado, intercambiamos la columna j de la matriz M_j por la columna $p+q-2j$, y denotamos por $\widetilde{M_j}$ la submatriz de $(p+q-2j) \times (p+q-2j)$ obtenida de tomar las últimas $p+q-2j$ columnas, de hecho, esta matriz es la asociada a $r_j(P,Q)$, es decir, $det(\widetilde{M_j}) = r_j(P,Q)$. Construimos la siguiente matriz de $(p+q-j) \times (p+q-j)$, denotada por T:



,

donde la parte superior denotada por S es la submatriz de M_j con la columna j intercambiada, de tal forma que en las últimas columnas quede $\widetilde{M}_j$ e I_j es la matriz identidad de $j \times j$. Por hipótesis, $det(\widetilde{M}_j) = 0$, de esta manera $det(T) = det(I_j)det(\widetilde{M}_j) = 0$ (resultado de álgebra lineal). Esto significa que el sistema lineal correspondiente a la ecuación $UP + VQ - C = 0$, donde $U = u_0 + \ldots + u_{q-j-1}x^{q-j-1}$, $V = v_0 + \ldots + v_{p-j-1}x^{p-j-1}$ y $C = c_0 + \ldots + c_{j-1}x^{j-1}$ tiene una solución no trivial (en las variables $u_0, \ldots, u_{q-j-1}, v_0, \ldots, v_{p-j-1}, c_0, \ldots, c_{j-1}$), ya que su expresión en forma matricial es

$$\begin{pmatrix} u_0 & \ldots & u_{q-j-1} & v_0 & \ldots & v_{p-j-1} & -c_0 & \ldots & -c_{j-1} \end{pmatrix} \cdot T = 0.$$

Así, la ecuación $UP + VQ = C$ tiene una solución no trivial. Como P y Q tienen al menos j raíces comunes, entonces sus raíces deben ser raíces de C. Dado que $gra(C) = j - 1$, entonces $C \equiv 0$. Así,

$$UP = -VQ. \tag{3.1}$$

Por otro lado, sea $G = MCD(P, Q)$. Supongamos que $gra(G) = j \geq 1$, así $P = G\widetilde{P}$ y $Q = G\widetilde{Q}$, de tal forma que $\widetilde{P}$ y $\widetilde{Q}$ no tienen factor común no constante. Por la observación 3.4 para todos $H, F \in \mathbb{K}[x]$ tales que $gra(H) < p - j$ y $gra(F) < q - j$ ocurre $\widetilde{P}F \neq H\widetilde{Q}$.

De (3.1) tenemos

$$\begin{aligned} & UG\widetilde{P} = -VG\widetilde{Q} \\ \Rightarrow \quad & U\widetilde{P} = -V\widetilde{Q} \end{aligned}$$

Lo cual es una contradicción, ya que $gra(U) = q-j-1 < q-j$ y $gra(-V) = p-j-1 < p - j$. Por lo tanto, $gra(G) \geq j + 1$. ■

3.3. Continuidad de raíces

El último corolario de esta sección es el que nos interesa para poder demostrar el primer teorema principal de estructura. Como en cada sección, para demostrarlo necesitamos algunos conceptos y un par de resultados.

Definición 3.6 Sea X cualquier conjunto. Denotaremos por $X^{(n)}$ el conjunto cociente de $X^n/_\sim = X \times X \times \ldots \times X/_\sim$ donde la relación $\sim$ es la siguiente: $(x_1, \ldots, x_n) \sim (y_1, \ldots, y_n)$ si y sólo si existe una permutación $q : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ tal que $(x_1, \ldots, x_n) = (y_{q(1)}, \ldots, y_{q(n)})$. De este modo, $X^{(n)}$ es llamado el *enésimo producto simétrico de* X.

Observación 3.5 *"$\sim$" es una relación de equivalencia.*

Prueba. Es reflexiva ya que para $(x_1, \ldots, x_n)$ existe la permutación identidad, es decir, existe $q : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ definida por $q(n) = n$, tal que $(x_1, \ldots, x_n) = (x_{q(1)}, \ldots, x_{q(n)})$. Por lo tanto, $(x_1, \ldots, x_n) \sim (x_1, \ldots, x_n)$.
Es simétrica, ya que si $(x_1, \ldots, x_n) \sim (y_1, \ldots, y_n)$ entonces, existe una permutación $q : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$, tal que $(x_1, \ldots, x_n) = (y_{q(1)}, \ldots, y_{q(n)})$. Como q es biyectiva, entonces existe q^{-1}, la cual vuelve a ser una permutación y $(y_1, \ldots, y_n) = (x_{q^{-1}(1)}, \ldots, x_{q^{-1}(n)})$. Por lo tanto, $(y_1, \ldots, y_n) \sim (x_1, \ldots, x_n)$.
Y es transitiva, ya que si $(x_1, \ldots, x_n) \sim (y_1, \ldots, y_n)$ y $(y_1, \ldots, y_n) \sim (z_1, \ldots, z_n)$, entonces, existen p y q permutaciones tales que $(x_1, \ldots, x_n) = (y_{p(1)}, \ldots, y_{p(n)})$ y $(y_1, \ldots, y_n) = (z_{q(1)}, \ldots, z_{q(n)})$. Sea $r(n) = q(p(n))$, la cual es una permutación y tenemos que $(x_1, \ldots, x_n) = (y_{p(1)}, \ldots, y_{p(n)}) = (z_{q(p(1))}, \ldots, z_{q(p(n))})$. Por lo tanto, $(x_1, \ldots, x_n) \sim (z_1, \ldots, z_n)$. ■

De esta observación tenemos que, si X es un espacio topológico, entonces $X^{(n)}$ adopta la topología cociente inducida por la proyección cociente

$$\pi : X^n \longrightarrow X^{(n)} \text{ tal que } \pi(x_1, \ldots, x_n) = [x_1, \ldots, x_n].$$

Así, los conjuntos de la forma

$$[U_1, \ldots, U_n] = \{[x_1, \ldots, x_n] \in X^{(n)} \mid x_i \in U_i,\ U_i \text{ es un conjunto abierto de } x_i \text{ en } X\},$$

forman una base de la topología de $X^{(n)}$.

Ahora bien, podemos identificar $\mathbb{C}^n$ con el conjunto de todos los polinomios mónicos de grado n en $\mathbb{C}[x]$, es decir, si $a = (a_0, \ldots, a_{n-1}) \in \mathbb{C}^n$, entonces $(a_0, \ldots, a_{n-1}) \sim P_a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$.

Observación 3.6 *Sea $c = (c_1, \ldots, c_n) \in \mathbb{C}^n$, entonces*

$$\prod_{j=1}^{n}(x - c_j) = x^n + (-1)^1 s_1(c)x^{n-1} + \ldots + (-1)^{n-1}s_{n-1}(c)x + (-1)^n s_n(c),$$

donde

$$\begin{aligned}
s_1(c) &= c_1 + c_2 + \ldots + c_n \\
s_2(c) &= c_1c_2 + \ldots + c_1c_n + c_2c_3 + \ldots + c_2c_n + \ldots + c_{n-1}c_n \\
s_3(c) &= c_1c_2c_3 + \ldots + c_1c_2c_n + \ldots + c_1c_{n-1}c_n + \ldots + c_{n-2}c_{n-1}c_n \\
&\vdots \\
s_{n-1}(c) &= c_1c_2 \ldots c_{n-3}c_{n-2}c_{n-1} + \ldots + c_2c_3 \ldots c_{n-1}c_n \\
s_n(c) &= c_1c_2 \ldots c_n
\end{aligned}$$

Prueba. La prueba se realizará por inducción sobre n. Tenemos que para $n = 1$, $c = (c_1)$ y así $\prod_{j=1}^{n}(x - c_j) = x - c_1$. Por otro lado, $s_1(c) = c_1$. Por lo tanto, se cumple la igualdad.

Para n=2, tenemos que $c = (c_1, c_2)$ y

$$\prod_{j=1}^{n}(x - c_j) = (x - c_1)(x - c_2) = x^2 - (c_1 + c_2)x + c_1c_2.$$

Como $s_1(c) = c_1 + c_2$ y $s_2(c) = c_1c_2$, entonces se cumple la igualdad.

Hipótesis de inducción: La igualdad se cumple para $n \geq 2$.

Sea $c = (c_1, \ldots, c_n, c_{n+1})$ y tenemos que

$$\begin{aligned}
s_1(c) &= c_1 + c_2 + \ldots + c_{n+1},\\
s_2(c) &= c_1c_2 + \ldots + c_1c_{n+1} + c_2c_3 + \ldots + c_2c_{n+1} + \ldots + c_nc_{n+1},\\
s_3(c) &= c_1c_2c_3 + \ldots + c_1c_2c_{n+1} + \ldots + c_1c_nc_{n+1} + \ldots + c_{n-1}c_nc_{n+1},\\
&\vdots\\
s_n(c) &= c_1c_2\ldots c_{n-2}c_{n-1}c_n + \ldots + c_2c_3\ldots c_nc_{n+1},\\
s_{n+1}(c) &= c_1c_2\ldots c_{n+1}.
\end{aligned}$$

Por hipótesis de inducción observamos que

$$\begin{aligned}
\prod_{j=1}^{n}(x - c_j) &= x^n + (-1)(c_1 + \ldots + c_n)x^{n-1} + (-1)^2(c_1c_2 + \ldots + c_1c_n + \ldots + c_{n-1}c_n)x^{n-2}\\
&\quad + \ldots + (-1)^n(c_1c_2\ldots c_n).
\end{aligned}$$

Siendo así tenemos que

$$\begin{aligned}
\prod_{j=1}^{n+1}(x - c_j) &= \Big[\prod_{j=1}^{n}(x - c_j)\Big](x - c_{n+1})\\
&= \big[x^n + (-1)(c_1 + \ldots + c_n)x^{n-1} + (-1)^2(c_1c_2 + \ldots + c_1c_n + \ldots + c_{n-1}c_n)x^{n-2}\\
&\quad + \ldots + (-1)^n(c_1c_2\ldots c_n)\big](x - c_{n+1})\\
&= \big[x^n + (-1)(c_1 + \ldots + c_n)x^{n-1} + (-1)^2(c_1c_2 + \ldots + c_1c_n + \ldots + c_{n-1}c_n)x^{n-2}\\
&\quad + \ldots + (-1)^n(c_1c_2\ldots c_n)\big]x + \big[x^n + (-1)(c_1 + \ldots + c_n)x^{n-1} +\\
&\quad + (-1)^2(c_1c_2 + \ldots + c_1c_n + \ldots + c_{n-1}c_n)x^{n-2} + \ldots +\\
&\quad + (-1)^n(c_1c_2\ldots c_n)\big](-c_{n+1})\\
&= x^{n+1} + (-1)(c_1 + \ldots + c_n)x^n + (-1)^2(c_1c_2 + \ldots + c_1c_n + \ldots + c_{n-1}c_n)x^{n-1}\\
&\quad + \ldots + (-1)^n(c_1c_2\ldots c_n)x + (-1)c_{n+1}x^n + (-1)^2(c_1 + \ldots + c_n)c_{n+1}x^{n-1} +\\
&\quad + (-1)^3(c_1c_2 + \ldots + c_1c_n + \ldots + c_{n-1}c_n)c_{n+1}x^{n-2} + \ldots +\\
&\quad + (-1)^{n+1}(c_1c_2\ldots c_n)c_{n+1}
\end{aligned}$$

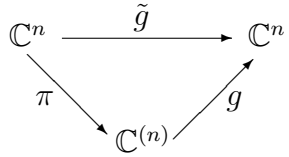
$$\begin{aligned} = \; & x^{n+1} + (-1)(c_1 + \ldots + c_n + c_{n+1})x^n + \\ & +(-1)^2(c_1c_2 + \ldots + c_1c_{n+1} + \ldots + c_nc_{n+1})x^{n-1} \\ & + \ldots + (-1)^{n+1}(c_1c_2 \ldots c_nc_{n+1}). \end{aligned}$$

Por lo tanto, la igualdad se cumple. ■

Además, también podemos observar que cada s_i es una función polinomial. Gracias a esta observación podemos definir una aplicación $\tilde{g} : \mathbb{C}^n \longrightarrow \mathbb{C}^n$, tal que $\tilde{g}(c) = (\tilde{g}_1(c), \ldots, \tilde{g}_n(c))$, donde $\tilde{g}_i(c) = (-1)^i s_i(c)$ con $1 \leq i \leq n$. Como cada $\tilde{g}_i$ está bien definida (ya que cada s_i está bien definida), entonces, $\tilde{g}$ está bien definida. Por la identificación que se hizo entre $\mathbb{C}^n$ y los polinomios mónicos de grado n en $\mathbb{C}[x]$, podemos ver a $\tilde{g}$ de la siguiente manera:

$$\tilde{g}(c_1, \ldots, c_n) = \prod_{j=1}^{n}(x - c_j) = x^n + \tilde{g}_1(c)x^{n-1} + \ldots + \tilde{g}_{n-1}(c)x + \tilde{g}_n(c).$$

Por otra parte, regresando a $\mathbb{C}^{(n)}$ (el enésimo producto simétrico de $\mathbb{C}$), tenemos que si $[x_1, \ldots, x_n] = [y_1, \ldots, y_n]$, entonces $\tilde{g}(x_1, \ldots, x_n) = \tilde{g}(y_1, \ldots, y_n)$. De esta manera, tenemos una función bien definida $g : \mathbb{C}^{(n)} \longrightarrow \mathbb{C}^n$, tal que $g([c]) = \tilde{g}(c)$. Esta g hace que el siguiente diagrama conmute:



Es decir, si $c = (c_1, \ldots, c_n) \in \mathbb{C}^n$ entonces $\tilde{g}(c) = (\tilde{g}_1(c), \ldots, \tilde{g}_n(c)) \in \mathbb{C}^n$. Por otra parte, $\pi(c) = [c]$ y $g([c]) = \tilde{g}(c)$, de este modo, tenemos que $\tilde{g} = g \circ \pi$.

Tenemos que $\tilde{g}$ es suprayectiva, ya que es una consecuencia inmediata del *teorema fundamental del álgebra*, y así, g también es suprayectiva. Además, g es inyectiva, porque

$$\prod_{j=1}^{n}(x - c_j) = \prod_{j=1}^{n}(x - c'_j),$$

implica inmediatamente que $[c_1, \ldots, c_n] = [c'_1, \ldots, c'_n]$, por lo tanto, g es biyectiva. Como $\tilde{g}_i$ son funciones polinomiales, entonces son continuas, y así, $\tilde{g}$ es continua, por lo tanto, g es continua. Sea $h : \mathbb{C}^n \longrightarrow \mathbb{C}^{(n)}$ la función inversa de g.

Proposición 3.6 *h es un homeomorfismo.*

Prueba. Como g es la inversa de h y es continua, sólo falta demostrar que h es continua. Observamos que si $n = 1$ entonces h es continua, pues en primer lugar, $\mathbb{C}$ coincide con el primer producto simétrico de $\mathbb{C}$ y entonces, h es la función identidad.
Asumimos que $n \geq 2$. Para cualquier entero $s > 0$, definimos

$$\begin{aligned} C_s &:= \{[x_1, \ldots, x_n] \in \mathbb{C}^{(n)} \mid |x_i| \leq sn \ \ (i = 1, \ldots, n)\}, \\ C'_s &:= \{(a_0, \ldots, a_{n-1}) \in \mathbb{C}^n \mid |a_j| \leq s \ \ (j = 0, \ldots, n-1)\}, \\ C''_s &:= g(C_s). \end{aligned}$$

Observemos que

1. Si $s' > s$, entonces $C'_{s'}$ es una vecindad de C'_s en $\mathbb{C}^n$. Esto es así, ya que

$$A = \{(a_0, \ldots, a_n) \in \mathbb{C}^n \mid |a_j| < \frac{s' + s}{2} \ (j = 0, \ldots, n-1)\},$$

   es abierto y $C'_s \subset A \subset C'_{s'}$.

2. C_s es un subconjunto compacto de $\mathbb{C}^{(n)}$. Para ver esto, primero consideramos el conjunto

$$(R_1, \ldots, R_n) = \{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid z_i \in R_i \text{ y } |z_i| \leq sn \ \forall \ 1 \leq i \leq n\},$$

   donde R_i es un abierto en $\mathbb{C}$. Este conjunto es cerrado y acotado, por lo tanto, compacto. Así, $\pi(R_1, \ldots, R_n)$ es compacto (ya que π es continua). Es claro que $C_s = \pi(R_1, \ldots, R_n)$.

3. Como g es continua, C''_s es también un conjunto compacto en $\mathbb{C}^n$ y además es de Hausdorff. Por el teorema 1.7 podemos concluir que $g_s = g|_{C_s}$ es un homeomorfismo de C_s en C''_s. Así $g_s^{-1} = h|_{C''_s} = h_s$ es continua.

Afirmación 1: Para cada $s > 0$, tenemos que $C'_s \subset C''_s$.

Supongamos que $C'_s \nsubseteq C''_s$, esto es, existe $a = (a_0, \ldots, a_{n-1}) \in C'_s$ tal que $a \notin C''_s$. Como $a \in C'_s$ entonces $|a_j| \leq s$, para toda $j = 0, \ldots, n-1$, y $a = g([x_1, \ldots, x_n])$ para alguna $[x_1, \ldots, x_n] \in \mathbb{C}^{(n)}$ (porque g es biyectiva). Por suposición, $g([x_1, \ldots, x_n]) \notin g(C_s)$, es decir, $[x_1, \ldots, x_n] \notin C_s$, esto implica que existe j tal que $|x_j| > sn$ (observemos que $sn \geq 2$, ya que estamos trabajando con $n \geq 2$ y s es un entero positivo). Sabemos que x_j es raíz de $P_a(x)$, es decir, $a_0 + \ldots + a_{n-1}x_j^{n-1} + x_j^n = 0$, esto implica que $-x_j^n = a_0 + \ldots + a_{n-1}x_j^{n-1}$ y $|-x_j^n| = |x_j^n|$. Además, como $|x_j| > 1$, entonces $|x_j|^p < |x_j|^q$ para cualesquiera $p, q \in \mathbb{N}$ tal que $p < q$. Así

$$\begin{aligned} |x_j^n| &= |a_0 + a_1x_j + \ldots + a_{n-1}x_j^{n-1}| \leq \\ &\leq |a_0| + |a_1||x_j| + \ldots + |a_{n-1}||x_j|^{n-1} \leq s + s|x_j| + \ldots + s|x_j|^{n-1} < \\ &< s|x_j|^{n-1} + \ldots s|x_j|^{n-1} = ns|x_j|^{n-1}, \end{aligned}$$

es decir, $|x_j|^n < ns|x_j|^{n-1}$, lo cual implica que $|x_j| < ns$, pero esto es una contradicción. Por lo tanto, $C'_s \subset C''_s$.

Sea $a \in \mathbb{C}^n$ arbitraria, elegimos $s > 0$ tal que $a \in C'_s$. Tenemos que $C'_s \subset C'_{2s}$ por el punto 1 y $C'_{2s} \subset C''_{2s}$ por la afirmación anterior. Así, h es continua en a porque es igual a h_{2s} en una vecindad de a en $\mathbb{C}^n$ (por el punto 3). Como a fue arbitrario, entonces h es continua en cualquier punto. Por lo tanto, h es un homeomorfismo. ■

Ahora, consideramos la función $\tilde{h} : \{a = (a_0, \ldots, a_n) \in \mathbb{C}^{n+1} \mid a_n \neq 0\} \longrightarrow \mathbb{C}^{(n)}$ definida por $\tilde{h}(a) = h(a_0/a_n, \ldots, a_{n-1}/a_n)$. Como h es continua, entonces $\tilde{h}$ es continua.

Necesitamos definir ciertos conjuntos para establecer una proposición y dos corolarios que nos ayudarán en la siguiente sección.

Definición 3.7 Para cada $(n, k) \in \mathbb{N} \times \mathbb{N}$ tal que $k \leq n$, definimos

$$B_k^n := \{a = (a_0, \ldots, a_n) \in \mathbb{C}^{n+1} \mid P_a(x) = a_0 + \ldots + a_n x^n \in \mathbb{C}[x]$$

$$\begin{aligned} & \text{tiene exactamente } k \text{ raíces complejas distintas}\}, \\ M_k^n &:= B_k^n \cap \{a \in \mathbb{C}^{n+1} \mid a_n \neq 0\}, \\ B_k^n(\mathbb{R}) &:= B_k^n \cap \mathbb{R}^{n+1}, \\ M_k^n(\mathbb{R}) &:= M_k^n \cap \mathbb{R}^{n+1}. \end{aligned}$$

Proposición 3.7 *Para cada $a \in M_k^n$, existe una vecindad U de a en M_k^n y funciones continuas $F_j : U \longrightarrow \mathbb{C}$ $(j = 1, \ldots, k)$ tales que, para cada $b \in U$,*

1. *$P_b(F_j(b)) = 0$ $(j = 1, \ldots, k)$,*
2. *$F_i(b) \neq F_j(b)$ si $i \neq j$.*

Prueba. Consideramos la función $\tilde{h}$ restringida a M_k^n. Así, $\tilde{h}(a) = [m_1x_1, \ldots, m_kx_k]$, donde $[x_1, \ldots, x_n]$ es el conjunto de raíces de $P_a(x)$ y cada m_i es la multiplicidad de la raíz x_i, es decir, $[m_1x_1, \ldots, m_kx_k] \in \mathbb{C}^{(n)}$ y x_i ocupa m_i entradas.
Sea $(\epsilon_1, \ldots, \epsilon_k) \in \mathbb{R}^k$, con $\epsilon_i > 0$ y tal que $B_i \cap B_j = \emptyset$ si $i \neq j$, donde $B_j := \{z \in \mathbb{C} \mid |z - x_j| < \epsilon_j\}$. Por la continuidad de $\tilde{h}$, existe una vecindad abierta de $a \in M_k^n$, tal que $\tilde{h}(U) \subset [m_1B_1, \ldots, m_kB_k]$. Esto implica que, para cada $b \in U$, cada B_j contiene exactamente una raíz de $P_b(x)$.
Entonces, definimos $F_j : U \longrightarrow B_j$ por $F_j(b) =$"la raíz de $P_b(x)$ contenida en B_j". Como $\tilde{h}$ es continua, entonces F_j es continua. ■

Corolario 3.1 *Sea A un subconjunto conexo de $M_k^n(\mathbb{R})$. Para cada $a \in A$, sea r_a "el número de raíces reales distintas de $P_a(x)$". Entonces*

1. *$r_a = r$ es constante en A;*
2. *Existen funciones continuas $f_j : A \longrightarrow \mathbb{R}$ $(j = 1, \ldots, r)$ tales que, para toda $a \in A$,*

   a) *$f_j(a) < f_{j+1}(a)$,*

b) $P_a(f_j(a)) = 0$.

Prueba. Sea $a \in A$ arbitraria, entonces existen U (vecindad de a) y $F_1, \ldots, F_k$ funciones continuas que cumplen lo que establece la proposición 3.7. Como a es real, entonces $P_a(x) \in \mathbb{R}[x]$ y así, para cada $j = 1, \ldots, k$ ocurre uno de los siguientes casos:

1. $F_j(a)$ es igual a su conjugado, es decir, $F_j(a) = \overline{F_j(a)}$ (esto es, $F_j(a)$ es una raíz real de $P_a(x)$) o

2. Existe $i \neq j$ tal que $F_j(a) = \overline{F_i(a)}$.

Afirmación 1: Existe una vecindad abierta $U' \subset U$ de a tal que si ocurre el caso 1 (o el 2) para a, entonces ocurre el caso 1 (o el 2) para cada $b \in U'$. En particular, r_a es localmente constante.

Supongamos que para alguna j ocurre el primer caso, es decir, $F_j(a) = \overline{F_j(a)}$. Y supongamos que para cada vecindad W de a, existe $b \in W$ e $i \neq j$ tal que $F_j(b) = \overline{F_i(b)}$. Así, existe una sucesión $\{b_s\}_{s\in\mathbb{N}}$ tal que $b_s \longrightarrow a$ y $F_j(b_s) = \overline{F_i(b_s)}$, pero

$$\overline{F_j(a)} = F_j(a) = \lim_{s\to\infty} F_j(b_s) = \lim_{s\to\infty} \overline{F_i(b_s)} = \overline{F_i(a)}$$

(por la continuidad de las F_j). De aquí que $F_j(a) = F_i(a)$, lo cual contradice la parte 2 de la proposición 3.7. Por lo tanto, existe tal vecindad U' de a.
Ahora, supongamos que para alguna j ocurre el segundo caso, es decir, existe $i \neq j$ tal que $F_j(a) = \overline{F_i(a)}$. Y supongamos que para cada vecindad W de a, existe $b \in W$ tal que $F_j(b) = \overline{F_j(b)}$. Así, existe una sucesión $\{b_s\}_{s\in\mathbb{N}}$ tal que $b_s \longrightarrow a$ y $F_j(b_s) = \overline{F_j(b_s)}$. Entonces

$$\overline{F_i(a)} = F_j(a) = \lim_{s\to\infty} F_j(b_s) = \lim_{s\to\infty} \overline{F_j(b_s)} = \overline{F_j(a)}$$

(por la continuidad de las F_j). De aquí que $F_j(a) = F_i(a)$, lo cual contradice la parte 2 de la proposición 3.7. Por lo tanto, existe tal vecindad U' de a.

De ambas partes se concluye que el número de raíces reales distintas de $P_a(x)$ es el mismo para $P_b(x)$ si $b \in U'$, es decir, r_a es localmente constante.

Como A es conexo y r_a es localmente constante, entonces $r_a = r$ es constante en A (si no fuera así, se podría dar una separación de A). Para probar el segundo enunciado del corolario, definimos

$$F = (F_1, \ldots, F_r) : A \longrightarrow \{(t_1, \ldots, t_r) \in \mathbb{R}^n \mid t_i < t_{i+1}\}$$

por la regla de correspondencia: para cada $a \in A$, $\{F_1(a), \ldots, F_r(a)\}$ es el conjunto de raíces reales distintas de $P_a(x)$. Sea $a \in A$ arbitraria, podemos asumir (reordenando las F_i) que $F(a) = (F_1(a), \ldots, F_r(a))$.

Afirmación 2: Podemos encontrar una vecindad $U'' \subset U'$ de a tal que, para cada $b \in U''$, $F_j(b) < F_{j+1}(b)$.

Supongamos que para cada vecindad W de a, existe $b \in W$ tal que $F_j(b) \geq F_{j+1}(b)$. Así, existe una sucesión $\{b_s\}_{s\in\mathbb{N}}$ tal que $b_s \longrightarrow a$ y $F_j(b_s) \geq F_{j+1}(b_s)$. Pero

$$F_j(a) = \lim_{s\to\infty} F_j(b_s) \geq \lim_{s\to\infty} F_{j+1}(b_s) = F_{j+1}(a),$$

lo cual es una contradicción, por lo tanto, existe tal vecindad $U'' \subset U$ de a.

Así, $F \equiv (F_1, \ldots, F_r)$ en U'' y de aquí que sea una función continua. ■

Los resultados anteriores los podemos resumir en un corolario, que será utilizado en el teorema más importante de este trabajo.

Corolario 3.2 *Sea T un espacio topológico conexo, $a_0(t), \ldots, a_n(t)$ funciones continuas: $T \longrightarrow \mathbb{C}$ (respectivamente $T \longrightarrow \mathbb{R}$) tales que:*

(i) $a_n(t) \neq 0$, *($t \in T$),*

(ii) el número de raíces complejas distintas de $P_t(x) = a_0(t) + a_1(t)x + \ldots + a_n(t)x^n$ *es constante para* $t \in T$.

Entonces

1. *Si $a_i(t) \in \mathbb{R}$, el número de raíces reales de $P_t(x)$ es también constante;*

2. *Existen funciones continuas $g_j : T \longrightarrow \mathbb{C}$ (respectivamente $T \longrightarrow \mathbb{R}$) $(1 \leq j \leq r)$ tales que*

   a) *$g_j(t)$ es una raíz de $P_t(x)$ $(1 \leq j \leq r)$,*

   b) *$g_j(t) \neq g_l(t)$ para toda $t \in T$ si $j \neq l$.*

Prueba. Las hipótesis (i) y (ii) implican que la función $\phi : T \longrightarrow \mathbb{C}^{n+1}$, definida por $\phi(t) = (a_0(t), \ldots, a_n(t))$ tiene su imagen contenida en M_k^n (respectivamente en $M_k^n(\mathbb{R})$); pero $Im(\phi)$ es conexa (ya que T es conexo y ϕ continua por que cada $a_i(t)$ es continua). Así podemos usar la proposición 3.7 y el corolario 3.1, componer ϕ con las funciones continuas f_j y obtenemos lo que queremos demostrar. ■

3.4. Primer teorema de estructura

Antes de abordar el primer teorema principal de estructura, necesitamos definir ciertos conjuntos.

Definición 3.8 Para cada $(n, k) \in \mathbb{N} \times \{\mathbb{N} \cup \{\infty\}\}$ definimos B_k^n como en la definición 3.7, para $(n, k) \in \mathbb{N} \times \mathbb{N}$ y $k \leq n$. $B_k^n := \emptyset$ si $(n, k) \in \mathbb{N} \times \mathbb{N}$ y $k > n$. $B_\infty^n := (0, \ldots, 0) \in \mathbb{C}^{n+1}$. Como en la definición 3.7,

$$\begin{aligned} M_k^n &:= B_k^n \cap \{a \in \mathbb{C}^{n+1} \mid a_n \neq 0\}, \\ B_k^n(\mathbb{R}) &:= B_k^n \cap \mathbb{R}^{n+1}, \\ M_k^n(\mathbb{R}) &:= M_k^n \cap \mathbb{R}^{n+1}. \end{aligned}$$

Proposición 3.8 *Sea $(n, k) \in \mathbb{N} \times \{\mathbb{N} \cup \{\infty\}\}$, entonces*

1. *B_k^n y M_k^n son subconjuntos construíbles de $\mathbb{C}^{n+1}$.*

2. $B_k^n(\mathbb{R})$ *y* $M_k^n(\mathbb{R})$ *son conjuntos semi-algebraicos en* $\mathbb{R}^{n+1}$.

Prueba. La demostración se hará por inducción sobre n. Si $n = 0$ entonces

$$\begin{aligned} B_0^0 &= \{a \in \mathbb{C} \mid P_a(x) = a \in \mathbb{C}[x] \text{ tiene exactamente cero raíces complejas} \\ &\quad \text{distintas}\} = \{a \in \mathbb{C} \mid a \neq 0\} = \mathbb{C} \setminus \{0\}. \end{aligned}$$

Es construíble porque si tomamos el polinomio $P(x) = x$, entonces B_0^0 se representa de la siguiente manera

$$B_0^0 = \{a \in \mathbb{C} \mid P(a) \neq 0\}.$$

Luego, tenemos que $B_k^0 = \emptyset$ para cada $0 < k \leq \infty$ (por definición). Es construíble porque si damos un polinomio constante distinto de cero Q, entonces B_k^0 es representado de la siguiente manera

$$B_k^0 = \{a \in \mathbb{C} \mid Q(a) = 0\}.$$

Por último, $B_\infty^0 = \{0\}$ (por definición), es construíble porque se representa como

$$B_\infty^0 = \{a \in \mathbb{C} \mid P(a) = 0\}.$$

Para toda n, B_0^n se identifica con $\mathbb{C} \setminus \{0\}$; de hecho

$$B_0^n = \{(a_0, 0, \ldots, 0) \in \mathbb{C}^{n+1} \mid a_0 \neq 0\}.$$

Si no fuera así, es decir, si algún a_i con $i > 0$ fuera distinto de cero, entonces como $\mathbb{C}$ es algebraicamente cerrado, $P_a(x)$ tendría al menos una raíz en $\mathbb{C}$, lo cual sería una contradicción.

Hipótesis de inducción: Supongamos que la proposición se cumple para $n-1$, es decir, que B_k^{n-1} es construíble.

Así, $B_k^{n-1} \times \{0\}$ también es construíble, ya que se representa de la siguiente manera

$$B_k^{n-1} \times \{0\} = \bigcup_{i=1}^{s} \bigcap_{j=1}^{r_i} \{x \in \mathbb{C}^{n+1} \mid P_{i,j}(x) \ \delta_{ij} \ 0\} \cap \{x \in \mathbb{C}^{n+1} \mid Q(x) = 0\},$$

donde los $P_{i,j}$ son los polinomios que representan a B_k^{n-1}, los cuales están definidos en $\mathbb{C}[x_1, \ldots, x_n]$ (es decir, no dependen de la variable x_{n+1}). El polinomio $Q \in \mathbb{C}[x_1, \ldots, x_{n+1}]$ está definido por $Q(x) = x_{n+1}$.
Afirmación: $B_k^n = (B_k^{n-1} \times \{0\}) \cup M_k^n$.

$\boxed{\subseteq}$ Sea $a = (a_0, \ldots, a_n) \in B_k^n$, esto es $P_a(x) \in \mathbb{C}[x]$ tiene exactamente k raíces complejas distintas. Tenemos dos casos, que $a_n = 0$ o $a_n \neq 0$.
Caso 1: Como $a_n = 0$ entonces $P_a(x) = a_0 + \ldots + a_{n-1}x^{n-1}$ y así, $(a_0, \ldots, a_{n-1}) \in B_k^{n-1}$. Por lo tanto $a \in B_k^{n-1} \times \{0\}$.
Caso 2: Como $a_n \neq 0$, entonces $a \in M_k^n$ por definición.
De ambos casos, concluimos que $B_k^n \subseteq (B_k^{n-1} \times \{0\}) \cup M_k^n$.
$\boxed{\supseteq}$ Sea $a = (a_0, \ldots, a_n) \in (B_k^{n-1} \times \{0\}) \cup M_k^n$. Tenemos dos casos, $a \in B_k^{n-1} \times \{0\}$ ó $a \in M_k^n$.
Caso 1: Si $a \in B_k^{n-1} \times \{0\}$, $a_n = 0$ y $P_a(x)$ tiene exactamente k raíces complejas distintas. Por definición, $a \in B_k^n$.
Caso 2: Si $a \in M_k^n$, entonces $a \in B_k^n$ por definición de M_k^n.
De ambos casos concluimos que $B_k^n \supseteq (B_k^{n-1} \times \{0\}) \cup M_k^n$. Por lo tanto, la afirmación se cumple.

Sólo resta probar que M_k^n es construíble. Usando la identificación de cualquier punto $a = (a_0, \ldots, a_n) \in \mathbb{C}^{n+1}$ con el polinomio $P_a(z) = a_0 + a_1 z + \ldots + a_n z^n$, definimos

$$W_k = \{a \in \mathbb{C}^{n+1} \mid a_n \neq 0 \text{ y } P_a(z) \text{ tiene a lo más } k \text{ raíces complejas distintas}\}.$$

Claramente $M_k^n = W_k \setminus W_{k-1}$. Por otro lado, como $P_a(z)$ tiene k raíces complejas distintas y éste es de grado n entonces tiene $n-k$ raíces que coinciden con algunas de las k anteriores. Por el teorema 1.4, estas raíces también son raíces de $P_a'(z)$, es decir, $P_a(z)$ y $P_a'(z)$ tienen al menos $n-k$ raíces comunes. Por la proposición 3.5 se sigue que

$$W_k = \{a \in \mathbb{C}^{n+1} \mid a_n \neq 0 \text{ y } gra(MCD(P_a(z), P_a'(z)) \geq n-k\},$$

y nuevamente, por la proposición 3.5, W_k es la intersección con $\{a_n \neq 0\}$ de los conjuntos algebraicos definidos por subresultantes apropiados de $P_a(z)$ y $P'_a(z)$. Por lo tanto, la primer parte de la proposición está probada.
La segunda parte es sencilla, ya que B_k^n y M_k^n son conjuntos construíbles, entonces, por la observación 3.1, $B_k^n(\mathbb{R})$ y $M_k^n(\mathbb{R})$ son semi-algebraicos. ■

También se utilizará el lema de Thom, por lo que a continuación se enunciará (la demostración de éste se puede encontrar en el libro *Real algebraic and semi-algebraic sets* [2]).

Proposición 3.9 (Lema de Thom) *Sea $\mathcal{F} = (P_1, \ldots, P_k)$ una familia finita de polinomios en $\mathbb{R}[x]$, y asumimos que cada derivada $P_j^{(i)} \in \mathcal{F}$. Sea X cualquier subconjunto de $\mathbb{R}$ de la forma $X = \cap\{t \in \mathbb{R} \mid P_i(t) \ *i \ 0\}$, donde $*i \in \{<, =, >\}$. Entonces X es conexo. Se obtiene una de las siguientes posibilidades*

1. *$X = \emptyset$,*
2. *$X = \{$un sólo punto$\}$ (esto pasa si y sólo si $X \neq \emptyset$ y al menos uno de los $*i =$ "$=$"),*
3. *X es un intervalo no trivial.*

Además, la cerradura $\overline{X}$ de X en $\mathbb{R}$ es obtenida al reemplazar "$>$" por "$\geq$" o "$<$" por "$\leq$" en los $*i$.

Definición 3.9 Una familia de conjuntos $\mathcal{F}$ no vacíos se llama *partición* de un conjunto A si:

(a) Los conjuntos que forman $\mathcal{F}$ son ajenos dos a dos, es decir, $C, D \in \mathcal{F}$ y $C \neq D$ implica $C \cap D = \emptyset$.

(b) La unión de $\mathcal{F}$ es A, es decir, $A = \bigcup \mathcal{F}$.

Teorema 3.1 (Primer Teorema de Estructura) *Sea X un conjunto semi-algebraico en $\mathbb{R}^n$. Expresemos $\mathbb{R}^n$ como $\mathbb{R}^{n-1} \times \mathbb{R}$ (con coordenadas $x = ((x_1, \ldots, x_{n-1}), t)$). Entonces*

a_n) *X tiene un número finito de componentes conexas y cada una es semi-algebraica.*

b_n) *Existe una partición finita $\mathcal{I}$ de $\mathbb{R}^{n-1}$ en conjuntos semi-algebraicos conexos tales que, para cada $A \in \mathcal{I}$, se define*

$$f_k^A : A \longrightarrow \overline{\mathbb{R}}, \ (\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}),$$

$k = 0, 1, \ldots, s_A, s_A + 1$ tales que

i) $f_0^A \equiv -\infty$, $f_{s_A+1}^A \equiv +\infty$;

ii) $f_k^A : A \longrightarrow \mathbb{R}$, $k = 1, \ldots, s_A$ *son funciones continuas y, para cada $x \in A$,* $f_k^A(x) < f_{k+1}^A(x)$;

iii) todos los conjuntos de forma $\mathcal{B}$ (tipo "banda")

$$\{(x,t) \in \mathbb{R}^n \mid x \in A, f_h^A(x) < t < f_{h+1}^A(x)\}, \quad h = 0, 1, \ldots, s_A,$$

o $\mathcal{G}$ (tipo "gráfica")

$$\{(x,t) \in \mathbb{R}^n \mid x \in A, t = f_h^A(x)\}, \quad h = 1, \ldots, s_A,$$

son semi-algebraicos;

iv) la colección de todos los conjuntos definidos en iii) forman una partición de $\mathbb{R}^n$; la subcolección de estos conjuntos que intersectan a X forman una partición de X.

Prueba. La prueba se realizará por inducción sobre n (el número de variables). Primero, si $n = 1$ entonces a_1) es claro, ya que si X es un conjunto semi-algebraico en $\mathbb{R}$, entonces X es la unión finita de intervalos (que pueden ser cerrados, abiertos o

semiabiertos). Sabemos que cada intervalo es conexo, por lo tanto X tiene un número finito de componentes conexas (que son semi-algebraicas).

Luego, observamos que $b_n)$ implica $a_n)$ ya que por cada conjunto definido en $b_n)$ por $iii)$ y $iv)$ se tiene $a_n)$. Así, hay que probar que $a_{n-1})$ implica $b_n)$.

Sea X un conjunto semi-algebraico en $\mathbb{R}^n$ y asumimos que $q_1, \ldots, q_N$ son todos los polinomios en una representación de X. Extendemos la familia $\{q_1, \ldots, q_N\}$ añadiendo todas las derivadas parciales respecto de t no cero

$$\frac{\delta^c q_r}{\delta t^c},\ r = 1, \ldots, N;\ c = 1, 2, \ldots$$

Sea $\{P_1, \ldots, P_R\}$ la familia resultante de polinomios. Para cada $T \subseteq \{1, \ldots, R\}$, definimos

$$\begin{aligned} Q_T &= \prod_{j \in T} P_j, \\ B_{T,k} &= \{x \in \mathbb{R}^{n-1} \mid Q_{T,x}(t) = Q_T(x,t) \text{ tiene exactamente } k \text{ raíces complejas distintas}\}. \end{aligned}$$

Además si fijamos un $Q_T(x,t)$ entonces la familia de los conjuntos $B_{T,k}$ forman una partición de $\mathbb{R}^{n-1}$. Sea $Q_T(x,t)$ de grado r, es claro que los conjuntos $B_{T,k}$ son ajenos dos a dos pues si no fuera así, es decir, si $x_0 \in B_{T,j} \cap B_{T,k}$ con $j \neq k$, entonces $Q_T(x_0,t)$ tiene exactamente j raíces complejas distintas y al mismo tiempo tiene k raíces complejas distintas, esto es una contradicción. Luego, como cada $B_{T,k} \subseteq \mathbb{R}^{n-1}$ entonces $B_{T,\infty} \cup \bigcup_{i=0}^{r} B_{T,i} \subseteq \mathbb{R}^{n-1}$. Falta ver la otra contención, para esto, supongamos que existe $x_0 \in \mathbb{R}^{n-1}$ tal que $x_0 \notin B_{T,\infty} \cup \bigcup_{i=0}^{r} B_{T,i}$. Esto implica que $Q_T(x_0,t)$ tiene más de r raíces complejas distintas pero esto es una contradicción porque dicho polinomio es de grado r. Por lo tanto, cada familia de conjuntos $B_{T,k}$ con $T \subseteq \{1, \ldots, R\}$ es una partición de $\mathbb{R}^{n-1}$.

Afirmación 1: Cada $B_{T,k}$ es semi-algebraico.

Definimos la aplicación polinomial

$$G : \mathbb{R}^{n-1} \longrightarrow \mathbb{R}^{m(T)+1},\ G(x) = (a_0(x), \ldots, a_{m(T)}(x)).$$

donde $Q_T(x,t) = a_0(x) + a_1(x)t + \ldots + a_{m(T)}(x)t^{m(T)}$. Está bien definida porque cada $a_i(x)$ es una función polinomial bien definida.

Podemos afirmar que $B_{T,k} = G^{-1}(B_k^{m(T)}(\mathbb{R}))$.

$\boxed{\subseteq}$ Sea $x \in B_{T,k}$, esto es, $x \in \mathbb{R}^{n-1}$ y $Q_T(x,t) = a_0(x) + \ldots + a_{m(T)}(x)t^{m(T)}$ tiene exactamente k raíces complejas distintas.

Así, $G(x) = (a_0(x), \ldots, a_{m(T)}(x)) \in B_k^{m(T)}$. Además, como $Q_T(x,t) \in \mathbb{R}[x,t]$ entonces $G(x) \in \mathbb{R}^{m(T)+1}$. Por lo tanto, $x \in G^{-1}(B_k^{m(T)}(\mathbb{R}))$.

$\boxed{\supseteq}$ Sea $x \in G^{-1}(B_k^{m(T)}(\mathbb{R}))$, esto es, $x \in \mathbb{R}^{n-1}$ y $G(x) \in B_k^{m(T)}(\mathbb{R})$, entonces, $G(x) = (a_0(x), \ldots, a_{m(T)}(x))$, donde $Q_T(x,t) = a_0(x) + \ldots + a_{m(T)}(x)t^{m(T)}$. Como $G(x) \in B_k^{m(T)}$, $Q_T(x,t)$ tiene exactamente k raíces complejas distintas, así $x \in B_{T,k}$. Por lo tanto, $B_{T,k} = G^{-1}(B_k^{m(T)}(\mathbb{R}))$. De ambas contenciones se tiene la igualdad.

La función G es semi-algebraica, ya que

$$Gr(G) = \{(\bar{x}, \bar{y}) \in \mathbb{R}^{n-1} \times \mathbb{R}^{m(T)+1} \mid \bar{y} = G(\bar{x})\},$$

se describe de la siguiente manera

$$\begin{aligned} Gr(G) \quad = \quad & \bigcap_{j=0}^{m(T)+1} \{(\bar{x}, y_0, \ldots, y_{m(T)+1}) \in \mathbb{R}^{n-1} \times \mathbb{R}^{m(T)+1} \mid a_j(\bar{x}) - y_j = 0, \\ & j = 0, \ldots, m(T)+1\}. \end{aligned}$$

Luego, por la proposición anterior $B_k^{m(T)}(\mathbb{R})$ es semi-algebraico y como G es semi-algebraica concluimos que $B_{T,k}$ es semi-algebraico.

Observación 1: Sea $M_{T,k}^i = G^{-1}(M_k^i(\mathbb{R}))$ (el cual es semi-algebraico ya que G es semi-algebraica y $M_k^i(\mathbb{R})$ es un conjunto semi-algebraico), entonces

$$B_{T,k} = M_{T,k}^0 \cup \ldots \cup M_{T,k}^{m(T)}.$$

$\boxed{\subseteq}$ Sea $x \in B_{T,k}$, esto es, $x \in \mathbb{R}^{n-1}$ y $Q_T(x,t) = a_0(x) + \ldots + a_{m(T)}(x)t^{m(T)}$ tiene exactamente k raíces complejas distintas. Vamos a demostrar que

$G(x) \in M_k^i = B_k^i \cap \{a \in \mathbb{C}^{i+1} \mid a_i \neq 0\} \cap \mathbb{R}^{i+1}$ para alguna i. Tenemos que $G(x) = (a_0(x), \ldots, a_{m(T)}(x))$.

Si el grado de $Q_T(x,t)$ es $m(T)$ entonces $a_{m(T)} \neq 0$, esto implica que $G(x) \in \{a \in \mathbb{C}^{m(T)+1} \mid a_{m(T)} \neq 0\} \cap \mathbb{R}^{m(T)+1}$ y por la afirmación anterior, $G(x) \in B_k^{m(T)}$. Por lo tanto, se tiene lo que se quería demostrar.

Si el grado de $Q_T(x,t)$ es i con $0 \leq i < m(T)$, esto implica que $a_i(x) \neq 0$ y $a_j(x) = 0$ para toda $j > i$. Así, $G(x) \in \{a \in \mathbb{C}^{i+1} \mid a_i \neq 0\}$. Además, como $G(x) = (a_0(x), \ldots, a_i(x), 0, \ldots, 0)$, entonces $G(x) \in \mathbb{R}^{i+1}$ y por la afirmación anterior $G(x) \in B_k^i$. Así, se tiene lo que se quería demostrar.

$\boxed{\supseteq}$ Sea $x \in M_{T,k}^0 \cup \ldots \cup M_{T,k}^{m(T)}$, esto es, $x \in M_{T,k}^i$ para alguna $i \in \{0, \ldots, m(T)\}$, esto implica que $G(x) \in B_k^i \cap \{a \in \mathbb{C}^{i+1} \mid a_i \neq 0\} \cap \mathbb{R}^{i+1}$. Como $G(x) \in \mathbb{R}^{i+1}$, entonces $a_j(x) = 0$ para toda $j > i$ y $a_k(x) \in \mathbb{R}$ para toda $0 \leq k \leq i$ y $a_i(x) \neq 0$. Entonces, $Q_T(x,t)$ es de grado i y como $G(x) \in B_k^i$, entonces $Q_T(x,t)$ tiene exactamente k raíces complejas distintas. Por lo tanto, $x \in B_{T,k}$ y se tiene lo que se quería probar.

Por lo tanto, $B_{T,k} = M_{T,k}^0 \cup \ldots \cup M_{T,k}^{m(T)}$.

Y los conjuntos $M_{T,k}^j$ son ajenos dos a dos, si no fuera así, es decir, si suponemos que existe $x_0 \in M_{T,k}^i \cap M_{T,k}^j$ con $i \neq j$, entonces $Q_T(x_0,t)$ tiene tanto grado i como grado j, lo cual es una contradicción. Por lo tanto, la familia formada por los conjuntos $M_{T,k}^j$ es una partición de $B_{T,k}$.

De esta manera, tenemos las siguientes particiones de $\mathbb{R}^{n-1}$:

1. Para cada $T \subseteq \{1, \ldots, R\}$, la partición

$$\mathcal{M}(T) = \{M_{T,k}^i\},\ k = 0, 1, \ldots, m(T), \infty,\ \ i = 0, 1, \ldots, m(T).$$

2. $\widetilde{\mathcal{I}}$ es la partición intersección de todas las $\mathcal{M}(T)$, con T variando en todos los subconjuntos de $\{1, \ldots, R\}$;

3. $\mathcal{I}$ es la partición obtenida de tomar todas las componentes conexas de todos los conjuntos en $\widetilde{\mathcal{I}}$.

Afirmación 2: $\mathcal{I}$ es finito y cada conjunto de $\mathcal{I}$ es semi-algebraico.

Por la afirmación 1, tenemos que cada componente de $\widetilde{\mathcal{I}}$ es semi-algebraica. Además, $\widetilde{\mathcal{I}}$ es finito porque cada $B_{T,k}$ tiene un número finito de $M^i_{T,k}$. Luego, por la hipótesis de inducción de a_{n-1}) cada componente de $\widetilde{\mathcal{I}}$ tiene un número finito de componentes conexas que son semi-algebraicas. Por lo tanto, $\mathcal{I}$ es finito y cada conjunto de $\mathcal{I}$ es semi-algebraico.

Ahora, para cada $A \in \mathcal{I}$ definimos

$$C_A := \{j \in \{1, \ldots, R\} \mid \text{existe } (x,t) \in A \times \mathbb{R} \text{ tal que } P_j(x,t) \neq 0\}.$$

Observamos que C_A puede ser vacío. Supongamos que, para una cierta A, $C_A \neq \emptyset$. De la definición de $\mathcal{I}$, se sigue que A está contenida en alguna $M^i_{C_A,k}$, es decir,

$$\begin{aligned} A \;\subseteq\; & M^i_{C_A,k} = \{x \in \mathbb{R}^{n-1} \mid G(x) \in M^i_k(\mathbb{R})\} = \{x \in \mathbb{R}^{n-1} \mid G(x) \in M^i_k \cap \mathbb{R}^{i+1}\} \\ = \; & \{x \in \mathbb{R}^{n-1} \mid Q_{C_A}(x,t) = a_0(x) + \ldots + a_i(x)t^i \text{ tiene exactamente } k \text{ raíces} \\ & \text{complejas distintas, } a_l(x) \in \mathbb{R} \;\forall\; l,\; a_i(x) \neq 0 \text{ y } a_j(x) = 0 \;\forall\; j > i\}. \end{aligned}$$

Como $a_i(x) \neq 0$, entonces $k \in \mathbb{R}$, es decir, k no es infinito. Así, para $j \in C_A$ y para cada $x \in A$, existe $t \in \mathbb{R}$ tal que $P_j(x,t) \neq 0$ (por definición de C_A). Y para cada $x \in A$,

$$Q_{C_A}(x,t) = \prod_{j \in C_A} P_j(x,t),$$

es de grado fijo i, esto es por definición de $M^i_{C_A,k}$ y la contención de A en éste.
Consideramos nuevamente la función G definida en la prueba de la afirmación 1. Así, denotamos $A' = G(A) \subseteq M^i_k(\mathbb{R})$, el cual es conexo porque A es conexo y G continua (ya que cada una de sus entradas son funciones polinomiales y por tanto continuas). Se cumplen las hipótesis del corolario 3.2, pues A' es conexo, $a_i(x) \neq 0$ y el número

de raíces complejas de $Q_{C_A}(x,t) = a_0(x) + a_1(x)t + \ldots + a_i(x)t^i$ es constante ya que $A' \subseteq M_k^i(\mathbb{R})$. Sean $f_1^{A'} < f_2^{A'} < \ldots < f_{s_{A'}}^{A'}$ las funciones continuas que van de A' a $\mathbb{R}$, tales que

(i) $f_j^{A'}(x)$ es raíz de $Q_{C_A}(x,t)$ con $1 \leq j \leq s_{A'}$.

(ii) $f_j^{A'}(x) \neq f_l^{A'}(x)$ si $j \neq l$.

Así, definimos $f_h^A : A \longrightarrow \mathbb{R}$ tal que

$$f_h^A(x) = f_h^{A'} \circ G(x), \ (h = 1, \ldots, s_A, \ s_A = s_{A'}).$$

Observación 2: Definidas así estas funciones, tenemos que

$$\{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } Q_{C_A}(x,t) = 0\} = \bigcup_{j=1}^{s_A} \{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } t = f_j^A(x)\}.$$

$\boxed{\subseteq}$ Sea $x' \in \{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } Q_{C_A}(x,t) = 0\}$, esto es, existe $t' \in \mathbb{R}$ tal que $Q_{C_A}(x',t') = 0$, es decir, t' es raíz del polinomio. Esto implica que $t' = f_j^A(x')$ para alguna $j \in \{1, \ldots, s_A\}$, es decir, $x' \in \bigcup_{j=1}^{s_A} \{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } t = f_j^A(x)\}$. Por lo tanto,

$$\begin{aligned} &\{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } Q_{C_A}(x,t) = 0\} \\ \subseteq &\bigcup_{j=1}^{s_A} \{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } t = f_j^A(x)\}. \end{aligned}$$

$\boxed{\supseteq}$ Sea $x' \in \bigcup_{j=1}^{s_A} \{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } t = f_j^A(x)\}$, esto es, existe $t' \in \mathbb{R}$ tal que $t' = f_j^A(x')$ para alguna j. Por definición de f_j^A tenemos que t' es raíz de $Q_{C_A}(x',t)$, es decir, $Q_{C_A}(x',t') = 0$. Esto implica que $x' \in \{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } Q_{C_A}(x,t) = 0\}$. Por lo tanto,

$$\begin{aligned} &\{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } Q_{C_A}(x,t) = 0\} \\ \supseteq &\bigcup_{j=1}^{s_A} \{x \in A \mid \exists\ t \in \mathbb{R} \text{ tal que } t = f_j^A(x)\}. \end{aligned}$$

De ambas contenciones se concluye la observación.

Afirmación 3: La partición $\mathcal{I}$ y las f_h^A así definidas satisfacen b_n).

Es claro que la unión de todos los conjuntos de la forma $\mathcal{B}$ y $\mathcal{G}$ hacen una partición de $\mathbb{R}^n$. Además, estos conjuntos son conexos ya que A es conexo y las f_h^A son continuas. Sea Γ un conjunto de cualquier forma.

Afirmación 3': Γ está contenido en un conjunto semi-algebraico de la forma

$$\begin{aligned}\Gamma' &= \bigcup_{j=1}^{R}\{(x,t)\in\mathbb{R}^n \mid x\in A, P_j\ \delta_j\ 0\}\\ &\quad \delta_j\in\{>,=,<\}.\end{aligned}$$

Elegimos cualquier P_j y supongamos que Γ es de la forma $\mathcal{B}$, es decir,

$$\Gamma=\{(x,t)\in\mathbb{R}^n \mid x\in A, f_h^A(x)<t<f_{h+1}^A(x)\},$$

para alguna $h\in\{0,1,\ldots,s_A\}$.

Afirmamos que $\{Q_{C_A}=0\}\cap\Gamma=\emptyset$. Supongamos que no, es decir, supongamos que existe $(x,t)\in\{Q_{C_A}=0\}\cap\Gamma$. Como $(x,t)\in\{Q_{C_A}=0\}$, entonces $Q_{C_A}(x,t)=0$, esto es, t es raíz de $Q_{C_A}(x,t)$. Esto implica que $t=f_i^A(x)$ para algún $i\in\{1,\ldots,s_A\}$. Si $i=h$ entonces $f_h^A(x)=t<f_{h+1}^A(x)$, lo cual es una contradicción. Si $i<h$ entonces $t<f_h^A(x)$, lo cual es una contradicción. Si $i>h$ entonces $f_{h+1}^A(x)\leq t$, lo cual es una contradicción.

De este modo, para el polinomio P_j que elegimos y de la definición de C_A, tenemos dos casos: $j\in C_A$ ó $j\notin C_A$.

Caso 1: Si $j\in C_A$, entonces $\{P_j=0\}\cap\Gamma=\emptyset$. Supongamos que no, es decir, existe $(x,t)\in\{P_j=0\}\cap\Gamma$. Como $x\in\{P_j=0\}$, entonces $P_j(x,t)=0$. Así, $Q_{C_A}(x,t)=0$ y entonces $(x,t)\in\{Q_{C_A}=0\}\cap\Gamma$, lo cual es una contradicción.

Caso 2: Si $j\notin C_A$ entonces $\{P_j=0\}\cap\Gamma=\Gamma$. Es evidente que $\{P_j=0\}\cap\Gamma\subseteq\Gamma$. Ahora, supongamos que existe $(x,t)\in\Gamma$ pero $(x,t)\notin\{P_j=0\}$,

esto es $P_j(x,t) \neq 0$. Tenemos que $x \in A$ porque $(x,t) \in \Gamma$, por definición de C_A, concluimos que $j \in C_A$, lo cual es una contradicción.

De esta manera, tenemos que $P_j(x,t) \neq 0$ para todo $(x,t) \in \Gamma$ si $j \in C_A$ y $P_j(x,t) = 0$ para todo $(x,t) \in \Gamma$ si $j \notin C_A$. Así, $P_j(x,t) < 0$ en Γ o $P_j(x,t) > 0$ en Γ (si no, si existieran $(x_0,t_0) \neq (x_1,t_1)$ en Γ tales que $P_j(x_0,t_0) > 0$ y $P_j(x_1,t_1) < 0$, entonces debería existir un (x_2,t_2) tal que $P_j(x_2,t_2) = 0$ porque Γ es conexo y P_j continua, lo cual sería una contradicción). Por lo tanto, $\Gamma \subseteq \Gamma'$.

Ahora supongamos que Γ es de la forma $\mathcal{G}$, esto es,

$$\Gamma = \{(x,t) \in \mathbb{R}^n \mid x \in A, t = f_h^A(x) \text{ para alguna } h\}.$$

Si $P_j(x,t) = 0$ para todo $(x,t) \in A \times \mathbb{R}$ entonces ya habríamos terminado. Supongamos entonces que existe $(x_0,t_0) \in A \times \mathbb{R}$ tal que $P_j(x_0,t_0) \neq 0$. Esto implica, por definición de C_A que $j \in C_A$.

Por otro lado, de la definición de $\mathcal{I}$ tenemos que A es conexo y está contenido en algún $M^i_{\{j\},k}$, donde

$$\begin{aligned} M^i_{\{j\},k} &= \{x \in \mathbb{R}^{n-1} \mid Q_{\{j\}}(x,t) = P_j(x,t) \text{ es de grado } i \\ &\qquad \text{y tiene } k \text{ raíces complejas distintas}\} \end{aligned}$$

Así, podemos aplicar el corolario 3.2 nuevamente para obtener funciones continuas $g_1, \ldots, g_v : A \longrightarrow \mathbb{R}$ tales que

(i) $g_i(x)$ es raíz de $P_j(x,t)$ con $1 \leq i \leq v$.

(ii) $g_j(x) \neq g_l(x)$ si $j \neq l$.

Afirmamos que

$$\{(x,t) \in \mathbb{R}^n \mid x \in A, P_j(x,t) = 0\} = \bigcup_{i=1}^{v} \{(x,t) \in \mathbb{R}^n \mid x \in A, t = g_i(x)\}$$

(la prueba es muy similar a la hecha para la observación 2). Además, para cada i,

$$\{x \in A \mid \exists\, t \in \mathbb{R} \text{ tal que } g_i(x) = t\} \subseteq \{x \in A \mid \exists\, t \in \mathbb{R} \text{ tal que } Q_{C_A}(x,t) = 0\}$$

ya que si $x' \in \{x \in A \mid \exists\, t \in \mathbb{R} \text{ tal que } g_i(x) = t\}$ entonces existe $t' \in \mathbb{R}$ tal que $g_i(x') = t'$, es decir, t' es raíz de $P_j(x', t)$ y como $j \in C_A$, entonces $Q_{C_A}(x', t') = 0$. Por lo tanto, la contención se cumple.

Cada conjunto $\{x \in A \mid \exists\, t \in \mathbb{R} \text{ tal que } g_i(x) = t\}$ es conexo, de hecho, $\{x \in A \mid \exists\, t \in \mathbb{R} \text{ tal que } g_i(x) = t\} = A$ ya que A es el dominio de g_i y sabemos que A es conexo.

Concluimos de esta contención y de la observación 2 que para cada i existe j tal que si $t = g_i(x)$ entonces $t = f_j^A(x)$.

Así, $P_j \equiv 0$ en Γ si existe i tal que $t = g_i(x) = f_h^A(x)$. En otro caso, $P_j(x,t) \neq 0$ para cada $(x,t) \in \Gamma$. Por lo tanto, $\Gamma \subseteq \Gamma'$.

Afirmación 3": $\Gamma = \Gamma'$. Esto prueba *iii)* del teorema.

Por la afirmación 3' tenemos que $\Gamma \subseteq \Gamma'$. Supongamos que existe $(x_0, t_0) \in \Gamma' \setminus \Gamma$. Sea $t_1 \in \mathbb{R}$ tal que $(x_0, t_1) \in \Gamma$, sin perdida de generalidad podemos suponer que $t_0 < t_1$.

La familia de polinomios $\{P_{j,x_0}(t) \in \mathbb{R}[t]\}_{j=1,\ldots,R}$ satisface la hipótesis del lema de Thom porque además de los polinomios iniciales $q_1, \ldots, q_N$ también tenemos todas las derivadas parciales $\delta^c q_r / \delta t^c$. De esta forma,

$$(\{x_0\} \times \mathbb{R}) \cap \Gamma' = \bigcap_{j=1}^{R} \{(x,t) \in \mathbb{R}^n \mid x \in A, P_{j,x_0}\ \delta_j\ 0\}$$

es conexo. Como $(x_0, t_1) \in \Gamma'$ (ya que $(x_0, t_1) \in \Gamma \subseteq \Gamma'$) y $(x_0, t_0) \in \Gamma'$, entonces $\{x_0\} \times [t_0, t_1] \subseteq (\{x_0\} \times \mathbb{R}) \cap \Gamma'$, en particular $\{x_0\} \times [t_0, t_1] \subseteq \Gamma'$.

Observación 3: Tenemos que $\{Q_{C_A} = 0\} \cap \Gamma' = \Gamma'$ si existe $j \in C_A$ tal que $\delta_j =$"=". Es claro que $\{Q_{C_A} = 0\} \cap \Gamma' \subseteq \Gamma'$, luego, si $(x,t) \in \Gamma'$, como

existe $j \in C_A$ tal que $P_j(x,t) = 0$, tenemos que $Q_{C_A}(x,t) = 0$, es decir, $(x,t) \in \{Q_{C_A} = 0\}$. Esto implica que $\{Q_{C_A} = 0\} \cap \Gamma' \supseteq \Gamma'$. Por lo tanto, $\{Q_{C_A} = 0\} \cap \Gamma' = \Gamma'$.

Si no existe tal j, es decir, si para toda $j \in C_A$, $\delta_j \in \{<, >\}$ entonces $\{Q_{C_A} = 0\} \cap \Gamma' = \emptyset$.

Así, si suponemos que Γ es de tipo $\mathcal{B}$, es decir,

$$\Gamma = \{(x,t) \in \mathbb{R}^n \mid x \in A, f_h^A(x) < t < f_{h+1}^A(x)\},$$

para alguna $h \in \{0, 1, \ldots, s_A\}$, entonces $Q_{C_A}(x_0, t_1) \neq 0$. Por otro lado, como $(x_0, t_0) \notin \Gamma$ entonces existe $t_2 \in [t_0, t_1)$ tal que $Q_{C_A}(x_0, t_2) = 0$ y $(x_0, t_2) \in \Gamma'$. Esto implica que existe $j \in C_A$ tal que $\delta_j =$"=", por la observación 3, entonces $\{Q_{C_A} = 0\} \cap \Gamma' = \Gamma'$. Como $(x_0, t_1) \in \Gamma'$, entonces $Q_{C_A}(x_0, t_1) = 0$, lo cual es una contradicción.

Ahora, supongamos que Γ es de tipo $\mathcal{G}$, es decir,

$$\Gamma = \{(x,t) \in \mathbb{R}^n \mid x \in A, t = f_h^A(x) \text{ para alguna } h\}.$$

Así tenemos que $Q_{C_A}(x_0, t_1) = 0$ y existe $t_2 \in [t_0, t_1)$ tal que $Q_{C_A}(x_0, t_2) \neq 0$ ya que $Q_{C_A}(x_0, t)$ es de grado fijo i, es decir, no es el polinomio cero. Por otro lado, como $Q_{C_A}(x_0, t_1) = 0$, entonces existe $j \in C_A$ tal que $\delta_j =$"=", y, por la observación 2 $\{Q_{C_A} = 0\} \cap \Gamma' = \Gamma'$. Como $(x_0, t_2) \in \Gamma'$ entonces $Q_{C_A}(x_0, t_2) = 0$, lo cual es una contradicción. Por lo tanto $\Gamma = \Gamma'$

De este modo, todos los conjuntos de tipo banda o de tipo gráfica son semi-algebraicos y la colección de estos hacen una partición de $\mathbb{R}^n$. Así como la subcolección de los conjuntos que están contenidos en X hacen una partición de X. ■

Un **ejemplo** en $\mathbb{R}^2$ es el siguiente

$$\begin{aligned} V &= \{(x,y) \in \mathbb{R}^2 \mid P_1(x,y) = x - (y-2)^2 < 0, P_2(x,y) = x - y > 0\} \cup \\ &\quad \cup \{(x,y) \in \mathbb{R}^2 \mid P_1(x,y) = x - (y-2)^2 > 0, P_2(x,y) = x - y < 0\}, \end{aligned}$$

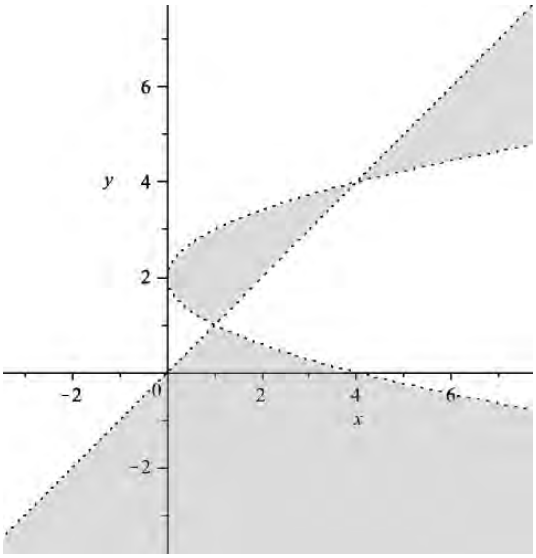


Figura 3.1: Representación geométrica de V

Su representación geométrica está en la figura 3.1.

De esta manera, $P_3(x, y) = -2y + 4$ es la derivada parcial de P_1 respecto de y, $P_4(x, y) = -2$ es la derivada parcial de P_3 respecto de y, por último, $P_5(x, y) = -1$ es la derivada parcial de P_2 respecto de y. Así, $T \subseteq \{1, 2, 3, 4, 5\}$ y por ejemplo si $T_1 = \{1, 2, 3, 4, 5\}$ entonces

$$\begin{aligned} Q_{T_1}(x, y) &= (x - y^2 + 4y - 4)(x - y)(-2y + 4)(-2)(-1) \\ &= -4[y^4 - (x + 6)y^3 + (5x + 12)y^2 + (x^2 - 10x - 8)y + (-2x^2 + 8x)] \\ &= -4(y - 2)(y - x)(y^2 - 4y - x + 4). \end{aligned}$$

Luego, $B_{T_1,\infty} = B_{T_1,0} = B_{T_1,1} = \emptyset$, $B_{T_1,2} = \{0\}$, $B_{T_1,3} = \{1, 4\}$ y $B_{T_1,4} = \mathbb{R} \setminus \{0, 1, 4\}$. Por lo que $\mathcal{M}(T_1) = \{0, 1, 4, \mathbb{R} \setminus \{0, 1, 4\}\}$. Determinando $\mathcal{M}(T)$ para todas las T,

obtenemos que la partición $\mathcal{I}$ está formada por los siguientes conjuntos

$$\begin{aligned}
&A_1 = \{x \in \mathbb{R} \mid x < 0\}, && A_2 = \{x \in \mathbb{R} \mid x = 0\},\\
&A_3 = \{x \in \mathbb{R} \mid 0 < x < 1\}, && A_4 = \{x \in \mathbb{R} \mid x = 1\},\\
&A_5 = \{x \in \mathbb{R} \mid 1 < x < 2\}, && A_6 = \{x \in \mathbb{R} \mid x = 2\},\\
&A_7 = \{x \in \mathbb{R} \mid 2 < x < 4\}, && A_8 = \{x \in \mathbb{R} \mid x = 4\},\\
&A_9 = \{x \in \mathbb{R} \mid x > 4\}.
\end{aligned}$$

Para cualquier A_i tenemos que $C_{A_i} = \{1, 2, 3, 4, 5\}$, lo que implica que $Q_{C_{A_i}}(x, t) = Q_{T_1}(x, y)$.

Para A_1 los conjuntos tipo $\mathcal{B}$ y tipo $\mathcal{G}$ son:

$$\begin{aligned}
&\{x < 0, -\infty < y < x\}, && \{x < 0, x < y < 2\},\\
&\{x < 0, 2 < y < \infty\},\\
&\{x < 0, y = x\}, && \{x < 0, y = 2\}.
\end{aligned}$$

Para A_2:

$$\begin{aligned}
&\{x = 0, -\infty < y < 0\}, && \{x = 0, 0 < y < 2\},\\
&\{x = 0, 2 < y < \infty\},\\
&\{x = 0, y = 0\}, && \{x = 0, y = 2\}.
\end{aligned}$$

Para A_3:

$$\begin{aligned}
&\{0 < x < 1, -\infty < y < x\}, && \{0 < x < 1, x < y < 2 - \sqrt{x}\},\\
&\{0 < x < 1, 2 - \sqrt{x} < y < 2\}, && \{0 < x < 1, 2 < y < 2 + \sqrt{x}\},\\
&\{0 < x < 1, 2 + \sqrt{x} < y < \infty\},\\
&\{0 < x < 1, y = x\}, && \{0 < x < 1, y = 2 - \sqrt{x}\},\\
&\{0 < x < 1, y = 2\}, && \{0 < x < 1, y = 2 + \sqrt{x}\}.
\end{aligned}$$

Para A_4:

$$\begin{aligned}
&\{x = 1, -\infty < y < 1\}, && \{x = 1, 1 < y < 2 - \sqrt{x}\},\\
&\{x = 1, 2 < y < 3\}, && \{x = 1, 3 < y < \infty\},\\
&\{x = 1, y = 1\}, && \{x = 1, y = 2\},\\
&\{x = 1, y = 3\}.
\end{aligned}$$

Para A_5:

$$\{1 < x < 2, -\infty < y < 2 - \sqrt{x}\}, \quad \{1 < x < 2, 2 - \sqrt{x} < y < x\},$$
$$\{1 < x < 2, x < y < 2\}, \quad \{1 < x < 2, 2 < y < 2 + \sqrt{x}\},$$
$$\{1 < x < 2, 2 + \sqrt{x} < y < \infty\},$$
$$\{1 < x < 2, y = 2 - \sqrt{x}\}, \quad \{1 < x < 2, y = x\},$$
$$\{1 < x < 2, y = 2\}, \quad \{1 < x < 2, y = 2 + \sqrt{x}\}.$$

Para A_6:

$$\{x = 2, -\infty < y < 2 - \sqrt{2}\}, \quad \{x = 2, 2 - \sqrt{2} < y < 2\},$$
$$\{x = 2, 2 < y < 2 + \sqrt{2}\}, \quad \{x = 2, 2 + \sqrt{2} < y < \infty\},$$
$$\{x = 2, y = 2 - \sqrt{2}\}, \quad \{x = 2, y = 2\},$$
$$\{x = 2, y = 2 + \sqrt{2}\}.$$

Para A_7:

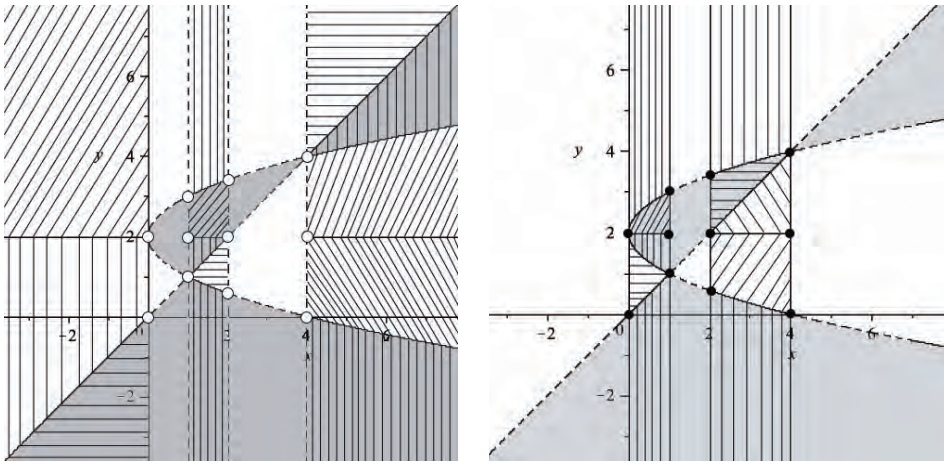
$$\{2 < x < 4, -\infty < y < 2 - \sqrt{x}\}, \quad \{2 < x < 4, 2 - \sqrt{x} < y < 2\},$$
$$\{2 < x < 4, 2 < y < x\}, \quad \{2 < x < 4, x < y < 2 + \sqrt{x}\},$$
$$\{2 < x < 4, 2 + \sqrt{x} < y < \infty\},$$
$$\{2 < x < 4, y = 2 - \sqrt{x}\}, \quad \{2 < x < 4, y = 2\},$$
$$\{2 < x < 4, y = x\}, \quad \{2 < x < 4, y = 2 + \sqrt{x}\}.$$

Para A_8:

$$\{x = 4, -\infty < y < 0\}, \quad \{x = 4, 0 < y < 2\},$$
$$\{x = 4, 2 < y < 4\}, \quad \{x = 4, 4 < y < \infty\},$$
$$\{x = 4, y = 0\}, \quad \{x = 4, y = 2\},$$
$$\{x = 4, y = 4\}.$$

Para A_9:

$$\{4 < x, -\infty < y < 2 - \sqrt{x}\}, \quad \{4 < x, 2 - \sqrt{x} < y < 2\},$$
$$\{4 < x, 2 < y < 2 + \sqrt{x}\}, \quad \{4 < x, 2 + \sqrt{x} < y < x\},$$
$$\{4 < x, x < y < \infty\},$$
$$\{4 < x, y = 2 - \sqrt{x}\}, \quad \{4 < x, y = 2\},$$
$$\{4 < x, y = 2 + \sqrt{x}\}, \quad \{4 < x, y = x\}.$$



a) Para A_1, A_5 y A_9 b) Para A_2, A_3, A_4, A_6, A_7 y A_8.

Figura 3.2: Representación geométrica de los conjuntos tipo $\mathcal{B}$ y tipo $\mathcal{G}$

Las componentes conexas de V son 21 en total, y son los conjuntos tipo $\mathcal{B}$ y tipo $\mathcal{G}$ que están contenidos en V. En la figura 3.2 se puede apreciar la representación geométrica de estos conjuntos.

El primer teorema de estructura no sólo asegura un número finito de componentes conexas si no que su demostración nos da un proceso para hallarlas, sin embargo, este número no es mínimo. Como se puede apreciar en el ejemplo anterior, podemos hallar un número menor de componentes conexas.

Conclusiones

Con lo realizado en este trabajo concluimos en primer lugar que cualquier ideal en un anillo de polinomios es generado por un número finito de polinomios, es decir, cualquier ideal tiene una base finita que lo genera. Este resultado es precisamente el Teorema de la Base de Hilbert tratado en el capítulo 2, además lo más importante es que su demostración nos muestra la manera de construir tal base generadora.

Dentro de este mismo capítulo establecimos la relación entre conjuntos algebraicos e ideales, es decir, dado un conjunto algebraico podemos construir un ideal que depende de dicho conjunto y también, dado un ideal podemos construir un conjunto algebraico que depende de dicho ideal.

Finalmente, la conclusión más importante de este capítulo es que se pueden describir los ideales cuando el campo es algebraicamente cerrado. Un ideal es igual al anillo de polinomios siempre y cuando, el conjunto algebraico asociado a este ideal sea vacío (este resultado es el Teorema Débil Nullstellensatz). Si un polinomio está en el ideal asociado a un conjunto algebraico entonces podemos concluir que una potencia de este polinomio está en el ideal generado por los polinomios que describen al conjunto algebraico (este resultado es el Teorema Nullstellensatz de Hilbert). Por último, y el más importante de estos resultados (Teorema Fuerte Nullstellensatz), es que el radical de cualquier ideal es igual al ideal asociado al conjunto algebraico asociado al ideal.

Sin embargo, aunque estos resultados son de gran utilidad, fue hasta el capítulo 3 que respondimos la pregunta que se estableció en la introducción de este trabajo y es que si, gracias al Primer Teorema de Estructura, concluimos que cualquier conjunto semi-algebraico real (en particular, cualquier conjunto algebraico real) tiene un número finito de componentes conexas. Más aún, podemos contestar una de las preguntas que se derivaron de la principal, ya que este teorema no sólo establece la existencia de un número finito de componentes conexas sino que también establece que cada una de estas componentes conexas es un conjunto semi-algebraico.

Así, para el caso real la pregunta está contestada, resulta interesante pensar en lo que sucede en otros campos, como en el caso de los complejos. No hay duda, la unión entre la geometría y el álgebra arroja una serie de resultados por de más interesantes.

Bibliografía

[1] Bartle Robert G., *Introducción al análisis matemático*, 2^a ed. [Tr. Ma. Cristina Gutierrez González], México, Edit. Limusa, 1989, 519 pp.

[2] Benedetti Riccardo & Jean-Jacques Risler, *Real algebraic and semi-algebraic sets*, Paris, Edit. Hermann, 1990, 340 pp.

[3] Bochnak Jacek, Michel Coste & Marie-Françoise Roy, *Real algebraic geometry*, New York, Edit. Springer, 1998, 430 pp.

[4] Burton David M., *A first course in rings and ideals*, U.S.A., Edit. Addison-Wesley Publishing Company, 1970, 309 pp.

[5] Cox David, John Little & Donal O'Shea, *Ideals, varieties, and algorithms, an introduction to computational algebraic geometry and commutative algebra*, 2^a ed., New York, Edit. Springer, 1996, 536 pp.

[6] Fraleigh John B., *Algebra abstracta, primer curso*, 3^a ed. [Tr. Manuel López Mateos], México, Edit. Sistemas Técnicos de Edición, 1987, 485 pp.

[7] Hernández Hernández Fernando, *Teoría de conjuntos, una introducción*, 2^a ed., México, Edit. Sociedad Matemática Mexicana, 2003, 342 pp.

[8] Hoffman Kenneth & Ray Kunze, *Algebra lineal*, 2^a ed. [Tr. Hugo E. Finsterbusch], México, Edit. Prentice-Hall, 1971, 400 pp.

[9] Lang Serge, *Complex Analysis*, 4^a ed., New York, Edit. Springer, 1999, 485 pp.

[10] Lipschutz S. Seymour, *Schaum's outline of theory and problems of general topology*, New York, Edit. McGraw-Hill, 1965, 239 pp.

[11] Massey William Schumacher, *Introducción a la topología algebraica*, Barcelona, Edit. Reverte, 1972, 263 pp.

[12] Rudin Walter, *Análisis funcional*, [Tr. Jesús Fernández Novoa], Barcelona, Edit. Reverte, 1979, 397 pp.