Universidad Nacional
Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

TEOREMA DEL IDEAL PRINCIPAL DE KRULL Y LA REDUCCIÓN DE LA DIMENSIÓN DE LAS COMPONENTES DE UNA VARIEDAD ALGEBRAICA

Línea de investigación:

Matemática pura y aplicada

Tesis para optar el título profesional de Licenciado en Matemática

Autor:

Castillo Ayaque, José Luis Enrique

Asesor:

Quicaño Barrientos, Carlos Gilberto

ORCID: 0000-0003-1140-1531

Jurado:

Contreras Tito, Vladimiro

Velásquez Alarcón, Jorge David

Aycho Flores, Milton Angelino

Lima - Perú

2024

RECONOCIMIENTO - NO COMERCIAL - SIN OBRA DERIVADA
(CC BY-NC-ND)

“TEOREMA DEL IDEAL PRINCIPAL DE KRULL Y LA REDUCCIÓN DE LA DIMENSIÓN DE LAS COMPONENTES DE UNA VARIEDAD ALGEBRAICA”

INFORME DE ORIGINALIDAD

12%	11%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	matematicas.unex.es Fuente de Internet	4%
2	www.math.unam.mx Fuente de Internet	4%
3	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	1%
4	docplayer.es Fuente de Internet	<1%
5	hdl.handle.net Fuente de Internet	<1%
6	Submitted to BENEMERITA UNIVERSIDAD AUTONOMA DE PUEBLA BIBLIOTECA Trabajo del estudiante	<1%
7	Submitted to Unviersidad de Granada Trabajo del estudiante	<1%
8	kolmogorov.unex.es	

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

TEOREMA DEL IDEAL PRINCIPAL DE KRULL Y LA REDUCCIÓN DE LA DIMENSIÓN DE LAS COMPONENTES DE UNA VARIEDAD ALGEBRAICA

Línea de investigación:

Matemática pura y aplicada

Tesis para optar el Título Profesional de

Licenciado en Matemática

Autor

Castillo Ayaque, José Luis Enrique

Asesor

Quicaño Barrientos, Carlos Gilberto

ORCID: 0000-0003-1140-1531

Jurado

Contreras Tito, Vladimiro

Velásquez Alarcón, Jorge David

Aycho Flores, Milton Angelino

Lima – Perú

2024

DEDICATORIA

A mis padres Clemencia Ayaque Quio y Manuel Castillo Castro, por su apoyo y fuerza incondicional, les debo todo.

A Manuel Castillo Ayaque, por soportarme en todo.

A Mayra Fernández Ramírez, por el amor y las risas.

AGRADECIMIENTOS

A mis padres, Clemencia y Manuel, por construir las bases para mis logros, a mis hermanos por todo su apoyo y soporte, a Mayra por hacer más plena mi vida universitaria.

A los docentes que me formaron como matemático, en especial a los profesores Carlos Quicaño, mi profesor de cálculo I, fuente de muchas enseñanzas; a Alex Cruz, gran profesor que me dio la libertad de adentrarme en el profundo mar algebraico; a Vladimiro Contreras, por ser un gran profesor; a David Velásquez, por sus enseñanzas en Álgebra y sugerir el tema de este trabajo; a Milton Aycho, por sus buenas enseñanzas, apoyo y consejos mis últimos años de carrera.

A mis compañeros que hicieron muy amena y feliz mi vida universitaria, a mi "base", Manuel y Marco, a mi "completación" de base Roy, Jampier, Yony, Pedroza, por todas las conversaciones fuera y dentro de la matemática; y a los demás que poco a poco se fueron uniendo para cerrar mi bonita historia universitaria: Gómez, Samuel, Doroteo, Huanca, José Inga "Chiroque", Galois, Pana, Lilian, Zurdo, Jaime; y también a los autodenominados "la mejor base": Mayra, Leonardo, Nicolás, Alex, Hernán. Quedando aún muchos por nombrar. Les agradezco las bellas anécdotas, que hicieron de mi vida universitaria una etapa completa de conocimientos y grandes vivencias.

Finalmente, a mis dos mascotas Panzas y Bobi por el talante que mostraron en las largas noches de estudio.

ÍNDICE

ÍNDICE DE FIGURAS

RESUMEN

El propósito de esta investigación es determinar una condición que debe cumplir un polinomio $f \in k[V] \coloneqq k[x_1, \dots, x_n]/I$ para que la dimensión de las componentes de un conjunto algebraico de una variedad algebraica V solo disminuya en 1 respecto a la variedad; luego se ve una generalización de esto y se logra una algebrización del teorema del ideal principal de Krull, es decir la condición encontrada se pone en términos de un ideal con una propiedad especial, de manera que se pueda ir hablando menos del anillo de polinomios y más de la estructura de anillo. Para tal fin usamos teoría de anillos, anillo cociente, extensiones de cuerpos y nociones de topología, puesto que la noción de dimensión está muy ligada a esta rama de la matemática.

Palabras clave: Polinomios, anillos, extensión de cuerpos, ideal radical, variedades algebraicas, dimensión de krull, Hilbert, Noether, Krull.

ABSTRACT

The purpose of this investigation is to determinate a condition that a polynomial $f \in k[V] := k[x_1, \dots, x_n]/I$ must fulfill so that the dimension of the components of an algebraic set of an algebraic variety only decreases by 1 with respect to the variety; then a generalization of this is seen and an algebrization of the Krull's principal ideal theorem, that is, the found condition is put in terms of an ideal with a special property, so that one can talk less about the polynomial ring and more about the ring structure. For this purpose, we use ring theory, quotient ring, field extensions and notions of topology, since the notion of dimension is closely linked to this branch of mathematics.

Key words: Polynomials, rings, fields extension, radical ideal, algebraic varieties, krull dimension, Hilbert, Noether, Krull.

I. INTRODUCCIÓN

En álgebra abstracta, específicamente en la geometría algebraica, a través de términos algebraicos se busca capturar la noción geométrica de variedad en geometría diferencial. La dimensión de un objeto matemático es un número que corresponde a sus características topológicas o métricas. Las conceptualizaciones más comunes de dimensión las conocemos de los espacios vectoriales y de los espacios topológicos, pero, en geometría, física o ciencias aplicadas, lo más intuitivo es referirse a un mínimo de coordenadas para ubicar con exactitud cualquier punto de lo que entendamos por espacio.

En este trabajo se desarrolla la definición de dimensión para una variedad algebraica teniendo siempre como referencia un cuerpo algebraicamente cerrado. Además, se explicará brevemente porque no es posible considerar otro tipo de cuerpos.

Para estudiar las variedades algebraicas se necesita de un espacio y un anillo de funciones que evalúen puntos de dicho espacio. Se trabajará entonces en el espacio k^n (sin estructura de espacio vectorial, donde k es un cuerpo) y en el anillo de polinomios en n indeterminadas. Este caso, que sirve como inicio para nuestro estudio, puede ser visto como el caso canónico. Para adentrarse ya en las variedades algebraicas se tendrá que definir subconjuntos del espacio con ciertas propiedades topológicas, estas propiedades afectarán directamente a lo que se empiece a entender por su anillo de funciones. La dimensión de la variedad está ligada a este anillo y al cuerpo sobre los que está definido el espacio, así el teorema del ideal principal de Krull es un resultado que necesita de definiciones de extensiones de cuerpos muy particulares la norma, grado de trascendencia, etc.

En la sección 2.1.1 se da contexto al trabajo y una introducción histórica, luego se dan definiciones básicas, se establecen notaciones y se enuncian proposiciones, lemas y teoremas fundamentales tales como El teorema de la base de Hilbert, que muestra como todo ideal del anillo $k[x_1, \dots, x_n]$, con k un cuerpo, es finitamente generado. Algunos enunciados serán demostrados debido a su interés dentro del estudio o su similitud en su forma a algunas demostraciones de secciones posteriores, además de buscar generar confianza o curiosidad en el lector con poco bagaje algebraico. Más adelante se ve teoría de Anillos como el anillo cociente y un estudio detallado del anillo de polinomios en n indeterminadas, la Extensión de cuerpos y la definición de grado de trascendencia, el concepto de Nilpotencia e Ideal radical que son una propiedad poco deseada en los anillos y un ideal importante para el teorema de los ceros de Hilbert.

En las secciones 2.1.9, 2.1.10 y 2.1.11 se formaliza lo que se entiende por espacio y su anillo de coordenadas, de manera análoga una variedad y su anillo de coordenadas afín. Algunas observaciones, definiciones y enunciados de este capítulo son el resultado del análisis de problemas propuestos y la justificación de ideas de los textos de referencia de este trabajo. Por ejemplo, el hecho de trabajar en los cocientes de ciertos anillos de coordenadas afín, la justificación de la definición de anillo de coordenadas afín y ciertas propiedades topológicas.

En la sección 3.7.1 se formaliza la noción de dimensión de una variedad algebraica y se muestran ciertas propiedades de la misma, por ejemplo, que la dimensión respeta la relación de inclusión de los subconjuntos. En la sección 3.7.2 se trata el Lema de normalización de Noether, el cual es una herramienta fundamental que goza de una interpretación geométrica muy didáctica.

En la sección de resultados se explica de manera detallada el teorema del ideal principal de Krull y su demostración, las secciones finales corresponden a sus consecuencias y el desarrollo de una “algebrización” de este teorema.

1.1. Descripción y formulación del problema

En geometría algebraica, una vez definida una variedad V, su anillo de funciones asociados $k[V]$ y su dimensión, ocurre un problema entre el "conjunto de polinomios" que generan la variedad y la dimensión de esta.

A medida que el subconjunto de ecuaciones polinomiales es más grande, su conjunto solución es más pequeño y esto hace que en general la dimensión disminuya.

Considérese el caso genérico del álgebra lineal, cuando un sistema homogéneo de ecuaciones lineales en n indeterminadas consta de una sola ecuación f (no trivial) entonces la dimensión del subespacio vectorial solución (que en realidad es una variedad algebraica) tiene dimensión $n-1$; a medida que aumentan las ecuaciones del sistema, la dimensión del subespacio solución disminuye llegando al punto que para n ecuaciones (linealmente independientes) solo quedará la solución trivial (dimensión cero). Todo lo dicho puede generalizarse al caso no lineal homogéneo solo que es más complicado de formalizar.

Dicho todo esto: ¿Será posible encontrar una condición polinómica adicional para que la dimensión de las componentes de un conjunto algebraico en una variedad no disminuya drásticamente? Por ejemplo, en el contexto de las variedades, el subespacio $n-1$ dimensional generado por una ecuación lineal f podría llegar a ser 0, dependiendo a qué ideal del anillo de coordenadas pertenezca esta ecuación f. Esto tendrá consecuencias fundamentales para entender mejor el concepto de dimensión de una variedad algebraica.

La importancia de mantener una disminución no tan estrepitosa de la dimensión de subconjuntos radica en el hecho que se puedan generar sucesiones descendentes de subconjuntos en los cuales la dimensión posee un comportamiento regular.

1.2. Antecedentes

La geometría algebraica tiene sus raíces en la matemática griega y la matemática Renacentista-Descartesiana, dos de los grandes matemáticos que vieron sus fundamentos fueron David Hilbert y Emmy Noether.

Hilbert aportó el teorema de la base de Hilbert y su Nullstellensatz o teorema de los ceros de Hilbert, que estableció una conexión más clara entre el álgebra abstracta y la geometría, aunque esto no fuera aplicado por el mismo Hilbert, sino por Emmy Noether dando lugar así a la naciente geometría algebraica. En 1921, el matemático alemán Wolfgang Krull, que estudiaba en Gotinga, fue influenciado por Emmy Noether hacia el Álgebra Abstracta.

Los trabajos que influyeron en este trabajo son lecturas recabadas de los siguientes trabajos de investigación, de Angulo (2004), Ideales generados por R-sucesiones, donde muestra una generalización basada en cadenas descendente de ideales primos cuando el anillo es Noetheriano. También influye en este trabajo la lectura de la investigación de Giral (1979), Dimensión de Krull y propiedad de “Going-Between” en una extensión de anillos, la cual expone como herramientas algunas de las propiedades de la dimensión de una variedad, en la parte introductoria muestra una interesante reseña histórica de Wolfgang Krull. Finalmente, el trabajo de investigación de Ruiz (2017), Álgebra local y algoritmos, muestra la dimensión de un objeto algebraico (anillo) como herramienta para demostrar teoremas que permite formar algoritmos avanzados que hará efectivo el resultado, llamado por el autor, Teorema de Representación; esto en el contexto de los anillos Henselianos, que son los anillos “más pequeños” que verifican el teorema de la Función Implícita.

1.3. Objetivos

1.3.1. Objetivo General

Determinar, en una variedad algebraica V, las condiciones que debe tener un polinomio f que pertenece al anillo de coordenadas afín $k[V]$, de manera que la dimensión de los subconjuntos irreducibles maximales de los ceros de este polinomio solo disminuya en 1 respecto a la dimensión de la variedad V.

1.3.2. Objetivos Específicos

1) Estudiar propiedades de los conjuntos algebraicos afines.
2) Estudiar las variedades algebraicas afín a través de su dimensión, primero viendo que es una propiedad invariante por lo que sirve para clasificarlas.
3) Mostrar la idea intuitiva de dimensión en un espacio geométrico, luego formalizarlo en el contexto de las variedades afín y llevarlo a su consecuencia más importante: la dimensión de Krull.
4) Demostrar el lema de normalización de Noether y explicar su interpretación geométrica.
5) Demostrar el teorema de los ceros de Hilbert.

1.4. Justificación

Actualmente la geometría algebraica es una rama de la Matemática con muchas líneas de investigación, a su vez goza con el calificativo de ser ultra-abstracto, sobre todo el enfoque alcanzado por el matemático Alexander Grothendieck.

Por otro lado, en geometría la propiedad que más resalta es la dimensión, pero al momento de generalizar es donde se presencia dificultad. Estudiar esta propiedad es fundamental en geometría.

La importancia de este trabajo es mostrar el camino a la dimensión de objetos abstractos como los anillos, un objeto algebraico que intuitivamente no da la idea de una dimensión geométrica. Para esto, la dimensión de una variedad algebraica se muestra en términos de difícil manipulación por eso la importancia de encontrar equivalencias más cómodas y además resolver el problema de la disminución de la dimensión al momento de “hacer más grande” su conjunto de polinomios que lo genera, por ello el estudio y aplicación del Teorema del Ideal Principal de Krull.

Entender mejor la noción de dimensión nos permite estudiar o caracterizar a través de su dimensión objetos más abstractos y complicados tales como el cono afín de una variedad proyectiva, ver la dimensión de las fibras $f(Q)^{-1}$, ver la dimensión del espacio tangente en puntos que sean lisos, etc.

1.5. Hipótesis

El teorema del ideal principal de Krull permite determinar como disminuye la dimensión de los subconjuntos irreducibles maximales de los ceros de un polinomio $f \in k[V]$, imponiéndole a este la condición de ser un polinomio no nulo de $k[V]$ pero al menos tener un cero en V.

Dicho de otra manera: Si V es una variedad afín y $f \in k[V]$ (al anillo de coordenadas afín de la variedad) es no nulo, pero tiene un cero en V, entonces las componentes irreducibles del conjunto de ceros $\mathcal{V}(f)$ tienen dimensión: $\dim\mathcal{V}(f) = \dim V - 1$.

Esto será resuelto gracias al TEOREMA DEL IDEAL PRINCIPAL DE KRULL.

II. MARCO TEÓRICO

2.1. Bases teóricas sobre el tema de investigación

2.1.1. Introducción histórica

La geometría algebraica puede definirse como el estudio de los espacios solución de sistemas de ecuaciones algebraicas. Sus raíces se encuentran en la matemática renacentista-Descartesiana y en la matemática griega con el estudio de los cuerpos geométricos. Como el inicio de toda rama de la ciencia, el aporte de los científicos a su objeto de estudio suele ser intuitivo y muy poco fundamentado; este fue el caso de la escuela italiana que alrededor de la mitad del siglo XIX floreció y tuvo un desarrollo enorme. A inicios del siglo XX los temas de estudio fueron más allá de los límites de las técnicas de la época, llegando a un punto que estas ya no podían expresar o llevar a cabo la idea de sus mejores matemáticos. Es aquí donde juega un papel importantísimo la escuela alemana con matemáticos como Max Noether, David Hilbert, Emmy Noether, Emanuel Lasker, Wolfgang Krull y otros. Max Noether, fue uno de los líderes en geometría algebraica del siglo XIX, siendo influenciado por matemáticos como Abel, Riemann, Cayley y Cremona. Fue llamado el padre de la geometría algebraica.

Un teorema que yace en los fundamentos mismos de la geometría algebraica es el de la base de Hilbert, y aunque fue expresado en un lenguaje diferente del moderno, condujo inmediatamente a la solución de uno de los problemas más sobresalientes de las Matemáticas en el periodo 1868-1888, conocido como "el problema de Gordan", en honor a Paul Gordan, quien fuera un experto líder en algoritmos increíblemente extensos en el campo de la Teoría de invariantes, en 1868 encontró una demostración computacional larga del teorema de la base para dos variables la cual mostraba, en esencia, como construir una base específica para un ideal dado. La generalización para n variables fue intentada sin éxito por los matemáticos más distinguidos de la época, el problema radicaba en la cantidad ingente de complicados cálculos algebraicos que aparecían. La perspicacia de Hilbert fue notar que el asunto a tratar era un problema de existencia más que un problema de construcción (producir una base). En 1888 mostró para el caso de n variables la existencia de una base finita para cualquier ideal, muchos en la comunidad matemática reaccionaron dudando que esto fuera siquiera matemática, la filosofía de aquellos días era que para probar que algo existe se debe encontrar explícitamente. Gordan realizó un comentario para la posteridad: “Eso no es Matemática, eso es Teología”. Sin embargo, más tarde, Hilbert fue capaz de hacer una prueba por construcción, esto sirvió como una vindicación monumental a la perspectiva de Hilbert y fue un gran cambio en el pensamiento matemático. Incluso Gordan admitió que “la Teología tiene sus méritos”.

Otro aporte notable de Hilbert es su Nullstellensatz o Teorema de los ceros, que estableció una conexión más clara entre el álgebra abstracta y el espacio geométrico (los conjuntos algebraicos). La filosofía de Hilbert ha posibilitado algunas de las contribuciones más elegantes e importantes a la Matemática.

Emmy Noether, en 1920, se adentró en la floreciente álgebra abstracta y con la colaboración de W. Schmeider publicó un artículo sobre la teoría de ideales para anillos no conmutativos, posteriormente publicó su Idealtheorie in Ringbereichen, un trabajo calificado como revolucionario, aquí analizó la condición de cadena ascendente al respecto de los ideales; su publicación dio lugar al término anillo Noetheriano, anillo que da condiciones de finitud muy deseadas.

En 1921, el matemático alemán Wolfgang Krull, que estudiaba en Gotinga, fue influenciado por Emmy Noether hacia el álgebra abstracta. Hizo aportes importantes en la Teoría de Galois y de grupos abelianos. En 1928 definió la dimensión de Krull de un anillo Noetheriano conmutativo y atrajo a la teoría de anillos un nuevo enfoque con el cual demostrar que se podía mantener un ideal principal. Una razón por la cual la idea de la dimensión de Krull es un concepto tan natural es que encapsula en un contexto abstracto las ideas análogas de dimensiones geométricas. El Teorema del ideal principal de Krull fue rápidamente reconocido como un avance decisivo en el programa de Noether sobre la emancipación de la teoría abstracta de anillos a partir de la de los anillos de polinomios.

Krull prosiguió con su trabajo, definiendo otros conceptos que hoy son centrales para la investigación moderna en teoría de anillos. Escribió un notable tratado Ideal Theory, que sigue siendo una hermosa introducción a la teoría de anillos, pero que simplemente es una teoría construida a partir de los resultados que Krull probó. La filosofía de Krull no se basó meramente en encontrar teoremas y probarlos, él quería organizarlos y agruparlos de tal manera que aparezcan no solo como correctos, sino también como imperativos y evidentes. Consideró que esta aspiración era más estética que basada en la cognición teórica. Se podría decir que Krull logró su objetivo.

Hasta ahora se ha hablado de los fundamentos de la geometría algebraica clásica, basados en ideales de polinomios. Pero es con Oscar Zariski y su escuela que los métodos del álgebra conmutativa son aplicados con todo rigor a la Geometría Algebraica.

Oscar Zariski fue un matemático estadounidense de origen polaco. Estudió en la Universidad de Kiev, en 1927 emigró a Estados Unidos y se estableció como profesor. Durante este periodo escribió Algebraic Surfaces como un compendio del trabajo de la escuela italiana, lo publicó en 1935. Fue reeditado 36 años después con apuntes detallados de sus discípulos, ilustrando el cambio de la geometría algebraica. Este texto todavía se mantiene como una referencia importante.

Parece que este trabajo estableció el descontento de Zariski con el enfoque de la escuela italiana, por su poco rigor, así aborda esta cuestión recurriendo al álgebra conmutativa de la mano de técnicas de la escuela alemana guiados por Emmy Noether. La resolución de singularidades de una variedad algebraica lo llevó a establecer la denominada Topología de Zariski.

2.1.2. Anillos

La estructura algebraica de anillo, además de generalizar muchas propiedades aritméticas de los números enteros, tiene un enfoque geométrico que se intentará mostrar en esta sección preliminar. Los puntos principales de este apartado son definir el anillo de polinomios, ver las propiedades del anillo cociente y el ideal primo e ideal maximal.

En este trabajo se entenderá anillo A a una estructura algebraica de dos operaciones suma y producto, denotados por $+$ y $\cdot$, sus elementos verifican:

1. $(A, +)$ tiene la estructura de grupo conmutativo.
2. El producto se asocia: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. El producto y la suma son distributivos:
   i. $a \cdot (b + c) = a \cdot b + a \cdot c$.
   ii. $(b + c) \cdot a = b \cdot a + c \cdot a$.
4. Existe un elemento de $1 \in A$ llamado unidad, tal que para todo $a \in A$ se cumple: $a \cdot 1 = 1 \cdot a = a$.
5. El producto es conmutativo: $a \cdot b = b \cdot a$.

Navarro (2013).

Por abuso de notación se escribe ab en lugar de $a \cdot b$, se dice que $a \in A$ es invertible si existe algún $b \in A$ tal que $ab = 1$ y se denota b^{-1} o $\frac{1}{b}$. Respeto al producto de A, tales elementos invertibles forman un grupo conmutativo que denotamos A^*. Un anillo $A \neq 0$ será denominado *cuerpo* si sus elementos no nulos son invertibles en A; es decir, $A^* = A - \{0\}$.

Un elemento $a \in A$ será un divisor de cero sí $ab = 0$ para algún $b \in A$ no nulo. Un anillo A será un dominio de integridad si no posee divisores de ceros, es decir, de tener el producto de elementos no nulos nunca tal resultado nunca es nulo; podemos ver claramente que cualquier cuerpo es un dominio de integridad.

En A se puede definir la resta $b - a \coloneqq b + (-a)$ y la división $a/b := ab^{-1}$, cuando el divisor b es invertible en A. Por último, un elemento propio (no nulo y no invertible) $p \in A$ será irreducible en A si en cualquier posible descomposición $p = ab$ alguno de sus factores es invertible.

Definición 2.1. Sea $B \subset A$, se dice que B es un subanillo de A si es un subgrupo de A, el producto es una operación interna (Si $a, b \in B$, entonces $ab \in B$) y $1 \in B$. Navarro (2013)

Es claro que la intersección de subanillos de un anillo A resulta ser subanillo de A, por otro lado para un subanillo $B \subset A$ y elementos $a_1, a_2, \dots, a_n$, el menor subanillo de A que los contiene se denota $B[a_1, a_2, \dots, a_n]$, de modo que puede ser caracterizado como:

$$B[a_1, a_2, \dots, a_n] = \{\sum_{i_1,\dots,i_n} b_{i_1 \dots i_n} a_1^{i_1} \dots a_n^{i_n} \ : \ b_{i_1 \dots i_n} \in B\}$$

y se dirá que $B[a_1, a_2, \dots, a_n]$ es el subanillo de A generado por B y $a_1, a_2, \dots, a_n$.

Definición 2.2. Se dice que un subconjunto $I \subset A$ es un ideal del anillo A si:

1. $(I, +)$ es un subgrupo de A.
2. Si $a \in A$ y $b \in I$, entonces $ab \in I$. Navarro (2013).

Es claro que la intersección de ideales de un anillo A resulta ser un ideal de A, más aún el mayor ideal de A contenido en los ideales que estamos intersecando.

La suma de dos ideales I_1, I_2 de un anillo A es el ideal:

$$I_1 + I_2 = \{a + b : a \in I_1, b \in I_2\}$$

y es el menor ideal de A que los contiene.

Dados elementos $a_1, a_2, \dots, a_n \in A$, el ideal $a_1A + a_2A + \cdots + a_nA$ es el menor ideal de A que los contiene y se denota $(a_1, a_2, \dots, a_n)$, decimos que $a_1, a_2, \dots, a_n$ generan tal ideal. Siguiendo esta idea se tiene un ideal generado por un solo elemento, $(a) = aA$.

El producto de dos ideales I_1, I_2 de un anillo A es el ideal generado por el conjunto:

$$I_1I_2 = \{a_1b_1 + \cdots + a_nb_n : a_1, \dots, a_n \in I_1, b_1, \dots, b_n \in I_2\}.$$

Definición 2.3. Un ideal $\mathfrak{m}$ de un anillo A será maximal si es un conjunto propio y los únicos ideales de A que lo contienen son él mismo y el anillo A. Un ideal $\mathfrak{p}$ de un anillo A será primo si es un conjunto propio y se cumple: $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}$, es decir, si un producto está en $\mathfrak{p}$, alguno de sus factores se encuentra en $\mathfrak{p}$. Navarro (2013)

Un ejemplo trivial de ideal primo de $\mathbb{Z}$ es el generado por 0. Uno más elaborado es el ideal generado por números primos $p\mathbb{Z}$, donde p es primo. En este anillo los ideales primos y maximales coinciden.

Definición 2.4. Una aplicación $f: A \to B$ entre anillos es un morfismo (de anillos) si respeta ambas estructuras de anillo, es decir:

1. $f(a + b) = f(a) + f(b)$.
2. $f(ab) = f(a)f(b)$.
3. $f(1) = 1$.

Navarro (2013)

Un morfismo $f: A \to B$ será un isomorfismo de anillos si existe un morfismo $g: B \to A$ tal que $f \circ g = I_B$ y $g \circ f = I_A$, en tal caso decimos que el morfismo g es el inverso de f y se denota f^{-1}.

Los morfismos $f: A \to B$ de anillos, con $a, b, a_1, \dots, a_n \in A$, cumplen las propiedades:

1. $f(0) = 0$; $f(a - b) = f(a) - f(b)$.
2. $f(\sum_{i=1}^{n} a_i) = \sum_{i=1}^{n} f(a_i)$; $f(a^{-1}) = f(a)^{-1}$.
3. $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$.
4. La imagen $f(C)$ de un subanillo de C de A es subanillo de B.
5. La imagen inversa $f^{-1}(D)$ de un subanillo de D de B es subanillo de A.
6. La imagen inversa $f^{-1}(X)$ de un ideal X de B es ideal de A.
7. Si f es sobreyectiva, la imagen $f(I)$ de un ideal I de A es ideal de B.

Definición 2.5. Sea $f: A \to B$ un morfismo de anillos, se denomina núcleo de f al conjunto $\mathrm{Ker}f = f^{-1}(0) = \{a \in A : f(a) = 0\}$.

La notación del núcleo procede del vocablo germano Kernel. Además, el núcleo de un morfismo es un ideal de A.

Proposición 2.6. Un morfismo $f: A \to B$ es inyectivo si y solamente si $\mathrm{Ker}f = 0$.

Demostración. Ver Del Río y Del Valle (2001), p. 49, Proposición 2.6.7.

Definición 2.7. El anillo de polinomios en una indeterminada x con coeficientes en A es el conjunto

$$\left\{\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \quad : \quad a_i \in A\right\},$$

el cual posee la estructura de anillo gracias a las operaciones usuales:

1. $\sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i + b_i) x^i$
2. $\left(\sum_i a_i x^i\right) \cdot \left(\sum_i b_i x^i\right) = \sum_{n\geq 0}\left(\sum_{i+j=n} a_i b_j\right) x^n$

y será denotado por $A[x]$. Navarro (2013).

Definición 2.8. El anillo de polinomios $A[x_1, \dots, x_n]$ en n indeterminadas con coeficientes en A se define como: $A[x_1, \dots, x_n] \coloneqq (A[x_1, \dots, x_{n-1}])[x_n]$. Navarro (2013).

Como caso particular tenemos $A[x, y] = A[x][y]$. Además, cada $a \in A$ define un polinomio constante que se denota a, obteniéndose un morfismo canónico $A \to A[x_1, \dots, x_n]$. Si $p(x) = c_0 x^n + c_1 x^{n-1} + \dots + c_n \in k[x]$, un elemento $a \in k$ es una raíz de $p(x)$ en k cuando $p(a) = c_0 a^n + c_1 a^{n-1} + \dots + c_n = 0$.

Los anillos de polinomios juegan un papel fundamental en este trabajo. Ya es conocido que lugares geométricos están asociados a polinomios (en general asociados a sistemas de ecuaciones polinomiales compatibles). El tipo de anillo del cual los polinomios recogen sus coeficientes es muy importante.

El procedimiento de particionar un conjunto a través de una relación de equivalencia tendrá su utilidad, como veremos más adelante, al momento de agrupar funciones definidas en un lugar geométrico. Por ejemplo, dos funciones pueden ser distintas en un plano, pero si nos restringimos a un lugar geométrico donde ambas sean iguales entonces como funciones en aquel lugar geométrico serán "indistinguibles" (como funciones estarán agrupadas en la misma clase).

Sea $\mathfrak{a}$ un ideal de un anillo A, se define una relación $a \equiv b (\text{mod } \mathfrak{a}) \Leftrightarrow b - a \in \mathfrak{a}$, su conjunto cociente se denotará por $A/\mathfrak{a}$. La clase de equivalencia de cualquier $a \in A$ es

$$a + \mathfrak{a} = \{a + x : x \in \mathfrak{a}\}$$

denominada la clase de restos de a módulo $\mathfrak{a}$. Tal clase se denota por $\bar{a}$ o $[a]$.

Teorema 2.9. Sea $\mathfrak{a} \subset A$ un ideal de A. El conjunto cociente $A/\mathfrak{a}$ con las operaciones $[a] + [b] = [a + b]$ y $[a][b] = [ab]$ posee una única estructura de anillo. La proyección canónica $\pi: A \to A/\mathfrak{a}$ es un morfismo que satisface: $\mathfrak{a} = \mathrm{Ker}\pi$.

Demostración. Ver Navarro (2013), p. 55, Teorema 3.5.1.

$A/\mathfrak{a}$ es llamado anillo cociente de A módulo $\mathfrak{a}$ o simplemente anillo cociente. El siguiente teorema describe los ideales de $A/\mathfrak{a}$.

Teorema 2.10. (Teorema de correspondencia). Sea A un anillo y $\mathfrak{a}$ un ideal de A, las correspondencias $J \mapsto J/\mathfrak{a}$ y $X \mapsto \pi^{-1}(X)$ son biunívocas (una inversa de la otra) y conservan el orden entre el conjunto de todos los ideales de $A/\mathfrak{a}$ y el conjunto de los ideales J de A que contienen a $\mathfrak{a}$.

Demostración. Ver Del Río y Del Valle (2001), p. 44, Teorema 2.4.8.

A continuación, se presentan los teoremas de isomorfismo.

Teorema 2.11. (Primer Teorema de Isomorfía) Sea $f: A \to B$ un morfismo. Entonces existe un isomorfismo $\bar{f}: A/\mathrm{Ker}f \to \mathrm{Im}f$ que cumple $\bar{f} \circ \pi = f$. En particular, $A/\mathrm{Ker}f \cong \mathrm{Im}f$.

Demostración. Ver Del Río y Del Valle (2001), p. 50, Teorema 2.7.4.

Teorema 2.12. (Segundo Teorema de Isomorfía) Sea A un anillo e I y J ideales de A tales que $I \subset J$. Entonces $J/I \subset A/\ \mathfrak{a}$ es un ideal y además:

$$\frac{A/\mathrm{I}}{J/I} \cong \frac{A}{J}.$$

Demostración. Ver Del Río y Del Valle (2001), p. 51, Teorema 2.7.5.

Teorema 2.13. (Tercer Teorema de Isomorfía) Sean $I, B \subset A$ un ideal y un subanillo de A, respectivamente. Entonces:

1. $B \cap I$ es un ideal de B.
2. $B + I$ es un subanillo de A que contiene a I como ideal.
3. Existe un isomorfismo entre $\frac{B}{B \cap I}$ y $\frac{B+I}{I}$.

Demostración. Ver Del Río y Del Valle (2001), p. 51, Teorema 2.7.6.

Algunos ejemplos de estos teoremas

1. El morfismo $f: A[x] \rightarrow A$ de evaluación en 0 (definido por $a_0 + a_1x + \cdots \mapsto a_0$) es sobreyectivo y tiene por núcleo a (x), así se tiene: $A[x]/(x) \cong A$.
2. Sean A un anillo e I un ideal de A. Para cada $a \in A$, sea $\bar{a} = a + I$. La aplicación $f: A[x] \rightarrow \left(\frac{A}{I}\right)[x]$ dada por $f(a_0 + a_1x + \cdots + a_nx^n) = \overline{a_0} + \overline{a_1}x + \cdots \overline{a_n}x^n$ es un morfismo sobreyectivo de anillos con núcleo:

$$I[x] = \{a_0 + a_1x + \cdots + a_nx^n : a_i \in I\}.$$

Utilizando el Primer Teorema de Isomorfía se obtiene:$(A/I)[x] \cong A[x]/I[x]$.

Teorema 2.14. Sea $I \subset A$ un ideal de A.

1. I es ideal primo de A sí y solo si $A/\mathfrak{a}$ es dominio de integridad.
2. I es ideal maximal de A sí y solo si $A/\mathfrak{a}$ es cuerpo.

Demostración. Ver Navarro (2013), p. 57, Teorema 3.5.3.

Como todo cuerpo es dominio de integridad, es sencillo afirmar:

Teorema 2.15. Todo ideal maximal es primo.

Corolario 2.16. Sea k un cuerpo y $a_1, a_2, \dots, a_n \in k$, entonces

$$\mathfrak{m} := \{f \in k[x_1, \dots, x_n] \,:\, f(a_1, \dots, a_n) = 0\}$$

es ideal maximal de $k[x_1, \dots, x_n]$, además, está finitamente generado, en efecto $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$ y se tiene el isomorfismo $k \to k[x_1, \dots, x_n]/\mathfrak{m}$.

Demostración. Ver Navarro (2013), p. 58, Corolario 3.5.3.

Teóricamente los ideales maximales son importantes porque los anillos cocientes de ideales maximales son cuerpos (en anillos no conmutativos los cocientes son llamados anillos simples). Los siguientes teoremas aseguran la existencia de este tipo de ideal tan importante, la demostración usa el Lema de Zorn, se hará uso de este lema más adelante en otros resultados.

Teorema 2.17. Todo anillo conmutativo no trivial posee algún ideal maximal.

Demostración. Ver Navarro (2013), p. 104, Teorema 6.1.3.

Teorema 2.18. Todo ideal propio I de un anillo conmutativo no trivial A está contenido en algún ideal maximal de A.

Demostración. Ver Navarro (2013), p. 104, Teorema 6.1.4.

A continuación, se ven tipos de anillos con más estructura algebraica que los anillos genéricos, y la relación que hay entre ellos.

Definición 2.19. Un anillo A es llamado un dominio euclídeo (DE) si es dominio de integridad y viene acompañado de una aplicación $\delta: A - \{0\} \to \mathbb{N}$ tal que:

1. $\delta(a) \leq \delta(ab)$ para todo $a, b \in A$ no nulos.
2. Si $a \in A$ no es nulo, para cada $b \in A$ existen $c, r \in A$ tales que $b = ac + r$ y

$$\delta(r) < \delta(a) \lor r = 0.$$

Navarro (2013).

Por ejemplo, el anillo $k[x]$, donde k es cuerpo, es dominio euclídeo, ya que se puede considerar $\delta(p(x)) = \text{gr}(p(x))$ y aplicar división de polinomios.

Un ideal I de un anillo A es principal cuando es generado por un elemento. Si un anillo es un dominio de integridad y todos sus ideales son principales, se dirá que es un dominio de ideales principales (DIP).

Definición 2.20. Un dominio de integridad A será un dominio de factorización única (DFU) si todo elemento propio (no nulo ni invertible) de A se descompone en producto de elementos irreducibles de A y tal descomposición es única salvo el orden y factores invertibles en A.

Navarro (2013).

La relación entre estos tipos de anillos es como sigue:

Teorema 2.21. Todo dominio euclídeo D es un dominio de ideales principales.

Demostración. Ver Del Río y Del Valle (2001), p. 72, Teorema 3.3.3 o ver Dummit y Foote (2004), p. 273, Proposición 1.

Teorema 2.22. Todo dominio de ideales principales D es un dominio de factorización única.

Demostración. Ver Del Río y Del Valle (2001), p. 78, Teorema 3.4.6 o ver Dummit y Foote (2004), p. 287, Teorema 14.

El recíproco de los dos últimos teoremas no se cumple en general, el ejemplo de un DIP que no es DE lo podemos encontrar en Del Río y Del Valle (2001, p. 72) y el ejemplo de un

DFU que no es DIP es el anillo $\mathbb{Z}[x]$ que resulta ser DFU, por la siguiente proposición, pero, el ideal generado por $\{2, x\}$ no es principal. Todo esto nos permite ver que los DFU son el tipo de anillo que contiene a las demás, en todo caso podemos resumir lo visto en la siguiente contención de conjuntos:

$$\text{Cuerpo} \subsetneq \text{DE} \subsetneq \text{DIP} \subsetneq \text{DFU} \subsetneq \text{Dominio de integridad} \subsetneq \text{Anillos}$$

haciendo hincapié en el hecho que, aunque es a partir de los dominios de integridad donde ya se puede usar la ley de cancelación, es a partir de los DFU de donde se tiene “más estructura algebraica” (por ejemplo, la unicidad de la descomposición de sus elementos).

Como el concepto de anillo de polinomios en varias indeterminadas se utiliza con frecuencia en el trabajo, se muestra algunos resultados importantes de los mismos.

Proposición 2.23. Para un anillo A y un entero positivo n se verifican:

1. $A[x_1, \dots, x_n]$ nunca es cuerpo.
2. $A[x_1, \dots, x_n]$ es dominio de integridad sí y solo si lo es A.
3. Si $n \geq 2$ entonces $A[x_1, \dots, x_n]$ no es un DIP.
4. $A[x_1, \dots, x_n]$ es un DFU si y solo si lo es A.

Demostración. Ver Del Río y Del Valle (2001), p. 104, Teorema 4.7.1.

Se hace una digresión para ver la importancia fundamental del anillo $A[x_1, \dots, x_n]$. En el caso de $A[x]$, donde A es un anillo con buen comportamiento como los dominios de integridad, el grado de cualquier polinomio $f \in k[x]$ acota su cantidad de raíces. En el caso de polinomios con varias indeterminadas ocurre algo diferente, para simplificar esto se verá el caso de los polinomios de grado 2 con coeficientes reales. Las generalizaciones pueden quedar en manos del lector.

Un elemento $(a,b) \in \mathbb{R}^2$ es un cero del polinomio $f \in \mathbb{R}[x,y]$ sí $f(a,b) = 0$, si se denota por $\mathcal{V}(f)$ al conjunto de ceros de f, no es difícil ver que $\mathcal{V}(xy)$ consiste en los ejes de $\mathbb{R}^2$, y $\mathcal{V}(x^2/a^2 + y^2/b^2 - 1)$ es una elipse centrada en el origen. Así puede verse que el grado de un polinomio en dos indeterminadas no restringe la cantidad de ceros del polinomio, generando así objetos geométricos con lo que trabajar y no simplemente puntos aislados. La complejidad de los ceros $\mathcal{V}(f)$ aumenta con el grado de f.

2.1.3. Extensión de cuerpos

Definición 2.24. Sean k y L dos cuerpos tal que k es subcuerpo de L, se dice que L es un cuerpo extensión de k, y se representa por L/k llamándolo una extensión de cuerpos de k. Si no hay opción de ambigüedad, L será la extensión de cuerpos. Jara (2017).

Es claro que toda extensión L/k hace que L posea una estructura de espacio vectorial sobre k. La dimensión de este k-espacio vectorial será llamado grado de L sobre k y se representa como $[L:k]$. Se dice que la extensión es finita sí $[L:k]$ es finito.

Ejemplos:

1. El morfismo $\mathbb{Q} \to \mathbb{R}$ es una extensión no finita, porque todo espacio vectorial de dimensión finita sobre $\mathbb{Q}$ es de cardinalidad numerable, mientras que $\mathbb{R}$ no lo es.
2. El morfismo $\mathbb{R} \to \mathbb{C}$ es una extensión finita de grado 2.

Si L una extensión de un cuerpo k y $\alpha_1, \dots, \alpha_n \in L$. Entonces

$$k(\alpha_1, \dots, \alpha_n) = \left\{\frac{a}{b} : a, b \in k[\alpha_1, \dots, \alpha_n], b \neq 0\right\},$$

es el subanillo de L más pequeño que es cuerpo y además contiene a k y a $\alpha_1, \dots, \alpha_n$, por ende, es una extensión de k, se dice que es generada por $\alpha_1, \dots, \alpha_n$ y k. Está conformada por los elementos de L que pueden obtenerse de $\alpha_1, \dots, \alpha_n$ y de elementos de k, es decir, con un número finito de sumas, restas, productos y divisiones por elementos no nulos. Esta idea se justifica en un próximo teorema (2.26).

Definición 2.25. Si L/k es una extensión de cuerpos, un $\alpha \in L$ será algebraico sobre k si existe un polinomio $f \in k[x]$ no nulo tal que $f(\alpha) = 0$. Un elemento que no es algebraico sobre k se denomina trascendente sobre k. Si todo elemento de L es algebraico sobre k, se dirá que la extensión L/k es algebraica. Jara (2017).

Por ejemplo, π y e son trascendentes sobre $\mathbb{Q}$.

Teorema 2.26. Sea L una extensión de k. Si $\alpha, \beta \in L$ son algebraicos sobre k, entonces también lo son $\alpha + \beta,\ \alpha\beta, \alpha/\beta$ cuando $\beta \neq 0$. Es decir, los elementos de L algebraicos sobre k forman una extensión de k.

Demostración. Ver Navarro (2013), p. 77, Teorema 4.4.6.

Teorema 2.27. Si F es una extensión finita de k y L es una extensión finita de F, entonces L es una extensión finita de k de grado

$$[L: k] = [L: F][F: k].$$

Demostración. Ver Navarro (2013), p. 75, Teorema del grado.

Proposición 2.28. Para todo $\alpha \in L/k$ elemento de algebraico sobre k, existe un polinomio irreducible $f \in k[x]$ que cumple $f(\alpha) = 0$. Tal polinomio $f(x)$ de $k[x]$ es el de menor grado en el cual α es raíz, y está determinado de forma única, salvo múltiplos de escalares en $k[x]$.

Demostración. Ver Jara (2017), p. 10, Proposición 2.7.

El polinomio de la proposición anterior puede ser tomado como mónico, así estar unívocamente determinado, se llamará polinomio mónico irreducible de α sobre k, y se denota por $\mathrm{Irr}(\alpha, k, x)$ o $\mathrm{Irr}(\alpha, k)$.

La definición más importante de esta sección es la norma de un elemento, que se da en términos de una extensión de cuerpos particular.

Definición 2.29. Un polinomio $f \in k[x]$ es separable sobre k si sus factores irreducibles sobre k tienen todas sus raíces simples. Jara (2017).

Definición 2.30. Dada una L/k una extensión de cuerpos, un elemento algebraico $\alpha \in L$ será un elemento separable sobre k si el polinomio $\mathrm{Irr}(\alpha, k)$ es separable. Jara (2017).

Definición 2.31. Una extensión algebraica L/k es una extensión separable si cada elemento de L es separable sobre k. Jara (2017).

Como las extensiones separables son algebraicas, se ve un tipo de extensión algebraica muy particular.

Teorema 2.32. Sea k un cuerpo. Las siguientes condiciones son equivalentes:

1. Toda extensión algebraica de k es trivial, es decir, de grado 1.
2. Todo polinomio irreducible $q(x) \in k[x]$ es de grado 1.
3. Todo polinomio no constante $p(x) \in k[x]$ tiene todas sus raíces en k.
4. Todo polinomio no constante $p(x) \in k[x]$ tiene alguna raíz en k.

Demostración. Ver Navarro (2013), p. 403, Apéndice J, Teorema J.1.1.

Definición 2.33. Un cuerpo será algebraicamente cerrado si satisface alguna condición del teorema anterior. Una extensión $\bar{k}$ de un cuerpo k será el cierre algebraico de k si $\bar{k}$ es un cuerpo algebraicamente cerrado y es una extensión algebraica. Navarro (2013).

Por el teorema de D'Alembert (1717-1783), también llamado Teorema fundamental del Álgebra, los números complejos es un cuerpo algebraicamente cerrado, y como es una extensión finita de los números reales, esto implica que $\mathbb{C}$ es *el* cierre algebraico de $\mathbb{R}$.

Se verán algunos resultados interesantes que tienen que ver con los cuerpos algebraicamente cerrados y su existencia.

Teorema 2.34. (De existencia). Todo cuerpo no trivial posee un cierre algebraico.

Demostración. Ver Navarro (2013), p. 404, Apéndice J.

Teorema 2.35. Sea $\bar{k}$ un cierre algebraico de un cuerpo k. Para toda extensión algebraica K de k, existe un morfismo inyectivo $K \to \bar{k}$.

Demostración. Ver Navarro (2013), p. 405, Apéndice J, Teorema J.1.2.

Teorema 2.36. (de unicidad). El cierre algebraico de un cuerpo k es único salvo isomorfismos.

Demostración. Ver Navarro (2013), p. 405, Apéndice J.

Una vez se tiene la seguridad de la existencia y unicidad de un cierre algebraico de un cuerpo k, se puede ver la norma de los elementos de una extensión.

Como las extensiones tienen una estructura de espacio vectorial, si se tienen las extensiones F/k y E/k entonces la notación $\mathrm{Hom}_{\mathrm{k}}(F, E)$ es largamente entendida, pero en el contexto de ser anillos, el conjunto denotado por $\mathrm{Hom}(F/k, E/k)$ será el de los morfismos de cuerpos (anillos) de F/k a E/k.

Lema 2.37. Sea F/k una extensión finita y $\bar{k}$ el cierre algebraico de k que contiene a F, las siguientes condiciones son equivalentes:

1. $|\mathrm{Hom}(F/k, \bar{k}/k)| = [F: k]$.
2. F/k es separable.

Demostración. Ver Jara (2017), p. 94, Lema 7.5.

El lema anterior dice que para una extensión F/k finita y separable con $[F: k] = n$ y cierre algebraico $\bar{k}$, se tiene:

$$\mathrm{Hom}(F/k, \bar{k}/k) = \{\sigma_1, \dots, \sigma_n\}.$$

Definición 2.38. Sea F/k una extensión finita y separable con $[F: k] = n$ y $\bar{k}$ cierre algebraico que contiene a F, para $\alpha \in F$ la norma de α relativa a F/k, representada por $\mathrm{Nm}_{F/k}(\alpha)$, es:

$$\mathrm{Nm}_{F/k}(\alpha) = \prod \{\sigma_i(\alpha) : \ 1 \leq i \leq n\}.$$

Jara (2017).

Proposición 2.39. Sea F/k una extensión separable de grado n y finita, se cumple:

1. $\mathrm{Nm}_{F/k}(\alpha\beta) = \mathrm{Nm}_{F/k}(\alpha)\mathrm{Nm}_{F/k}(\beta)$, para cada $\alpha, \beta \in F$.
2. $\mathrm{Nm}_{F/k}(a) = a^n$, para cada $a \in k$.
3. $\mathrm{Nm}_{F/k}(\alpha) \in k$ para cada $\alpha \in F$.

Demostración. Ver Jara (2017), p. 189, Proposición 14.2.

A continuación, una extensión que involucra a los elementos trascendentes.

Definición 2.40. Sea Σ una extensión de k. Los elementos $\alpha_1, \dots, \alpha_n \in \Sigma$ son algebraicamente independientes sobre k si el morfismo $k[x_1, \dots, x_n] \to \Sigma$, definida por $x_i \mapsto \alpha_i$, es inyectivo; es decir, de tener cualquier relación

$$\sum_{i_1,\dots,i_n} a_{i_1 \dots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} = 0$$

con coeficientes en k, esta se cumple solo cuando todos los coeficientes son nulos.

Navarro (2013).

Es claro que los elementos $\alpha_1, \dots, \alpha_n$ son trascendentes en k.

Definición 2.41. Los elementos $\alpha_1, \dots, \alpha_n \in \Sigma$ formarán una base de trascendencia de Σ sobre k si son algebraicamente independientes y Σ es una extensión algebraica de $k(\alpha_1, \dots, \alpha_n)$; en efecto, los elementos son algebraicamente independientes sobre k y $k(\alpha_1, \dots, \alpha_n)$ no puede ampliarse con ningún elemento de Σ sin que sigan siendo algebraicamente independientes sobre k. Navarro (2013).

La cardinalidad de una base de trascendencia sobre un cuerpo k no es un resultado obvio en sí mismo, el siguiente teorema asegura que, de existir, entonces, estas tienen el mismo número.

Teorema 2.42. Para toda extensión Σ de un cuerpo k, generada por una cantidad finita de elementos, existen bases de trascendencia de Σ sobre k. Estas poseen el mismo número de elementos, y se denomina grado de trascendencia de Σ sobre k.

Demostración. Ver Navarro (2013), p. 405, Apéndice J, Teorema J.2.1.

Se hace una digresión más, se verá una idea sencilla, que en el capítulo 4 estará totalmente formalizada. Si k es un cuerpo, también es dominio de integridad, luego por Proposición 2.23, el anillo $k[x_1, \dots, x_n]$ también es dominio de integridad, que como se verá a continuación, generará un cuerpo denotado por $k(x_1, \dots, x_n)$; un cálculo muestra que las n indeterminadas son algebraicamente independientes y forman una base de trascendencia. Por lo que si el anillo de polinomios $k[x_1, \dots, x_n]$ estuviera asociado a un espacio geométrico, un número que nos indique "su dimensión" tendría que ver con su grado de trascendencia, recordando que la idea intuitiva de dimensión siempre tiene que ver con independencia de coordenadas o vectores, etc.

2.1.4. Localización

En esta sección se muestra la construcción de los anillos con elementos fraccionarios, sistematizado por Claude Chevaley (1909-1984), de manera análoga a la construcción de $\mathbb{Q}$. La importancia de la construcción de estos anillos (que llegarán a ser también cuerpos) será notoria en el tema de variedades algebraicas. Este proceso de localización también es muy importante en otras ramas de la matemática.

Definición 2.43. Sea A un anillo. Un subconjunto $S \subset A$ es un sistema multiplicativo si $1 \in S$ y $a, b \in S \Rightarrow ab \in S$. Navarro (2013).

Si S es un sistema multiplicativo de A, para la construcción del anillo de fracciones con numerador de elementos en A y denominador en S; definimos en $A \times S$ la siguiente relación de equivalencia:

$$(a, s) \equiv (b, t) \Leftrightarrow \exists\, u, v \in S : au = bv \wedge su = tv,$$

en algunos casos se usa su equivalente: $(a, s) \equiv (b, t) \Leftrightarrow \exists\, u \in S : (at - bs)u = 0$.

Definición 2.44. Sea S un sistema multiplicativo de A. Se denomina como anillo de fracciones o localización de A por S, denotado $S^{-1}A$ o A_S, al conjunto cociente $(A \times S) \equiv$ junto a las operaciones:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st},$$

donde $a/s = \pi(a, s)$ y $\pi: A \times S \to (A \times S)/\equiv$ es la proyección. Navarro (2013).

Es claro que las dos operaciones definen en $(A \times S) \equiv$ una estructura de anillo, el cero es $0/1$, la unidad es $1/1$ y el opuesto de a/s es $(-a)/s$.

La aplicación $\gamma: A \to S^{-1}A$, definida por $\gamma(a) = a/1$ es morfismo de anillos, y vuelve invertible a todo $s \in S$, pues su inverso es $1/s$. El morfismo canónico $\gamma: A \to S^{-1}A$ se llama morfismo de localización. Lo anterior generaliza la construcción de los números racionales $\mathbb{Q}$ a partir de $\mathbb{Z}$, con $S = \mathbb{Z} - 0$.

Es sencillo verificar que el complemento de un ideal primo $\mathfrak{p} \subset A$ es multiplicativo. En este caso usamos la notación $A_{\mathfrak{p}} \coloneqq S^{-1}A$.

Teorema 2.45. Sea A un dominio de integridad y $S = A - 0$ multiplicativo, entonces el anillo $S^{-1}A \coloneqq K(A)$ es un cuerpo, denominado cuerpo de fracciones de A, y el morfismo de localización $\gamma: A \to S^{-1}A$ es inyectivo.

Demostración. Ver Navarro (2013), p., 85, Teorema 5.1.1.

Como en un dominio de integridad A el ideal $0 \subset A$ es primo, se puede considerar, $A_0 = K(A)$ es el cuerpo de fracciones de A. Por otro lado, si $f \in A$ no es cero y $S = \{f^n : n \geq 0\}$, entonces claramente S es multiplicativo. En tal caso se usa la notación $A_f \coloneqq S^{-1}A$.

Lema 2.46. (Rabinowitsch). Sea A_f es la localización de A con respecto al conjunto multiplicativo $S = \{f^n : n \geq 0\}$, con $f \in A$, entonces la función

$$A[t]/\langle ft - 1\rangle \to A_f$$

dada por $a_n t^n + \cdots + a_1 t + a_0 \mapsto a_n/f^n + \cdots + a_1/f \ + a_0$ es un isomorfismo.

Demostración. Ver Zaldívar (s.f.), p. 23, Lema 1.26.

2.1.5. Módulos y álgebras

Definición 2.47. Sea A un anillo conmutativo y sea M un grupo conmutativo. Una aplicación $A \times M \to M$ define en M una estructura de *A-módulo* si cumple los siguientes axiomas:

1. $a \cdot (m + n) = a \cdot m + a \cdot n$
2. $(a + b) \cdot m = a \cdot m + b + \cdot m$
3. $(ab) \cdot m = a \cdot (b \cdot m)$
4. $1 \cdot m = m$ para todo $a, b, 1 \in A$; $m, n \in M$. Navarro (2013).

Como todo ideal I de un anillo es cerrado bajo el producto por elementos de A, esto define en I una estructura de A-módulo. En particular, el propio A es un A-módulo.

Definición 2.48. Sea M un A-modulo. Un subconjunto $N \subset M$ será un submódulo si:

1. Si $a, b \in \Rightarrow a - b \in N$.
2. Si $a \in A$ y $n \in N \Rightarrow an \in N$. Solotar et al. (2007).

Siguiendo la definición, si N es un submódulo de un A-módulo M, entonces N es un A-módulo.

Un A-módulo M es de tipo finito o finitamente generado si existen $m_1, \dots, m_n \in M$ tales que $(m_1, \dots, m_n) = M$.

Definición 2.49. Sea A un anillo. Un álgebra B sobre A, o una A-álgebra, es un anillo B junto a un morfismo de anillos $j: A \to B$. Dada una A-álgebra B, el morfismo j dota a B una estructura de A-módulo: $a \cdot b = j(a)b, a \in A, b \in B$. Por lo que, $j(a)$ se denotará a cuando no origine confusión.

Dadas dos A-álgebras $j: A \to B$ y $j': A \to C$. Una aplicación $f: B \to C$ es un morfismo de A-álgebras si $f(a) = a$ para todo $a \in A$ y es morfismo de anillos, $j' = f \circ j$. Es decir, cuando f es morfismo de anillos y de A-módulos. El conjunto de los morfismos de A-álgebras de B en C se denota $\mathrm{Hom}_{\text{A-alg}}(B, C)$.

Se dice que un morfismo de A-álgebras es un isomorfismo si admite un morfismo de A-álgebras inverso. Navarro (2013).

Es claro que las composiciones de morfismos de A-álgebras también son morfismos y los isomorfismos de A-álgebras son morfismos biyectivos.

Definición 2.50. Un subanillo C de una A-álgebra B es una subálgebra cuando $A \subset C$, es decir, cuando C contiene la imagen de morfismo $j: A \to B$. Navarro (2013).

La intersección de subálgebras de una A-álgebra B también lo es. La subálgebra de B generada por elementos $b_1, \dots, b_n \in B$ es

$$A[b_1, \dots, b_n] \coloneqq \{p(b_1, \dots, b_n) : p \in A[x_1, \dots, x_n]\},$$

y resulta ser la menor subálgebra que los contiene.

2.1.6. Anillos Noetherianos

El siguiente objeto lleva su nombre en honor a Emmy Noether (1882-1935).

Definición 2.51. Sea A un anillo. Un A-módulo M es noetheriano, si todo submódulo de M es finitamente generado. Un anillo A es noetheriano si lo es como A-módulo; esto es, todos sus ideales son de tipo finito. Navarro (2013).

En particular, como condición necesaria ser noetheriano implica que él mismo módulo M es de tipo finito.

Si A es DIP, entonces es A-módulo noetheriano, también todo k-espacio vectorial V de dimensión finita es noetheriano. En el caso de anillos noetherianos; $\mathbb{Z}$ y $k[x]$ son anillos noetherianos porque son DIP. Todo cuerpo es noetheriano, en el sentido que solo posee sus dos ideales triviales 0 y él mismo. El anillo con numerables indeterminadas $k[x_1, \dots, x_n]$ es un anillo que no es noetheriano, pero como puede construírsele su cuerpo de fracciones, $k[x_1, \dots, x_n]$ puede considerarse como subanillo de su cuerpo de fracciones. Así se tiene un ejemplo de un subanillo no noetheriano contenido en un anillo noetheriano, patología que no ocurre con los ideales.

Ahora se presenta una caracterización de estos módulos de vital importancia en la teoría (variedades algebraicas).

Proposición 2.52. Sea A un anillo y M un A-módulo. Son equivalentes:

1. M es noetheriano.
2. Toda sucesión no vacía y creciente de submódulos se estabiliza.
3. Todo conjunto no vacío de submódulos de M tiene un elemento maximal respecto a la inclusión.

Demostración. Ver Solotar-Farinati et al. (2007), p. 129, Proposición 4.1.4.

El siguiente teorema muestra la noetherianidad de un anillo.

Teorema 2.53. (Teorema de la base de Hilbert) Si A es un anillo noetheriano, entonces $A[x]$ es un anillo noetheriano.

Demostración. Ver Solotar-Farinati et al. (2007), p. 133, Teorema 4.2.1.

Corolario 2.54. De ser A es un anillo noetheriano y $n \in \mathbb{N}$, entonces el anillo $A[x_1, \dots, x_n]$ es anillo noetheriano.

Demostración. Usando inducción al Teorema de la base de Hilbert. ■

En particular, si k es un cuerpo, entonces $k[x_1, \dots, x_n]$ es noetheriano.

2.1.7. Extensiones enteras

Se dará un vistazo a los enteros algebraicos sobre un anillo, esta teoría es equivalente al de los elementos algebraicos sobre un cuerpo. La necesidad de esta teoría surge en situaciones en las que se trabaje con anillos, pero, no se pueda pasar a sus cuerpos de fracciones.

Sean $A \subseteq B$ anillos de manera que B es una A-álgebra.

Definición 2.55. Se dice que B es una A-álgebra finita si B es finitamente generado como A-módulo, es decir, si existen $\alpha_1, \dots, \alpha_n \in B$ tales que todo $b \in B$ es una combinación lineal:

$$b = a_1\alpha_1 + \cdots + a_n\alpha_n : a_i \in A.$$

Zaldívar (s.f.).

Definición 2.56. Se dice que B es de tipo finito sobre A si existen $\alpha_1, \dots, \alpha_n \in B$ tales que todo elemento $b \in B$ puede expresarse como un polinomio en los α_i con coeficientes en A, es decir, existe un polinomio $f \in A[x_1, \dots, x_n]$ tal que $b = f(\alpha_1, \dots, \alpha_n)$. Zaldívar (s.f.).

Definición 2.57. Si $b \in B$, se dice que b es entero algebraico sobre A si existe un polinomio

$$\phi(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in A[x]$$

tal que $\phi(b) = 0$. Si todo elemento de B es entero sobre A, se dirá que B es entero sobre A.

Zaldívar (s.f.).

De las dos definiciones, ser A-álgebra finita implica ser de tipo finito vía el polinomio de primer grado $f(x) = a_1x_1 + \cdots + a_nx_n$. También, B es una A-álgebra de tipo finito si y solo si existe un morfismo sobreyectivo de A-álgebras

$$\varphi: A[x_1, \dots, x_n] \to B$$

definiendo por $\alpha_i = \varphi(x_i)$.

En una inclusión de anillos $A \subset B$, todo elemento α de A es entero sobre A gracias al polinomio mónico $x - \alpha \in A[x]$. La definición que se acaba de dar es una generalización del contexto de los números enteros y racionales, los números racionales que son *enteros* son justamente los elementos de $\mathbb{Z}$.

Los enteros algebraicos, al tener una equivalencia con los elementos algebraicos sobre un cuerpo, deben cumplir la existencia de un anillo formado por enteros algebraicos, ese es el propósito del siguiente lema y sus corolarios.

Lema 2.58. Sean $A \subset B$ anillos y $\alpha \in B$. Las siguientes condiciones son equivalentes:

1. α es entero sobre A.
2. Existe un subanillo C con $A \subset C \subset B$ tal que $\alpha \in C$ y C es finitamente generado como A-módulo.
3. El subanillo $A[\alpha] \subset B$ es finitamente generado como A-módulo.

Demostración. Ver Zaldívar, (s.f.), p. 18, Lema 1.16 o ver Atiyah y MacDonald (1978), p. 66, Proposición 5.1.

Corolario 2.59. Si $A \subset B$ son anillos y $\alpha_1, \ldots, \alpha_n \in B$ son enteros sobre A, entonces $A[\alpha_1, \ldots, \alpha_n]$ es un A-módulo finitamente generado.

Demostración. Utilizar el lema anterior e inducción. ■

Corolario 2.60. El conjunto de los elementos enteros de B sobre A es estable (o cerrado) bajo la suma y producto, es decir, $\alpha \pm \beta$ y $\alpha\beta$ son enteros sobre A, si $\alpha, \beta \in B$ son enteros sobre A.

Demostración. Utilizar los últimos dos resultados. ■

Corolario 2.61. Si $A \subset B$ son anillos y $\bar{A} = \{\alpha \in B : \alpha \text{ es entero sobre } A\}$, entonces $\bar{A}$ es un anillo tal que $A \subset \bar{A} \subset B$.

Demostración. Directo de corolario anterior. ■

Definición 2.61. El anillo $\bar{A}$ se denomina cerradura entera de A en B. Si además A es igual a su cerradura entera se dice que A es integralmente cerrado en B. Si A es un dominio de integridad, su cerradura entera en su cuerpo de fracciones se llama la cerradura entera de A. Si A es integralmente cerrado en su cuerpo de fracciones, decimos que A es integralmente cerrado. Zaldívar (s.f.).

Una herramienta central en este trabajo es lema de normalización de Noether, el siguiente resultado permitirá demostrarlo.

Corolario 2.62. (Transitividad de la dependencia entera) Si $A \subset B \subset C$ son anillos y si B es entero sobre A y C es entero sobre B, entonces C es entero sobre A.

Demostración. Ver Atiyah y MacDonald (1978), p. 67, Corolario 5.4.

El siguiente corolario muestra una relación entre las álgebras finitas y de tipo finito.

Corolario 2.63. Si $A \subset B$ son anillos, se tienen las condiciones equivalentes:

1. B es una A-álgebra de tipo finito y es entero sobre A.
2. B es una A-álgebra finita.

Demostración. Ver Zaldívar (s.f.), p. 20, Lema 1.20.

Proposición 2.64. Sea $A \subset K \subset L$, con A dominio de integridad, K su cuerpo de fracciones y L otro cuerpo. Si $\alpha \in L$ es algebraico sobre K, existe un $d \in A$ tal que $d\alpha$ es entero sobre A.

Demostración. Ver Zaldívar (s.f.), p. 20, Lema 1.21.

El siguiente resultado, dado por Zariski, servirá al momento de demostrar el teorema de los ceros de Hilbert.

Corolario 2.65. (Lema de Zariski) Si $K \subset L$ son cuerpos con L de tipo finito, entonces L/K es una extensión algebraica.

Demostración. Ver Zaldívar (s.f.), p. 20, Lema 1.22.

Es claro que L/K es una extensión finita.

2.1.8. Nilpotencia, ideal radical

La nilpotencia siempre ha sido una propiedad poco deseada por los matemáticos. Especialmente en teoría de álgebras la presencia de estos elementos desencadena en ellos complicaciones o situaciones complejas. La existencia de estos elementos se puede ver por ejemplo en el anillo de matrices, sin embargo, también existen anillos que carecen de él, como los cuerpos.

Se tuvieron que hacer profundos estudios de la estructura misma de los anillos para conocer, y en medida, evitar estos elementos a través de construcciones; uno de los matemáticos involucrados en este desarrollo es el americano Nathan Jacobson (1910-1999), reconocido como uno de los principales algebristas de su generación, su apellido acompaña muchos teoremas y conjeturas. El radical de Jacobson, en su honor, es la intersección de los ideales maximales de un anillo A.

Al inicio del capítulo 2 se trabaja con el ideal que se está por definir, los siguientes resultados aseguran que podemos construir anillos que carezcan de elementos nilpotentes.

Definición 2.66. Sea I un ideal de un anillo R. El radical de I, denotado por $\sqrt{I}$, es la colección de elementos de R en el que alguna potencia pertenece a I, i.e.,

$$\sqrt{I} = \{a \in A : a^m \in I \text{ para algún } m \geq 1\}.$$

El radical del ideal nulo 0 es llamado Nilradical de R. Un ideal I es llamado ideal radical si: $I = \sqrt{I}$. Dummit y Foote (2004).

Proposición 2.67. Sea I un ideal de un anillo conmutativo R. Entonces $\sqrt{I}$ es un ideal que contiene a I y $\sqrt{I}/I$ es el nilradical del anillo R/I. En particular, $I=\sqrt{I}$ es un ideal radical si y solo si R/I no tiene elementos nilpotentes.

Demostración. Es claro que $I\subset\sqrt{I}$. Para la segunda parte, se empieza probando que el nilradical N de cualquier anillo R es un ideal. Es obvio que $0\in N$, sea $a\in R$ y $p\in N\Rightarrow p^m=0$, para algún m. Luego $(ap)^m=a^m p^m=a^m 0=0\Rightarrow ap\in N$. Por último, sean $a,b\in N\Rightarrow a^n=0, b^m=0$ para algunos m,n, luego

$$(a-b)^{m+n}=\sum_{k=0}^{m+n}(-1)^k\binom{m+n}{k}a^{m+n-k}b^k=0\Rightarrow a-b\in N$$

ya que cada sumando posee al menos una potencia de a o b que se anula.

En el caso particular del nilradical N del anillo R/I, por el teorema de correspondencia (2.10), está asociado a un ideal que contiene a I, luego:

$$\pi^{-1}(N)=\{a\in R:\pi(a)\in N\}=\{a\in R:\bar{a}^m=\bar{0}\text{ , para algún } m\}$$
$$=\{a\in R:\overline{a^m}=\bar{0}\text{ , para algún } m\}=\{a\in R:a^m\in I\text{ , para algún } m\}=\sqrt{I}.$$

Por lo tanto $\sqrt{I}$ es un ideal y además el nilradical de R/I es $N=\sqrt{I}/I$.

Finalmente, R/I no tiene elementos nilpotentes $\Leftrightarrow\sqrt{I}/I=\bar{0}$, y $\bar{0}=I/I$, luego $\sqrt{I}/I=I/I\Leftrightarrow\sqrt{I}=I\Leftrightarrow I$ es ideal radical.■

Proposición 2.68. La intersección de todos los ideales primos que contienen a I es el radical de un ideal propio I. En particular, la intersección de todos los ideales primos en R es el nilradical.

Demostración. Se empieza con este resultado. Se denota por N' la intersección de todos los ideales primos de un anillo R y N el nilradical, se demostrará $N'=N$.

Sea P un ideal primo arbitrario. Sea $a \in N$, desde que existen un m tal que $a^m = 0$ luego existe el mínimo n tal que $a^n = 0 \in P$, así por ser P ideal primo: $a^{n-1} \in P \vee a \in P$, pero a^{n-1} contradice la minimalidad de n, así $a \in P$, para todo ideal primo $P \Rightarrow a \in N'$. Por lo tanto $N \subset N'$.

Recíprocamente, si $a \notin N$ y sea S la familia de ideales propios que no contiene alguna potencia de a; $S \neq \emptyset$ ya que $\{0\} \in S$. Además, si a^k no está contenido en los ideales de la cadena $I_1 \subset I_2 \subset \cdots$, entonces a^k no está contenido en la unión de esos ideales, lo que muestra que toda cadena en S tiene una cota superior. Por el lema de Zorn, S tiene un elemento maximal, puede denotarse como M'. Se afirma que el ideal M' es un ideal primo. En efecto, sean $x, y \notin M'$, si $xy \in M'$, por la maximalidad de M', $a^n \in (x) + M'$ y $a^m \in (y) + M'$ para algunos m, n (si no ocurriera esto M' no sería maximal porque lo contendría $(x) + M'$ por ejemplo). Luego

$$a^{m+n} \in (xy) + (x)M' + (y)M' + M' = (xy) + M' = M'$$

que contradice el hecho que M' es un ideal que no potencia de $a \Rightarrow xy \notin M'$, que es la condición equivalente de un ideal primo. Por lo tanto M' es ideal primo. Finalmente

$a^t \notin M'$ para algún t, por ser elemento (aún más maximal) de S entonces

$a^k = aa^{k-1} \notin M' \Rightarrow a^{k-1} \notin M'$ y $a \notin M'$. Es decir, existe un ideal primo que no contiene a a, luego $a \notin N'$ Por lo tanto $a \notin N \Rightarrow a \notin N'$ equivale a $N' \subset N$.

Ahora se usa este resultado para demostrar la proposición. Sea I un ideal propio de R, en el anillo cociente R/I su nilradical $\sqrt{I}/I$ es igual a la intersección a todos los ideales primos de R/I, pero por teorema de correspondencia, estos ideales primos en R/I se corresponden con los ideales primos que contienen a I; por lo tanto, se puede afirmar: $\sqrt{I}$ es la intersección de todos los ideales primos que contienen a I.■

Corolario 2.69. Todo ideal primo (y de aquí también maximal) es ideal radical.

Demostración. Sea P ideal primo, luego $\sqrt{P}$ es la intersección de todos los ideales primos que contienen P, pero el mismo P es ideal primo $\Rightarrow \sqrt{P} = P$, es decir P es ideal radical. ■

VARIEDADES ALGEBRAICAS

2.1.9. El espacio afín

Esta sección empieza definiendo el espacio geométrico, se buscará una relación biunívoca entre términos algebraicos y geométricos. Esto servirá para describir propiedades topológicas del espacio geométrico en términos de subconjuntos (ideales) de la estructura algebraica (anillo) asociada.

Definición 2.70. Sea k un cuerpo. El espacio afín de dimensión n sobre k es:

$$\mathbb{A}^n = \mathbb{A}_k^n = \mathbb{A}^n(k) \coloneqq \{(a_1, \ldots, a_n) : a_i \in k\}.$$

Zaldívar (s.f.).

Definición 2.71. Si $E \subset k[x_1, \ldots, x_n]$, se denomina conjunto algebraico afín, o un conjunto afín a:

$$\mathcal{V}(E) \coloneqq \{P = (a_1, \ldots, a_n) \in \mathbb{A}_k^n : f(P) = 0 \text{ para todo } f \in E\}$$

que vienen a ser los ceros comunes, en $\mathbb{A}_k^n$, de los polinomios en E. Al anillo de polinomios se le llama anillo de coordenadas del espacio afín. Zaldívar (s.f.).

Si $I = \langle E \rangle$ es el ideal de $k[x_1, \ldots, x_n]$ generado por E, entonces $\mathcal{V}(E) = \mathcal{V}(I)$. Esto dice que al definir conjuntos algebraicos afines basta considerar ideales de $k[x_1, \ldots, x_n]$. La letra $\mathcal{V}$ viene del inglés “vanishing” que se entiende como “convertirse en cero”, el vanishing de un conjunto E hace referencia a $\mathcal{V}(E)$.

A continuación las propiedades de los conjuntos algebraicos $\mathcal{V}(I)$:

Lema 2.72. Sea k un cuerpo. Entonces:

1. $\mathbb{A}_k^n$ y $\emptyset$ son conjuntos algebraicos afines.
2. Si $V_1, \dots, V_s$ son conjuntos algebraicos, entonces $V_1 \cup \cdots \cup V_s$ es afín.
3. Dada una familia $\{V_i\}$ de conjuntos afines, entonces $\bigcap_i V_i$ es afín.
4. Si $I_1 \subset I_2$ son ideales de $k[x_1, \dots, x_n]$, entonces $\mathcal{V}(I_2) \subset \mathcal{V}(I_1)$.
5. Si $I \subset k[x_1, \dots, x_n]$ es cualquier ideal, entonces $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.

Demostración.

1. Se tiene $\mathbb{A}_k^n = \mathcal{V}(0)$, donde 0 es el ideal nulo que vuelve cero a todo elemento del espacio afín. Por otro lado, $\emptyset = \mathcal{V}(1)$ ya que al ser 1 polinomio constante ningún punto del espacio afín lo anulará y como observación, la unidad 1 genera todo el anillo:$(1) = k[x_1, \dots, x_n]$.

2. Basta probar para $s = 2$, si $V_1 = \mathcal{V}(I), V_2 = \mathcal{V}(J)$.

Afirmación: $V_1 \cup V_2 = \mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$.

En efecto, sea $P \in \mathcal{V}(I) \cup \mathcal{V}(J) \Rightarrow P \in \mathcal{V}(I) \vee P \in \mathcal{V}(J)$ entonces $f(P) = 0,\ \forall f \in I \vee f(P) = 0,\ \forall f \in J$; y como $I \cap J$ está contenido en ambos conjuntos tendremos: $f(P) = 0$, $\forall f \in I \cap J \Rightarrow P \in \mathcal{V}(I \cap J)$. Para la otra contención, si $P \notin \mathcal{V}(I) \cup \mathcal{V}(J) \Rightarrow P \notin \mathcal{V}(I) \wedge P \notin \mathcal{V}(J)$ entonces existen polinomios f, g en I y J respectivamente tal que: $f(P) \neq 0, g(P) \neq 0 \Rightarrow (fg)(P) \neq 0$; además es claro $fg \in I \cap J$ entonces se deduce que: $P \notin \mathcal{V}(I \cap J)$. Por lo que se tiene: $P \notin \mathcal{V}(I) \cup \mathcal{V}(J) \Rightarrow P \notin \mathcal{V}(I \cap J)$ que es equivalente a: $P \in \mathcal{V}(I \cap J) \Rightarrow P \in \mathcal{V}(I) \cup \mathcal{V}(J)$.

3. Si $V_i = \mathcal{V}(I_i)$, afirmamos: $\bigcap_i V_i = \mathcal{V}(\sum_i I_i)$.

Sea $P \in \bigcap_i V_i \Rightarrow P \in V_i, \forall i \Rightarrow h(P) = 0,\ \forall h \in I_i,\ \forall i$. Ahora sea cualquier f de $\sum_i I_i \Rightarrow f = \sum_{i=1}^m g_i\, h_i$; para $g_i \in k[x_1, \dots, x_n], h_i \in I_i$ y evaluando en P:

$$f(P) = \sum_{i=1}^{m} g_i\,(P) h_i(P) = \sum_{i=1}^{m} g_i\,(P) 0 = 0 \Rightarrow P \in \mathcal{V}\left(\sum_i I_i\right).$$

Sea $P \in \mathcal{V}(\sum_i I_1) \Rightarrow f(P) = 0$, $\forall f \in \sum_i I_i$, pero $I_i \subset \sum_i I_i\,, \forall i$ por lo que en particular anula todos los polinomios de I_i entonces $f(P) = 0, \forall f \in I_i, \forall i$ entonces $P \in \mathcal{V}(I_i), \forall i \Rightarrow P \in \bigcap_i \mathcal{V}(I_i)$. Así $\bigcap_i V_i$ es afín.

4. Sea $P \in \mathcal{V}(I_2) \Rightarrow f(P) = 0$, $\forall f \in I_2$, luego se cumple en particular para los polinomios de $I_1 \subset I_2 \Rightarrow g(P) = 0, \forall g \in I_1 \Rightarrow P \in \mathcal{V}(I_1)$.

Para 5. Como $I \subset \sqrt{I} \Rightarrow$ por (4): $\mathcal{V}(\sqrt{I}) \subset \mathcal{V}(I)$. De otro lado, sea $P \in \mathcal{V}(I)$ y sea cualquier $f \in \sqrt{I} \subset \exists m \in \mathbb{N}$ tal que $f^m \in I \Rightarrow \left(f(P)\right)^m = 0 \Rightarrow f(P) = 0 \Rightarrow P \in \mathcal{V}(\sqrt{I})$. Por lo tanto $\mathcal{V}(I) = \mathcal{V}\left(\sqrt{I}\right)$. ■

A continuación se muestra como los conjuntos afines resultan ser los ceros comunes de un conjunto finito de polinomios. Por el teorema de la base de Hilbert, el anillo de coordenadas afín $k[x_1, \dots, x_n]$ del espacio afín es noetheriano, entonces todos sus ideales son finitamente generados, es decir, existen finitos polinomios $\{f_1, \dots, f_s\} \subset E \subset I$ tal que:

$$\mathcal{V}(E) = \mathcal{V}(I) = \mathcal{V}(\{f_1, \dots, f_s\}) = \mathcal{V}(f_1) \cap \dots \cap \mathcal{V}(f_r).$$

Note que esta propiedad "geométrica" en el espacio afín es una consecuencia de una propiedad "algebraica" del correspondiente anillo de coordenadas $k[x_1, \dots, x_n]$.

Ejemplo 1. Las conjuntos algebraicos de la forma $\mathcal{V}(ax^2 + bxy + cy^2 + dx + ey + f)$ de $\mathbb{A}^2_{\mathbb{R}}$ son los respectivos círculos, elipses, parábolas e hipérbolas. Curvas más interesantes son por ejemplo $\mathcal{V}(y^2 - x^3)$ y $\mathcal{V}(y^2 - x^2(x + 1))$. Ver Figura 1.

Ejemplo 2. El conjunto algebraico $\mathcal{V}(y^2 - x(x^2 - 1))$ es una muestra que estas curvas en $\mathbb{A}^2_{\mathbb{R}}$ no necesariamente son conexas. Si se tiene dos conjuntos algebraicos de la forma $V = \mathcal{V}(x^2 + y^2 - 4)$ y $W = \mathcal{V}(x^2 + y^2 - 9)$, por el lema 2.3 (ver la demostración del inciso 2):

$$V \cup W = \mathcal{V}(x^2 + y^2 - 4) \cup \mathcal{V}(x^2 + y^2 - 9) = \mathcal{V}((x^2 + y^2 - 4) \cap (x^2 + y^2 - 9))$$

pero como

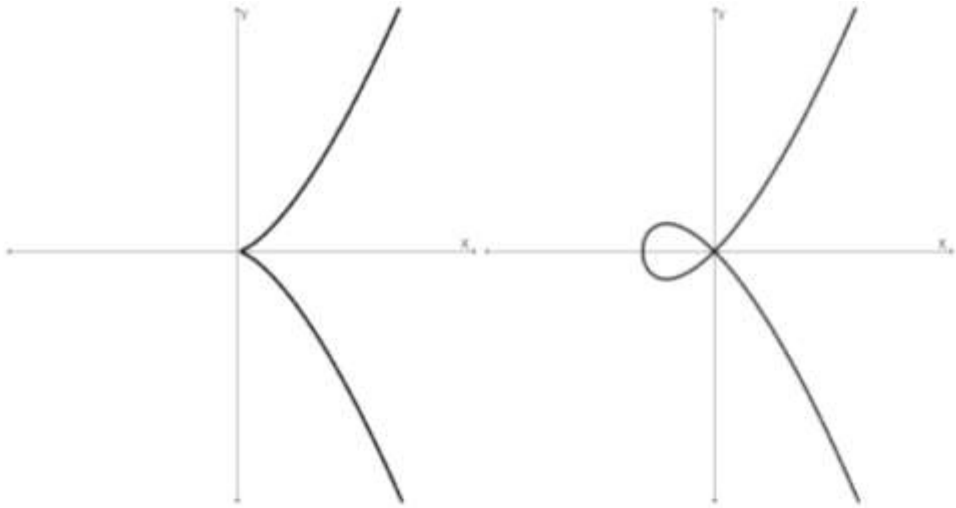
$$\langle (x^2+y^2-4)(x^2+y^2-9)\rangle = (x^2+y^2-4) \cap (x^2+y^2-9),$$

entonces

$$V \cup W = \mathcal{V}\big((x^2+y^2-1)(x^2+y^2-9)\big).$$

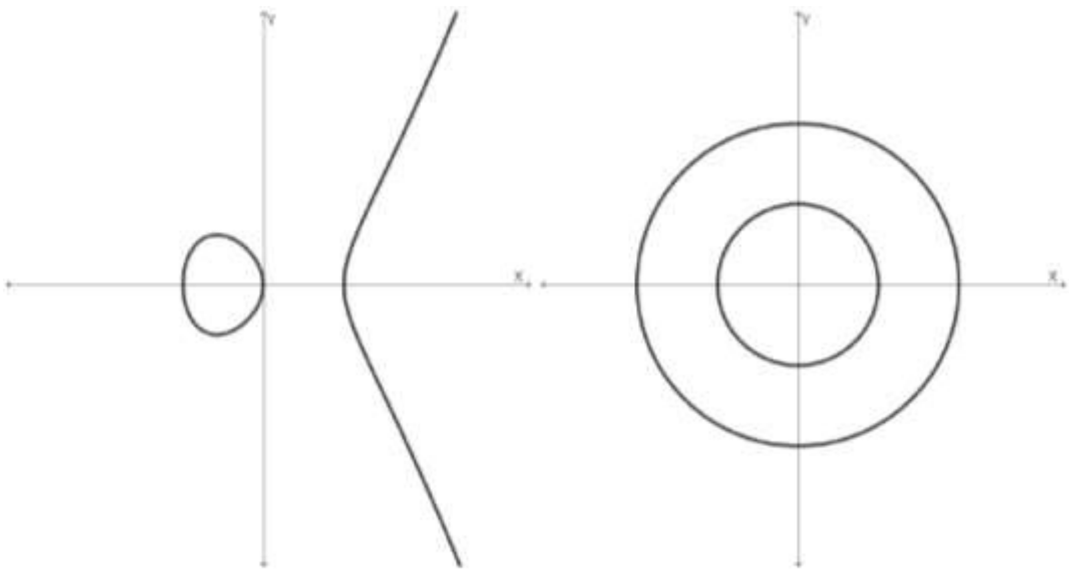
Esta es una forma de construir todo tipo de nuevos conjuntos algebraicos, en este caso $(x^2+y^2-4)(x^2+y^2-9)=0$ define la unión de dos circunferencias. Ver Figura 2.

Figura 1. Ambas curvas son conexas.



(a) La curva cúspide (b) La curva alfa

Figura 2. Ambas curvas son no conexas.



(a) Curva de polinomio grado 3 (b) Circunferencias concéntricas

Ejemplo 3. Si $p_1, p_2 \in \mathbb{R}[x,y]$, entonces $\mathcal{V}(p_1, p_2)$, representa la solución simultánea de dos ecuaciones polinomiales. Por ejemplo, el conjunto algebraico $\mathcal{V}(x,y) = \{(0,0)\} \subset \mathbb{A}^2_{\mathbb{R}}$, mientras $\mathcal{V}(x^2 + y^2 - 1, x - y)$ es el conjunto conformado por $\{(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}), (-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2})\}$ en $\mathbb{A}^2_{\mathbb{R}}$.

Ejemplo 4. En $\mathbb{A}^3_{\mathbb{R}}$, cualquier cónica es un subconjunto algebraico afín, por ejemplo la esfera $\mathcal{V}(x^2 + y^2 + z^2 - r^2)$, el cilindro $\mathcal{V}(x^2 + y^2 - r^2)$, el hiperboloide $\mathcal{V}(x^2 - y^2 - z^2 - r)$. Una circunferencia en $\mathbb{A}^3_{\mathbb{R}}$ es también un conjunto algebraico afín, siendo representado, por ejemplo, como $\mathcal{V}(x^2 + y^2 + z^2 - 1, x)$ (geométricamente es la intersección de una esfera y el plano YZ). Cualquier punto $(a,b,c) \in \mathbb{A}^3_{\mathbb{R}}$ es la variedad $\mathcal{V}(x - a, y - b, z - c)$ (geométricamente la intersección de los planos $x = a$, $y = b$, $z = c$).

El lema 2.3 además nos dice: La unión finita de conjuntos algebraicos afines también es afín, la intersección de conjuntos algebraicos afines es afín, $\emptyset$ y $\mathbb{A}^n_k$ son afines; es decir, los conjuntos afines tienen el comportamiento de conjuntos cerrados en (por lo que definen) una topología, conocida como la *Topología de Zariski* de $\mathbb{A}^n_k$.

Definición 2.73. La Topología de Zariski en el espacio afín de dimensión n sobre k es la topología en la cual los conjuntos cerrados son conjuntos algebraicos afín en $\mathbb{A}^n_k$.

Dummit, Foote (2004)

La topología de Zariski en un conjunto algebraico (afín) $X \subset \mathbb{A}^n_k$ es la inducida por la inclusión como subespacio topológico, así un subconjunto $X' \subset X$ es cerrado en X si y solo si $X' = X \cap V$; con $V \subset \mathbb{A}^n_k$ un conjunto algebraico afín, luego por (3) del lema anterior X' es cerrado en $\mathbb{A}^n_k$. Es decir, en la topología de Zarisiki los cerrados de un conjunto algebraico también son conjuntos algebraicos en el espacio afín.

Ahora se relaciona un subconjunto X de $\mathbb{A}^n_k$ con un ideal de $k[x_1, \ldots, x_n]$ de la siguiente manera:

Definición 2.74. Dado $X \subset \mathbb{A}_k^n$. El ideal asociado a X en $k[x_1, \dots, x_n]$ es:

$$\mathcal{J}(X) := \{f \in k[x_1, \dots, x_n] : f(P) = 0 \text{ para todo } P \in X\}.$$

Zaldívar (s.f.).

Este conjunto goza de las propiedades.

Lema 2.75. Sea k un cuerpo. Entonces,

1. $\mathcal{J}(\emptyset) = k[x_1, \dots, x_n]$.
2. Si $X_1 \subset X_2$ son subconjuntos de $\mathbb{A}_k^n \Rightarrow \mathcal{J}(X_2) \subset \mathcal{J}(X_1)$.
3. Si $V, W \subset \mathbb{A}_k^n \Rightarrow \mathcal{J}(V \cup W) = \mathcal{J}(V) \cap \mathcal{J}(W)$.
4. Si $V \subset \mathbb{A}_k^n \Rightarrow \sqrt{\mathcal{J}(V)} = \mathcal{J}(V)$, es decir, $\mathcal{J}(V)$ es un ideal radical.

Demostración.

1. Suponga que $\mathcal{J}(\emptyset) \neq k[x_1, \dots, x_n] \Rightarrow \exists f \in k[x_1, \dots, x_n]$ y $f \notin \mathcal{J}(\emptyset) \Rightarrow f(P) \neq 0$, $\forall P \in \emptyset (\Rightarrow\Leftarrow)$, así ambos conjuntos son iguales.

2. Sea $f \in \mathcal{J}(X_2) \Rightarrow f(P) = 0$, $\forall P \in X_2 \supset X_1$, en particular para todo $P \in X_1$, entonces $f(P) = 0, \forall P \in X_1 \Rightarrow f \in \mathcal{J}(X_1)$.

3. Sea $f \in \mathcal{J}(V \cup W) \Rightarrow f(P) = 0, \forall P \in V \cup W$ y como $V \subset V \cup W$ y $W \subset V \cup W \Rightarrow f \in \mathcal{J}(V) \wedge f \in \mathcal{J}(W) \Rightarrow f \in \mathcal{J}(V) \cap \mathcal{J}(W)$. Por otro lado, si $f \in \mathcal{J}(V) \cap \mathcal{J}(W) \Rightarrow f \in \mathcal{J}(V) \wedge f \in \mathcal{J}(W) \Rightarrow f(P) = 0,\ \forall P \in V \ \wedge f(P) = 0,\ \forall P \in W \Rightarrow f(P) = 0,\ \forall P \in V \cup W \Rightarrow f \in \mathcal{J}(V \cup W)$.

4. Se sabe que $\mathcal{J}(V) \subset \sqrt{\mathcal{J}(V)}$ por propiedad de ideal radical. Sea $f \in \sqrt{\mathcal{J}(V)} \Rightarrow \exists m > 0$ tal que $f^m \in \mathcal{J}(V) \Rightarrow f^m(P) = 0, \forall P \in V \Rightarrow f(P) = 0, \forall P \in V \Rightarrow f \in \mathcal{J}(V)$. ■

En síntesis, se tiene dos relaciones:

$$\mathcal{V}: \{\text{Ideales de } k[x_1, \dots, x_n]\} \to \{\text{Subconjuntos de } \mathbb{A}_k^n\}$$

y

$$\mathcal{J}: \{\text{Subconjuntos de } \mathbb{A}_k^n\} \to \{\text{Ideales de } k[x_1, \dots, x_n]\}.$$

Se observa que las igualdades $\mathcal{V}(1) = \emptyset$ y $\mathcal{J}(\emptyset) = k[x_1, \dots, x_n]$ se corresponden como imagen e imagen inversa y viceversa de $\mathcal{V}$ y $\mathcal{J}$. La propiedad $\mathcal{J}(0) = \mathbb{A}_k^n$ no goza necesariamente de su propiedad "inversa", se necesita que $\mathcal{J}(\mathbb{A}_k^n) = 0$ que equivale a decir que el único polinomio que anula a todos los puntos del espacio afín es el polinomio nulo. Por ejemplo, para el cuerpo finito $\mathbb{Z}_5$, simples cálculos muestran que el polinomio $f(x) = x^5 - x \in \mathbb{Z}_5[x]$ se anula en todo $\mathbb{A}_{\mathbb{Z}_5}^1$, sin que $f(x)$ sea necesariamente un polinomio nulo. Esto puede evitarse si el cuerpo k es infinito (como los cuerpos algebraicamente cerrados), el siguiente lema formaliza la idea:

Lema 2.76. Sea k un cuerpo infinito. Entonces, $\mathcal{J}(\mathbb{A}_k^n) = 0$.

Demostración. Ver Zaldívar (s.f.), p. 3, Lema 1.3.

El último lema enunciado es un primer paso para buscar, por medio de $\mathcal{V}$ y $\mathcal{J}$, una correspondencia entre ideales del anillo de polinomios $k[x_1, \dots, x_n]$ y subconjuntos (algebraicos afines) del espacio afín $\mathbb{A}_k^n$; es decir, una composición $\mathcal{J}(\mathcal{V}(-)) = -$, y viceversa. La búsqueda de las condiciones para que esto ocurra no es algo trivial, es necesario un teorema, dado por Hilbert, que hará posible una traducción de conjuntos geométricos en términos de una clase particular de ideales.

Ejemplo 5. Si $J \subset k[x_1, \dots, x_n]$ es un ideal, la inclusión $J \subset \mathcal{J}(\mathcal{V}(J))$ puede ser estricta (negando rotundamente una posible igualdad). Un caso típico seria con $k = \mathbb{R}$ y $f(x) = x^2 + 1 \in \mathbb{R}[x]$ tomando $J = \langle x^2 + 1 \rangle \subset \mathbb{R}[x]$. Es obvio que $1 \notin J = \langle x^2 + 1 \rangle$ luego J es un ideal propio de $\mathbb{R}[x]$. Por otro lado $\mathcal{V}(J) = \{P \in \mathbb{A}^1_{\mathbb{R}} : f(P) = P^2 + 1 = 0, \forall f \in J\} = \emptyset$, ya que ese polinomio no posee raíces reales, entonces $\mathcal{J}(\mathcal{V}(J)) = \mathcal{J}(\emptyset) = \mathbb{R}[x]$, y así se tiene la inclusión estricta deseada $J \subsetneq \mathcal{J}(\mathcal{V}(J))$.

Ejemplo 6. Y a pesar del esfuerzo de considerar k como algebraicamente cerrado, aún la inclusión $J \subset \mathcal{J}(\mathcal{V}(J))$ puede ser estricta. Para el polinomio $f(x) = x \in \mathbb{C}[x]$, si $J = \langle f^2 \rangle = \langle x^2 \rangle \subset \mathbb{C}[x]$ se tiene $J \subsetneq \mathcal{J}(\mathcal{V}(J))$, i.e. $J = \langle x^2 \rangle = \{p(x)x^2 : p(x) \in \mathbb{C}[x]\} =$ {Polinomios de grado mayor o igual a 2}; ahora aplicando $\mathcal{V}$ se tendrá $\mathcal{V}(J) = \{P \in \mathbb{A}^1_{\mathbb{C}} : h(P)P^2 = 0; \forall h(x)x^2 \in J\} = \{0\}$. Por otro lado $\mathcal{J}(0) = \{xq(x) : q(x) \in \mathbb{C}[x]\} =$ {Polinomios de grado mayor o igual a 1}. Por lo que: $\langle x^2 \rangle \subsetneq \mathcal{J}(\mathcal{V}(\langle x^2 \rangle)) = \mathcal{J}(0) = \langle x \rangle$.

La demostración del teorema que dará la correspondencia necesita de un resultado dado por David Hilbert, la cual necesita de herramientas como el lema de Zariski sobre extensiones algebraicas, el lema de Rabinowitsch que utiliza localización de anillos.

Teorema 2.77. Teorema de los ceros de Hilbert (Hilbert's Nullstellensatz). Sea k un cuerpo algebraicamente cerrado. Se cumple que:

1. Los ideales maximales $\mathfrak{m}$ del anillo de polinomio $k[x_1, \dots, x_n]$ son de la forma:

$$\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n \rangle \text{ con los } a_j \in k.$$

2. Todo ideal propio $I \subsetneq k[x_1, \dots, x_n]$ tiene conjunto algebraico afín no vacío, $\mathcal{V}(I) \neq \emptyset$.
3. Para todo ideal $I \subset k[x_1, \dots, x_n]$ se cumple $\mathcal{J}(\mathcal{V}(I)) = \sqrt{I}$.

Demostración.

1. Sin pérdida de generalidad se puede suponer que $a_i = 0$, el caso general es el morfismo de traslación. Así el morfismo de evaluación:

$$k[x_1, \dots, x_n] \to k$$

$$p(x_1, \dots, x_n) \mapsto p(0, \dots, 0)$$

es obviamente sobreyectivo y tiene núcleo $\langle x_1, \dots, x_n \rangle$, entonces $k[x_1, \dots, x_n]/\langle x_1, \dots, x_n \rangle \simeq k \Rightarrow \langle x_1, \dots, x_n \rangle$ es ideal maximal. Es decir, todo ideal de la forma $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ es maximal. Ahora lo recíproco. Sea $\mathfrak{m} \subset k[x_1, \dots, x_n]$ un ideal maximal, considere la composición de morfismos

$$\varphi: k \hookrightarrow k[x_1, \dots, x_n] \twoheadrightarrow k[x_1, \dots, x_n]/\mathfrak{m} =: A$$

y como $\mathfrak{m}$ es ideal maximal se tiene que A es un cuerpo. Note que A es una k-álgebra finitamente generada por las clases $\overline{x_i} = x_i + \mathfrak{m}$; es decir, es una k-álgebra finita, luego de tipo finito y además de ser un cuerpo, luego por el Lema de Zariski 2.65 A es una extensión algebraica sobre k, pero como k es algebraicamente cerrado, entonces $\varphi: k \xrightarrow{\cong} A$, y por biyectividad para cada $\overline{x_i} \in A$ existe un único $a_i \in k$ tal que $\varphi(a_i) = \bar{x}_i \Leftrightarrow \bar{a}_i = \bar{x}_i \Leftrightarrow x_i - a_i \in \mathfrak{m} \Rightarrow \langle x_1 - a_1, \dots, x_n - a_n \rangle \subset \mathfrak{m}$, pero como $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ es maximal (por la primera parte) entonces se tiene $\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. Así todo ideal maximal es de la forma requerida.

2. Sea I un ideal propio de $k[x_1, \dots, x_n]$, por teorema 2.18 está contenido en algún ideal maximal, que por el ítem anterior tiene una forma predeterminada, es decir:

$$I \subset \langle x_1 - a_1, \dots, x_n - a_n \rangle; \text{ para algún } P = (a_1, \dots, a_n) \in k^n,$$

luego por lema (2.3-4): $\mathcal{V}(\langle x_1 - a_1, \dots, x_n - a_n \rangle) \subset \mathcal{V}(I) \Rightarrow \mathcal{V}(I) \neq \emptyset$, por el ítem anterior.

3. Sea $f \in \sqrt{I} \Rightarrow f^m \in I$; para algún m, luego para todo $P \in \mathcal{V}(I)$ se tiene $f^m(P) = 0 \Rightarrow f(P) = 0 \Rightarrow f \in \mathcal{J}(\mathcal{V}(I))$. Para la otra inclusión, sea $f \in \mathcal{J}(\mathcal{V}(I))$ y como el anillo de coordenadas es noetheriano se puede escribir $I = \langle h_1, \dots, h_r \rangle$. Si se denota por $A = k[x_1, \dots, x_n]$ y $A_f = k[x_1, \dots, x_n]_f$ para tener el morfismo de localización

$$\gamma: A \to A_f$$

y sea IA_f el ideal generado por $\gamma(I)$ en A_f. Por el lema de Rabinowitsch (2.46):

$$A_f \simeq A[t]/\langle ft-1\rangle = k[x_1, \dots, x_n, t]/\langle ft-1\rangle$$

$\Rightarrow IA_f \simeq Ik[x_1, \dots, x_n, t]/\langle ft-1\rangle = \langle I, ft-1\rangle/\langle ft-1\rangle$, denote por $I_f := \langle I, ft-1\rangle = \langle h_1, \dots, h_r, ft-1\rangle \subset k[x_1, \dots, x_n, t]$.

Afirmación: $\mathcal{V}(I_f) = \emptyset$. Suponga que $(a_1, \dots, a_n, b) \in \mathcal{V}(I_f)$; con $I = \langle h_1, \dots, h_r\rangle$, luego los h_i se anulan en $P = (a_1, \dots, a_n)$ (los h_i no contienen la variable t); es decir $P \in \mathcal{V}(I)$ y por hipótesis $f \in \mathcal{J}(\mathcal{V}(I)) \Rightarrow f(P) = 0$; además como $(a_1, \dots, a_n, b) \in \mathcal{V}(I_f)$, entonces $ft-1$ se debe anular en $(a_1, \dots, a_n, b) = (P, b)$; es decir $f(P)b - 1 = 0 \Rightarrow f(P)b = 1 \Rightarrow f(P) \neq 0$, que contradice lo anterior, entonces $\mathcal{V}(I_f) = \emptyset$, luego por el ítem 2 de este teorema I_f no es ideal propio; es decir $\langle 1\rangle = I_f \Rightarrow IA_f = \langle 1\rangle$, de aquí 1 es suma finita del tipo

$$1 = \sum_i \frac{g_i h_i}{f^i} = \frac{\sum_i g_i' h_i}{f^s};\ \text{homogenizando para algún } s \text{ positivo}$$

$\Rightarrow f^s = \sum_i g_i' h_i$, pero $I = \langle h_1, \dots, h_r\rangle \Rightarrow f^s \in I$, para algún $s \Rightarrow f \in \sqrt{I}$. ■

La consecuencia 2 del teorema dice que siempre existe al menos un cero en común ("nullstellen" en alemán) para todos los polinomios contenidos en un ideal propio (sobre un cuerpo algebraicamente cerrado). Un caso muy conocido donde no ocurre esto es para $x^2 + 1 \in \mathbb{R}[x]$, que no posee raíces reales, por eso: $\mathcal{V}(x^2+1) = \emptyset$.

A continuación, el teorema que da la correspondencia buscada.

Teorema 2.78. Sea k un cuerpo algebraicamente cerrado.

1. Si V es un subconjunto $\mathbb{A}_k^n$, entonces $V \subset \mathcal{V}(\mathcal{J}(V))$. La igualdad se da si y solo si V es un conjunto algebraico.
2. Si I es un ideal de $k[x_1, \dots, x_n]$, entonces $I \subset \mathcal{J}(\mathcal{V}(I))$, tal ideal es radical, $\mathcal{J}\big(\mathcal{V}(I)\big) = \sqrt{I}$, por lo que la igualdad $\mathcal{J}(\mathcal{V}(I)) = I$ se da si y solo si I es un ideal radical.

Demostración.

1. Si $P \in V$, para todo $f \in \mathcal{J}(V)$ se tiene $f(P) = 0 \Rightarrow P \in \mathcal{V}(\mathcal{J}(V))$, por lo tanto, $V \subset \mathcal{V}(\mathcal{J}(V))$. Por otra parte, si $V = \mathcal{V}(\mathcal{J}(V))$, entonces V es algebraico por definición, ya que tiene asociado el ideal $\mathcal{J}(V)$; y si $V = \mathcal{V}(I)$ es algebraico afín, es un resultado claro que $I \subset \mathcal{J}(V)$, entonces por lema 2.72 se tiene $\mathcal{V}(\mathcal{J}(V)) \subset \mathcal{V}(I) = V$; por lo tanto $\mathcal{V}(\mathcal{J}(V)) = V$.

2. Sea $f \in I$, y sea $P \in \mathcal{V}(I) \Rightarrow f(P) = 0, \forall\, f \in I \Rightarrow f(P) = 0, \forall P \in \mathcal{V}(J) \Rightarrow f \in \mathcal{J}(\mathcal{V}(I))$. El teorema de los ceros de Hilbert hace el resto del trabajo.■

El teorema anterior dice que las funciones $\mathcal{V}, \mathcal{J}$.

$$\{\text{subconjuntos algebraicos de } \mathbb{A}_k^n\} \underset{\mathcal{V}}{\overset{\mathcal{J}}{\longleftrightarrow}} \{\text{ideales radicales de } k[x_1, \dots, x_n]\}$$

son inversas entre ellas. Esto permite un vaivén de ideas entre la geometría de los conjuntos algebraicos afines y alguna cualidad algebraica.

Ejemplo 7. Suponga que k es algebraicamente cerrado. Se mostrarán los conjuntos algebraicos de la recta afín $\mathbb{A}_k^1$. Como k es cuerpo, él y $k[x]$ son Dominios de ideales principales (Proposición 2.23, ítem 3), por lo que para cualquier conjunto algebraico afín se tendrá:

$\mathcal{V}(I) \neq \emptyset$; para cualquier ideal radical propio,

$\mathcal{V}(I) = \mathcal{V}(\langle f \rangle)$; para algún $f \in k[x]$ por ser este un DIP,

$$\mathcal{V}(I) = \mathcal{V}\big(c(x - a_1) \dots (x - a_n)\big)$$; por ser k alg. cerrado, con $c, a_1, \dots, a_n \in k$.

Finalmente: $\mathcal{V}(I) = \mathcal{V}(a_1, \dots, a_n)$, que dice los conjuntos algebraicos afín de la recta afín $\mathbb{A}_k^1$ *son:* $\emptyset$, los conjuntos finitos y la misma recta afín.

Esto muestra que la topología de Zariski en $\mathbb{A}_k^1$ es, por decirlo menos, extraña comparada con topologías usuales $\mathbb{A}_k^1 = k$, por ejemplo, $k = \mathbb{C}$ con su topología usual tiene más conjuntos cerrados.

Ejemplo 8. Si $E \subset k[x_1, \dots, x_n]$ es un conjunto de polinomios lineales, el conjunto $\mathcal{V}(E) \subset \mathbb{A}_k^n$ es conocido como una k-variedad lineal. Si E consta de un solo polinomio no constante $f \in k[x_1, \dots, x_n]$, la variedad $\mathcal{V}(E) =: \mathcal{V}(f) \subset \mathbb{A}_k^n$ es llamada hipersuperficie; si f es de grado 1, su conjunto de ceros $\mathcal{V}(f)$ se denomina hiperplano afín. En particular sí $n = 2$, $\mathcal{V}(f)$ es una curva y si f es lineal entonces será una recta.

2.1.10. Variedad algebraica

Habiendo definido los conjuntos cerrados de nuestro espacio afín, se hace necesario el estudio de sus propiedades topológicas; principalmente los conjuntos cerrados que no pueden "dividirse" en otros cerrados más pequeños. A medida que avanza esta sección daremos definiciones, propiedades topológicas y sus respectivos términos geométricos.

Definición 2.79. Se dice que un subespacio no vacío Z de un espacio topológico X es irreducible si no puede escribirse como unión de dos subconjuntos cerrados propios de Z.

Zaldívar (s.f.).

Esto último puede expresarse como: si para cualquier par de cerrados $P, Q \subset Z$ tal que $P \cup Q = Z \Rightarrow P = Z \vee Q = Z$.

Definición 2.80. Una variedad algebraica afín es un conjunto algebraico irreducible de algún $\mathbb{A}_k^n$. Zaldívar (s.f.).

Una variedad (algebraica) al ser un conjunto algebraico es un cerrado en $\mathbb{A}_k^n$, y al ser un tipo más restringido de conjunto algebraico su equivalente en $k[x_1, \dots, x_n]$ viene a ser un tipo más restringido de ideal radical, es decir, es un ideal radical y algo más; la siguiente proposición establece.

Proposición 2.81. Un conjunto algebraico V es variedad si y solo si su ideal asociado $\mathcal{J}(V)$ es primo.

Demostración. Sea $fg \in \mathcal{J}(V)$. Afirmación: $V \subset \mathcal{V}(f) \cup \mathcal{V}(g)$. Sea $P \in V \Rightarrow fg(P) = 0 \Rightarrow f(P)g(P) = 0 \Rightarrow f(P) = 0 \vee g(P) = 0 \Rightarrow P \in \mathcal{V}(f) \cup \mathcal{V}(g)$.

Luego $V = V \cap (\mathcal{V}(f) \cup \mathcal{V}(g)) = (V \cap \mathcal{V}(f)) \cup (V \cap \mathcal{V}(g))$, así por ser V irreducible: $V \cap \mathcal{V}(f) = V$ o $V \cap \mathcal{V}(g) = V \Rightarrow V \subset \mathcal{V}(f)$ o $V \subset \mathcal{V}(g)$, así aplicando $\mathcal{J}$, $\mathcal{J}(\mathcal{V}(f)) \subset \mathcal{J}(V)$ o $\mathcal{J}(\mathcal{V}(g)) \subset \mathcal{J}(V)$, luego por teorema (2.78-1) $f \in \mathcal{J}(V)$ o $g \in \mathcal{J}(V)$.

Recíprocamente, si $\mathcal{J}(V)$ es ideal primo, su condición por definición es equivalente a: $f \notin \mathcal{J}(V) \wedge g \notin \mathcal{J}(V) \Rightarrow fg \notin \mathcal{J}(V)$.

Suponga que existen dos subconjuntos cerrados propios $W_i \subsetneq V$ con $i = 1{,}2$ tal que $V = W_1 \cup W_2 \Rightarrow \mathcal{J}(V) = \mathcal{J}(W_1 \cup W_2) = \mathcal{J}(W_1) \cap \mathcal{J}(W_2)$, y $\mathcal{J}(V) \subsetneq \mathcal{J}(W_i)$; luego existe $f_i \in \mathcal{J}(W_i) \wedge f_i \notin \mathcal{J}(V); i = 1{,}2 \Rightarrow$ como $\mathcal{J}(V)$ es ideal primo, se tiene: $f_1 f_2 \notin \mathcal{J}(V)$, pero f_1, f_2 pertenecen al anillo, luego $f_1 f_2 \in \mathcal{J}(W_1)$ y $f_2 f_1 \in \mathcal{J}(W_2) \Rightarrow f_1 f_2 \in \mathcal{J}(W_1) \cap \mathcal{J}(W_2) = \mathcal{J}(V)$ que es una contradicción, por lo que no existen dos subconjuntos cerrados propios cuya unión sea V. ■

Ejemplo 9. $\mathbb{A}_k^n$ es irreducible porque sus conjuntos cerrados propios son finitos, mientras él es infinito (porque k es algebraicamente cerrado) y así es imposible mostrarlo como unión de dos conjuntos cerrados propios; usando la proposición el espacio afín (ambiente) es una variedad ya que le corresponde el ideal 0 que es primo.

Ejemplo 10. Si $f \in k[x_1, x_2]$ es un polinomio irreducible su ideal generado $\mathfrak{p} = \langle f \rangle$ es un ideal primo por lo que sus ceros $X = \mathcal{V}(f) \subset \mathbb{A}_k^2$ es un conjunto algebraico irreducible. Representar el conjunto de ceros de f es ver los (x_1, x_2) que cumplen $f(x_1, x_2) = 0$, que en general suelen ser curvas. Por ejemplo, en Figura 1 ambas curvas son irreducibles.

Los ideales primos (maximales) serán muy deseados en nuestro estudio ya que, como vimos en la sección preliminar, su respectivo anillo cociente es un dominio de integridad (cuerpo), siendo estos anillos que se comportan muy bien, se puede trabajar tranquilamente (no hay divisores de cero).

Los siguientes resultados muestran que todo conjunto algebraico puede expresarse como una unión de subconjuntos algebraicos irreducibles, esto en forma única, es decir, estudiar un conjunto algebraico se puede resumir, muchas veces, en estudiar los subconjuntos algebraicos irreducibles (variedades) que lo componen.

Se empieza con una caracterización puramente topológica muy útil de los conjuntos irreducibles.

Lema 2.82. Sea X un espacio topológico. Lo siguiente son condiciones equivalentes:

1. X es irreducible.
2. Todo subconjunto abierto no vacío de X es denso en X.
3. Si U_1, U_2 son subconjuntos abiertos no vacíos de $X \Rightarrow U_1 \cap U_2 \neq \emptyset$.

Demostración. 1⇒3. Sean U_1, U_2 abiertos no vacíos de X, suponga que $U_1 \cap U_2 = \emptyset \Rightarrow U_1^c \cup U_2^c = X$, unión de 2 cerrados, entonces por ser X irreducible tenemos: $U_1^c = X$ o $U_2^c = X \Rightarrow U_1 = \emptyset$ o $U_2^c = \emptyset$, que es una contradicción, así; $U_1 \cap U_2 \neq \emptyset$.

3⇒1. Suponga que X no es irreducible, entonces existe P, Q cerrados propios tal que $P \cup Q = X \Rightarrow P^c \cap Q^c = \emptyset$, además P^c y Q^c son abiertos propios. Es decir: X es no es irreducible por lo que existen abiertos no vacíos C y D tal que $C \cap D = \emptyset$; que es equivalente:

Para todo abierto $C \cap D \neq \emptyset \Rightarrow X$ es irreducible.

1⇔2. Obvio.■

Corolario 2.83. Sea $Y \subset X,$ con X espacio topológico. Si Y es un irreducible entonces su clausura $\bar{Y}$ es irreducible.

Demostración. Un abierto U intercepta a Y si y solo si intercepta a $\bar{Y}$. ■

Definición 2.84. Un subconjunto irreducible maximal de X será llamado componente irreducible del espacio topológico X. Zaldívar (s.f.).

Se sabe qué $Y \subset \bar{Y}$; y por el corolario anterior si Y es irreducible también $\bar{Y}$ es irreducible, por lo que si Y es componente irreducible entonces por ser irreducible máximo $Y = \bar{Y}$, y así en topología toda componente irreducible es cerrado; en la situación de los conjuntos algebraicos, las componentes irreducibles son un tipo de variedades algebraicas.

Proposición 2.85. Cualquier espacio topológico X cumple:

1. Todo subconjunto irreducible de X está contenido en una componente irreducible.
2. X puede expresarse como unión de sus componentes irreducibles.

1. Considere la familia $\mathfrak{F}$ de subconjuntos irreducibles de X que contienen a W subconjunto irreducible de X. La familia $\mathfrak{F}$ es no vacía ya que $W \in \mathfrak{F}$. Sea $\{X_i\}_{i\in\lambda}$ una cadena en $\mathfrak{F}$.

Afirmación: $Y = \bigcup_{i\in\lambda} X_i \in \mathfrak{F}$. Es obvio que $W \subset Y$, por otro lado, si U_1, U_2 son abiertos de X con $U_i \cap Y \neq \emptyset \Rightarrow \exists i_1, i_2 \in \lambda$ tales que $U_i \cap X_{i_k} \neq \emptyset$ para $i = 1{,}2$, al ser $\{X_i\}_{i\in\lambda}$ una cadena se puede considerar: $X_{i_2} \subset X_{i_1}$, luego $U_i \cap X_{i_k} \neq \emptyset$, pero al ser X_{i_k} irreducibles entonces por lema

2.82 se tiene $U_1 \cap U_2 \cap X_{i_k} \neq \emptyset \Rightarrow U_1 \cap U_2 \cap Y \neq \emptyset$, es decir para cualquier par de abiertos no nulos en Y se tiene que su intersección es no vacía, entonces nuevamente por lema 2.82 se tiene que Y es irreducible; así $Y \in \mathfrak{F}$. Con lo que podemos afirmar que toda cadena en $\mathfrak{F}$ posee cota superior, vía el lema de Zorn, la familia $\mathfrak{F}$ tiene un elemento máximo, por definición, una componente irreducible de X que contiene a W.

2. Sea C_x la componente irreducible de los conjuntos unitarios $\{x\}$, irreducibles, de $X \Rightarrow \bigcup_{x\in X}\{x\} \subset \bigcup_{x\in X} C_x \Rightarrow X = \bigcup_{x\in X} C_x$ cómo se buscaba. ■

Definición 2.86. Sea X un espacio topológico, se dice que es noetheriano si toda cadena descendente de conjuntos cerrados de X:

$$Y_1 \supset Y_2 \supset \cdots \supset Y_i \supset \cdots$$

se estaciona, es decir a partir de cierto índice $Y_j = Y_{j+1} = Y_{j+2} = \cdots$. Zaldívar (s.f.).

Como ya se dijo, si X es un conjunto algebraico afín, sus cerrados también lo son, entonces se puede afirmar:

Corolario 2.87. Si $X \subset \mathbb{A}_k^n$ es un conjunto algebraico, entonces X es un espacio noetheriano.

Demostración. Sea $Y_1 \supset Y_2 \supset \cdots \supset Y_i \supset \cdots$ una cadena descendente de cerrados en X, es decir, también de conjuntos algebraicos de $\mathbb{A}_k^n$, por el lema 2.75 se le asocia la cadena $\mathcal{J}(Y_1) \subset \mathcal{J}(Y_2) \subset \cdots \subset \mathcal{J}(Y_i) \subset \cdots$ de ideales de $k[x_1, \dots, x_n]$ y al ser este anillo noetheriano, se estaciona superiormente, de aquí la primera cadena descendente también se estaciona. ■

Proposición 2.88. Los espacios topológicos noetherianos X poseen una cantidad finita de componentes irreducibles y ninguna se superpone una a otra.

Demostración. Denote por $\mathfrak{F}$ a la familia de cerrados de X que no pueden expresarse como unión finita de conjuntos irreducibles de X.

Suponga que $\mathfrak{F} \neq \emptyset$. Por ser X espacio topológico noetheriano, es decir toda cadena descendente de cerrados se estaciona, gracias al lema de Zorn la familia $\mathfrak{F}$ posee un elemento minimal $Y \in \mathfrak{F}$; como caso particular Y no es irreducible porque si lo fuera se escribiría como unión finita de irreducibles (1 irreducible, él mismo), entonces $Y_1, Y_2 \subsetneq Y$ cerrados tales que $Y_1 \cup Y_2 = Y$. Luego por minimalidad $Y_i \in \mathfrak{F} \Rightarrow Y_i$ es unión finita de irreducibles entonces Y es unión finita de irreducibles, que es una contradicción $\Rightarrow \mathfrak{F} = \emptyset$; es decir los cerrados de X se escriben como unión finita de irreducibles, en particular el mismo X, además por proposición 2.85 cada irreducible está contenido en una componente irreducible, así

$$X = X_1 \cup \cdots \cup X_n$$

donde los X_i son componentes irreducibles de X, y $X_i \neq X_j$, para $i \neq j$. Si Y es cualquier componente irreducible de X, de $Y = X \cap Y = \bigcup_{i=1}^{n}(X_i \cap Y)$. Afirmación: $Y = X_i \cap Y$ para algún i. Suponga que $Y \cap X_i \subsetneq Y$ para todo i; como $Y \cap X_i$ vienen a ser cerrados relativos de Y entonces Y es reducible, y esto es una contradicción, entonces $Y \cap X_i \subset Y$ para algún i, la inclusión faltante es obvia para ese mismo i, y se tiene la igualdad, con lo que también se deduce $Y \subset X_i$, pero al ser Y componente irreducible (maximal) $\Rightarrow Y = X_i$; es decir se tienen todas las componentes irreducibles X_i,$1 \leq i \leq n$; de X, i.e., una cantidad finita.

Por último, usando la idea anterior, si $X_i \subset \bigcup_{j \neq i} X_j \Rightarrow X_i = X_j$ para algún $j \neq i$ que contradice el hecho que son distintos dos a dos, por lo que ninguna componente se superpone una a otra. ■

Corolario 2.89. Cualquier conjunto afín $V \subset \mathbb{A}_k^n$ posee una cantidad finita de componentes irreducibles $V_1, V_2, \dots, V_n$ y en la representación

$$V = V_1 \cup \dots \cup V_n$$

ningún V_i es superfluo, i.e., ningún V_i está contenido en algún otro.

Demostración. Directo de la proposición anterior. ■

2.1.11. Anillo de coordenadas de una variedad

Siguiendo las ideas del anillo cociente en el capítulo preliminar, se organizan las funciones que se puedan evaluar solo en una variedad V. Así como el anillo $k[x_1, \dots, x_n]$ está asociado de forma natural al espacio afín $\mathbb{A}_k^n$ como funciones que pueden evaluarse en todo el espacio, a cada variedad algebraica $V \subset \mathbb{A}_k^n$ se le asociará un objeto similar que agrupe a los funciones que definen la misma función en V, es decir, se justificará la siguiente definición del anillo de coordenadas afín de una variedad:

$$k[V] := k[x_1, \dots, x_n]/\mathcal{J}(V).$$

Sea $\mathfrak{F}(V, k)$ el conjunto de todas las funciones de V en k, donde $V \subset \mathbb{A}_k^n$ una variedad algebraica. Es sencillo ver que las operaciones de k como cuerpo hacen de $\mathfrak{F}(V, k)$ un anillo conmutativo con unidad que contiene a k.

Definición 2.90. Se dice que $f \in \mathfrak{F}(V, k)$ es polinomial si existe un $F \in k[x_1, \dots, x_n]$ tal que $f(a_1, \dots, a_n) = F(a_1, \dots, a_n)$; para todo $(a_1, \dots, a_n) \in V$.

Zaldívar (s.f.).

Como en el caso del espacio afín donde no se trabaja con todas las funciones posibles, sino con el conjunto $k[x_1, \dots, x_n]$; en el caso de una variedad no se trabaja con todo $\mathfrak{F}(V, k)$ sino solo con las que son polinomiales.

Proposición 2.91. El conjunto de funciones polinomiales es un subanillo de $\mathfrak{F}(V, k)$ que además contiene a k.

Demostración. Es claro que todos los elementos de k son polinomiales, además si f, g son polinomiales entonces existen $F, G \in k[x_1, \dots, x_n]$ tal que $f(a_1, \dots, a_n) = F(a_1, \dots, a_n)$ y $g(a_1, \dots, a_n) = G(a_1, \dots, a_n)$, $\forall\ (a_1, \dots, a_n) \in V$, además $F - G$ y $F \cdot G$ también pertenecen al anillo de polinomios. Así $(f - g)(a) = f(a) - g(a) = F(a) - G(a) = (F - G)(a)$, $\forall\ a =$

$(a_1, \dots, a_n) \in V \Rightarrow f - g$ es polinomial; lo mismo para $f \cdot g$. Por lo tanto, el conjunto de funciones polinomiales es un subanillo. ■

Proposición 2.92. La aplicación $\Phi: k[x_1, \dots, x_n] \to \mathfrak{F}(V, k)$ con asignación $F \mapsto F|_V: V \to k$ es un morfismo de anillos con *kernel* $\mathcal{J}(V)$.

Demostración. Es claro que $\Phi(1) = 1$, mientras:

$$\Phi(F + G) = (F + G)|_V = F|_V + G|_V = \Phi(F) + \Phi(G)$$

$$\Phi(F \cdot G) = (F \cdot G)|_V = F|_V \cdot G|_V = \Phi(F) \cdot \Phi(G)$$

para $F, G \in k[x_1, \dots, x_n]$, así Φ es un morfismo de anillos.

Por otro lado, sea $\psi \in \ker\Phi \Leftrightarrow \Phi(\psi) = 0 \Leftrightarrow \psi|_V = 0 \Leftrightarrow \psi \in \mathcal{J}(V)$, por lo tanto, $\mathrm{Ker}\Phi = \mathcal{J}(V)$. ■

Por la proposición anterior y el teorema de isomorfía de anillos, tenemos:

$$\frac{k[x_1, \dots, x_n]}{\mathcal{J}(V)} \cong \mathrm{Im}\Phi$$

pero, $\mathrm{Im}\Phi = \{\text{Funciones polinomiales}\}$, en efecto: si f es polinomial $\Rightarrow f(v) = F(v)\ \forall\ v \in V$ para algún $F \in k[x_1, \dots, x_n] \Rightarrow f = \Phi(F) \Rightarrow f \in \mathrm{Im}\Phi$. Y también, si $h \in \mathrm{Im}\Phi \Rightarrow \exists\ H \in k[x_1, \dots, x_n]$ tal que $\Phi(H) = h \Leftrightarrow H|_V = h \Leftrightarrow H(v) = h(v), \forall\ v \in V \Rightarrow h$ es polinomial. Por lo que podemos afirmar la:

Proposición 2.93. Sea $V \subset \mathbb{A}_k^n$ una variedad algebraica. El anillo de funciones polinomiales en V es isomorfo al anillo:

$$k[V] := \frac{k[x_1, \dots, x_n]}{\mathcal{J}(V)}$$

por lo que $k[V]$ es el anillo de coordenadas afín de V.

Las clases ϕ del anillo $k[V]$ se pueden considerar como funciones $\phi: V \to k$, en V, i.e., $\phi = f + \mathcal{J}(V) \in k[V]$, con $f \in k[x_1, \dots, x_n]$, para $P = (a_1, \dots, a_n) \in V$ se define:

$$\phi(P) := f(a_1, \dots, a_n),$$

que no depende del representante f de la clase ϕ. En efecto, suponga sea g otro representante, entonces $f - g \in \mathcal{J}(V) \Rightarrow (f - g)(P) = 0, \forall P \in V \Rightarrow f(P) = g(P), \forall P = (a_1, \dots, a_n) \in V$.

Siempre que no cause confusión, abusando de la notación, se escribe solo al representante f, así las coordenadas $x_i \in k[V] = k[x_1, \dots, x_n]/\mathcal{J}(V)$ resultan ser funciones $x_i: V \to k$ que asigna a cada punto $P = (a_1, \dots, a_n) \in V$ su i-ésima coordenada $x_i(P) := a_i$. Finalmente $k[V]$ es finitamente generado como una k-álgebra por $x_1, \dots, x_n$ (aunque este necesariamente no sea un conjunto generador mínimo).

Ejemplo 11. Si $V = \mathcal{V}(xy - 1)$ es la hipérbola $y = 1/x$ en $\mathbb{A}^2_{\mathbb{R}}$, entonces $\mathbb{R}[V] = \mathbb{R}[x, y]/(xy - 1)$. Los polinomios $f(x, y) = x$ (la función coordenada x) y $g(x, y) = x + (xy - 1)$, que son funciones diferentes en $\mathbb{A}^2_{\mathbb{R}}$, pero, definen la misma función en el subconjunto V. En el punto $(\frac{1}{2}, 2) \in V$, por ejemplo, ambas dan el valor $\frac{1}{2}$. En el anillo cociente $\mathbb{R}[V]$ tenemos: $\bar{x}\bar{y} = 1$, así que $\mathbb{R}[V] \cong \mathbb{R}[x, 1/x]$. Para cualquier $(a, b) \in V$ tenemos $\bar{f}(a, b) = f(a, 1/a)$ para algún $f \in \mathbb{R}[x, y]$ que resulte ser $\bar{f}$ en el cociente.

Corolario 2.94. El conjunto algebraico $V \subset \mathbb{A}^n_k$ es variedad si y solo si su anillo de coordenadas $k[V]$ es un dominio de integridad.

Demostración. Por la proposición 2.81 tenemos que V es irreducible $\Leftrightarrow \mathcal{J}(V)$ es ideal primo $\Leftrightarrow k[V]$ es dominio de integridad, por el teorema 2.14. ■

Por un lado los cerrados del espacio afín $\mathbb{A}^n_k$ están asociados a los ideales radicales de $k[x_1, \dots, x_n]$; mientras que los conjuntos cerrados de un subconjunto afín $V \subset \mathbb{A}^n_k$ han sido visto como lo que son, cerrados relativos de V, en este contexto, como en teorema 2.78 se debe tener una correspondencia con los ideales radicales de su respectivo anillo de coordenadas afín $k[V]$, en eso se enfoca los siguientes resultados.

Proposición 2.95. Sea $\pi: k[x_1, \dots, x_n] \twoheadrightarrow k[V] = k[x_1, \dots, x_n]/\mathcal{J}(V)$ la proyección canónica, que induce la correspondencia entre ideales de $k[V]$ e ideales de $k[x_1, \dots, x_n]$ que contienen a $\mathcal{J}(V)$, se tiene que ideales radicales y maximales de $k[x_1, \dots, x_n]$ se corresponden a ideales radicales y maximales de $k[V]$, respectivamente.

Demostración. Sea I un ideal radical que contiene a $\mathcal{J}(V)$. Por ser π un morfismo sobreyectivo la imagen de un ideal también es ideal. Sea $\bar{q} \in \sqrt{\pi(I)} \Rightarrow \bar{q}^m \in \pi(I)$, para algún $m \Rightarrow \overline{q^m} \in \pi(I) \Rightarrow q^m \in I$, para algún $m \Rightarrow q \in \sqrt{I} = I \Rightarrow \bar{q} \in \pi(I)$. Por lo tanto $\sqrt{\pi(I)} \subset \pi(I)$, la otra inclusión es obvia; así el ideal radical I se corresponde con $\pi(I)$ también ideal radical.

Sea H ideal radical de $k[V]$, se sabe que $\pi^{-1}(H)$ es ideal. Sea $r \in \sqrt{\pi^{-1}(H)} \Rightarrow r^m \in \pi^{-1}(H)$, para algún $m \Rightarrow \overline{r^m} \in H \Rightarrow \bar{r}^m \in H \Rightarrow \bar{r} \in \sqrt{H} = H \Rightarrow r \in \pi^{-1}(H)$. Por lo tanto $\sqrt{\pi^{-1}(H)} \subset \pi^{-1}(H)$, la otra inclusión es obvia; así el ideal radical H se corresponde con el ideal radical $\pi^{-1}(H)$.

Para ideales maximales, supongamos $\mathfrak{m}$ es ideal maximal de $k[x_1, \dots, x_n]$, y sea S un ideal de $k[V]$ tal que

$$\pi(\mathfrak{m}) \subset S \subset k[V] \Rightarrow \mathfrak{m} \subset \pi^{-1}(\pi(\mathfrak{m})) \subset \pi^{-1}(S) \subset \pi^{-1}(k[V])$$

y por ser $\mathfrak{m}$ maximal $\mathfrak{m} = \pi^{-1}(S)$ o $\pi^{-1}(S) = k[x_1, \dots, x_n]$, y al ser π sobreyectiva $\pi(\pi^{-1}(X)) = X, \forall\, X$, entonces $S = \pi(\mathfrak{m})$ o $S = k[V]$, por lo tanto, $\pi(\mathfrak{m})$ es ideal maximal de $k[V]$.

Por último, suponga que M es ideal maximal de $k[V]$, y sea S un ideal de $k[x_1, \dots, x_n]$ tal que

$$\pi^{-1}(M) \subset S \subset k[x_1, \dots, x_n] \Rightarrow M = \pi(\pi^{-1}(M)) \subset \pi(S) \subset k[V]$$

y por ser M maximal $\pi(S) = M$ o $\pi(S) = k[V]$, entonces

$$S = k[x_1, \dots, x_n] \vee S \subset \pi^{-1}\big(\pi(S)\big) = \pi^{-1}(M)$$

y por hipótesis $\pi^{-1}(M) \subset S$ entonces $S = \pi^{-1}(M)$, por lo que $\pi^{-1}(M)$ es ideal maximal. ■

Corolario 2.96. Existe una correspondencia entre los cerrados de V con los ideales radicales de $k[V]$.

Demostración. Sea C un cerrado relativo a V, entonces $C = V \cap X$, donde X es cerrado en $\mathbb{A}_k^n$, pero V al ser conjunto algebraico también lo es, entonces C es cerrado en $\mathbb{A}_k^n$, pero $C \subset V \Rightarrow \mathcal{J}(V) \subset \mathcal{J}(C)$; y por proposición anterior $\mathcal{J}(C)$ se corresponde con un ideal radical en $k[V] := k[x_1, \dots, x_n]/\mathcal{J}(V)$.

Por otro lado, un ideal radical $\bar{I} \subset k[V]$ se corresponde con el ideal radical I con $\mathcal{J}(V) \subset I \Rightarrow \mathcal{V}(I) \subset \mathcal{V}(\mathcal{J}(V)) = V$ y claramente es un conjunto cerrado en V. ■

Siguiendo la idea de la correspondencia anterior, se puede utilizar el teorema de los ceros de Hilbert para ver lo que sucede con los puntos en una variedad.

Proposición 2.97. Sea k un cuerpo algebraicamente cerrado y sea $V \subset \mathbb{A}_k^n$ algebraico. Existe una correspondencia entre los puntos de V y los ideales maximales de $k[V]$.

Demostración. Si $\bar{\mathfrak{m}}$ es un ideal maximal de $k[V]$ se le hace corresponder el ideal maximal $\mathfrak{m}$ de $k[x_1, \dots, x_n]$ que contiene a $\mathcal{J}(V) \Rightarrow \mathcal{V}(\mathfrak{m}) \subset \mathcal{V}(\mathcal{J}(V)) = V$; además por ser $\mathfrak{m}$ ideal maximal, por lema 2.72, el conjunto de ceros asociado $\mathcal{V}(\mathfrak{m})$ es un cerrado mínimo, pero por teorema de los ceros de Hilbert $\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n \rangle \Rightarrow \mathcal{V}(\mathfrak{m}) = P = (a_1, \dots, a_n) \in V$.

Por último, si $P \in V \Rightarrow \{P\} \subset V \subset \mathbb{A}_k^n \Rightarrow \mathcal{J}(V) \subset \mathcal{J}(P)$, es claro que $\mathcal{J}(P) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ y por el teorema de los ceros de Hilbert es ideal maximal del anillo de coordenadas $k[x_1, \dots, x_n]$ luego por proposición 2.95 este se corresponde con un único ideal maximal de $k[V]$. ■

Teniendo esas correspondencias, se define una subvariedad.

Definición 2.98. Sea $V \subset \mathbb{A}_k^n$ una variedad afín, una subvariedad de V es un subconjunto afín irreducible $W \subset \mathbb{A}_k^n$ tal que $W \subset V$. Zaldívar (s.f.), ejercicio 15, pp. 14.

Proposición 2.99. Sea $V \subset \mathbb{A}_k^n$ una variedad. Existe una correspondencia entre el conjunto de ideales primos de $k[V]$ y la familia de subvariedades de V.

Demostración. Basta ver la relación entre ideales primos de $k[x_1, \dots, x_n]$ que contienen a $\mathcal{J}(V)$ e ideales primos de $k[V]$.

Sea $\bar{P}$ ideal primo de $k[V]$, es claro que $\pi^{-1}(\bar{P})$ es un ideal en $k[x_1, \dots, x_n]$. Sea $pq \in \pi^{-1}(\bar{P}) \Rightarrow \overline{pq} = \bar{p}\bar{q} \in \bar{P} \Rightarrow \bar{p} \in \bar{P}$ o $\bar{q} \in \bar{P} \Rightarrow p \in \pi^{-1}(\bar{P})$ o $q \in \pi^{-1}(\bar{P})$. Por lo tanto $\pi^{-1}(\bar{P})$ es un ideal primo.

Ahora considere P ideal primo que contiene a $\mathcal{J}(V)$ entonces $k[x_1, \dots, x_n]/P$ es un dominio de integridad, además por el segundo teorema de Isomorfía:

$$\frac{k[x_1, \dots, x_n]}{P} \cong \frac{k[x_1, \dots, x_n]/\mathcal{J}(V)}{P/\mathcal{J}(V)} = \frac{k[V]}{P/\mathcal{J}(V)}$$

donde se ve que $\frac{k[V]}{P/\mathcal{J}(V)}$ es un dominio de integridad también, entonces $P/\mathcal{J}(V)$ es ideal primo de $k[V]$, por lo tanto, $P/\mathcal{J}(V) = \pi(P)$ es ideal primo. ■

Los siguientes resultados formalizan en este contexto lo dicho en la sección sobre nilpotencia.

Definición 2.100. Un anillo A es reducido si $\sqrt{0} = 0$, es decir, no tiene elementos nilpotentes.

Zaldívar (s.f.)

Proposición 2.101. Si $I \subset k[x_1, \dots, x_n]$ y $V = \mathcal{V}(I)$, entonces el anillo de coordenadas $k[V]$ es reducido.

Demostración. Directamente por proposición 2.67, ya que todos los ideales con los que se trabaja son ideales radicales.

Otra forma de demostrar se sigue de teorema 2.78, $\mathcal{J}(\mathcal{V}(I)) = \sqrt{I}$ y así $k[V] = k[x_1, \dots, x_n]/\sqrt{I}$ por lo que el nilradical de $k[V]$ es $\sqrt{\sqrt{I}} = \sqrt{I}$, i.e., es cero. ■

Proposición 2.102. Toda variedad V es compacta.

Demostración. Sea $\{U_\lambda\}_{\lambda \in L}$ un cubrimiento abierto de V, tomando complemento y teniendo en cuenta que $1 \in k[V]$ se tendrá:

$$\bigcup_{\lambda \in L} U_\lambda = V \Rightarrow \bigcap_{\lambda \in L} U_\lambda^c = \emptyset = \mathcal{V}(1) = \mathcal{V}(k[V]).$$

Si llamamos $U_\lambda^c =: V_\lambda := \mathcal{V}(I_\lambda)$, para ideales $I_\lambda \in k[V]$, se tendrá:

$$\bigcap_{\lambda \in L} \mathcal{V}(I_\lambda) = \mathcal{V}(\sum_{\lambda \in L} I_\lambda) = \mathcal{V}(k[V]).$$

Por la suma de ideales, existen $m_i \in I_{\lambda_i}$ con $i = 1, \dots, r$, para algún r entero positivo, tal que $\sum_{j=1}^r a_j\, m_j = 1 \in k[V] \Rightarrow \sum_{\lambda \in L} I_\lambda = k[V]$, es decir, existen finitos ideales I_{λ_j} con índices en L tal que $\sum_{j=1}^r I_{\lambda_j}$ entonces:

$$\emptyset = \mathcal{V}(\sum_{j=1}^{r} I_{\lambda j}) = \bigcap_{j=1}^{r} \mathcal{V}\,(I_{\lambda_j}) \Rightarrow V = \bigcup_{j=1}^{r} U_{\lambda_j}$$

es decir, todo cubrimiento abierto posee un subcubrimiento finito, por lo tanto, V es compacto. Además, V es irreducible, y por lema 2.82, ítem 2, no puede llegar a ser de Hausdorff, estos espacios topológicos suelen denominarse casicompactos. ■

2.1.12. Morfismos entre variedades

Una vez definidas las variedades algebraicas afín, se necesita una aplicación que respeta su estructura para así poder compararlas.

Definición 2.103. Si $V \subset \mathbb{A}_k^n$ y $W \subset \mathbb{A}_k^m$ son conjuntos algebraicos, una función $f: V \to W$ se denomina una aplicación polinomial si existen polinomios $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ para los cuales todo punto $P \in V$ cumple

$$f(P) = (f_1(P), \dots, f_m(P)).$$

Si $W = \mathbb{A}_k^n = k$, la noción de aplicación polinomial $f: V \to W = k$ coincide con los elementos de $k[V]$ como funciones $f: V \to k$. Aunque la aplicación polinomial es un morfismo entre variedades todavía está en términos del anillo $k[x_1, \dots, x_n]$, la siguiente proposición da una equivalencia que depende de los anillos de coordenadas de cada variedad.

Proposición 2.104. Sea $V \subset \mathbb{A}_k^n$, $W \subset \mathbb{A}_k^m$ conjuntos afines. Denote con $k[x_1, \dots, x_n]$ y $k[y_1, \dots, y_m]$ a sus anillos de coordenadas correspondientes. Entonces, $f: V \to W$ es una aplicación polinomial si y solo si $y_j \circ f \in k[V]$, para todas las funciones coordenadas $y_j \in k[W]$:

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[dr, "f_j"'] & W \subset \mathbb{A}_k^m \arrow[d, "y_j"] \\ & k \end{tikzcd}$$

Demostración. Si f es polinomial viene dada por $f = (f_1, \dots, f_m)$, entonces la composición $y_j \circ f$ evaluada en un punto P es

$$y_j \circ f(P) = y_j(f_1(P), \dots, f_m(P)) = f_j(P)$$

que resulta una función polinomial ya que los f_j lo son y así $y_j \circ f \in k[V]$.

Recíprocamente, si $f = (f_1, \dots, f_m)$ y suponga que $y_j \circ f = f_j \in k[V] = k[x_1, \dots, x_n]/\mathcal{J}(V)$ para toda j, entonces existen $F_j \in k[x_1, \dots, x_n]$ tales que $f_j \equiv F_j(\text{mod}\mathcal{J}(V))$ y por lo tanto para todo $P \in V$ se tiene que $f_j(P) = F_j(P)$ y así $f = (F_1, \dots, F_m)$ con cada F_i un polinomio, en consecuencia f es polinomial. ■

De manera natural se define la composición de aplicaciones polinomiales:

Si $V \subset \mathbb{A}_k^n$, $W \subset \mathbb{A}_k^m$, $U \subset \mathbb{A}_k^r$ son conjuntos afines y si $f: V \to W$ y $g: W \to U$ son aplicaciones polinomiales, entonces

$$g \circ f: V \to U$$

es polinomial, debido a que si $f = (f_1, \dots, f_m)$, donde $f_i \in k[x_1, \dots, x_n]$, y $g = (g_1, \dots, g_r)$, con $g_j \in k[y_1, \dots, y_m]$, entonces $g \circ f$ está dada por polinomios

$$g_1(f_1, \dots, f_m), \dots, g_r(f_1, \dots, f_m) \in k[x_1, \dots, x_n].$$

La identidad $\text{id}_V: V \to V$ es una aplicación polinomial. Así se tiene una categoría, cuyos objetos son las variedades afines y cuyas flechas son las aplicaciones polinomiales, definiendo así un isomorfismo de variedades si para un $f: V \to W$ existe un $g: W \to V$ (ambas aplicaciones polinomiales) tal que $f \circ g = \text{id}_W$ y $g \circ f = \text{id}_V$. Esta categoría puede relacionarse con la categoría de las k-álgebras del tipo $k[V]$.

Teorema 2.105. Sean $V \subset \mathbb{A}_k^n$, $W \subset \mathbb{A}_k^m$ conjuntos algebraicos.

1. Toda aplicación polinomial $f: V \to W$ induce un morfismo de k-álgebras $f^*: k[W] \to k[V]$.
2. Todo morfismo de k-álgebras $\varphi: k[W] \to k[V]$ puede expresarse como $\varphi = f^*$ con $f: V \to W$ aplicación polinomial única.

   Los dos ítems implican la biyección

$$\{\text{Aplicaciones polinomiales } f: V \to W\} \leftrightarrow \text{Hom}_{k-\text{álg}}(k[W], k[V])$$

dada por $f \leftrightarrow f^*$.

3. Si $f: V \to W$ y $g: W \to U$ son aplicaciones polinomiales, entonces

$$(g \circ f)^* = f^* \circ g^*,$$

dicho de manera elegante, la correspondencia anterior es contravariante.

Demostración.

1. Si $f: V \to W$ es una aplicación polinomial y sean las k-álgebras $k[W]$ y $k[W]$; defínase

$$f^*: k[W] \to k[V]$$

con $g \in k[W] \mapsto f^*(g) = g \circ f \in k[V]$, resulta que:

$$f^*(g+h) = (g+h) \circ f = g \circ f + h \circ f = f^*(g) + f^*(h);$$

$$f^*(gh) = (gh) \circ f = (g \circ f)(h \circ f) = f^*(g)f^*(h);$$

$$f^*(\lambda g) = (\lambda g) \circ f = \lambda(g \circ f) = \lambda f^*(g); \forall g, h \in k[W], \lambda \in k$$

es decir, f^* es un morfismo de álgebras.

2. Sea $\varphi: k[W] \to k[V]$ un morfismo de k-álgebras, sea $y_j \in k[W] = k[y_1, \dots, y_m]/\mathcal{J}(W)$; aplicando φ se tiene $\varphi(y_j) \in k[V]$; llámesele $f_j := \varphi(y_j)$. Sea $f = (f_1, \dots, f_m): V \to \mathbb{A}_k^n$, como los f_j son polinomios entonces f es una aplicación polinomial; el enunciado requiere que f tenga su imagen en W, para eso suponga que $g \in \mathcal{J}(W) \subset k[y_1, \dots, y_m]$, entonces por abuso de notación $g(y_1, \dots, y_m) = 0 \in k[W] \Rightarrow \varphi(g(y_1, \dots, y_m)) = \varphi(0) = 0 \in k[V] \Rightarrow g(\varphi(y_1), \dots, \varphi(y_m)) = 0 \in k[V]$; porque φ es un morfismo de k-álgebras y los coeficientes de g están en $k \Rightarrow g(f_1, \dots, f_m) = 0 \in k[V]$, donde los f_i son funciones en V, y $g(f_1, \dots, f_m) = 0 \in k[V]$ es la función $P \in V \mapsto g(f_1(P), \dots, f_m(P))$, pero $g(f_1(P), \dots, f_m(P)) = 0$ para todo $g \in \mathcal{J}(W)$; y como W es el conjunto de ceros de $\mathcal{J}(W) \Rightarrow (f_1(P), \dots, f_m(P)) \in W \Rightarrow f(P) \in W$ para todo $P \in V$.

Además, como $f = (f_1, \dots, f_m)$, $f_i = \varphi(y_i)$ y los y_i generan $k[W]$, para demostrar $f^* = \varphi: k[W] \to k[V]$ basta ver que: $f^*(y_j) = y_j \circ f = f_j = \varphi(y_j)$. Para la unicidad, supongamos existe otro $l: V \to W$ tal que $\varphi = l^*$, entonces $f^*(y_j) = \varphi(y_j) = l^*(y_j)$; para $y_j \in k[W] \Rightarrow f^* = l^* \Leftrightarrow f = l$.

3. Sea $f \in \mathrm{Hom}(V, W)$ y $g \in \mathrm{Hom}(W, U) \Rightarrow g \circ f \in \mathrm{Hom}(V, U)$; mientras que $f^* \in \mathrm{Hom}(k[W], k[V]), g \in \mathrm{Hom}(k[U], k[W]) \Rightarrow (g \circ f)^* \in \mathrm{Hom}(k[U], k[V])$. Se tiene para todo $z \in k[U]$:

$$(g \circ f)^*(z) = z \circ (g \circ f) = (z \circ g) \circ f = f^*(z \circ g) = f^*(g^*(z)) = (f^* \circ g^*)(z)$$

$\Rightarrow (g \circ f)^* = f^* \circ g^*$, por lo que el funtor es contravariante. ■

Es inmediato que una aplicación polinomial $f: V \to W$ es un isomorfismo si y solo si $f^*: k[W] \to k[V]$ es un isomorfismo de k-álgebras.

Ejemplo 12. La aplicación $f: \mathbb{A}^1_{\mathbb{R}} \to \mathcal{C} = \mathcal{V}(y^2 - x^3)$ definida por $f(t) = (t^2, t^3)$ no es un isomorfismo. Note que el morfismo de $\mathbb{R}$-álgebras

$$f^*: \mathbb{R}[\mathcal{C}] = \mathbb{R}[x, y]/\langle y^2 - x^3 \rangle \to \mathbb{R}[t]$$

definido $x \mapsto x \circ (t^2, t^3) = t^2$ y $y \mapsto y \circ (t^2, t^3) = t^3$. La imagen de f^* resulta en la $\mathbb{R}$-álgebra $\langle t^2, t^3 \rangle$, es decir $\mathbb{R}[t^2, t^3]$ (polinomios en la indeterminada t de grado mayor o igual que 2) que no es todo $\mathbb{R}[t]$.

Es claro que f es una aplicación polinomial biyectiva, sin embargo, su inversa $g: \mathcal{C} \to \mathbb{A}^1_{\mathbb{R}}$ viene dada por $g(x, y) = 0$ si $(x, y) = (0,0)$ y, $g(x, y) = y/x$, si $x \neq 0$, que no es polinomial.

Ejemplo 13. La proyección $\pi: C \to \mathbb{A}^1_k$, de la curva $C = \mathcal{V}(y - x^2) \subset \mathbb{A}^2_k$, $\pi(x, y) = x$ es polinomial cuya inversa $\varphi: \mathbb{A}^1_k \to C \subset \mathbb{A}^2_k$ con $\varphi(t) = (t, t^2)$ también es polinomial.

2.1.13. Funciones racionales en una variedad

Si $V \subset \mathbb{A}_k^n$ es una variedad afín, se sabe que su anillo de coordenadas $k[V]$ es un dominio de integridad, el cual se puede localizar, obteniendo un cuerpo de funciones racionales asociado a la variedad V que se denotará $k(V)$, sus elementos son cocientes g/h con $h \neq 0$, que en general no son funciones en todo V.

Definición 2.106. Una función $f \in k(V)$ será regular en $P \in V$ sí existe un cociente tal que $f = g/h$, donde $g, h \in k[V]$ y $h(P) \neq 0$. Si f es regular en todo $U \subset V$ se dice que f es regular en U.

Zaldívar (s.f.).

Se puede definir el valor de una función racional $f \in k(V)$ en un punto regular $P \in V$ simplemente evaluando en las funciones de su numerador y denominador:

$$f(P) = g(P)/h(P) \in k,$$

tal valor $f(P)$ no depende del representante g/h, por lo tanto $f \in k(V)$ puede considerarse como una función con su dominio $\mathrm{dom}f$ (de puntos regulares):

$$\mathrm{dom}f = \{P \in V: f \text{ es regular en } P\}.$$

Como se verá que el conjunto $\mathrm{dom}f$ es abierto, se muestran algunas propiedades de estos.

Proposición 2.107. Sea $V \subset \mathbb{A}_k^n$ un conjunto algebraico. Si $f \in k[V]$ considere

$$D(f) := \{a \in V: f(a) \neq 0\} = V - \mathcal{V}(f).$$

Se tiene:

1. $D(f) \subset D(g) \Leftrightarrow \mathcal{V}(f) \supset \mathcal{V}(g) \Leftrightarrow \sqrt{f} \subset \sqrt{g}$.

2. $D(fg) = D(f) \cap D(g)$.

3. $D(f^n) = D(f)$.

4. Todo abierto de V puede expresarse como unión finita de abiertos $D(f)$, por lo tanto, conforman una base de la topología del conjunto algebraico V.

5. f es nilpotente si y solo si $D(f) = \emptyset$.

6. Para todo $g \in k[V]$ no nilpotente se tiene que fg es nilpotente si y solo si $D(f)$ es denso en V.

7. f no es un divisor de cero en $k[V]$ si y solo si $D(f)$ es denso en V.

Demostración.

1. $D(f) \subset D(g) \Leftrightarrow V - \mathcal{V}(f) \subset V - \mathcal{V}(g) \Leftrightarrow \mathcal{V}(f) \supset \mathcal{V}(g)$. Para lo otro, sea $h \in \sqrt{f} \Rightarrow \exists m \in \mathbb{N}$ tal que $h^m \in (f)$, como $\mathcal{V}(g) \subset \mathcal{V}(f)$, entonces $h^m(P) = 0, \forall,\ P \in \mathcal{V}(f)$, en particular para todo $P \in \mathcal{V}(g) \Rightarrow h^m(P) = 0, \forall P \in \mathcal{V}(g) \Rightarrow h^m \in (g) \Rightarrow h \in \sqrt{g}$. Finalmente, si $\sqrt{f} \subset \sqrt{g} \Rightarrow \mathcal{V}(\sqrt{g}) \subset \mathcal{V}(\sqrt{f}) \Rightarrow \mathcal{V}(g) \subset \mathcal{V}(f)$, por lema 2.72, ítem 4 y 5.

2. Sea $P \in D(fg) \Leftrightarrow P \in V : fg(P) \neq 0 \Leftrightarrow f(P) \neq 0 \wedge g(P) \neq 0 \Leftrightarrow P \in D(f) \wedge P \in D(g) \Leftrightarrow P \in D(f) \cap D(g)$.

3. $D(f^n) = D(f \cdots f) = \bigcap_{i=1}^{n} D(f) = D(f)$.

4. Obvio interpretando los ítems anteriores.

5. $D(f) = \emptyset \Leftrightarrow \forall P \in V$ se cumple $f(P) = 0 \Rightarrow f = 0$, así, existe $m = 1$ tal que $f^1 = 0 \Rightarrow f$ es nilpotente. Recíprocamente, si f es nilpotente $\Rightarrow \exists m \in \mathbb{N}$ tal que $f^m = 0 \Rightarrow D(f^m) = D(0) = V - \mathcal{V}(0) = V - V = \emptyset \Rightarrow D(f) = \emptyset$, por el ítem 3.

Prueba de 6. (⇐) Suponga que $g' \in k[V]$ no nilpotente tal que fg es nilpotente ⇒ por ítem 3 y 5: $D(fg) = \emptyset \Rightarrow D(f) \cap D(g) = \emptyset$, además como g no es nilpotente se tiene $D(g) \neq \emptyset$, luego en la intersección no vacía existen dos casos:

- $D(f)$ es disjunto con $D(g)$, y observando que $D(g)$ no puede ser todo V ya que no podría ser disjunto con $D(f)$. Así $D(f) \cap D(g) = \emptyset$ implica que $D(f) \subset \mathcal{V}(g) \neq V$, por lo que un subconjunto cerrado propio contiene a $D(f)$, esto es suficiente para afirmar: $\overline{D(f)} \neq V$, por lo tanto, $D(f)$ no es denso.
- $D(f)$ es vacío ⇒ $D(f)$ no es denso.

Todo esto es equivalente a: $D(f)$ es denso ⇒ $\forall g \in k[V]$ no nilpotente, fg no es nilpotente.

(⇒). Se usará la siguiente condición equivalente de conjunto denso. Sea (X, τ) un espacio topológico y $A \subset X$, se tiene que A es denso en $X \Leftrightarrow \forall Q \in \tau : A \cap Q = \emptyset \Rightarrow Q = \emptyset$.

Procediendo. Sea $D(g)$ un abierto tal que $D(f) \cap D(g) = \emptyset$. La hipótesis $\forall g \in k[V]$ no nilpotente, fg no es nilpotente equivale a: para todo abierto $D(g)$ no vacío se tiene $D(fg)$ es no vacía, es decir, $D(fg) = D(f) \cap D(g) \neq \emptyset$; pero, como $D(f) \cap D(g) = \emptyset \Rightarrow D(g) = \emptyset$ ⇒ por equivalencia $D(f)$ es denso en V.

7. (⇒) Si f no es divisor de cero en $k[V] \Rightarrow f \neq 0$ y $\forall\ g \neq 0 \in k[V]$ se tiene $fg \neq 0$, en particular para todo g no nulo y nilpotente. Suponga que fg es nilpotente ⇒ $\exists m \in \mathbb{N}$ tal que $(fg)^m = 0 \Rightarrow f(f^{m-1}g^m) = 0 \Rightarrow f$ es divisor de cero (contradicción)⇒ fg no es nilpotente ⇒ por item 6: $D(f)$ es denso.

Recíprocamente (⇐), suponga que f es divisor de cero ⇒ $\exists g \in k[V]$ no nulo (que implica $D(g) \neq \emptyset$ y $\mathcal{V}(g) \neq V$) tal que $fg = 0 \Rightarrow D(fg) = D(0) \Leftrightarrow D(f) \cap D(g) = \emptyset \Rightarrow D(f) \subset \mathcal{V}(g) \neq V$, que, como se vio anteriormente, es condición suficiente para afirmar que $D(f)$ no es denso. Por lo tanto, si $D(f)$ es denso ⇒ f no es divisor de cero. ■

Si se analiza con cuidado el ítem 5 de la proposición anterior, este dice que los elementos nilpotentes del anillo $k[V]$ no afectan la topología ya que dan el abierto vacío, esto puede llegar a interpretarse como una equivalencia de la proposición 2.101.

Ahora las propiedades del dominio de los $f \in k(V)$.

Proposición 2.108. Sean $V \subset \mathbb{A}_k^n$ una variedad afín y $f \in k(V)$.

1. El conjunto $\mathrm{dom} f$ es abierto y denso en la topología de Zariski.
2. f es regular en todo V si y solo si f es polinomial en V, es decir, $\mathrm{dom} f = V \Leftrightarrow f \in k[V]$.

Demostración. Como $f \in k(V) \Rightarrow f = g/h$; con $g, h \in k[V]$ y $h \neq 0$. Así $hf = g \in k[V]$. Defínase el *ideal de denominadores* de f, unido con 0:

$$I_f = \{h \in k[V]: hf \in k[V]\} \cup \{0\} \subset k[V]$$

Es claro que I_f es un ideal de $k[V]$ y observe ahora que

$$V - \mathrm{dom} f = \{P \in V: h(P) = 0 \text{ para todo } h \in I_f\} = \mathcal{V}(I_f)$$

es decir $V - \mathrm{dom} f$ es algebraico contenido en V, entonces $V - \mathcal{V}(I_f) = \mathrm{dom} f$ es abierto y además no nulo. Al ser V irreducible, por lema 2.82 ítem 3, se deduce que $\mathrm{dom} f$ es denso en V.

2. Tenemos las equivalencias $\mathrm{dom} f = V \Leftrightarrow V - \mathcal{V}(I_f) = V \Leftrightarrow \mathcal{V}(I_f) = \emptyset \Leftrightarrow I_f = k[V] \Leftrightarrow 1 \in I_f \Leftrightarrow f = \frac{g}{1} \in k[V] \Leftrightarrow f \in k[V]$. ■

Proposición 2.109. Sea $U \subset V$ un abierto en una variedad. En la topología de Zariski, una función $f \in k(V)$ regular en U es continua, si se le considera como $f: U \to k$ con $k = \mathbb{A}_k^n$.

Demostración. Si C es cerrado en k, se mostrará que $f^{-1}(C)$ es cerrado en U. Se sabe que en la topología de Zariski los cerrados propios de k son conjuntos finitos, suponga que $C = \{c_1, \dots, c_s\}$, además $f^{-1}(C) = f^{-1}(\bigcup_{i=1}^{s} c_i) = \bigcup_{i=1}^{s} f^{-1}(c_i)$.

Afirmación: $f^{-1}(c_i)$ es cerrado en U.

Como f es regular en U, existen $g, h \in k[V]$ con $h \neq 0$ en U, tal que $f(P) = g(P)/h(P)$. Por lo que:

$$f^{-1}(c_i) \cap U = \{P \in U : c_i = f(P) = g(P)/h(P)\}$$

y $c_i = g(P)/h(P) \Leftrightarrow g(P) - c_i h(P) = 0 \Leftrightarrow (g - c_i h)(P) = 0$, entonces:

$$f^{-1}(c_i) \cap U = \mathcal{V}(g - c_i h) \cap U$$

el cual es cerrado (relativo) en U ya que $\mathcal{V}(g - c_i h)$ lo es.

Finalmente $\bigcup_{i=1}^{s}(f^{-1}(c_i) \cap U)$ también es cerrado en $U \Rightarrow (\bigcup_{i=1}^{s} f^{-1}(c_i)) \cap U = f^{-1}(C) \cap U$ es cerrado. Para los cerrados triviales es claro que $f^{-1}(\emptyset) = \emptyset$ y $f^{-1}(k) = U \cap V$ que también son cerrados, por lo tanto f es continua. ■

Corolario 2.110. (Teorema de la identidad). Si $f, g: V \to k$ son funciones regulares en una variedad $V \subset \mathbb{A}_k^n$, y coinciden en un abierto $U \subset V$, entonces f y g coinciden en todo V.

Demostración. Como f, g son regulares en V, por la proposición anterior son continuas en V entonces $f - g$ es continua en V, por lo que para el conjunto cerrado $\{0\} \subset k$ el conjunto $(f - g)^{-1}(0) \subset V$ también es cerrado.

Por otro lado, el conjunto $U = \{P \in V : f(P) = g(P)\}$, por hipótesis, es un abierto en V. Es claro que:

$$U \subset f^{-1}(0) \subset V.$$

Como V es irreducible, por lema 2.82, todo abierto es denso en V, entonces:

$$\overline{U} \subset \overline{f^{-1}(0)} = f^{-1}(0) \text{ y } \overline{U} = V.$$

Por lo tanto $f^{-1}(0) = V$, es decir: $f = g$ en todo V. ■

III. MÉTODO

3.1. Tipo de investigación

El tipo de investigación que se realiza es la “Investigación teórica”, orientada a entender principios e incrementar las bases del conocimiento de los conceptos fundamentales dentro del álgebra conmutativa y la geometría algebraica.

El método de investigación es el inherente a la matemática misma, el método axiomático, que utiliza símbolos para la representación de múltiples objetos que permite el análisis de fenómenos.

3.2. Ámbito temporal y espacial

La investigación se realizó entre el periodo de enero de 2023 y agosto de 2024, en la Facultad de Ciencias Naturales y Matemática de la Universidad Nacional Federico Villarreal, en el distrito de El Agustino, Lima.

3.3. Variables

Los conjuntos algebraicos y las variedades algebraicas.

3.4. Población y muestra

La naturaleza de este trabajo no requiere se consideren poblaciones ni muestras.

3.5. Instrumentos

Libros, artículos y algunos softwares de dibujo para representar ciertos fenómenos.

3.6. Procedimiento

El recojo de información será a través de los libros citados en la bibliografía, primero recolectando todas las definiciones y teoremas que se necesitan, segundo se organizan y tercero se brindan las demostraciones que se muestren muy relacionadas al tema de la tesis, caso contrario se remite al texto del cual se extrajo la información.

La parte teórica empieza con definiciones básicas del álgebra y la topología, luego se estudian los conjuntos algebraicos y sus propiedades básicas; en ese proceso se definen las variedades y se muestra una caracterización de ellas con herramientas del álgebra. A continuación, en el análisis de datos se estudia la dimensión de una variedad para finalmente en los resultados demostrar la hipótesis que se han planteado.

3.7. Análisis de datos

3.7.1. Dimensión de una variedad

La dimensión en el caso canónico de todo el espacio $\mathbb{A}_k^n$ es simple ya que toda coordenada en si no depende de las demás, las n coordenadas son independientes, es decir elegida una aún se está en la libertad de escoger las demás coordenadas. Se verá, esto tiene que ver con el cuerpo de fracciones de su anillo de coordenadas.

En las secciones preliminares se definió el grado de trascendencia de una extensión Σ de un cuerpo k, incluso se mostró que el grado de trascendencia de la extensión $k(x_1, \dots, x_n)$ de k es n, extensión que contiene al anillo de coordenadas del espacio.

En el caso de una variedad, siguiendo la idea canónica de todo el espacio, el número de coordenadas independientes puede variar. Para una "circunferencia" $x^2 + y^2 = 1$, puede asignársele cualquier x_0, luego para cumplir la ecuación solo hay una cantidad finita de valores para y_0, como máximo dos, esto debido a que las funciones coordenadas $\bar{x}, \bar{y} \in k(V)$, son algebraicamente dependientes, puesto que cumplen $x^2 + y^2 = 1$. Así, la dimensión de una variedad tiene que ver con la cantidad de coordenadas algebraicamente independientes que se consigan.

Definición 3.1. Sea V una variedad algebraica afín, con anillo de coordenadas $k[V]$ y cuerpo de fracciones $k(V)$ que es a la vez una extensión de k. La dimensión de la variedad V es el grado de trascendencia de tal extensión.

$$\dim V := \mathrm{grtr}_k k(V).$$

Zaldívar (s.f.).

Ejemplo 14. Los conjuntos unitarios en $\mathbb{A}_k^n$ son variedades ya que su ideal correspondiente en $k[\mathbb{A}_k^n]$ es maximal, así el anillo de coordenadas de un punto es isomorfo al cuerpo k y a la vez al cuerpo de funciones racionales, por lo tanto, la dimensión de un conjunto unitario es 0. Cualquier conjunto finito es la unión de sus conjuntos unitarios, y esta es su única descomposición en subvariedades afín.

Ejemplo 15. El eje X en $\mathbb{A}_k^2$ es irreducible ya que su anillo de coordenadas $\mathbb{R}[x,y]/(y) \cong \mathbb{R}[x]$, es un dominio de integridad. De manera similar, el eje Y, y de manera más general, las rectas $\mathbb{A}_k^2$ también son irreducibles. Los conjuntos lineales en $\mathbb{A}_k^n$ son variedades afines. El cuerpo de funciones racionales en el eje Y es el cuerpo cociente $\mathbb{R}(x)$ de $\mathbb{R}[x]$, aquí del por qué $\mathbb{R}(x)$ es llamado un cuerpo de funciones racionales. La dimensión del eje Y (o, de maneras más general, de cualquier recta) es 1.

Ejemplo 16. La unión del eje X y Y, es decir $\mathcal{V}(xy)$, no es una variedad, ya que puede descomponerse en las subvariedades $\mathcal{V}(x) \cup \mathcal{V}(y)$. Con el otro enfoque se puede afirmar lo mismo indicando que su correspondiente anillo de coordenadas $\mathbb{R}[x,y]/(xy)$ contiene divisores de cero.

Ejemplo 17. La hipérbola $xy = 1$ en $\mathbb{A}_k^2$ es una variedad ya que, como se puede ver, su anillo de coordenadas $\mathbb{R}[x, 1/x]$ es un dominio de integridad. Note que las ramas disjuntas de la hipérbola (definido por $x > 0$ y $x < 0$) no son subvariedades.

Ejemplo 18. Si $V = \mathcal{V}(f_1, \dots, f_n)$ es el conjunto de ceros de polinomios lineales $f_1, \dots, f_n$ en $k[x_1, \dots, x_n]$, entonces V es una variedad afín (llamada variedad lineal). Note que determinar si $V \neq \emptyset$ es un problema de álgebra lineal y al ser esta una rama que se subsume a la geometría algebraica, se verifica que la definición de dimensión de V como cardinal mínimo de vectores linealmente independientes y que lo generan coincide con la definición del grado de trascendencia $\mathrm{grtr}_k k(V)$. Ver Zaldívar (s.f., p. 78).

Ejemplo 19. Si $f \in k[x_1, \dots, x_n]$ es un polinomio no constante irreducible, el ideal generado por el (f) es un ideal primo por lo que su anillo de coordenadas $k[V]$ es un dominio de integridad y $\mathcal{V}(f)$ una hipersuperficie irreducible.

Como $k[V]$ es una k-álgebra finitamente generada, definimos $t_i = x_i + (f)$, y tenemos:

$$k[V] = \frac{k[x_1, \dots, x_n]}{(f)} = k[t_1, \dots, t_n]$$

con cuerpo de fracciones $k(t_1, \dots, t_n)$.

Como f es no nulo, f tiene al menos una indeterminada x_i, sin pérdida de generalidad suponga que es x_n. Luego todo elemento no nulo de (f) posee a x_n; por lo que todo polinomio no nulo $g(x_1, \dots, x_{n-1})$ no pertenece a (f); es decir no se tiene ninguna expresión no nula

$$g(t_1, \dots, t_{n-1}) = 0 \text{ en } k[V]$$

de aquí $t_1, \dots, t_{n-1}$ son algebraicamente independientes, además t_n es algebraico sobre $k(t_1, \dots, t_{n-1})$ porque resulta ser el polinomio no nulo f visto como

$$f = a_r(t_1, \dots, t_{n-1})x_n^r + \cdots + a_1(t_1, \dots, t_{n-1})x + a_0(t_1, \dots, t_{n-1})$$

con los $a_i(t_1, \dots, t_{n-1}) \in k(t_1, \dots, t_{n-1}) \Rightarrow t_1, \dots, t_{n-1}$ es una base de trascendencia para $k(t_1, \dots, t_n)$ sobre k.

Finalmente:

$$\dim V = \mathrm{grtr}_k k(V) = \mathrm{grtr}_k k(t_1, \dots, t_n) = n - 1.$$

Por lo tanto, f es irreducible, es decir $\mathcal{V}(f)$ es una hipersuperficie irreducible afín $\Rightarrow$ $\dim \mathcal{V}(f) = n - 1$.

El ejemplo anterior posee su recíproco, de una manera más general, pero para eso se necesita el siguiente resultado.

Lema 3.2. Si $V \subset \mathbb{A}_k^n$ es una variedad (irreducible) y $W \subsetneq V$ es un conjunto algebraico propio, entonces $\dim W < \dim V$.

Demostración. Suponga que W es irreducible, esto es posible ya que como V es unión finita de sus componentes irreducibles, bastará mostrar que cada uno de ellos cumple la desigualdad. Así, tenemos ideales primos $\mathcal{J}(V), \mathcal{J}(W) \subset k[x_1, \dots, x_n]$.

Como $W \subsetneq V \Rightarrow \mathcal{J}(V) \subsetneq \mathcal{J}(W)$, así en $k[V] = k[x_1, \dots, x_n]/\mathcal{J}(V)$, el ideal $\mathcal{J}(W)$ se corresponde con el ideal primo $\mathfrak{p} = \mathcal{J}(W)/\mathcal{J}(V) \neq 0 \subset k[V]$, luego por el teorema de isomorfía 2.12:

$$k[W] = \frac{k[x_1, \dots, x_n]}{\mathcal{J}(W)} \cong \frac{k[x_1, \dots, x_n]/\mathcal{J}(V)}{\mathcal{J}(W)/\mathcal{J}(V)} = \frac{k[V]}{\mathfrak{p}}.$$

Como el anillo de coordenadas afín de una variedad es una k-álgebra finita, se puede escribir: $K[V] = k[t_1, \dots, t_n]$ con $t_i = x_i + \mathcal{J}(V)$ y además las inclusiones $W \subset V \subset \mathbb{A}_k^n$ hacen que los morfismos inducidos en los anillos de coordenadas correspondientes sean restricciones, es decir, en:

$$k[x_1, \dots, x_n] \to k[V] \to k[W]$$

para $f \in k[V]$, su imagen $\bar{f}$ en $k[V]/\mathfrak{p} = k[W]$ es su restricción de V a W, así para las indeterminadas $t_i \in k[V]$ se tiene que $k[W] = k[\bar{t_1}, \dots, \bar{t_n}]$.

Se probará que la dimensión de V es mayor estricto que la de W. Para eso, suponga que $\dim W = d$, es decir de sus n indeterminadas $\bar{t}_i$, d son algebraicamente independientes, así renumerando los elementos algebraicamente independientes: $\bar{t_1}, \dots, \bar{t_d}$ es una base de trascendencia.

Se mostrará que es posible encontrar al menos un elemento algebraicamente independiente más, sea cualquier $f \in \mathfrak{p}$ no nulo. Suponga que $t_1, \dots, t_d, f$ no son algebraicamente independientes en $k(V)$, entonces existe una relación no trivial entre los t_i y f:

$$a_m(t_1, \dots, t_d)f^m + a_{m-1}(t_1, \dots, t_d)f^{m-1} + \cdots + a_0(t_1, \dots, t_d) = 0 \qquad (3.1)$$

con $a_i(t_1, \dots, t_d) \in k[t_1, \dots, t_n]$ alguno de ellos no nulo. Si la ecuación anterior no posee término independiente $a_0(t_1, \dots, t_d)$ se puede dividir entre la potencia de f conveniente, así podemos suponer que el término $a_0(t_1, \dots, t_d) \neq 0$.

Aplicando el morfismo $k[V] \to k[W]$ a la igualdad (3.1), es decir, restringiendo las funciones de (3.1) a W, como $f \in \mathfrak{p}$ entonces $\bar{f} = 0$, por lo que al final se tiene como imagen a:

$$a_0(\bar{t_1}, \dots, \bar{t_d}) = 0$$

es decir, hay una relación polinomial no trivial entre los $\bar{t}_i$, claramente una contradicción puesto que son algebraicamente independientes.

Por lo tanto, la extensión $k(V)$ tiene al menos $d + 1$ elementos algebraicamente independientes. Es decir:

$$\dim W = d < d + 1 \leq \dim V \Rightarrow \dim W < \dim V. \blacksquare$$

Antes de proceder a esta importante proposición, se usará una denominación para el tipo de variedad que aparecerá: "Se dice que una variedad V tiene *dimensión pura* d, o es *equidimensional* de dimensión d o *pura*, si todas las componentes irreducibles de un conjunto algebraico afín V tienen la misma dimensión d".

Proposición 3.3. Sea $V \subset \mathbb{A}_k^d$ una variedad con su anillo de coordenadas $k[V]$ un DFU (por ejemplo, $V = \mathbb{A}_k^d$). Si $W \subsetneq V$ es una subvariedad cerrada propia, entonces W es pura de dimensión $\dim W = \dim V - 1 \Leftrightarrow \mathcal{J}(W) = \langle f \rangle$, para algún $f \in k[V]$, i.e., si y solo si W es una hipersuperficie afín.

Demostración. La implicancia ($\Leftarrow$) fue hecha en el ejemplo 19. Si $\mathcal{V}(f)$ es una hipersuperficie $\mathcal{V}(f_1 \cdots f_s) = \bigcup_{i=1}^{s} \mathcal{V}(f_i)$ que es su descomposición en componentes irreducibles, es decir los f_i son polinomios irreducibles, luego por ejemplo 19: $\dim \mathcal{V}(f_i) = \dim V - 1$, para $i = 1, \ldots, s$.

($\Rightarrow$). Suponga que W es pura de $\dim W = \dim V - 1$. Si $W = \bigcup_{i=1}^{r} W_i$ es la descomposición en irreducibles de W, entonces:

$$\mathcal{J}(W) = \mathcal{J}(\bigcup_{i=1}^{r} W_i) = \bigcap_{i=1}^{r} \mathcal{J}(W_i)$$

por lema 2.75. Si se demuestra que $\mathcal{J}(W_i) = (f_i)$, entonces:

$$\bigcap_{i=1}^{r} \mathcal{J}(W_i) = \bigcap_{i=1}^{r} (f_i) = (f_1 \cdots f_r)$$

para f_i polinomios irreducibles, así W sería una hipersuperficie, por lo tanto, se puede suponer que W es irreducible, así $\mathfrak{p} := \mathcal{J}(W)$ es un ideal primo no nulo de $k[V]$, si lo fuera entonces se tendría: $\dim W = \dim V$ contradiciendo la hipótesis.

Como $\mathfrak{p}$ es ideal primo no nulo entonces contiene un polinomio irreducible f y al ser $k[V]$ un DFU el ideal (f) es primo, además como:

$$f \neq 0 \Rightarrow (0) \subsetneq (f) \Rightarrow \mathcal{V}(f) \subsetneq \mathcal{V}(0) = V$$

y también es claro que $f \in \mathfrak{p} \Rightarrow (f) \subset \mathfrak{p}$. Como nuestro objetivo es probar $(f) = \mathfrak{p}$, se requiere que $\mathfrak{p} \subset (f)$ que es equivalente a $x \in \mathfrak{p} \Rightarrow x \in (f)$. Suponga que no ocurre eso, es decir:

$$\exists x \in \mathfrak{p} \wedge x \notin (f) \Leftrightarrow (f) \subsetneq \mathfrak{p} \Rightarrow W = \mathcal{V}(\mathfrak{p}) \subsetneq \mathcal{V}(f) \subsetneq V$$

luego por lema 3.2: $\dim W < \dim \mathcal{V}(f) < \dim V \Rightarrow \dim W \leq \dim V - 2$ contradiciendo la hipótesis. Por lo que: $\mathfrak{p} \subset \mathcal{V}(f) \Rightarrow \mathfrak{p} = \mathcal{J}(W) = (f)$. Por lo tanto, $\mathcal{J}(W) = (f)$ para algún $f \in k[V]$. ■

Como observación a esta última demostración, se ha trabajado en un anillo cociente $k[V]$ y normalmente sus ideales deberían tener la forma también de cocientes, por ejemplo $I/\mathcal{J}(V)$ para un ideal $I \subset k[x_1, \dots, x_n]$; la flexibilidad de usar notaciones menos cargadas de términos lo dan las relaciones entre ideales del anillo de polinomios y el anillo cociente $k[V]$ dados en las Proposiciones 2.95 y 2.99.

3.7.2. Lema de normalización de Noether

En general los resultados de esta sección se cumplen simplemente considerando un cuerpo infinito, no necesariamente un cuerpo algebraicamente cerrado.

Lema 3.4. Si k es un cuerpo infinito y $f \in k[x_1, \dots, x_n]$ es un polinomio de grado d no nulo, entonces existe un cambio de variable lineal $x_i{}' = x_i - a_i x_n$ para $1 \leq i \leq n - 1$, y con $a_i \in k$, tales que el polinomio

$$f(x_1{}' + a_1 x_n, \dots, x_{n-1}{}' + a_{n-1} x_n, x_n) \in k[x_1{}', \dots, x_{n-1}{}', x_n]$$

posee un monomio del tipo $c x_n^d$ con $c \in k$.

Demostración. Ver Águeda (s.f.), p. 113, Lema B.6 o ver Zaldívar (s.f.) p. 97, Lema 3.22.

Lema 3.5. (Lema de Nakayama) Sean $A \subset B$ anillos, tal que B es una A-álgebra finita y $B \neq 0$. Entonces

$$\mathfrak{m}B \subsetneq B,$$

para todo ideal propio $\mathfrak{m} \subsetneq A$.

Demostración. Ver Águeda (s.f.) p. 114, Lema B.7 o ver Zaldívar (s.f.) p. 92), Lema 3.17.

Lema 3.6. (Lema de normalización de Noether). Si k es un cuerpo infinito y A es una k-álgebra de grado de trascendencia d, de tipo finito y que es dominio de integridad, entonces existen $y_1, \dots, y_d \in A$ algebraicamente independientes sobre k tales que A es entera sobre el subanillo $k[y_1, \dots, y_d]$ generado por los y_i:

$$k \subset k[y_1, \dots, y_d] \subset A.$$

Demostración. Como A es una k-álgebra de tipo finito, existen $\xi_1, \dots, \xi_n \in A$ tal que para todo $\in A$, $\exists$ $p(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$ tal que $p(\xi_1, \dots, \xi_n) = a$, de este modo existe un epimorfismo $k[x_1, \dots, x_n] \twoheadrightarrow A$.

Por el teorema de isomorfismo de anillos, se tiene $k[x_1, \dots, x_n]/\mathfrak{p} \cong A$, donde $\mathfrak{p}$ es ideal primo ya que A es dominio de integridad, y es claro que $d \leq n$ (Si n fuera menor que d, por el grado de trascendencia, no habría un epimorfismo). Observe que la cantidad d es fija, la cantidad n varía, así que se probarán todas las condiciones del teorema a través de inducción para $n \geq d$.

Para $n = d$, por hipótesis del grado de trascendencia hay un morfismo inyectivo $k[x_1, \dots, x_n] \to A$ definido por $x_i \mapsto \alpha_i$, donde los α_i son algebraicamente independientes, luego $\mathfrak{p} = 0 \Rightarrow A = k[\alpha_1, \dots, \alpha_d]$, y no hay nada que probar porque $A = k[\alpha_1, \dots, \alpha_d]$ ya es entera sobre $k[\alpha_1, \dots, \alpha_d]$ (sobre si misma) y los α_i pueden ser tomados como los y_i para $1 \leq i \leq d$.

Suponga ahora que $n > d$ y $\mathfrak{p} \neq 0$ luego como A es k-álgebra de tipo finito el morfismo $k[x_1, \dots, x_n] \to A$ con $x_i \mapsto \alpha_i$, cumple que los α_i no son algebraicamente independientes puesto que $n > d = \mathrm{grtr}_k A = d$. Por lo tanto, se tiene una relación no trivial que muestra la dependencia algebraica:

$$f(\alpha_1, \dots, \alpha_n) = 0$$

es decir, $f(x_1, \dots, x_n) \in \mathfrak{p} - \{0\}$, luego por el lema 3.4 se tiene un cambio de variable $x_i' = x_i - a_i x_n$ para $1 \leq i \leq n-1$, tal que el polinomio

$$f(x_1{}' + a_1 x_n, \dots, x_{n-1}{}' - a_{n-1} x_n, x_n) \in k[x_1{}', \dots, x_{n-1}{}', x_n]$$

sea mónico ($c = 1$ para el lema anterior), y puede verse como un polinomio mónico en x_n para el anillo $k[x_1{}', \dots, x_{n-1}{}'] \subset k[x_1, \dots, x_n]$. Entonces si se sustituye $x_i = \alpha_i$ y escribiendo $\alpha_i{}' = \alpha_i - a_i \alpha_n$ para $1 \leq i \leq n-1$, se tiene:

$$f(\alpha_1{}', \dots, \alpha_{n-1}{}', \alpha_n) = 0$$

es decir, α_n es entero sobre $k[\alpha_1{}', \dots, \alpha_{n-1}{}']$. Observe que los $\alpha_i{}'$ son enteros (trivialmente) en $k[\alpha_1{}', \dots, \alpha_{n-1}{}']$ luego por el corolario 1.60 los $\alpha_i = \alpha_i{}' + a_i \alpha_n$ también son enteros sobre $k[\alpha_1{}', \dots, \alpha_{n-1}{}']$ para $1 \leq i \leq n-1$, entonces se puede así afirmar que $k[\alpha_1, \dots, \alpha_n]$ es entera sobre $k[\alpha_1{}', \dots, \alpha_{n-1}{}']$.

Usando hipótesis inductiva $(n - 1 \geq d)$ para $k[\alpha_1{}', \dots, \alpha_{n-1}{}']$ existen $y_1, \dots, y_d \in k[\alpha_1{}', \dots, \alpha_{n-1}{}']$ que son algebraicamente independientes sobre k y $k[\alpha_1{}', \dots, \alpha_{n-1}{}']$ es entera sobre $k[y_1, \dots, y_d]$. Así $k[\alpha_1, \dots, \alpha_n]$ es entera sobre $k[\alpha_1{}', \dots, \alpha_{n-1}{}']$ y $k[\alpha_1{}', \dots, \alpha_{n-1}{}']$ es entera sobre $k[y_1, \dots, y_d]$, luego por el lema de la transitividad entera $k[\alpha_1, \dots, \alpha_n]$ es entera sobre $k[y_1, \dots, y_d]$.

Por lo tanto $A = k[\alpha_1, \dots, \alpha_n]$ es entera sobre $k[y_1, \dots, y_d]$. ■

Al reemplazar la k-álgebra A por $k[V]$, el lema de normalización de Noether tiene una interpretación geométrica. Suponga que $V \subset \mathbb{A}_k^n$ es una variedad afín, es claro que $k[V] = k[x_1, \dots, x_n]/\mathcal{J}(V)$ además de ser un dominio de integridad es una k-álgebra de tipo finito, que se puede generar con las clases α_i de x_i módulo $\mathcal{J}(V)$, es decir:

$$\alpha_i \equiv x_i (\mathrm{mod} \mathcal{J}(V)) \text{ y } k[V] = k[\alpha_1, \dots, \alpha_n].$$

Si V es de dimensión d entonces la k-álgebra $k[V]$ se puede utilizar el lema de normalización de Noether, por lo que existen $y_1, \dots, y_d \in k[V]$ algebraicamente independientes con $d \leq n$ tales que:

$$k \hookrightarrow k[y_d, \dots, y_d] \to k[V]$$

y $k[V]$ es entera sobre $k[y_1, \dots, y_d]$ y de tipo finito entonces por el corolario 2.63 es finitamente generada como módulo, es decir, es finita.

Así cada y_j es una expresión lineal en los α_i (por definición de álgebra finita) y cada $\alpha_i \equiv x_i (\mathrm{mod} \mathcal{J}(V))$ para cada i, entonces cada $y_j \in k[V] = k[x_1, \dots, x_n]/\mathcal{J}(V)$ se puede "levantar" (en el sentido que posee preimagen en $k[x_1, \dots, x_n]$) a formas lineales $\tilde{y}_j$ en $x_1, \dots, x_n$, además $\tilde{y}_j \equiv y_j (\mathrm{mod} \mathcal{J}(V))$ para cada j. Con estas formas lineales $\tilde{y}_j \in k[x_1, \dots, x_n]$, $1 \leq j \leq d$, se define una aplicación lineal:

$$\pi = (\widetilde{y_1}, \dots, \widetilde{y_d}) : \mathbb{A}_k^n \to \mathbb{A}_k^d$$

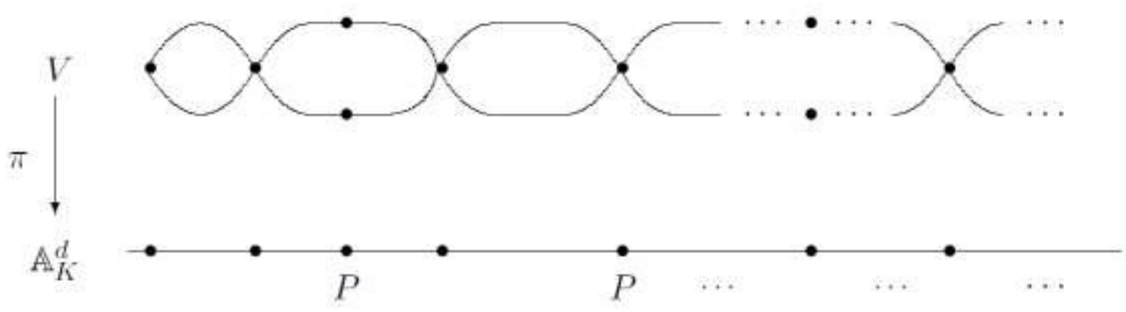
cómo $a = (a_1, \dots, a_n) \mapsto (\widetilde{y_1}(a), \dots, \widetilde{y_d}(a))$, que al restringirse a $V \subset \mathbb{A}_k^n$ induce una aplicación polinomial

$$\pi: V \to \mathbb{A}_k^d$$

que ha de ser independiente de los "levantamientos" $\tilde{y}_j$, ya que, si se tiene otro, entonces $\tilde{y}_j|_V = \tilde{\tilde{y}}_j|_V$, porque $\tilde{y}_j = \tilde{\tilde{y}}_j + h$ para algún $h \in \mathcal{J}(V)$.

Teorema 3.7. (Normalización de Noether). Si k es algebraicamente cerrado, la aplicación $\pi: V \to \mathbb{A}_k^d$ satisface que para cada punto $P \in \mathbb{A}_k^d$ la fibra $\pi^{-1}(P)$ es finita no vacía. En particular, π es sobreyectiva.

Figura 3. Interpretación geométrica de la normalización de Noether.



Las imágenes inversas de cada punto son finitas y no vacías. (Zaldívar, s.f., p. 96).

Demostración. Sea k un cuerpo algebraicamente cerrado y $P \in \mathbb{A}_k^d$.

Afirmación: $\pi^{-1}(P) \neq \emptyset$.

Si $P = (b_1, \dots, b_d) \in \mathbb{A}_k^d$, defínase:

$$I_p = \mathcal{J}(V) + \langle y_1 - b_1, \dots, y_d - b_d \rangle \subset k[x_1, \dots, x_n]$$

primero observe que $\mathcal{V}(I_p) \subset V$, en efecto, si

$Q \in \mathcal{V}(I_p) \Rightarrow g(Q) = 0 \forall\, g \in \mathcal{J}(V) + \langle y_1 - b_1, \dots, y_d - b_d \rangle$, luego en particular

$\forall g \in \mathcal{J}(V) + 0 \Rightarrow g(Q) = 0 \forall g \in \mathcal{J}(V) \Rightarrow Q \in V$, por lo que $\mathcal{V}(I_p) \subset V$.

Segundo, se verá que $\pi^{-1}(P) = \mathcal{V}(I_p)$.

En efecto, si $Q \in \mathcal{V}(I_p) \Rightarrow g(Q) = 0, \forall g \in \mathcal{J}(V) + \langle y_1 - b_1, \dots, y_d - b_d \rangle$, en particular para todo $g \in 0 + \langle y_1 - b_1, \dots, y_d - b_d \rangle$, entonces:

$$y_1(Q) = b_1$$

$$y_2(Q) = b_2$$

$$\dots$$

$$y_d(Q) = b_d$$

$\Rightarrow P = (y_1(Q), \dots, y_d(Q)) \Rightarrow Q \in \pi^{-1}(P)$.

Por otro lado, si $Q \in \pi^{-1}(P) \Rightarrow (y_1(Q), \dots, y_d(Q)) = \pi(Q) = P = (b_1, \dots, b_d)$

$\Rightarrow y_i(Q) = b_i, \forall i \Rightarrow (y_i - b_i)(Q) = 0, \forall i \Rightarrow Q \in \mathcal{V}(\langle y_1 - b_1, \dots, y_d - b_d \rangle)$; y como $Q \in \pi^{-1}(p) \subset V = \mathcal{V}(\mathcal{J}(V))$ entonces:

$$Q \in \mathcal{V}(\mathcal{J}(V)) \cap \mathcal{V}(\langle y_1 - b_1, \dots, y_d - b_d \rangle)$$

por lema 2.72, la intersección de conjuntos algebraicos es la suma de sus ideales, entonces:

$$Q \in \mathcal{V}(\mathcal{J}(V) + \langle y_1 - b_1, \dots, y_d - b_d \rangle) = \mathcal{V}(I_p).$$

Por lo tanto $\mathcal{V}(I_p) = \pi^{-1}(P)$, es decir cada fibra es una variedad afín, que en este caso depende del ideal I_p; si este es un ideal propio en $k[x_1, \dots, x_n]$, la fibra será no vacía.

En efecto:

Es claro que $\langle y_1 - b_1, \dots, y_d - b_d \rangle$ es un ideal maximal de $k[y_1, \dots, y_d]$ (por el teorema de los ceros de Hilbert 2.78) por lo que se tiene la siguiente inclusión:

$$\langle y_1 - b_1, \dots, y_d - b_d \rangle \subsetneq k[y_1, \dots, y_d] \subset k[V]$$

con $k[V]$ finita sobre $k[y_1, \dots, y_d]$ (consecuencia de lema de normalización de Noether), y así se tiene las hipótesis del lema de Nakayama, entonces:

$$\langle y_1 - b_1, \dots, y_d - b_d \rangle k[V] \subsetneq k[V] = \frac{k[x_1, \dots, x_n]}{\mathcal{J}(V)}$$

luego por el teorema de correspondencia 2.10 el ideal anterior se corresponde con el ideal propio:

$$\mathcal{J}(V) + \langle y_1 - b_1, \dots, y_d - b_d \rangle \subsetneq k[x_1, \dots, x_n]$$

entonces por el teorema de los ceros de Hilbert logramos: $\mathcal{V}(I_p) \neq \emptyset \Rightarrow \pi^{-1}(P) \neq \emptyset$.

Afirmación: $\pi^{-1}(P)$ es finita.

Por el lema de normalización de Noether $k[V] = k[\alpha_1, \dots, \alpha_n]$ es entera sobre $k[y_1, \dots, y_d]$ por lo que en particular cada $\alpha_i \in k[V]$ es raíz de un polinomio mónico de $k[y_d, \dots, y_d][x]$:

$\alpha_i^m + f_{i,m-1}(y_1, \dots, y_d)\alpha_i^{m-1} + \cdots + f_{i,0}(y_1, \dots, y_d) = 0 \quad (3.2)$

con los coeficientes $f_{i,j} \in k[y_1, \dots, y_d]$.

La expresión anterior contenida en $k[V]$ puede ser llevada a $k[x_1, \dots, x_n]$ gracias a los levantamientos $\tilde{y}_j \in k[x_1, \dots, x_n]$ y el hecho que $x_i \equiv \alpha_i (\mathrm{mod} \mathcal{J}(V))$ hace que se tenga:

$x_i^m + f_{i,m-1}(\widetilde{y_1}, \dots, \widetilde{y_d})x_i^{m-1} + \cdots + f_{i,0}(\widetilde{y_1}, \dots, \widetilde{y_d}) = g_i(x_1, \dots, x_n) \quad (3.3)$

para algún $g_i \in \mathcal{J}(V) \subset k[x_1, \dots, x_n]$.

Si $a = (a_1, \dots, a_n) \in V \Rightarrow g_i(a) = 0$ (ya que $g_i \in \mathcal{J}(V)$), así por la expresión (3.3) cada coordenada a_i es raíz del polinomio:

$$f_i = x^m + f_{i,m-1}(y_1, \dots, y_d)x^{m-1} + \cdots + f_{i,0}(y_1, \dots, y_d) \in k[y_1, \dots, y_d][x]$$

y como $\mathcal{J}(V)$ es primo (ya que V es variedad), entonces $k[V] = k[\alpha_1, \dots, \alpha_n]$ es un dominio de integridad por lo que se puede tener su cuerpo de fracciones $k(V)$, es decir:

$$k[y_1, \dots, y_d] \subset k[V] = k[\alpha_1, \dots, \alpha_n] \subset k(V) = k(\alpha_1, \dots, \alpha_n)$$

así poder considerar a $f_i(x)$ un elemento de $k(V)[x] = k(\alpha_1, \dots, \alpha_n)[x]$.

Así para cada $(a_1, \dots, a_n) \in \pi^{-1}(P) \subset V$, las coordenadas a_i son raíces del polinomio mónico $f_i(x)$ con coeficientes en el cuerpo $k(V)$, al haber una cantidad finita de raíces se sigue que hay una cantidad finita de puntos $(a_1, \dots, a_n) \in \pi^{-1}(P)$. ■

Esta importante interpretación geométrica puede resumirse en la siguiente frase: "Toda variedad algebraica afín se proyecta de modo finito en un espacio afín". (Sancho de Salas 2001, p. 179).

3.8. Consideraciones éticas

Los resultados usados están debidamente referenciados.

IV. RESULTADOS

El objetivo de esta investigación es determinar, en una variedad algebraica V, las condiciones que debe tener un polinomio f que pertenece al anillo de coordenadas afín $k[V]$, de manera que la dimensión de los subconjuntos irreducibles maximales de los ceros de este polinomio, es decir $\mathcal{V}(f)$, solo disminuya en 1 respecto a la dimensión de la variedad V. Luego se verán consecuencias importantes de este resultado.

4.1. Teorema del ideal principal de Krull

Primero el resultado preliminar importante.

Proposición 4.1. Sea A un dominio de integridad con cuerpo de fracciones K y sea L una extensión finita de grado n de K. Si $\alpha \in L$ es entero sobre A, entonces su norma $\mathrm{Nm}_{L/K}(\alpha) \in L$ también es entera sobre A y, de hecho, $\mathrm{Nm}_{L/K}(\alpha) \in A$, y α divide a $\mathrm{Nm}_{L/K}(\alpha)$ en el anillo $A[\alpha]$.

Demostración. Ver Zaldívar (s.f., 83), Proposición 3.5. ■

A continuación, se presenta el resultado central de la tesis.

Teorema 4.2. (Teorema del ideal principal de Krull). Si V es una variedad afín irreducible y $f \in k[V]$ es no nula, pero tiene un cero en V, entonces su conjunto de ceros $\mathcal{V}(f)$ es puro de dimensión $\dim\mathcal{V}(f) = \dim V - 1$.

Demostración. Primero se muestra que es suficiente probar la proposición cuando $\mathcal{V}(f)$ es irreducible. Si $\mathcal{V}(f) = \bigcup_{i=0}^{r} W_i$ es la descomposición en componentes irreducibles, como no puede ocurrir:

$$W_0 \subset W_1 \cup \cdots \cup W_r$$

ya que la descomposición seria redundante (Proposición 2.88), tampoco puede ocurrir que (aplicando $\mathcal{J}$ y usando lema 2.75):

$$\mathcal{J}(W_0) \supset \mathcal{J}(W_1 \cup \cdots \cup W_r) = \bigcap_{i=1}^{r} \mathcal{J}\,(W_i)$$

por lo que debe existir un $g \in k[V]$ no nulo tal que $g \in \bigcap_{i=1}^{r} \mathcal{J}\,(W_i)$ y $g \notin \mathcal{J}(W_0)$, luego si:

$$g \in \bigcap_{i=1}^{r} \mathcal{J}\,(W_i) \Rightarrow (g) \subset \bigcap_{i=1}^{r} \mathcal{J}\,(W_i) \Rightarrow \mathcal{V}(\bigcap_{i=1}^{r} \mathcal{J}\,(W_i)) \subset \mathcal{V}(g)$$

$$\Rightarrow \bigcup_{i=1}^{r} W_i \subset \mathcal{V}(g) \Rightarrow D(g) \subset (\bigcup_{i=1}^{r} W_i)^c$$

luego por la descomposición en componentes irreducibles se tiene $D(g) \subset W_0$ y además por proposición 2.101 el anillo $k[V]$ es reducido entonces g no es nilpotente entonces $D(g) \neq \emptyset$, por lo tanto, se puede afirmar lo siguiente:

Existe una vecindad no nula $D(g) \subset W_0$, disjunta con los demás W_i. Como $g \notin \mathcal{J}(W_0)$ esto implica que $\mathcal{V}(f|_{D(g)}) = \{P \in D(g) : f(P) = 0\} = D(g) \cap W_0$, llámesele U, es un abierto en W_0, pero más importante, irreducible, ya que suponiendo lo contrario:

$\exists\ P \cap U, Q \cap U$ cerrados propios en U tal que $(P \cap U) \cup (Q \cap U) = U$ donde P, Q son cerrados en W_0 (topología inducida)

$\Rightarrow (P \cup Q) \cap U = U$
$\Rightarrow P \cup Q \supset U;$ con $P \cup Q$ cerrado en W_0
$\Rightarrow (P \cup Q)^c \subset U^c;$ con $(P \cup Q)^c$ abierto en W_0
$\Rightarrow (P \cup Q)^c \cap U = \emptyset (\Rightarrow\Leftarrow)$ (Proposición 2.82, al ser W_0 irreducible, la intersección de todo par de abiertos es no vacía).

Así $\mathcal{V}(f|_{D(g)})$ es irreducible por lo que basta ver que es de dimensión $\dim V - 1$.

Suponiendo a $\mathcal{V}(f)$ irreducible $\Rightarrow \mathcal{J}(\mathcal{V}(f)) = (f) = \sqrt{(f)} =: \mathfrak{p}$ es ideal primo de $k[V]$ por lo que, además:

$$\frac{k[V]}{(f)} =: k[\mathcal{V}(f)] \text{ es dominio de integridad.}$$

Como $k[V]$ es k-álgebra finitamente generada (por lo tanto, de tipo finito) y dominio de integridad, por el Lema de normalización de Noether 3.6 entonces existen $y_1, \dots, y_d \in k[V]$ algebraicamente independientes sobre k tal que $k[V]$ es entero sobre $k[y_1, \dots, y_d] =: k[\mathbb{A}_k^d]$. Luego la inclusión:

$$k[y_1, \dots, y_d] \subset k[V]$$

induce la extensión de cuerpos:

$$k(\mathbb{A}^d) \to k(V)$$

De la inclusión $k[\mathbb{A}_k^d] \subset k(\mathbb{A}_k^d) \subset k(V)$, el hecho que $f \in k[V] \subset k(V)$ es entero sobre $k[\mathbb{A}_k^d]$, y la función norma $\mathrm{Nm}(f) =: f_0 \in k(V)$, por proposición 4.1, se tiene:

$$\mathrm{Nm}(f) =: f_0 \in k\left(\mathbb{A}_k^d\right),$$

también es entero sobre $k[\mathbb{A}_k^d]$, más aún, pertenece a $k[\mathbb{A}_k^d]$.

Afirmación (1):

$$\mathfrak{p} \cap k[\mathbb{A}_k^d] = \sqrt{(f_0)} \qquad \dots(4.1).$$

De (4.1) y el morfismo inclusión de $k[\mathbb{A}_k^d] \hookrightarrow k[V]$ al pasar a los cocientes se tiene:

Afirmación (2): El siguiente morfismo es inyectivo.

$$\frac{k[\mathbb{A}_k^d]}{\sqrt{(f_0)}} = \frac{k[\mathbb{A}_k^d]}{\mathfrak{p} \cap k[\mathbb{A}_k^d]} \rightarrowtail \frac{k[V]}{\mathfrak{p}} = k[\mathcal{V}(f)] \qquad \dots(4.2)$$

Como $k[V]$ es finitamente generado como $k[\mathbb{A}_k^d]$-módulo, por (4.2)

$\Rightarrow \frac{k[V]}{\mathfrak{p}} = k[\mathcal{V}(f)]$ es finitamente generado como $\frac{k[\mathbb{A}_k^d]}{\sqrt{(f_0)}}$-módulo, por lo que:

$$\dim\mathcal{V}(f) = \operatorname{grtr}_k k\big(\mathcal{V}(f)\big) = \operatorname{grtr}_k k\big(\mathcal{V}(f_0)\big) = \dim\mathcal{V}(f_0).$$

Además, como $f \neq 0 \Rightarrow f_0 \neq 0$ y $f_0 \in \mathfrak{p}$ implica que f no es constante (si lo fuera se tendría $f_0 \subset \mathfrak{p} \Rightarrow k[V] \subset \mathfrak{p}$, que es una contradicción al hecho de ser un ideal primo), entonces por la proposición 4.3 para el cerrado $\mathcal{V}(f_0) \subset \mathbb{A}_k^d$ se tiene que $\dim\mathcal{V}(f_0) = d-1$. Lo que se quería demostrar, resta demostrar las dos afirmaciones hechas.

Prueba de afirmación (1). ($\supset$). Como $f_0 = \mathrm{Nm}(f) \in k[\mathbb{A}_k^d]$ y además f divide a f_0 en $k[\mathbb{A}_k^d][f] \subset k[V]$:

$$\begin{aligned}
\Rightarrow \quad & f_0 = fq \quad \text{para algún } q \in k[\mathbb{A}_k^d] \\
\Rightarrow \quad & f_0 \in (f) \subseteq \sqrt{(f)} \\
\Rightarrow \quad & (f_0) \subseteq \mathfrak{p} \cap k[\mathbb{A}_k^d] \\
\Rightarrow \quad & \sqrt{(f_0)} \subseteq \mathfrak{p} \cap k[\mathbb{A}_k^d]
\end{aligned}$$

ya que $\mathfrak{p}$ es ideal primo y por lo tanto radical.

($\subset$). De manera análoga:

$$\begin{aligned}
\text{Si } g \in \mathfrak{p} \cap k[\mathbb{A}_k^d] \qquad & \Rightarrow g \in \mathfrak{p} = \sqrt{(f)} \\
& \Rightarrow g^m \in (f), \ \ \exists\, m \in \mathbb{N} \\
& \Rightarrow g^m = fh, \ \ \exists\, h \in k[V]
\end{aligned}$$

Tomando norma en la última igualdad:

$$\mathrm{Nm}(g^m) = \mathrm{Nm}(fh)$$

Si e es el grado de la extensión de cuerpos $k(V)/k(\mathbb{A}_k^d)$ por proposición 2.39, ítems 1 y 2:

$$\begin{aligned}
(g^m)^e &= \mathrm{Nm}(f)\mathrm{Nm}(h) \\
&= f_0\mathrm{Nm}(h)
\end{aligned}$$

$\Rightarrow g^{me} \in (f_0) \Rightarrow g \in \sqrt{(f_0)}$.

Prueba de afirmación (2). Es claro que el morfismo $k[\mathbb{A}_k^d] + \mathfrak{p} \hookrightarrow k[V]$ inclusión de anillos es inyectivo, y al pasar al cociente del mismo ideal el morfismo:

$$\frac{k[\mathbb{A}_k^d] + \mathfrak{p}}{\mathfrak{p}} \hookrightarrow \frac{k[V]}{\mathfrak{p}}$$

sigue siendo inyectivo. De otro lado, por el Tercer Teorema de Isomorfía 2.13, se tiene el isomorfismo (que implica inyectividad):

$$\frac{k[\mathbb{A}_k^d] + \mathfrak{p}}{\mathfrak{p}} \cong \frac{k[\mathbb{A}_k^d]}{k[\mathbb{A}_k^d] \cap \mathfrak{p}}$$

luego componer estas dos funciones inyectivas se tiene el resultado que se buscaba. ■

4.2. Consecuencias 1

Corolario 4.3. Si V es una variedad y $W \subsetneq V$ es un subconjunto cerrado irreducible propio máximo entonces $\dim W = \dim V - 1$.

Demostración. Si $W \subsetneq V \Rightarrow \mathcal{J}(V) = \mathfrak{P} \subsetneq \mathcal{J}(W) = \mathfrak{p}$. Como:

$$k[V] = \frac{k[\mathbb{A}_k^n]}{\mathcal{J}(V)} = \frac{k[\mathbb{A}_k^n]}{\mathfrak{p}}$$

existe un $f \in k[V]$ no nulo tal que $f \notin \mathfrak{P}$, en realidad se puede tomar un $f \in \mathfrak{p} - \mathfrak{P}$, es decir, existe una función f no cero en V (porque sino pertenecería a $\mathcal{J}(V) = \mathfrak{P}$) que se anula en W (ya que $f \in \mathfrak{p} = \mathcal{J}(W)$), entonces $f \neq 0$ en $k[V] \Rightarrow \mathcal{V}(f) \subset V$ y como f se anula en W entonces $W \subset \mathcal{V}(f)$, por lo que se tiene:

$$W \subset \mathcal{V}(f) \subset V$$

y W debe ser componente irreducible de $\mathcal{V}(f)$ porque de no serlo no sería máximo en V.

Por el teorema anterior $\mathcal{V}(f)$ es puro de dimensión $\dim V - 1$ y al ser W una de sus componentes irreducibles se cumple $\dim W = \dim \mathcal{V}(f) = \dim V - 1$. ■

Teorema 4.4. La dimensión de una variedad V es el supremo de las longitudes de las cadenas de subconjuntos cerrados irreducibles no vacíos de V

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_n \qquad (4.3)$$

También, la dimensión de V es el supremo de las longitudes de las cadenas de ideales primos del anillo de coordenadas $k[V]$

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \qquad (4.4)$$

Demostración. Por el corolario (2.87) la variedad V es un espacio topológico noetheriano por lo que las cadenas tipo (4.3) son finitas. Considere $V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_d$ una cadena de cerrados irreducibles no vacíos de V que sea máxima. Por el anterior corolario (4.3), ya que los elementos deben ser irreducibles máximos propios, se tiene:

$$\dim V_{i+1} = \dim V_i - 1, \text{ para } i = 0, \dots, d-1.$$

Esto implica que:

$$\dim V_0 = \dim V_1 + 1 = \dim V_2 + 1 + 1 = \cdots = \dim V_{d-1} + (d-1) = \dim V_d + d.$$

Como V es afín, por proposición (2.97) sus puntos son irreducibles, y como la cadena es máxima ha de cumplirse que V_d es un punto y por lo tanto de dimensión 0, entonces:

$$\dim V_0 = \dim V_d + d = 0 + d = d, \text{ con } V = V_0.$$

Por lo tanto, $\dim V = d$. Finalmente, a las cadenas tipo (4.3) de cerrados irreducibles no vacíos de V se le puede aplicar el lema (2.72) y lema (2.75) para obtener:

$$\mathfrak{p}_0 = \mathcal{J}(V_0) \subsetneq \mathfrak{p}_1 = \mathcal{J}(V_1) \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathcal{J}(V_d)$$

una sucesión de ideales primos de $k[V]$ del tipo (4.4), siendo esta también máxima porque la cadena de donde provienen lo es. ■

Este último teorema hace que aparezca la siguiente definición.

Definición 4.5. Si X es un espacio topológico, su dimensión (topológica de Krull), denotado $\dim X$, es el supremo de las longitudes de las cadenas de subconjuntos cerrados irreducibles no vacíos de X:

$$Z_0 \supsetneq Z_1 \supsetneq \cdots \supsetneq Z_n \qquad (4.5)$$

Zaldívar (s.f.).

Esta definición se acomoda al teorema 4.4 pudiendo afirmar que la dimensión de una variedad es su dimensión topológica de Krull.

Definición 4.6. La dimensión de Krull de un anillo A es el supremo de las longitudes de las cadenas de ideales primos de A, y también lo denotaremos como $\dim A$. Zaldívar (s.f.).

De manera similar a la idea anterior, esta definición también se acomoda al teorema 4.4, afirmado que la dimensión de una variedad es la dimensión de Krull del anillo de coordenadas $k[V]$.

A continuación, una propiedad que debe ser natural al concepto de dimensión.

Proposición 4.7. Sea X un espacio topológico. Si $Y \subset X$ es cualquier subconjunto, entonces $\dim Y \leq \dim X$.

Demostración. Si $Y_1 \supset Y_2$ son cerrados irreducibles de Y y si $X_i = \bar{Y}_i$ son sus cerraduras en X, entonces por corolario (2.83) los X_i son irreducibles en Y y $X_1 \supsetneq X_2$, luego el resultado sigue ya que si no ocurre $X_1 \supsetneq X_2 \supsetneq \cdots \supsetneq X_n$ la dimensión será estricta. ■

4.3. Consecuencias 2

En Zaldívar (s.f.), p. 85, el autor menciona que *el Teorema del ideal principal de Krull (4.9)*, ***puede ser algebrizado***, tal demostración implicó tratar con un polinomio irreducible f, y por ende con el ideal primo $\langle f \rangle = \mathfrak{p}$.

Esta investigación propone demostrar este resultado, pero para eso se necesita de una definición y un resultado dado, que generaliza el Teorema del ideal principal de Krull, pero aún no lo algebriza.

Definición 4.8. Si X es un espacio topológico de dimensión de Krull $\dim X$ finita, por proposición (4.7), para todo subespacio $Y \subseteq X$ se tiene que $\dim Y \leq \dim X$. Se define la codimensión de Y en X como

$$\operatorname{codim} Y = \operatorname{codim}_X Y = \dim X - \dim Y.$$

Zaldívar (s.f.).

De tener una subvariedad $W \subset V$ de una variedad afín V, la codimensión de W en V es

$$\operatorname{codim} W = \operatorname{codim}_V W = \dim V - \dim W.$$

Corolario 4.9. Si tenemos $V \subset \mathbb{A}_k^n$ es una variedad afín (irreducible), r funciones regulares en V $f_1, \dots, f_r \in k[V]$ y W es una componente irreducible de $\mathcal{V}(f_1, \dots, f_r)$, entonces

$$\operatorname{codim} W \leq r,$$

es decir, $\dim W \geq \dim V - r$. Equivalentemente, $\dim \mathcal{V}(f_1, \dots, f_r) \geq \dim V - r$.

Demostración. Ver Zaldívar (s.f.) 89, Proposición 3.14.

Este corolario ha generalizado el Teorema del ideal principal de Krull.

A continuación, el resultado central de esta sección.

Proposición 4.10. Si A es una k-álgebra, i.e., $A = k[x_1, \dots, x_n]/I$, y si $f \in A$ no es cero ni unidad y si $\mathfrak{p}$ es un ideal primo de A, mínimo entre los ideales que contienen a f, entonces

$$\dim A/\mathfrak{p} = \dim A - 1.$$

Demostración. Como f no es unidad, entonces f posee un cero en $\mathcal{V}(I)$; de lo contrario se podría definir un g tal que $fg = 1_{\mathcal{V}(I)}$, teniendo como ceros el conjunto vacío; así f tiene al menos un cero, luego por el teorema del ideal principal de Krull $\mathcal{V}(f)$ es pura de dimensión $\dim A - 1$.

De hipótesis $f \in A = k[\mathcal{V}(I)]$, por corolario (4.9), si W es una componente irreducible de $\mathcal{V}(f)$

$$\begin{aligned} &\Rightarrow \operatorname{codim} W \leq 1 \\ &\Rightarrow \dim A - \dim W \leq 1 \\ &\Rightarrow \dim A - 1 \leq \dim W \qquad (4.6) \end{aligned}$$

Además, es claro que $W \subset \mathcal{V}(f)$

$$\begin{aligned} &\Rightarrow (f) \subset \mathcal{J}(W) \\ &\Rightarrow (f) \subset \mathfrak{p} \subset \mathcal{J}(W), \end{aligned}$$

ya que $\mathcal{J}(W)$ es un ideal primo que contiene a f y $\mathfrak{p}$ es un ideal primo mínimo respecto a esta propiedad, luego viendo las dimensiones de los ceros de estos conjuntos y usando la expresión (4.6) se tiene

$$\Rightarrow W \subset \mathcal{V}(\mathfrak{p}) \subset \mathcal{V}(f) \Rightarrow \dim A - 1 \leq \dim W \leq \dim A/\mathfrak{p} \qquad (4.7)$$

Para la otra desigualdad, para cualquier cadena máxima (de mayor longitud) en $A/\mathfrak{p}$

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_{\dim A/\mathfrak{p}} \qquad (4.8)$$

de ideales primos de $A/\mathfrak{p}$. Por el teorema de correspondencia se puede hacer corresponder

$$\mathfrak{q}_i \leftrightarrow \text{Ideales primos de } A \text{ que contienen a } \mathfrak{p}$$

por lo que se tiene una cadena de ideales primos en A de longitud $\dim A/\mathfrak{p}$

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{\dim A/\mathfrak{p}} \qquad (4.9)$$

En el primer eslabón de la cadena (4.8) el ideal $\mathfrak{q}_0$ es 0 en $A/\mathfrak{p} \Rightarrow \mathfrak{p}_0 = \mathfrak{p}$ en A, por lo que la cadena (4.9) aún puede ser extendida al menos 1 eslabón más, por lo que se puede afirmar

$$\dim A \geq \dim A/\mathfrak{p} + 1 \Rightarrow \dim A - 1 \geq \dim A/\mathfrak{p}.$$

Usando la última desigualdad obtenida y la desigualdad en (4.10) se obtiene el resultado. ■

V. DISCUSIÓN DE RESULTADOS

5.1. La proposición 3.3 dice que dado un polinomio f de un anillo de coordenadas que es un DFU, entonces las componentes irreducibles tienen la misma dimensión disminuida en 1 respecto a la variedad en la que están, que es muy parecido a lo que se busca, sin embargo, ser un DFU es una condición muy restrictiva.

5.2. Por otro lado, los resultados de Noether dicen: dada una k-álgebra de grado de trascendencia d (y por ende una variedad de dimensión d), puede ser proyectada de manera finita en un espacio afín d-dimensional, todo esto sin hacer mención a si el anillo de coordenadas afín es o no DFU, esto no da una pista importante.

5.3. Es decir, si f genera un conjunto algebraico afín no vacío, este se va poder proyectar a algún espacio de afín de cierta dimensión, dicho de otra forma, el anillo de coordenadas de la variedad, por ejemplo, un $k[V]$, va a contener un anillo de coordenadas "más ordenado", por ejemplo, algún $k[y_1, \dots, y_d]$, y en este tipo de anillos es más sencillo ver su cuerpo de fracciones y por ende ver la extensión de cuerpos que pide la definición de dimensión.

5.4. Con todo esto en mente se vio el resultado central de este trabajo de investigación, para esto se necesitó de un resultado que se pudo haber dado en la sección preliminar del marco teórico, pero por su importancia en la prueba se mencionó al iniciar tal sección.

5.5. La condición que se le dio al polinomio f es ser no nulo (para que no genere toda la variedad), y para no ser vacío f debe poseer al menos un cero en la variedad.

VI. CONCLUSIONES

6.1. Dada una variedad algebraica V, para que las componentes irreducibles del conjunto algebraico de un polinomio f de $k[V]$ afín tengan la misma dimensión es necesario que el polinomio f de $k[V]$ sea no nulo, y al menos tenga un cero en la variedad V.

6.2. Lo anterior permite que se puedan obtener cadenas de subconjuntos irreducibles maximales, todo esto de manera finita, por lo que se puede definir una dimensión topológica y además otra relacionada al anillo de coordenadas, en lugar de la dimensión en términos de la extensión trascendente del cuerpo de fracciones del anillo de coordenadas.

6.3. El teorema del ideal principal de Krull se pudo algebrizar, en el sentido que el resultado inicial considera a un polinomio f, pero luego se logra considerar cierto tipo de ideal. Esto es una ventaja, ya que en la teoría del algebra conmutativa la principal herramienta de trabajo son justamente los ideales.

6.4. La propiedad minimal que se le dio al ideal del último resultado se interpreta del siguiente modo: en una cadena decreciente de variedades que trata de tener la mayor longitud, las variedades que la conformen deben ser lo más grande posible, llevando esto al caso de los ideales, si se tiene una cadena creciente de ideales primos que trata de tener la mayor longitud, los ideales que la conformen deben ser las más pequeñas "en lo posible", para que la cadena pueda tener la mayor cantidad de eslabones posibles.

VII. RECOMENDACIONES

7.1. Para entender el trabajo es necesario manejar conocimientos de álgebra conmutativa, topología y de manera puntual las definiciones de categoría y funtor.

7.2. Este trabajo puede ser extendido para el estudio de las dimensiones de las variedades que se encuentran en el plano proyectivo, el enfoque es similar, pero hay que tener ciertas consideraciones en el tipo de anillo que se utilice debido a la naturaleza del espacio proyectivo.

7.3. Este trabajo también puede ser extendido para el estudio de las dimensiones de los espacios tangentes de variedades, el enfoque es el mismo, pero se necesitan definiciones adicionales además muchas ideas de la geometría diferencial.

7.4. Este trabajo puede servir como preámbulo al estudio de la geometría algebraica en la que los anillos son generalizados al punto de ser solamente eso, anillos conmutativos, y no necesariamente ser el anillo cociente de algún anillo de polinomios, es decir ser una k-álgebra afín. El lector irá encontrando paralelismos entre los conceptos, teniendo como base este trabajo.

VIII. REFERENCIAS

Águeda, R. (s.f.), *Variedades Algebraicas y Esquemas, Una introducción a la Geometría Algebraica*, Universidad Nacional Autónoma de México. https://www.yumpu.com/es/document/read/14567960/variedades-algebraicas-y-esquemas-intermat-unam/1

Atiyah, M. y MacDonald, I. (1978), *Introducción al álgebra conmutativa*, Reverté.

Del Río, A., Simón, J. y Del Valle, A. (2001), *Álgebra básica*, Universidad de Murcia.

Dummit, D. y Foote, R. (2004), *Abstract Algebra – 3era (tercera) edición*. John Wiley & Son.

Harris, J. (1992), *Algebraic Geometry, A First Course*, Springer.

Hartshorne, R. (1977), *Algebraic Geometry*, Springer.

Ivorra, C. (s.f.), *Geometría Algebraica*. https://www.uv.es/ivorra/Libros/GA.pdf

Jara, P. (2017), *Notas de trabajo 16, Extensiones de cuerpos*, Universidad de Granada. http://www.ugr.es/~anillos/textos/pdf/2017/4000-TGalois.Texto.pdf

Kending, K. (1977), *Elementary Algebraic Geometry*, Springer.

Navarro, J. (2013), *Álgebra Conmutativa Básica*. https://matematicas.unex.es/~navarro/acb.pdf

Sancho, F. y Sancho, P. (2012), *Geometría Algebraica*. https://es.scribd.com/document/596447973/Geometria-Algebraica-Fernando-Sancho-y-Pedro-Sancho

Sancho, C. y Sancho, P. (2013), *Álgebra Conmutativa y Geometría Algebraica*. https://matematicas.unex.es/~sancho/LibroGeometriaAlgebraica/LibroUnex.pdf

Solotar, A., Farinati, M. y Suárez, M. (2007), *Anillos y sus categorías de representaciones*, Universidad de Buenos Aires.

Zaldívar, F. s.f., *Notas de geometría algebraica*. https://www.yumpu.com/es/document/read/14567725/notas-de-geometra-algebraica-instituto-de-matematicas-de-la-unam