Una Introducción a las **Subálgebras de Mishchenko-Fomenko**

Wilson Fernando Mutis Cantero
Fernando Andrés Benavides Agredo
German Benitez Monsalve

Editorial
Universidad de Nariño

êditorial
Universidad de Nariño

Una introducción a las subálgebras de Mishchenko-Fomenko

Una introducción a las subálgebras de Mishchenko-Fomenko

Wilson Fernando Mutis Cantero
Fernando Andrés Benavides Agredo
Germán Benitez Monsalve

êditorial
Universidad de **Nariño**

Mutis Cantero, Wilson Fernando
Una introducción a las subálgebras de Mishchenko-Fomenko / Wilson Fernando Mutis Cantero, Fernando Andrés Benavides Agredo, Germán Benítez Monsalve—1ª. ed. – San Juan de Pasto : Editorial Universidad de Nariño, 2025

124 páginas : ilustraciones, gráficas

Incluye referencias bibliográficas p. 121-122
ISBN: 978-628-7771-30-7

1. Álgebra de Lie 2. Anillos graduados 3. Geometría algebraica 4. Subálgebras de Mishchenko-Fomenko 5. Álgebra envolvente universal. I. Benavides Agredo, Fernando Andrés II. Benítez Monsalve, Germán

512.482 M992 – SCDD-Ed. 22

SECCIÓN DE BIBLIOTECA

Una introducción a las subálgebras de Mishchenko-Fomenko

©Wilson Fernando Mutis Cantero
wilsonmutis@udenar.edu.co
©Fernando Andrés Benavides Agredo
fandresbenavides@udenar.edu.co
©Germán Benitez Monsalve
gabm@ufam.edu.br

ISBN: 978-628-7771-30-7
Primera edición

Corrección de estilo: Ricardo Erazo Mera
Diseño de portada: Liseth Motta Realpe
Diagramación: Fernando Andrés Benavides Agredo

Fecha de publicación: abril de 2025
San Juan de Pasto - Nariño

Índice general

Introducción

El libro *Una introducción a las subálgebras de Mishchenko-Fomenko* es el resultado del proyecto de investigación titulado **subálgebras de Mishchenko-Fomenko en $U(\mathfrak{gl}_n)$ y secuencias regulares**, desarrollado gracias al respaldo financiero de la Vicerrectoría de Investigación e Interacción Social de la Universidad de Nariño.

La teoría de álgebras de Lie, cuyo desarrollo comenzó debido a los trabajos de Sophus Lie en el siglo XIX, ocupa un lugar de importancia en la matemática moderna y a lo largo del tiempo, ha demostrado ser fundamental no solo en el avance de esta disciplina, sino también en sus múltiples aplicaciones en diversas áreas del conocimiento, desde la geometría diferencial y la teoría de grupos de Lie hasta la física teórica. La comprensión de esta teoría puede ser especialmente desafiante incluso para matemáticos experimentados, debido a la complejidad conceptual de sus temáticas y el requisito de tener conocimientos básicos de otras áreas como la geometría, el álgebra y la topología.

Con este libro, los autores pretenden ofrecer una introducción comprensiva a las álgebras de Lie y sus representaciones, combinando rigor matemático con un enfoque didáctico, con el cual se espera que el lector alcance un mejor entendimiento de los temas que aquí se exponen. Aunque la mayoría de las demostraciones que aparecen en este texto no son originales, es de resaltar el esfuerzo de los autores por presentar pruebas detalladas que permitan una profunda comprensión de los complejos conceptos matemáticos que se estudian, tomando distancia de los libros especializados que, en general, omiten muchos detalles de las pruebas y, con ello, dificultan la accesibilidad a la teoría.

El otro propósito de este texto es hacer una introducción al problema de determinar si las subálgebras de Mishchenko-Fomenko son generadas por una secuencia regular de polinomios en el álgebra simétrica del álgebra de Lie $\mathfrak{gl}_n$. Las subálgebras de Mishchenko-Fomenko son una clase particularmente importante de subálgebras conmutativas las cuales juegan un papel crucial en la teoría de representaciones del álgebra de Lie.

El texto se estructura en cinco capítulos. El primero ofrece los fundamentos básicos de la teoría de álgebras de Lie, incluidas sus definiciones y propiedades esenciales. El segundo aborda una introducción general a las álgebras graduadas y filtradas haciendo énfasis en el álgebra envolvente universal de un álgebra de Lie de dimensión finita y el teorema PBW, que permite identificar el álgebra simétrica con el álgebra de polinomios. Con estos temas se pretende guiar al lector desde los conceptos básicos de las álgebras graduadas hasta su relación con la teoría de representaciones de álgebras de Lie.

El tercer capítulo elabora una sencilla pero rigurosa introducción a la geometría algebraica, incluyendo los conceptos y resultados fundamentales de los conjuntos algebraicos afines y su relación con el álgebra de polinomios en varias indeterminadas. De esta manera, se hace un preámbulo al concepto de dimensión de una variedad algebraica afín, el cual es indispensable para determinar si las subálgebras de Mishchenko-Fomenko en $\mathfrak{gl}_n$ son generadas por una secuencia regular.

El cuarto capítulo está dedicado a desarrollar el concepto de secuencias regulares en anillos conmutativos. El estudio de estas secuencias proporciona una base sólida para avanzar en el análisis de la dimensión de variedades algebraicas.

El último capítulo desarrolla una presentación no rigurosa de las subálgebras de Mishchenko-Fomenko en $S(\mathfrak{gl}_n)$. Aunque la falta de formalismo en la definición de estas subálgebras puede parecer desconcertante para matemáticos versados en esta temática, el objetivo es permitir a los lectores no experimentados captar las ideas centrales sin perderse en la complejidad formal de la temática, y de esta manera, darle la oportunidad de comprender el problema de investigación, en concreto, determinar si las subálgebras de Mishchenko-Fomenko son generadas por una secuencia regular de polinomios en $S(\mathfrak{gl}_n)$. Asimismo, este capítulo expone el resultado principal obtenido durante la investigación.

Además, en los apéndices de este libro, los lectores cuentan con un soporte teórico que les permite profundizar en los temas tratados. En este capítulo se incluye información clave que cubre los conceptos fundamentales necesarios para entender el contenido del texto, como definiciones, ejemplos prácticos y explicaciones detalladas de ciertos teoremas que refuerzan los conocimientos básicos requeridos. De esta manera, los apéndices ofrecen una guía complementaria para que el lector asegure una comprensión sólida de los temas expuestos en este texto.

Por último, los autores quieren reiterar su enorme agradecimiento a la Vicerrectoría de Investigación e Interacción Social de la Universidad de Nariño por su gran colaboración para que este libro sea una realidad y confian en que el texto sirva, por un lado, como una guia para quienes estén interesados en comenzar a estudiar la teoría de álgebras de Lie y sus representaciones y, por otro, que se convierta en una fuente de inspiración para futuras investigaciones en esta rica y dinámica área de las matemáticas.

Universidad de Nariño
Febrero de 2025

CAPÍTULO 1

Álgebras de Lie

En este capítulo se presentan las definiciones básicas y los resultados más relevantes de la teoría de álgebras de Lie. Asimismo, se exponen diferentes ejemplos para que el lector tenga una mejor comprensión de los conceptos a presentarse. Pese a que la teoría de álgebras de Lie se puede desarrollar sobre cualquier cuerpo, en adelante solo se considerarán álgebras de Lie sobre el cuerpo $\mathbb{C}$ de los números complejos; sin embargo, todos los resultados que aquí se presenten son válidos para álgebras de Lie sobre cuerpos algebraicamente cerrados de característica cero. El lector interesado en profundizar en estos temas puede consultar Humphreys (1997) o SanMartin (1999).

1.1 Álgebras y subálgebras de Lie

Definición 1.1 (**Álgebra y álgebra asociativa**)**.** Un álgebra sobre el cuerpo $\mathbb{C}$ es un espacio vectorial $\mathcal{A}$ sobre $\mathbb{C}$, junto con un aplicación $\mathbb{C}$-bilineal $* : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$, llamada multiplicación. Esto significa que para cada par de vectores $x, y \in \mathcal{A}$ existe un único vector $x * y \in \mathcal{A}$ y se satisfacen las condiciones de bilinealidad sobre $\mathbb{C}$, es decir, para toda terna de vectores $x, y, z \in \mathcal{A}$ y todo par de escalares $\alpha, \beta \in \mathbb{C}$, se tiene,

1. $(\alpha x + \beta y) * z = \alpha(x * z) + \beta(y * z)$.
2. $z * (\alpha x + \beta y) = \alpha(z * x) + \beta(z * y)$.

Además, se dice que $\mathcal{A}$ es asociativa si para toda terna $x, y, z \in \mathcal{A}$ se cumple $x * (y * z) = (x * y) * z$.

Es usual escribir $\mathbb{C}$-álgebra, álgebra compleja o simplemente álgebra para expresar que se tiene un álgebra sobre el cuerpo $\mathbb{C}$ de los números complejos y, buscando familiarizar al lector con estas expresiones, a lo largo de este texto se utilizarán en forma indistinta.

Ejemplo 1.1. Para cada entero $n > 0$, el espacio $M_n(\mathbb{C})$ de las matrices cuadradas de orden n y componentes complejas, con la multiplicación usual de matrices es una $\mathbb{C}$-álgebra asociativa. Igualmente, son álgebras asociativas: el cuerpo $\mathbb{C}$ con la multiplicación usual de números complejos, el anillo $\mathcal{P}$ de polinomios en un variable y coeficientes complejos con la multiplicación usual de polinomios y el $\mathbb{C}$-espacio vectorial $\mathcal{F}$ de las funciones $f : \mathbb{C} \to \mathbb{C}$ con la multiplicación definida por

$$(fg)(x) = f(x)g(x), \text{ para todo par de funciones } f, g \in \mathcal{F},$$

.

Definición 1.2 (**Álgebra de Lie**)**.** Un álgebra de Lie compleja es una $\mathbb{C}$-algebra $\mathfrak{g}$, con vector nulo $\mathbf{0}$, y multiplicación $[,] : \mathfrak{g} \times \mathfrak{g} \longrightarrow \mathfrak{g}$, llamada corchete de Lie, tal que a cada par ordenado $(x, y) \in \mathfrak{g} \times \mathfrak{g}$ asigna el vector $[x, y] \in \mathfrak{g}$, satisfaciendo las siguientes propiedades:

1. **Anticonmutatividad:** Para todo vector $x \in \mathcal{A}$, se tiene, $[x, x] = \mathbf{0}$.
2. **Identidad de Jacobi:** Para cualesquier tres vectores $x, y, z \in \mathfrak{g}$, se tiene,

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = \mathbf{0}.$$

Observación 1.1. Todo $\mathbb{C}$-espacio vectorial V tiene estructura de álgebra de Lie definiendo el corchete trivialmente, es decir

$$[x, y] = \mathbf{0}, \text{ para todo par de vectores } x, y \in V.$$

Esta estructura de $\mathbb{C}$-álgebra de Lie se denomina **abeliana** y no tiene un mayor interés teórico.

La identidad de Jacobi no es una condición simplemente técnica, su presencia en la definición de álgebra de Lie asegura la coherencia matemática necesaria para que estas estructuras sean útiles tanto en teoría abstracta como en aplicaciones prácticas. Un álgebra de Lie, en general, no es asociativa ya que la identidad de Jacobi garantiza una estructura algebraica que es más general que la asociatividad estricta, sin embargo existe una relación entre la teoría de álgebras asociativas y la de álgebras de Lie, debido a que toda $\mathbb{C}$-álgebra asociativa induce sobre sí misma una estructura de $\mathbb{C}$-álgebra de Lie, como se ilustra en el siguiente ejemplo:

Ejemplo 1.2. Considere el álgebra asociativa $M_n(\mathbb{C})$, de las matrices cuadradas de orden n y componentes complejas, con la multiplicación usual de matrices. Para dar una estructura de $\mathbb{C}$-álgebra de Lie a $M_n(\mathbb{C})$, se define el corchete como sigue:

$$[A, B] = AB - BA, \text{ para todo par de matrices } A, B \in M_n(\mathbb{C}).$$

En efecto, considere las matrices $A, B, C \in M_n(\mathbb{C})$ y sean $\alpha, \beta \in \mathbb{C}$, por las propiedades de la suma y multiplicación de matrices, se tiene,

$$\begin{aligned}
[\alpha A + \beta B, C] &= (\alpha A + \beta B)\, C - C\,(\alpha A + \beta B) \\
&= \alpha\,(AC - CA) + \beta\,(BC - CB) \\
&= \alpha[A, C] + \beta[B, C]
\end{aligned}$$

de forma similar se cumple la segunda condición de bilinialidad, la anticonmutatividad es inmediata y en seguida se prueba la identidad de Jacobi:

$$\begin{aligned}
[A, [B, C]] + [B, [C, A]] &= [A, BC - CB] + [B, CA - AC] \\
&= A(BC) + (CB)A - B(AC) - (CA)B \\
&= -\,(C(AB - BA) - (AB - BA)C) \\
&= -\,[C, AB - BA] \\
&= -\,[C, [A, B]]\,.
\end{aligned}$$

Con $\mathfrak{gl}_n$ se denota la estructura de álgebra de Lie de $M_n(\mathbb{C})$. En general, si $\mathcal{A}$ es un álgebra asociativa, entonces $\mathcal{A}$ tiene estructura de álgebra de Lie definiendo el corchete de la siguiente manera:

$$[x, y] = xy - yx, \text{ para todo par de vectores } x, y \in \mathcal{A}. \tag{1.1}$$

Para probar que la ecuación (1.1) define una estructura de $\mathbb{C}$-álgebra de Lie en el álgebra asociativa $\mathcal{A}$, se procede de forma similar a la prueba presentada para $\mathfrak{gl}_n$, de hecho, $\mathfrak{gl}_n$ es un caso particular de esta situación general. Similarmente, si V es un $\mathbb{C}$-espacio vectorial, entonces el espacio $Hom(V)$ de las transformaciones $\mathbb{C}$-lineales de V en V, con la composición de funciones, es un álgebra asociativa, y con el corchete definido en la ecuación (1.1), se tiene que $Hom(V)$ es un álgebra de Lie que se denotará $\mathfrak{gl}(V)$.

Ejemplo 1.3. (Suma directa de álgebras de Lie) Si $\mathfrak{g}$ y $\mathfrak{s}$ son dos $\mathbb{C}$-álgebras de Lie, la suma directa $\mathfrak{g} \oplus \mathfrak{s} = \{(w, x) : w \in \mathfrak{g}, x \in \mathfrak{s}\}$ tiene estructura de álgebra de Lie, definiendo el corchete de dos vectores $(w, x), (y, z) \in \mathfrak{g} \oplus \mathfrak{s}$ como sigue:

$$[(w, x), (y, z)] = ([w, y], [x, z]) .$$

La suma de vectores y la multiplicación por escalar en $\mathfrak{g} \oplus \mathfrak{s}$, junto con la bilinealidad de los corchetes en $\mathfrak{g}$ y $\mathfrak{s}$, garantizan la bilinealidad del corchete definido en $\mathfrak{g} \oplus \mathfrak{s}$. Para la anticonmutatividad, sea $(u, x) \in \mathfrak{g} \oplus \mathfrak{s}$, entonces

$$[(u, x), (u, x)] = ([u, u], [x, x]) = (\mathbf{0}, \mathbf{0}).$$

La identidad de Jacobi en $\mathfrak{g} \oplus \mathfrak{s}$, se prueba de forma similar y se deja como ejercicio para el lector.

Proposición 1.1. Si $\mathfrak{g}$ es un álgebra de Lie sobre un cuerpo $\mathbb{C}$ y $x, y \in \mathfrak{g}$, entonces

1. $[x, y] = -[y, x]$.
2. $[x, \mathbf{0}] = [\mathbf{0}, x] = \mathbf{0}$.
3. Si $[x, y] \neq \mathbf{0}$, entonces $\{x, y\}$ es linealmente independiente sobre $\mathbb{C}$.

Demostración. De la anticonmutatividad se tiene $[x - y, x - y] = \mathbf{0}$, y de la bilinealidad del corchete se sigue

$$[x, x] - [x, y] - [y, x] + [y, y] = -[x, y] - [y, x] = \mathbf{0},$$

entonces $[x, y] = -[y, x]$. El segundo ítem es consecuencia de las siguientes igualdades:

$$[x, \mathbf{0}] = [x, \mathbf{0} + \mathbf{0}] = [x, \mathbf{0}] + [x, \mathbf{0}],$$

similarmente,

$$[\mathbf{0}, x] = [\mathbf{0} + \mathbf{0}, x] = [\mathbf{0}, x] + [\mathbf{0}, x].$$

Para mostrar el tercer enunciado, note que el ítem anterior garantiza que $x \neq \mathbf{0}$ y $y \neq \mathbf{0}$, cuando $[x, y] \neq \mathbf{0}$. Sean $\alpha, \beta \in \mathbb{C}$, tales que $\alpha x + \beta y = \mathbf{0}$, entonces

$$\mathbf{0} = [x, \mathbf{0}] = [x, \alpha x + \beta y] = \alpha[x, x] + \beta[x, y] = \beta[x, y].$$

Pero $[x, y] \neq \mathbf{0}$, luego $\beta = 0$, en consecuencia, $\alpha x = \mathbf{0}$ y se tiene $\alpha = 0$. Por tanto, el conjunto $\{x, y\}$ es linealmente independiente sobre $\mathbb{C}$. $\square$

Proposición 1.2. Si $\mathfrak{g}$ es un álgebra de Lie compleja no abeliana de dimensión 2, entonces existe una $\mathbb{C}$-base $\{x, y\}$ de $\mathfrak{g}$, tal que $[x, y] = y$.

Demostración. Sea $\{u, w\}$ una $\mathbb{C}$-base para $\mathfrak{g}$, luego existen escalares $\alpha, \beta \in \mathbb{C}$, tales que

$$[u, w] = \alpha u + \beta w.$$

Dado que $\mathfrak{g}$ es no abeliana, se debe tener $[u, w] \neq \mathbf{0}$, y no se pierde generalidad en suponer que $\beta \neq 0$, entonces

$$[u, [u, w]] = [u, \alpha u + \beta w] = \alpha[u, u] + \beta[u, w] = \beta[u, w],$$

luego $[u, w] = \frac{1}{\beta}[u, [u, w]] = \left[\frac{1}{\beta}u, [u, w]\right]$. Ahora, tomando $x = \frac{1}{\beta}u$ y $y = [u, w]$, se tiene, $y = [x, y] \neq \mathbf{0}$. Por la Proposición (1.1), el subconjunto $\{x, y\}$ es una $\mathbb{C}$-base para $\mathfrak{g}$ que cumple la condición solicitada. $\square$

Definición 1.3 (Subálgebra de Lie). Sea $\mathfrak{g}$ una $\mathbb{C}$-álgebra de Lie. Una subálgebra de Lie (o simplemente subálgebra) es un subespacio $\mathfrak{s}$ de $\mathfrak{g}$ que es cerrado para el corchete definido en $\mathfrak{g}$, es decir

$$[x, y] \in \mathfrak{s}, \text{ para todo par de vectores } x, y \in \mathfrak{s}.$$

Observación 1.2. En toda álgebra de Lie $\mathfrak{g}$, los subespacios $\{\mathbf{0}\}$ y $\mathfrak{g}$ son subálgebras de $\mathfrak{g}$. De hecho, para todo vector $x \in \mathfrak{g}$ el subespacio $span\{x\} = \{\alpha x : \alpha \in \mathbb{C}\}$ es una subálgebra abeliana de $\mathfrak{g}$.

Ejemplo 1.4. Sea $\tau_n = \{A \in \mathfrak{gl}_\mathfrak{n} : A \text{ es triangular superior}\}$. Se conoce que τ_n es un subespacio de $\mathfrak{gl}_\mathfrak{n}$ cerrado para la suma y multiplicación de matrices, entonces para todo par de matrices $A, B \in \tau_n$, se tiene, $[A, B] = AB - BA \in \tau_n$. En consecuencia, τ_n es una subálgebra de $\mathfrak{gl}_n$.

Ejemplo 1.5. El subespacio δ_n de $\mathfrak{gl}_n$ conformado por las matrices diagonales es una subálgebra abeliana de $\mathfrak{gl}_n$. En efecto, δ_n es una subálgebra de $\mathfrak{gl}_n$ porque es cerrado para la suma y multiplicación de matrices. Además, el producto de matrices es conmutativo en δ_n, es decir, para todo par de matrices $A, B \in \delta_n$, se cumple $[A, B] = AB - BA = \mathbf{0}$.

Definición 1.4 (Centro). Sea $\mathfrak{g}$ un álgebra de Lie compleja. El centro de $\mathfrak{g}$, denotado $Z(\mathfrak{g})$, es el conjunto de vectores de $\mathfrak{g}$ que conmutan con todo elemento de $\mathfrak{g}$, es decir

$$Z(\mathfrak{g}) = \{x \in \mathfrak{g} : [x, y] = \mathbf{0}, \text{ para todo } y \in \mathfrak{g}\}.$$

La Proposición (1.1) garantiza que $\mathbf{0} \in Z(\mathfrak{g})$ y, de la bilinealidad del corchete, se tiene que $Z(\mathfrak{g})$ es un subespacio de $\mathfrak{g}$. El lector puede comprobar que dados dos vectores $x, y \in Z(\mathfrak{g})$, se tiene $[x, y] \in Z(\mathfrak{g})$. Por tanto, $Z(\mathfrak{g})$ es una subálgebra de $\mathfrak{g}$.

Ejemplo 1.6. Sea n un entero mayor que 1 y sea I_n la matriz idéntica de orden n, se probará que

$$Z(\mathfrak{gl}_n) = span\{I_n\} = \{\alpha I_n : \alpha \in \mathbb{C}\}.$$

En efecto, sea $A = (a_{ij})_{n\times n}$ una matriz de $Z(\mathfrak{gl}_n)$, entonces

$$AB = BA, \text{ para toda matriz } B \in \mathfrak{gl}_n.$$

Para $i, j = 1, \ldots, n$ sea E_{ij} la matriz de $\mathfrak{gl}_n$ cuya ij-ésima componente es 1 y las otras componentes son iguales a 0, entonces

$$AE_{ii} = \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ii} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix},$$

también,

$$E_{ii}A = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} \\ 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}.$$

Dado que $AE_{ii} = E_{ii}A$, se deduce que

$$a_{ij} = 0, \text{ siempre que } i \neq j.$$

Luego, A es un elemento de la subálgebra δ_n de matrices diagonales de orden n, más aún,

$$A = a_{11}E_{11} + \cdots + a_{nn}E_{nn}.$$

Ahora, para $j = 2, \ldots, n$ se tiene

$$AE_{1j} = a_{11}E_{1j} \quad \text{y} \quad E_{1j}A = a_{jj}E_{1j}$$

entonces $\left(a_{11} - a_{jj}\right)E_{1j} = \mathbf{0}$, así que

$$a_{jj} = a_{11}, \text{ para toda } j = 2, \ldots, n.$$

Luego, $A = a_{11}\left(E_{11} + \cdots + E_{nn}\right) = a_{11}I_n$. Por tanto

$$Z\left(\mathfrak{gl}_n\right) = \{\alpha I_n : a \in \mathbb{C}\} = span\left\{I_n\right\}.$$

Proposición 1.3. Sea $\mathfrak{g}$ un álgebra de Lie compleja. El corchete definido en $\mathfrak{g}$ es asociativo, si y solo si, para todo par de vectores $x, y \in \mathfrak{g}$ se tiene $[x, y] \in Z(\mathfrak{g})$.

Demostración. Sean $x, y, z \in \mathfrak{g}$ y suponga que el corchete definido en $\mathfrak{g}$ es asociativo, luego

$$[y, [z, x]] - [[y, z], x] = \mathbf{0}.$$

Lo anterior, junto con la Proposición (1.1), implican que

$$[z, [x, y]] = [x, [y, z]] + [y, [z, x]] + [z, [x, y]].$$

Por la identidad de Jacobi, se obtiene $[z, [x, y]] = \mathbf{0}$, lo que significa que $[x, y] \in Z(\mathfrak{g})$. Para el recíproco, suponga que $[x, y] \in Z(\mathfrak{g})$, para todo par de vectores $x, y \in \mathfrak{g}$. Por la definición de centro, se obtiene,

$$[[x, y], z] = \mathbf{0} = [x, [y, z]].$$

□

Proposición 1.4 (Normalizador). Si $\mathfrak{g}$ es un álgebra de Lie compleja y $\mathfrak{s}$ es una subálgebra de $\mathfrak{g}$, entonces el normalizador de $\mathfrak{s}$ en $\mathfrak{g}$, denotado $N_{\mathfrak{g}}(\mathfrak{s})$ y definido por

$$N_{\mathfrak{g}}(\mathfrak{s}) = \{x \in \mathfrak{g} : [x, y] \in \mathfrak{s}, \text{ para todo vector } y \in \mathfrak{s}\},$$

es una subálgebra de $\mathfrak{g}$ que contiene a $\mathfrak{s}$.

Demostración. Observe que $N_{\mathfrak{g}}(\mathfrak{s})$ es un subespacio de $\mathfrak{g}$ debido a que el corchete es una forma $\mathbb{C}$-bilineal. Ahora, sean $x, y \in N_{\mathfrak{g}}(\mathfrak{s})$ y sea $z \in \mathfrak{s}$, por la identidad de Jacobi se tiene

$$[x,[y,z]] + [y,[z,x]] = -[z,[x,y]] = [[x,y],z],$$

pero $[y,z]$ y $[z,x]$ son vectores de $\mathfrak{s}$, luego

$$[[x,y],z] = [x,[y,z]] + [y,[z,x]] \in \mathfrak{s},$$

entonces $[x,y] \in N_{\mathfrak{g}}(\mathfrak{s})$. Por tanto, $N_{\mathfrak{g}}(\mathfrak{s})$ es una subálgebra de $\mathfrak{g}$ y claramente $\mathfrak{s}$ está contenida en $N_{\mathfrak{g}}(\mathfrak{s})$. $\square$

Ejemplo 1.7. Recuerde que $\mathcal{T}_2$ es una subálgebra de $\mathfrak{gl}_2$, ver Ejemplo (1.4). Si la matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N_{\mathfrak{g}}(\mathcal{T}_2)$, entonces

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -b \\ c & 0 \end{pmatrix} \in \mathcal{T}_2.$$

Luego, $c = 0$, es decir $A \in \mathcal{T}_2$. Por tanto, $N_{\mathfrak{g}}(\mathcal{T}_2) = \mathcal{T}_2$.

Definición 1.5 (Centralizador). Sea $\mathfrak{g}$ un álgebra de Lie compleja y sea X un subconjunto de $\mathfrak{g}$, no vacío. El centralizador de X en $\mathfrak{g}$, denotado $C_{\mathfrak{g}}(X)$, es el conjunto de vectores de $\mathfrak{g}$ que conmutan con todos los vectores de X, es decir

$$C_{\mathfrak{g}}(X) = \{y \in \mathfrak{g} : [y,x] = \mathbf{0}, \ \text{para todo vector } x \in X\}.$$

Dado que el corchete es una aplicación bilineal, se deduce que $C_{\mathfrak{g}}(X)$ es un subespacio de $\mathfrak{g}$. Además, si $x \in X$ y los vectores $y, z \in C_{\mathfrak{g}}(X)$, entonces

$$[x,[y,z]] = -[y,[z,x]] - [z,[x,y]] = -[y,\mathbf{0}] - [z,\mathbf{0}] = \mathbf{0}.$$

Por tanto, $[y,z] \in C_{\mathfrak{g}}(X)$, es decir, $C_{\mathfrak{g}}(X)$ es una subálgebra de $\mathfrak{g}$. Asimismo, el lector puede notar que un vector $x \in Z(\mathfrak{g})$, si y solo si, $C_{\mathfrak{g}}(\{x\}) = \mathfrak{g}$.

Definición 1.6 (Ideal). Sea $\mathfrak{g}$ un álgebra de Lie compleja. Un ideal es un subespacio $\mathcal{I}$ de $\mathfrak{g}$, tal que para todo vector $x \in \mathcal{I}$ y todo vector $y \in \mathfrak{g}$, se tiene $[x,y] \in \mathcal{I}$.

Observe que los subespacios $\{\mathbf{0}\}$ y $\mathfrak{g}$ son ideales del álgebra de Lie $\mathfrak{g}$.

Ejemplo 1.8. Sea $\mathfrak{sl}_n$ el conjunto de matrices de $\mathfrak{gl}_n$ que tienen traza[1] igual a 0, es decir, $\mathfrak{sl}_n = \{A \in \mathfrak{gl}_n : tr(A) = 0\}$. Por la propiedad de linealidad de la traza, se sigue que $\mathfrak{sl}_n$ es un subespacio de $\mathfrak{gl}_n$, además se sabe que

$$tr(AB) = tr(BA), \text{ para todo par de matrices } A, B \in \mathfrak{gl}_n,$$

en particular, para matrices $A \in \mathfrak{sl}_n$ y $B \in \mathfrak{gl}_n$, se tiene

$$tr([A, B]) = tr(AB - BA) = tr(AB) - tr(BA) = 0,$$

luego $[A, B] \in \mathfrak{sl}_n$, por tanto, $\mathfrak{sl}_n$ es un ideal de $\mathfrak{gl}_n$.

Ejemplo 1.9. El centro $Z(\mathfrak{g})$ de un álgebra de Lie compleja $\mathfrak{g}$ es un ideal de $\mathfrak{g}$. En efecto, sea $x \in Z(\mathfrak{g})$ y sean $y, z \in \mathfrak{g}$, por la identidad de Jacobi, se tiene

$$[[x, y], z] = [x, [y, z]] + [y, [z, x]] = \mathbf{0} + [y, \mathbf{0}] = \mathbf{0},$$

por tanto, $[x, y] \in Z(\mathfrak{g})$, así que $Z(\mathfrak{g})$ es un ideal de $\mathfrak{g}$.

Observación 1.3. Todo ideal de un álgebra de Lie $\mathfrak{g}$ es una subálgebra de $\mathfrak{g}$, pero no toda subálgebra de $\mathfrak{g}$ es un ideal de $\mathfrak{g}$. Por ejemplo, para $n \geq 2$, la subálgebra τ_n de las matrices triangulares superiores de tamaño $n \times n$ no es un ideal de $\mathfrak{gl}_n$, porque $E_{11} \in \tau_n$ y $E_{n1} \in \mathfrak{gl}_n$; sin embargo

$$[E_{11}, E_{n1}] = E_{11}E_{n1} - E_{n1}E_{11} = -E_{n1} \notin \tau_n.$$

Proposición 1.5. Si $\mathfrak{g}$ es un álgebra de Lie compleja y $\mathfrak{s}$ es una subálgebra de $\mathfrak{g}$, entonces

$$N_{\mathfrak{g}}(\mathfrak{s}) = \mathfrak{g}, \text{ si y solo si, } \mathfrak{s} \text{ es un ideal de } \mathfrak{g}.$$

Demostración. Una consecuencia de las definiciones de normalizador (1.4) e ideal (1.6) es que $N_{\mathfrak{g}}(\mathfrak{s}) = \mathfrak{g}$, si y solo si, para toda $x \in \mathfrak{s}$ y toda $y \in \mathfrak{g}$ se cumple $[x, y] \in \mathfrak{s}$, lo cual equivale a decir que $\mathfrak{s}$ es un ideal de $\mathfrak{g}$. □

Proposición 1.6. Sea $\mathfrak{g}$ un álgebra de Lie compleja. Si $\mathcal{I}$ y $\mathcal{J}$ son dos ideales de $\mathfrak{g}$ y $\mathfrak{s}$ es una subálgebra de $\mathfrak{g}$, entonces

1. $\mathcal{I} \cap \mathcal{J}$ y $\mathcal{I} + \mathcal{J} = \{x + y : x \in \mathcal{I}, y \in \mathcal{J}\}$ son ideales de $\mathfrak{g}$.
2. $[\mathcal{I}, \mathcal{J}] = span\{[x, y] : x \in \mathcal{I}, y \in \mathcal{J}\}$ es un ideal de $\mathfrak{g}$. En particular, $\mathfrak{g}^{'} = [\mathfrak{g}, \mathfrak{g}]$ se denomina **álgebra derivada de** $\mathfrak{g}$.

[1] Recuerde que la traza de una matriz cuadrada $A = (a_{ij})_{n \times n}$, denotada $tr(A)$, es la suma de las componentes en su diagonal principal, es decir, $tr(A) = a_{11} + \cdots + a_{nn}$.

3. $\mathcal{I} \cap \mathfrak{s}$ es un ideal de $\mathfrak{s}$.
4. El espacio $\mathfrak{g}/\mathcal{I} = \{x + \mathcal{I} : x \in \mathfrak{g}\}$ es un álgebra de Lie definiendo el corchete como sigue

$$[x + \mathcal{I}, y + \mathcal{I}] = [x, y] + \mathcal{I} \quad \text{para todo par de vectores} \quad x, y \in \mathfrak{g}.$$

Demostración. Para el primer enunciado observe que $\mathcal{I} \cap \mathcal{J}$ y $\mathcal{I} + \mathcal{J}$ son subespacios de $\mathfrak{g}$. Sean $w \in \mathcal{I} \cap \mathcal{J}$ y $z \in \mathfrak{g}$, de la definición de ideal se tiene $[w, z] \in \mathcal{I}$ y $[w, z] \in \mathcal{J}$, por tanto $\mathcal{I} \cap \mathcal{J}$ es un ideal de $\mathfrak{g}$. Ahora, considere los vectores $u \in \mathcal{I}$, $v \in \mathcal{J}$ y $z \in \mathfrak{g}$, entonces

$$[u + v, z] = [u, z] + [v, z] \in \mathcal{I} + \mathcal{J},$$

por tanto, $\mathcal{I} + \mathcal{J}$ es un ideal de $\mathfrak{g}$.

Para continuar, note que $[\mathcal{I}, \mathcal{J}]$ es un subespacio de $\mathfrak{g}$. Considere los vectores $u \in \mathcal{I}$, $v \in \mathcal{J}$ y $z \in \mathfrak{g}$. Por la identidad de Jacobi, se tiene

$$[[u, v], z] = -[z, [u, v]] = [u, [v, z]] + [v, [z, u]], \tag{1.2}$$

pero $[v, z] \in \mathcal{J}$ y $[z, u] \in \mathcal{I}$, luego $[[u, v], z] \in [\mathcal{I}, \mathcal{J}]$. Ahora, tome un vector arbitrario $w \in [\mathcal{I}, \mathcal{J}] = span\{[x, y] : x \in \mathcal{I}, y \in \mathcal{J}\}$, entonces existen vectores $u_1, \ldots, u_s \in \mathcal{I}$, $v_1, \ldots, v_s \in \mathcal{J}$ y existen escalares $\alpha_1, \ldots, \alpha_s \in \mathbb{C}$, tales que

$$w = \alpha_1 [u_1, v_1] + \cdots + \alpha_s [u_s, v_s]$$

luego,

$$[w, z] = \alpha_1 [[u_1, v_1], z] + \cdots + \alpha_s [[u_s, v_s], z],$$

por la ecuación (1.2), cada vector $[[u_i, v_i], z]$ de la anterior combinación lineal está en $[\mathcal{I}, \mathcal{J}]$, entonces $[w, z] \in [\mathcal{I}, \mathcal{J}]$. Por tanto, $[\mathcal{I}, \mathcal{J}]$ es un ideal de $\mathfrak{g}$.

Para probar la tercera afirmación, observe que $\mathcal{I} \cap \mathfrak{s}$ es un subespacio de $\mathfrak{s}$. Sean $x \in \mathcal{I} \cap \mathfrak{s}$ y $z \in \mathfrak{s}$, por definición de ideal $[x, z] \in \mathcal{I}$, y por la definición de subálgebra $[x, z] \in \mathfrak{s}$, luego $[x, z] \in \mathcal{I} \cap \mathfrak{s}$. Por tanto, $\mathcal{I} \cap \mathfrak{s}$ es un ideal de $\mathfrak{s}$.

Para el último enunciado, note que $\mathfrak{g}/\mathcal{I}$ es un $\mathbb{C}$-espacio vectorial y que la bilinealidad del corchete en $\mathfrak{g}$ garantiza la bilinealidad del corchete en el espacio cociente $\mathfrak{g}/\mathcal{I}$. Se deja como ejercicio comprobar que todas las condiciones de la definición (1.2) se cumplen en $\mathfrak{g}/\mathcal{I}$ y en seguida se probará que el corchete está bien definido en el cociente $\mathfrak{g}/\mathcal{I}$. Suponga que $u_1 + \mathcal{I} = u_2 + \mathcal{I}$ y $w_1 + \mathcal{I} = w_2 + \mathcal{I}$, entonces existen vectores $x, y \in \mathcal{I}$, tales que $u_1 = u_2 + x$ y $w_1 = w_2 + y$, y se tiene

$$[u_1 + \mathcal{I}, w_1 + \mathcal{I}] = [u_1, w_1] + \mathcal{I} = [u_2 + x, w_2 + y] + \mathcal{I},$$

por la bilinealidad del corchete en $\mathfrak{g}$ y del hecho que $\mathcal{I}$ es un ideal de $\mathfrak{g}$, se obtiene,

$$[u_1+\mathcal{I}, w_1+\mathcal{I}] = ([u_2, w_2]+[u_2, y]+[x, w_2]+[x, y])+\mathcal{I} = [u_2, w_2]+\mathcal{I}.$$

Por tanto $[u_1+\mathcal{I}, w_1+\mathcal{I}] = [u_2+\mathcal{I}, w_2+\mathcal{I}]$, es decir, el corchete está bien definido en el cociente $\mathfrak{g}/\mathcal{I}$. $\square$

Observación 1.4 (Constantes de estructura). Sea $\mathfrak{g}$ un álgebra de Lie compleja de dimensión finita y sea $B = \{x_1, \dots, x_n\}$ una base ordenada de $\mathfrak{g}$. Cada vector $[x_i, x_j]$ se puede expresar como combinación lineal de los vectores de la base B, luego existen escalares únicos $a_{ij}^k \in \mathbb{C}$, tales que

$$[x_i, x_j] = \sum_{k=1}^{n} a_{ij}^k x_k.$$

Los escalares a_{ij}^k se denominan constantes de estructura del álgebra de Lie $\mathfrak{g}$ con respecto a la base B.

Ejemplo 1.10. Considere la $\mathbb{C}$-álgebra de Lie $\mathfrak{sl}_2$ de matrices de tamaño 2×2 y componentes complejas y sea $B = \{e, f, h\}$ la base canónica de $\mathfrak{sl}_2$, en la cual

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Entonces

$$[e, f] = ef - fe = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = h.$$

$$[e, h] = eh - he = \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix} = -2e.$$

$$[f, h] = fh - hf = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} = 2f.$$

Por tanto, las constantes de estructura de $\mathfrak{sl}_2$ con respecto a su base canónica pertenecen al conjunto $\{0, 1, -1, 2, -2\}$.

Definición 1.7 (Álgebra de Lie simple). Un álgebra de Lie compleja no abeliana $\mathfrak{g}$ se denomina simple, si los únicos ideales de $\mathfrak{g}$ son $\{\mathbf{0}\}$ y $\mathfrak{g}$.

Ejemplo 1.11. El álgebra de Lie $\mathfrak{sl}_2$ es simple, porque tomando un ideal $\mathcal{I} \neq \{\mathbf{0}\}$ de $\mathfrak{sl}_2$ y una matriz no nula $X \in \mathcal{I}$, existen escalares $\alpha, \beta, \gamma \in \mathbb{C}$, no todos cero, tal que

$X = \alpha e + \beta f + \gamma h$, y se tiene

$$[[X,h],f] = [-2\alpha e + 2\beta f, f] = -\,2\alpha h \in \mathcal{I}.$$

$$[[X,h],e] = [-2\alpha e + 2\beta f, e] = -\,2\beta h \in \mathcal{I}.$$

$$[[X,e],h] = [-\beta h + 2\gamma e, h] = -\,4\gamma e \in \mathcal{I}.$$

Dado que alguno de los escalares α, β o γ es diferente de cero, se sigue que $e \in \mathcal{I}$ o $h \in \mathcal{I}$, y en cualquiera de estos casos se obtiene $\{e, f, h\} \subset \mathcal{I}$. Luego $\mathcal{I} = \mathfrak{sl}_2$, así que $\mathfrak{sl}_2$ es un álgebra de Lie compleja simple.

1.2 Homomorfismos de álgebras de Lie

Definición 1.8 (Homomorfismo de álgebras de Lie). Sean $\mathfrak{g}_1$ y $\mathfrak{g}_2$ dos álgebras de Lie complejas. Un homomorfismo de $\mathfrak{g}_1$ en $\mathfrak{g}_2$ es una transformación $\mathbb{C}$-lineal $\phi : \mathfrak{g}_1 \to \mathfrak{g}_2$, tal que

$$\phi([x,y]) = [\phi(x), \phi(y)], \text{ para todo par de vectores } x, y \in \mathfrak{g}_1.$$

El homomorfismo ϕ se denomina monomorfismo si ϕ es inyectiva, epimorfismo si ϕ es sobreyectiva e isomorfismo si ϕ es biyectiva. Se dice que $\mathfrak{g}_1$ y $\mathfrak{g}_2$ son álgebras de Lie isomorfas, lo que se denota $\mathfrak{g}_1 \cong \mathfrak{g}_2$, si existe un isomorfismo $\phi : \mathfrak{g}_1 \to \mathfrak{g}_2$.

Ejemplo 1.12. (Epimorfismo Canónico) Sea $\mathfrak{g}$ un álgebra de Lie compleja, y sea $\mathcal{I}$ un ideal de $\mathfrak{g}$. La transformación lineal $\pi : \mathfrak{g} \longrightarrow \mathfrak{g}/\mathcal{I}$ definida por $\pi(x) = x + \mathcal{I}$, para todo vector $x \in \mathfrak{g}$ es un epimorfismo de álgebras de Lie. En efecto, no es complicado comprobar que ϕ es una transformación $\mathbb{C}$-lineal sobreyectiva y tomando $x, y \in \mathfrak{g}$, se tiene

$$\pi([x,y]) = [x,y] + \mathcal{I} = [x + \mathcal{I}, y + \mathcal{I}] = [\pi(x), \pi(y)].$$

Así π es un epimorfismo de álgebras de Lie, denominado epimorfismo canónico.

Ejemplo 1.13. Dos álgebras de Lie complejas abelianas son isomorfas, si y sólo si, tienen la misma dimensión. En efecto, la primera implicación es evidente y para el recíproco, sean $\mathfrak{b}_1$ y $\mathfrak{b}_2$ dos $\mathbb{C}$-álgebras de Lie complejas abelianas de la misma dimensión. Luego, existe una transformáción $\mathbb{C}$-lineal biyectiva $\phi : \mathfrak{b}_1 \longrightarrow \mathfrak{b}_2$, y dados un par de vectores $u, w \in \mathfrak{b}_1$ se tiene

$$\phi\left([u, w]\right) = \mathbf{0} = [\phi(u), \phi(w)]\,.$$

Por tanto, ϕ es un isomorfismo de álgebras de Lie.

Ejemplo 1.14. Todas las álgebras de Lie complejas no abelianas de dimensión dos son isomorfas. Para justificar esta afirmación, sean $\mathfrak{g}_1$ y $\mathfrak{g}_2$ dos álgebras de Lie complejas no abelianas de dimensión dos. Por la Proposición (1.2) existen $\mathbb{C}$-bases $\{x_1, x_2\}$ de $\mathfrak{g}_1$ y $\{y_1, y_2\}$ de $\mathfrak{g}_2$, tal que $[x_1, x_2] = x_2$ y $[y_1, y_2] = y_2$. Considere el isomorfismo de espacios vectoriales $\gamma : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_2$, definido por

$$\gamma(x_i) = y_i, \ \text{para } i = 1, 2.$$

Luego,

$$\gamma([x_1, x_2]) = \gamma(x_2) = y_2 = [y_1, y_2] = [\gamma(x_1), \gamma(x_2)].$$

Por tanto, γ es un isomorfismo de álgebras de Lie.

Ejemplo 1.15. Dos álgebras de Lie no abelianas de dimensión $n > 2$, no siempre son isomorfas. Por ejemplo, el álgebra $\mathfrak{sl}_2$ es un álgebra de Lie de dimensión 3 y por lo expuesto en el Ejemplo (1.11) se sabe que $\mathfrak{sl}_2$ es simple. Por el Teorema (1.2), que se presenta más adelante, se deduce que toda álgebra de Lie isomorfa a $\mathfrak{sl}_2$ debe ser simple. Ahora, sea $\mathfrak{b}$ el subespacio de $\mathfrak{gl}_3$ conformado por toda matriz triangular superior con diagonal nula. Una base para $\mathfrak{b}$ es el conjunto $\{E_{12}, E_{13}, E_{23}\}$. Observe que

$$[E_{12}, E_{23}] = E_{13}, \quad [E_{12}, E_{13}] = [E_{13}, E_{23}] = \mathbf{0}. \tag{1.3}$$

Las anteriores relaciones implican que $\mathfrak{b}$ es una subálgebra de $\mathfrak{g}$ de dimensión 3 y que $span\,\{E_{23}\}$ es un ideal no trivial de $\mathfrak{b}$; en consecuencia, $\mathfrak{sl}_2$ y $\mathfrak{b}$ son álgebras de Lie no isomorfas.

Observación 1.5. Los siguientes enunciados son verdaderos

1. Si $\mathfrak{g}_1$ y $\mathfrak{g}_2$ son dos álgebras de Lie complejas, la transformación lineal nula $\mathcal{O} : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_2$, definida por $\mathcal{O}(x) = \mathbf{0}$ para toda $x \in \mathfrak{g}_1$, es un homomorfismo de álgebras de Lie.
2. Si $\mathfrak{g}$ es un álgebra de Lie compleja, entonces la transformación lineal idéntica $id_{\mathfrak{g}} : \mathfrak{g} \longrightarrow \mathfrak{g}$, definida por $id_{\mathfrak{g}}(x) = x$ para toda $x \in \mathfrak{g}$, es un isomorfismo de álgebras de Lie.
3. Si $\phi : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_2$ y $\gamma : \mathfrak{g}_2 \longrightarrow \mathfrak{g}_3$ son homomorfismo de álgebras de Lie, entonces $\gamma \circ \phi : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_3$ es un homomorfismo de álgebras de Lie, porque dados dos vectores $u, w \in \mathfrak{g}_1$, se tiene

$$\gamma \circ \phi\left([u, w]\right) = \gamma\left([\phi(u), \phi(w)]\right) = [\gamma \circ \phi(u), \gamma \circ \phi(w)]\,.$$

Teorema 1.1. Si $\mathfrak{g}_1, \mathfrak{g}_2$ y $\mathfrak{g}_3$ son álgebras de Lie complejas, entonces

1. $\mathfrak{g}_1 \cong \mathfrak{g}_1$.
2. Si $\mathfrak{g}_1 \cong \mathfrak{g}_2$, entonces $\mathfrak{g}_2 \cong \mathfrak{g}_1$.
3. Si $\mathfrak{g}_1 \cong \mathfrak{g}_2$ y $\mathfrak{g}_2 \cong \mathfrak{g}_3$, entonces $\mathfrak{g}_1 \cong \mathfrak{g}_3$.

Demostración. Dado que $id_{\mathfrak{g}_1} : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_1$ es un isomorfismo de álgebras de Lie, se tiene $\mathfrak{g}_1 \cong \mathfrak{g}_1$. Ahora, suponga que $\phi : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_2$ es un isomorfismo de álgebras de Lie, entonces se tiene la transformación $\mathbb{C}$-lineal biyectiva $\phi^{-1} : \mathfrak{g}_2 \longrightarrow \mathfrak{g}_1$, y dados $u, w \in \mathfrak{g}_2$ existen vectores $x, y \in \mathfrak{g}_1$, tal que $\phi(x) = u$ y $\phi(y) = w$, entonces

$$\phi([x, y]) = [\phi(x), \phi(y)] = [u, w].$$

Luego

$$\phi^{-1}([u, w]) = [x, y] = [\phi^{-1}(u), \phi^{-1}(w)],$$

Así, ϕ^{-1} es un isomorfismo de álgebras de Lie, es decir, $\mathfrak{g}_1 \cong \mathfrak{g}_2$. Para finalizar, el tercer enunciado es consecuencia del ítem 3 de la Observación (1.5), porque la composición de isomorfismos de álgebras de Lie también es un isomorfismo de álgebras de Lie. □

Teorema 1.2 (Propiedades de los homomorfismos). Si $\phi : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_2$ es un homomorfismo de álgebras de Lie, $\mathfrak{s}$ una subálgebra de $\mathfrak{g}_1$ y $\mathfrak{r}$ una subálgebra de $\mathfrak{g}_2$, entonces

1. $\phi(\mathfrak{s}) = \{\phi(x) : x \in \mathfrak{s}\}$ es una subálgebra de $\mathfrak{g}_2$, en particular, $Im(\phi) = \phi(\mathfrak{g}_1)$ es una subálgebra de $\mathfrak{g}_2$. Además, si $\mathfrak{s}$ es un ideal de $\mathfrak{g}_1$ y ϕ es epimorfismo, entonces $\phi(\mathfrak{s})$ es un ideal de $\mathfrak{g}_2$.
2. $\phi^{-1}(\mathfrak{r}) = \{x \in \mathfrak{g}_1 : \phi(x) \in \mathfrak{r}\}$ es una subálgebra de $\mathfrak{g}_1$. Además, si $\mathfrak{r}$ es un ideal de $\mathfrak{g}_2$, entonces $\phi^{-1}(\mathfrak{r})$ es un ideal de $\mathfrak{g}_1$, en particular, $Ker(\phi) = \phi^{-1}(\mathbf{0})$ es un ideal de $\mathfrak{g}_1$.

Demostración. Se presenta la prueba del primer ítem, el segundo se muestra de forma similar y se deja como ejercicio para el lector. Claramente $\phi(\mathfrak{s})$ es un subespacio de $\mathfrak{g}_2$. Sean $x, y \in \mathfrak{s}$, se tiene $[x, y] \in \mathfrak{s}$, luego

$$[\phi(x), \phi(y)] = \phi([x, y]) \in \phi(\mathfrak{s}),$$

por tanto, $\phi(\mathfrak{s})$ es una subálgebra de $\mathfrak{g}_2$. Ahora, suponga que $\mathfrak{s}$ es un ideal de $\mathfrak{g}_1$ y que ϕ es epimorfismo. Escoja vectores $u \in \phi(\mathfrak{s})$ y $w \in \mathfrak{g}_2$, entonces existen vectores $x \in \mathfrak{s}$ y $y \in \mathfrak{g}_1$, tal que $\phi(x) = u$ y $\phi(y) = w$, luego $[x, y] \in \mathfrak{s}$, y se tiene

$$[u, w] = [\phi(x), \phi(y)] = \phi([x, y]) \in \phi(\mathfrak{s}).$$

Por tanto, $\phi(\mathfrak{s})$ es un ideal de $\mathfrak{g}_2$. □

Teorema 1.3 (Primer Teorema del isomorfismo). Si $\varphi : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_2$ es un homorfismo de $\mathbb{C}$-álgebras de Lie, entonces

$$\frac{\mathfrak{g}_1}{Ker(\varphi)} \cong Im(\varphi).$$

Demostración. Sea $Ker(\varphi) = \mathfrak{s}$, considere la correspondencia $\overline{\varphi} : \mathfrak{g}_1/\mathfrak{s} \longrightarrow Im(\varphi)$ definida por

$$\overline{\varphi}(x+\mathfrak{s}) = \varphi(x), \text{ para toda } x \in \mathfrak{g}_1.$$

Se mostrará que $\overline{\varphi}$ es un isomorfismo de álgebras de Lie. Primero suponga que $x+\mathfrak{s} = y+\mathfrak{s}$ en $\mathfrak{g}_1/\mathfrak{s}$, luego $y - x \in \mathfrak{s}$, entonces

$$\overline{\varphi}(x+\mathfrak{s}) = \varphi(x) = \varphi(x+(y-x)) = \varphi(y) = \overline{\varphi}(y+\mathfrak{s}).$$

Así, $\overline{\varphi}$ es una función bien definida, claramente sobreyectiva; además es $\mathbb{C}$-lineal, porque φ lo es. Para mostrar que $\overline{\varphi}$ es inyectiva, sea $x+\mathfrak{s} \in Ker(\overline{\varphi})$, entonces

$$\varphi(x) = \overline{\varphi}(x+\mathfrak{s}) = \mathbf{0},$$

de aquí $x \in \mathfrak{s}$, lo que implica que $\overline{\varphi}$ es inyectiva. Resta probar que $\overline{\varphi}$ es un homomorfismo de álgebras de Lie. Sean $x+\mathfrak{s}, y+\mathfrak{s} \in \mathfrak{g}_1/\mathfrak{s}$, entonces

$$\overline{\varphi}([x+\mathfrak{s}, y+\mathfrak{s}]) = \overline{\varphi}([x,y]+\mathfrak{s}) = \varphi([x,y]),$$

pero φ es un homomorfismo de álgebras de Lie, entonces

$$\varphi([x,y]) = [\varphi(x), \varphi(y)] = [\overline{\varphi}(x+\mathfrak{s}), \overline{\varphi}(y+\mathfrak{s})].$$

Asi, $\overline{\varphi}$ es un homomorfismo de álgebras de Lie. Por tanto, $\mathfrak{g}_1/Ker(\varphi) \cong Im(\varphi)$. □

Ejemplo 1.16. Considere la aplicación $\mathbb{C}$-lineal $\phi : \mathfrak{gl}_n \longrightarrow span\,(I_n)$, definida por

$$\phi(A) = tr(A)I_n, \text{ para toda } A \in \mathfrak{gl}_n.$$

Observe que

$$\phi\left([A,B]\right) = tr\left(AB - BA\right) I_n = 0I_n = [tr(A)I_n, tr(B)I_n] = [\phi(A), \phi(B)]\,,$$

luego, ϕ es un epimorfismo de álgebras de Lie con $Ker(\phi) = \{A \in \mathfrak{gl}_n : tr(A) = 0\} = \mathfrak{sl}_n$, por tanto

$$\frac{\mathfrak{gl}_n}{\mathfrak{sl}_n} \cong span(I_n).$$

Corolario 1.1. Sea $\mathfrak{g}$ un álgebra de Lie compleja. Si $\mathcal{I}$ y $\mathcal{J}$ son ideales de $\mathfrak{g}$, entonces

$$\frac{\mathcal{I}}{(\mathcal{J}\cap\mathcal{I})} \cong \frac{(\mathcal{J}+\mathcal{I})}{\mathcal{J}},$$

además, si $\mathcal{I}\subset\mathcal{J}$, entonces

$$\frac{\left(\frac{\mathfrak{g}}{\mathcal{I}}\right)}{\left(\frac{\mathcal{J}}{\mathcal{I}}\right)} \cong \frac{\mathfrak{g}}{\mathcal{J}}.$$

Demostración. Para iniciar observe que $\mathcal{J}\cap\mathcal{I}$ es un ideal de $\mathcal{I}$, además, $\mathcal{J}$ es un ideal de $\mathcal{J}+\mathcal{I}$ y $\frac{\mathcal{J}}{\mathcal{I}}$ es un ideal de $\frac{\mathfrak{g}}{\mathcal{I}}$. Considere la aplicación $\mathbb{C}$-lineal $\phi:\mathcal{I}\longrightarrow\frac{(\mathcal{J}+\mathcal{I})}{\mathcal{J}}$ definida por $\phi(x)=x+\mathcal{J}$. Dados los vectores $x,y\in\mathcal{I}$, se tiene

$$\phi([x,y]) = [x,y]+\mathcal{J} = [x+\mathcal{J}, y+\mathcal{J}] = [\phi(x),\phi(y)].$$

Luego, ϕ es un homomorfismo de álgebras de Lie, más aún, si $u\in\mathcal{J}+\mathcal{I}$, existen vectores $z\in\mathcal{J}$ y $x\in\mathcal{I}$, tal que $u=z+x$, y se tiene

$$\phi(x) = x+\mathcal{J} = (z+x)+\mathcal{J} = u+\mathcal{J},$$

es decir, ϕ es un epimorfismo. Adicionalmente, $Ker(\phi)=\{x\in\mathcal{I}: x\in\mathcal{J}\}=\mathcal{J}\cap\mathcal{I}$ y aplicando el Teorema (1.3), se obtiene $\frac{\mathcal{I}}{(\mathcal{J}\cap\mathcal{I})}\cong\frac{(\mathcal{J}+\mathcal{I})}{\mathcal{J}}$.

Para probar el segundo enunciado, considere la correspondencia $\varphi:\frac{\mathfrak{g}}{\mathcal{I}}\longrightarrow\frac{\mathfrak{g}}{\mathcal{J}}$, definida por $\varphi(x+\mathcal{I})=x+\mathcal{J}$. Esta correspondencia es una función, ya que dado $x+\mathcal{I}=y+\mathcal{I}$, se tiene $y-x\in\mathcal{I}\subset\mathcal{J}$, entonces

$$\varphi(x+\mathcal{I}) = x+\mathcal{J} = x+(y-x)+\mathcal{J} = y+\mathcal{J} = \varphi(y+\mathcal{I}).$$

El lector puede comprobar que φ es $\mathbb{C}$-lineal y sobreyectiva. Ahora, sean $x,y\in\mathfrak{g}$, se tiene

$$\varphi([x+\mathcal{I},y+\mathcal{I}]) = \varphi([x,y]+\mathcal{I}) = [x,y]+\mathcal{J} = [x+\mathcal{J},y+\mathcal{J}] = [\varphi(x+\mathcal{I}),\varphi(y+\mathcal{I})].$$

Así, φ es un epimorfismo de álgebras de Lie, además

$$Ker(\varphi) = \left\{x+\mathcal{I}\in\frac{\mathfrak{g}}{\mathcal{I}} : x+\mathcal{J}=\mathcal{J}\right\} = \left\{x+\mathcal{I}\in\frac{\mathfrak{g}}{\mathcal{I}} : x\in\mathcal{J}\right\} = \frac{\mathcal{J}}{\mathcal{I}}$$

Por el primer Teorema del isomorfismo, se tiene $\dfrac{\left(\dfrac{\mathfrak{g}}{\mathcal{I}}\right)}{\left(\dfrac{\mathcal{J}}{\mathcal{I}}\right)} \cong \dfrac{\mathfrak{g}}{\mathcal{J}}$. $\square$

Ejemplo 1.17. Sean $\mathfrak{g} = \mathfrak{gl}_2, \mathfrak{s} = \mathfrak{sl}_2$ y $\mathfrak{r} = span\,(\mathcal{I}_2) = \{\alpha\mathcal{I}_2 : \alpha \in \mathbb{C}\}$. Usando la base canónica de $\mathfrak{s}$, expuesta en el Ejemplo (1.10), se tiene que $\{e, f, h, I_2\}$ es una $\mathbb{C}$-base de $\mathfrak{g}$. Considere la aplicación $\mathbb{C}$-lineal biyectiva $\gamma : \mathfrak{g} \longrightarrow \mathfrak{s} \oplus \mathfrak{r}$, definida por

$$\gamma(e) = (e, \mathbf{0}), \quad \gamma(f) = (f, \mathbf{0}), \quad \gamma(h) = (h, \mathbf{0}), \quad \gamma(I_2) = (\mathbf{0}, I_2),$$

entonces,

$$\gamma\left([e, f]\right) = \gamma(h) = (h, \mathbf{0}) = ([e, f], \mathbf{0}) = [(e, \mathbf{0}), (f, \mathbf{0})] = [\gamma(e), \gamma(f)]\,,$$

$$\gamma\left([e, h]\right) = \gamma(-2e) = (-2e, \mathbf{0}) = ([e, h], \mathbf{0}) = [(e, \mathbf{0}), (h, \mathbf{0})] = [\gamma(e), \gamma(h)]\,,$$

$$\gamma\left([f, h]\right) = \gamma(2f) = (2f, \mathbf{0}) = ([f, h], \mathbf{0}) = [(f, \mathbf{0}), (h, \mathbf{0})] = [\gamma(f), \gamma(h)]\,.$$

Además,

$$\gamma\left([e, I_2]\right) = [\gamma(e), \gamma(I_2)]\,,\ \gamma\left([f, I_2]\right) = [\gamma(f), \gamma(I_2)]\,,\ \gamma\left([h, I_2]\right) = [\gamma(h), \gamma(I_2)]$$

Por tanto, γ es un isomorfismo de álgebras de Lie, es decir, $\mathfrak{gl}_2 \cong \mathfrak{sl}_2 \oplus span(I_2)$.

1.3 Representaciones de un álgebra de Lie

Definición 1.9 (Representación de un álgebra de Lie). Sea $\mathfrak{g}$ una $\mathbb{C}$-álgebra de Lie. Una representación de $\mathfrak{g}$ es un par (V, ϕ), en la cual V es un $\mathbb{C}$-espacio vectorial y $\phi : \mathfrak{g} \longrightarrow \mathfrak{gl}(V)$ es un homomorfismo de álgebras de Lie. Si ϕ es monomorfismo, la representación se denomina fiel.

Sean $\mathfrak{g}$ un álgebra de Lie compleja y V un $\mathbb{C}$-espacio vectorial y denote con $\mathcal{O}$ la aplicación nula en $\mathfrak{gl}(V)$. La transformación lineal $\mathbf{0} : \mathfrak{g} \longrightarrow \mathfrak{gl}(V)$ definida por

$$\mathbf{0}(x) = \mathcal{O}, \text{ para todo vector } x \in \mathfrak{g},$$

es un homomorfismo de álgebras de Lie, así que $(V, \mathbf{0})$ es una representación del álgebra de Lie $\mathfrak{g}$ denomina **representación trivial**.

Observación 1.6. Toda representación no trivial de un álgebra de Lie simple es fiel. En efecto, si $\mathfrak{g}$ es un álgebra de Lie simple y (V, ϕ) es una representación no trivial de $\mathfrak{g}$, entonces $Ker(\phi) \neq \mathfrak{g}$, en consecuencia, $Ker(\phi) = \{\mathbf{0}\}$.

Ejemplo 1.18. (Representación adjunta) Sea $\mathfrak{g}$ un álgebra de Lie compleja. Para cada $x \in \mathfrak{g}$ defina $ad_x : \mathfrak{g} \longrightarrow \mathfrak{g}$, de la siguiente forma

$$ad_x(y) = [x, y], \text{ para toda } y \in \mathfrak{g}.$$

Si $y, z \in \mathfrak{g}$ y $\beta \in \mathbb{C}$, por la bilinealidad del corchete en $\mathfrak{g}$, se tiene

$$ad_x(\beta y + z) = [x, \beta y + z] = \beta[x, y] + [x, z] = \beta ad_x(y) + ad_x(z).$$

Luego, $ad_x \in \mathfrak{gl}(\mathfrak{g})$. Ahora, sea $ad : \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g})$ la función que asigna a cada $x \in \mathfrak{g}$ la aplicación $\mathbb{C}$-lineal ad_x, a continuación se mostrará que $(\mathfrak{g}, ad)$ es una representación de $\mathfrak{g}$. Dados los vectores $x, y, z \in \mathfrak{g}$ y el escalar $\beta \in \mathbb{C}$, se tiene

$$ad_{\beta x+y}(z) = [\beta x + y, z] = \beta[x, z] + [y, z] = \beta ad_x(z) + ad_y(z) = \left(\beta ad_x + ad_y\right)(z).$$

Luego, $ad_{\beta x+y} = \beta ad_x + ad_y$, esto significa que $ad : \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g})$ es una aplicación $\mathbb{C}$-lineal. Además, de la identidad de Jacobi, se tiene

$$ad_{[x,y]}(z) = [[x, y], z] = [x, [y, z]] + [y, [z, x]] = [x, [y, z]] - [y, [x, z]]\,,$$

pero,

$$[x, [y, z]] - [y, [x, z]] = ad_x\left(ad_y(z)\right) - ad_y\left(ad_x(z)\right) = \left(ad_x \circ ad_y - ad_y \circ ad_x\right)(z),$$

de las dos ecuaciones anteriores se obtiene,

$$ad_{[x,y]} = ad_x \circ ad_y - ad_y \circ ad_x = \left[ad_x, ad_y\right].$$

Por tanto, $ad : \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g})$ es un homomorfismo de álgebras de Lie. En consecuencia, $(\mathfrak{g}, ad)$ es una representación de $\mathfrak{g}$ denominada **representación adjunta**. El lector puede verificar que $Ker(ad) = \{x \in \mathfrak{g} : [x, y] = \mathbf{0}, \text{ para toda } y \in \mathfrak{g}\} = Z(\mathfrak{g})$.

Observación 1.7. Si $\mathfrak{g}$ es un $\mathbb{C}$-álgebra de Lie simple, entonces $Z(\mathfrak{g}) = \{\mathbf{0}\}$, y en consecuencia $(\mathfrak{g}, ad)$ es una representación fiel de $\mathfrak{g}$. Si adicionalmente $\text{dím}(\mathfrak{g}) = n$, se tiene $\mathfrak{gl}(\mathfrak{g}) \cong \mathfrak{gl}_n$, por tanto, $\mathfrak{g}$ es isomorfa a una subálgebra de $\mathfrak{gl}_n$, esto significa que toda álgebra de Lie simple de dimensión finita se puede visualizar como una subálgebra del álgebra de matrices $\mathfrak{gl}_n$.

Proposición 1.7. Si $\mathfrak{g}$ es un álgebra de Lie compleja, entonces el conjunto

$$ad_{\mathfrak{g}} = \{ad_x : x \in \mathfrak{g}\}$$

es una subálgebra de $\mathfrak{gl}(\mathfrak{g})$.

Demostración. Por la bilinealidad del corchete en $\mathfrak{g}$, se sigue que $ad_{\mathfrak{g}}$ es un subespacio de $\mathfrak{gl}(\mathfrak{g})$. Sean $ad_x, ad_y \in ad_{\mathfrak{g}}$, dado que $(\mathfrak{g}, ad)$ es una representación de $\mathfrak{g}$, se tiene

$$\left[ad_x, ad_y\right] = ad_{[x,y]} \in ad_{\mathfrak{g}}.$$

Por tanto, $ad_{\mathfrak{g}}$ es una subálgebra de $\mathfrak{gl}(\mathfrak{g})$. $\square$

Ejemplo 1.19. Representación natural Sea $\mathfrak{g}$ una subálgebra de $M_n(\mathbb{C})$ y considere la función $\phi : \mathfrak{g} \longrightarrow gl(\mathbb{C}^n)$ que asigna a cada matriz $A \in \mathfrak{g}$ la transformación $\mathbb{C}$-lineal $\phi_A \in gl(\mathbb{C}^n)$ definida por $\phi_A(x) = Ax$, para toda $x \in \mathbb{C}^n$. En este ejemplo se mostrará que el par $(\mathbb{C}^n, \phi)$ es una representación de $\mathfrak{g}$ denominada **representación natural**. En efecto, sean $A, B \in M_n(\mathbb{C})$, $v \in \mathbb{C}^n$ y $\alpha, \beta \in \mathbb{C}$, entonces

$$\phi_{\alpha A+\beta B}(v) = (\alpha A + \beta B)v = \alpha Av + \beta Bv = \alpha\phi_A(v) + \beta\phi_B(v) = (\alpha\phi_A + \beta\phi_B)(v),$$

es decir, ϕ es transformación $\mathbb{C}$-lineal. Además

$$\phi_{[A,B]}(v) = (AB - BA)(v) = ABv - BAv = (\phi_A\phi_B - \phi_B\phi_A)(v).$$

Luego,

$$\phi\left([A, B]\right) = \phi_A\phi_B - \phi_B\phi_A = [\phi_A, \phi_B].$$

En consecuencia, ϕ es un homomorfismo de álgebras de Lie, por tanto, $(\mathbb{C}^n, \phi)$ es una representación de $\mathfrak{g}$.

Definición 1.10 (**Módulo sobre un álgebra de Lie**)**.** Sea $\mathfrak{g}$ un álgebra de Lie compleja. Un módulo sobre $\mathfrak{g}$ (o $\mathfrak{g}$-módulo) es un $\mathbb{C}$-espacio vectorial V junto con una aplicación $\mathbb{C}$-bilineal $\cdot : \mathfrak{g} \times V \longrightarrow V$ que asigna a cada par ordenado $(x, v) \in \mathfrak{g} \times V$ el vector $x \cdot v \in V$, y , tal que para todo par $x, y \in \mathfrak{g}$ y toda $v \in V$ se cumple

$$[x, y] \cdot v = x \cdot (y \cdot v) - y \cdot (x \cdot v).$$

Si V es un $\mathfrak{g}$-módulo, entonces la aplicación $\cdot : \mathfrak{g} \times V \longrightarrow V$ se denomina acción de $\mathfrak{g}$ en V.

Observación 1.8. Sea $\mathfrak{g}$ un álgebra de Lie.

1. Todo espacio vectorial V tiene estructura de $\mathfrak{g}$-módulo con la acción de $\mathfrak{g}$ en V definida de forma trivial, es decir,

$$x \cdot v = 0, \text{ para toda } x \in \mathfrak{g} \text{ y toda } v \in V.$$

2. Un álgebra de Lie $\mathfrak{g}$ tiene estructura de $\mathfrak{g}$-módulo, en la cual, la acción de $\mathfrak{g}$ en $\mathfrak{g}$ se define como sigue

$$x \cdot y = [x, y], \text{ para toda } x, y \in \mathfrak{g}.$$

3. Si V es un espacio vectorial y $\mathfrak{g}$ es una subálgebra de $\mathfrak{gl}(V)$, entonces V es un $\mathfrak{g}$-módulo con la aplicación $\cdot : \mathfrak{g} \times V \longrightarrow V$ definida por $x \cdot v = x(v)$. En efecto, la bilinealidad de esta aplicación es consecuencia de las estructuras de espacio vectorial de $\mathfrak{g}$ y V. Sean $x, y \in \mathfrak{g}$ y $v \in V$, entonces

$$[x, y] \cdot v = [x, y](v) = (xy - yx)(v) = xy(v) - yx(v) = x \cdot (y \cdot v) - y \cdot (x \cdot v).$$

Teorema 1.4. Sean V un espacio vectorial y $\mathfrak{g}$ una álgebra de Lie. El par (V, ϕ) es una representación de $\mathfrak{g}$ si, y solo si, la aplicación $\cdot : \mathfrak{g} \times V \longrightarrow V$ dada por $x \cdot v := \phi(x)(v)$ define una estructura de $\mathfrak{g}$-módulo en V.

Demostración. Si el par (V, ϕ) es una representación de $\mathfrak{g}$, entonces $\phi : \mathfrak{g} \longrightarrow \mathfrak{gl}(V)$ es un homomorfismo de álgebras de Lie, así se garantiza la bilinealidad de $\cdot : \mathfrak{g} \times V \longrightarrow V$. Sean $x, y \in \mathfrak{g}$ y $v \in V$, se tiene

$$\begin{aligned}
[x, y] \cdot v = \phi([x, y])(v) &= ([\phi(x), \phi(y)])(v) \\
&= (\phi(x)\phi(y))(v) - (\phi(y)\phi(x))(v) \\
&= \phi(x)(\phi(y)(v)) - \phi(y)(\phi(x)(v)) \\
&= \phi(x)(y \cdot v) - \phi(y)(x \cdot v) \\
&= x \cdot (y \cdot v) - y \cdot (x \cdot v).
\end{aligned}$$

Por tanto, V es un $\mathfrak{g}$-módulo. Ahora suponga que V tiene estructura de $\mathfrak{g}$-módulo con la aplicación $\cdot : \mathfrak{g} \times V \longrightarrow V$ y defina la transformación $\phi : \mathfrak{g} \longrightarrow \mathfrak{gl}(V)$ por $\phi(x)(v) = x \cdot v$, para toda $x \in \mathfrak{g}, v \in V$. Sean $x, y \in \mathfrak{g}$, $v \in V$ y $\alpha, \beta \in \mathbb{C}$, entonces

$$\phi(\alpha x + \beta y)(v) = (\alpha x + \beta y) \cdot v = \alpha x \cdot v + \beta y \cdot v = \alpha\phi(x)(v) + \beta\phi(y)(v).$$

De esta manera, ϕ es una transformación lineal. Por otro lado, observe que

$$\phi([x, y])(v) = x \cdot (y \cdot v) - y \cdot (x \cdot v) = (\phi(x)\phi(y))(v) - (\phi(y)\phi(x))(v) = [\phi(x), \phi(y)](v).$$

Así, ϕ es un homomorfismo de álgebras de Lie y, en consecuencia, el par (V, ϕ) es una representación de $\mathfrak{g}$. $\square$

El Teorema anterior garantiza que representaciones y módulos de un álgebra de Lie son conceptos equivalentes. Dependiendo del contexto, puede resultar más adecuado emplear el lenguaje de representaciones o el de módulos. Esta equivalencia conceptual resalta la fuerte conexión entre las estructuras algebraicas y sus manifestaciones geométricas. Este dualismo proporciona una herramienta poderosa para estudiar tanto las propiedades internas de las álgebras de Lie como sus aplicaciones en contextos más amplios. A través de esta equivalencia, se establece un puente entre la abstracción algebraica y las aplicaciones concretas, consolidando el papel central de las álgebras de Lie en la matemática moderna.

1.4 Álgebras de Lie solubles y nilpotentes

Una forma de estudiar las álgebras de Lie es a través de sus ideales, esto conduce a analizar ciertos ideales especiales, como el álgebra derivada, que permite la clasificación de las álgebras de Lie en solubles y nilpotentes.

Definición 1.11 (Serie derivada). Sea $\mathfrak{g}$ un álgebra de Lie. La serie derivada en $\mathfrak{g}$, es la sucesión no creciente

$$\mathfrak{g}^{(0)} \supseteq \mathfrak{g}^{(1)} \supseteq \cdots \supseteq \mathfrak{g}^{(i)} \supseteq \cdots$$

de ideales de $\mathfrak{g}$, en la cual

$$\mathfrak{g}^{(0)} = \mathfrak{g} \quad \text{y} \quad \mathfrak{g}^{(i)} = \left[\mathfrak{g}^{(i-1)}, \mathfrak{g}^{(i-1)}\right], \text{ para toda } i \in \mathbb{Z}_{>0}.$$

Ejemplo 1.20. Considere el álgebra de Lie $\mathfrak{g} = \tau_3$ de matrices triangulares superiores de tamaño 3×3. Observe que

$$\mathfrak{g}^{(0)} = \tau_3 = span\{E_{11}, E_{12}, E_{13}, E_{22}, E_{23}, E_{33}\},$$

dado que

$$E_{ij}E_{kl} = \begin{cases} E_{il} & \text{cuando } j = k. \\ \mathbf{0} & \text{cuando } j \neq k. \end{cases}$$

Entonces, los ideales que conforman la serie derivada de τ_3 son:

$$\mathfrak{g}^{(1)} = span\{E_{12}, E_{13}, E_{23}\}, \quad \mathfrak{g}^{(2)} = span\{E_{13}\} \quad \text{y} \quad \mathfrak{g}^{(3)} = \{\mathbf{0}\}.$$

Observación 1.9. Sea $\mathfrak{g}$ un álgebra de Lie simple. Dado que $\mathfrak{g}$ es no abeliana y los únicos ideales de $\mathfrak{g}$ son $\{\mathbf{0}\}$ y $\mathfrak{g}$, se tiene que la serie derivada de $\mathfrak{g}$ es constante, con $\mathfrak{g}^{(i)} = \mathfrak{g}$, para toda $i \geq 0$.

Definición 1.12 (Álgebra de Lie soluble). Sea $\mathfrak{g}$ un álgebra de Lie, se dice que $\mathfrak{g}$ es soluble si para algún entero $m \geq 1$, se cumple que $\mathfrak{g}^{(m)} = \{\mathbf{0}\}$.

Ejemplo 1.21. Del Ejemplo (1.20), el álgebra de Lie τ_3 es soluble. De hecho, tomando la base $\left\{E_{ij} : 1 \leq i \leq j \leq n\right\}$ para τ_n, se puede probar que para toda $k \in \{0, 1, \dots, n\}$, se tiene

$$\tau_n^{(k)} = span\left\{E_{ij} : 1 \leq i \leq j \leq n, \text{ y } j - i \geq k\right\},$$

En particular, $\tau_n^{(n)} = \{\mathbf{0}\}$, por tanto τ_n es soluble.

Proposición 1.8. Sea $\mathfrak{g}$ un álgebra de Lie.

1. Si $\mathfrak{g}$ es soluble, entonces toda subálgebra de $\mathfrak{g}$ es soluble.
2. Si $\mathfrak{g}$ es soluble, entonces toda imagen homomorfa de $\mathfrak{g}$ es soluble.
3. Si $\mathfrak{g}$ tiene un ideal $\mathcal{I}$, tal que $\mathcal{I}$ y $\dfrac{\mathfrak{g}}{\mathcal{I}}$ son solubles, entonces $\mathfrak{g}$ es soluble.
4. Si $\mathcal{I}$ y $\mathcal{J}$ son ideales solubles de $\mathfrak{g}$, entonces $\mathcal{I} + \mathcal{J}$ es un ideal soluble de $\mathfrak{g}$.

Demostración. A continuación se presentan las pruebas de cada uno de los enunciados de esta proposición.

1. Sea $\mathfrak{s}$ una subálgebra de $\mathfrak{g}$, como $\mathfrak{g}$ es soluble, existe $n \in \mathbb{Z}_{>0}$, tal que $\mathfrak{g}^{(n)} = \{\mathbf{0}\}$. Así, $\mathfrak{s}^{(n)} \subseteq \mathfrak{g}^{(n)} = \{\mathbf{0}\}$, por tanto $\mathfrak{s}$ es soluble.

2. Sea $\mathfrak{s}$ una imagen homomorfa de $\mathfrak{g}$, es decir, existe un epimorfismo $\varphi : \mathfrak{g} \to \mathfrak{s}$. Para comenzar, se probará por inducción que $\varphi\left(\mathfrak{g}^{(m)}\right) = \mathfrak{s}^{(m)}$, para todo $m \in \mathbb{Z}_{>0}$. Sea $[w, z] \in \mathfrak{s}^{(1)}$, por la sobreyectividad de φ existen $x, y \in \mathfrak{g}$, tales que

$$\varphi(x) = w \quad \text{y} \quad \varphi(y) = z,$$

entonces

$$[w, z] = [\varphi(x), \varphi(y)] = \varphi([x, y]) \in \varphi(\mathfrak{g}^{(1)}),$$

luego $\mathfrak{s}^{(1)} \subseteq \varphi(\mathfrak{g}^{(1)})$. Ahora, sea $z \in \varphi(\mathfrak{g}^{(1)})$, entonces existen un entero positivo n, escalares $\alpha_i \in \mathbb{C}$ y vectores $x_i, y_i \in \mathfrak{g}$, con $i = 1, \cdots, n$, tales que

$$z = \varphi\left(\sum_{i=1}^{n} \alpha_i [x_i, y_i]\right) = \sum_{i=1}^{n} \alpha_i [\varphi(x_i), \varphi(y_i)] \in [\mathfrak{s}, \mathfrak{s}] = \mathfrak{s}^{(1)},$$

entonces, $\varphi(\mathfrak{g}^{(1)}) \subseteq \mathfrak{s}^{(1)}$, en consecuencia, $\varphi(\mathfrak{g}^{(1)}) = \mathfrak{s}^{(1)}$. Ahora, suponga que el enunciado se cumple para algún entero positivo r, es decir, $\varphi\left(\mathfrak{g}^{(r)}\right) = \mathfrak{s}^{(r)}$, por consiguiente $\mathfrak{s}^{(r)}$ es una imagen homomorfa de $\mathfrak{g}^{(r)}$, y por el primer paso de inducción, se tiene

$$\varphi([\mathfrak{g}^{(r)}, \mathfrak{g}^{(r)}]) = [\mathfrak{s}^{(r)}, \mathfrak{s}^{(r)}], \quad \text{o su equivalente,} \quad \varphi\left(\mathfrak{g}^{(r+1)}\right) = \mathfrak{s}^{(r+1)}.$$

De hecho, dado que $\mathfrak{g}$ es soluble, existe un entero positivo n, tal que $\mathfrak{g}^{(n)} = \{\mathbf{0}\}$, entonces

$$\mathfrak{s}^{(n)} = \varphi(\mathfrak{g}^{(n)}) = \varphi(\{\mathbf{0}\}) = \{\mathbf{0}\}.$$

3. Considere el epimorfismo canónico $\pi : \mathfrak{g} \to \dfrac{\mathfrak{g}}{\mathcal{I}}$. Por un razonamiento similar al utilizado en el ítem anterior, se tiene

$$\pi\left(\mathfrak{g}^{(n)}\right) = \left(\frac{\mathfrak{g}}{\mathcal{I}}\right)^{(n)}, \text{ para todo entero positivo } n.$$

Por hipótesis, el álgebra $\dfrac{\mathfrak{g}}{\mathcal{I}}$ es soluble, luego existe un entero positivo k, tal que $\left(\dfrac{\mathfrak{g}}{\mathcal{I}}\right)^{(k)} = \{\mathcal{I}\}$, en consecuencia $\pi\left(\mathfrak{g}^{(k)}\right) = \{\mathcal{I}\}$, es decir,

$$\mathfrak{g}^{(k)} \subseteq Ker(\pi) = \mathcal{I},$$

pero $\mathcal{I}$ es soluble, así que $\mathfrak{g}^{(k)}$ es soluble y debe existir un entero positivo r, tal que

$$(\mathfrak{g}^{(k)})^{(r)} = \{\mathbf{0}\},$$

además, es facil comprobar que $\mathfrak{g}^{(k+r)} = (\mathfrak{g}^{(k)})^{(r)}$, por tanto $\mathfrak{g}$ es soluble.

4. Sea $\mathcal{I} \cap \mathcal{J} = \mathfrak{s}$, por el epimorfismo canónico $\pi : \mathcal{J} \longrightarrow \mathcal{J}/\mathfrak{s}$, se tiene que $\mathcal{J}/\mathfrak{s}$ es una imagen homomorfa de $\mathcal{J}$, y dado que $\mathcal{J}$ es soluble, por ítem 2, se tiene $\mathcal{J}/\mathfrak{s}$ es soluble. Pero $(\mathcal{J}+\mathcal{I})/\mathcal{I} \cong \mathcal{J}/\mathfrak{s}$, entonces $(\mathcal{J}+\mathcal{I})/\mathcal{I}$ es soluble, asimismos $\mathcal{I}$ es soluble y por ítem 3, se tiene $\mathcal{J}+\mathcal{I}$ es soluble.

□

Proposición 1.9. Si $\mathfrak{g}$ es un álgebra de Lie de dimensión finita, entonces $\mathfrak{g}$ contiene un único ideal $\mathcal{R}$ que satisface las dos condiciones siguientes:

1. El ideal $\mathcal{R}$ es soluble.
2. Todo ideal de $\mathfrak{g}$ que sea soluble está contenido en $\mathcal{R}$.

Demostración. Considere la colección $\mathcal{E} = \{I : I \text{ es ideal soluble de } \mathfrak{g}\}$. Esta colección es no vacía porque $\{\mathbf{0}\} \in \mathcal{E}$. Dado que $\mathfrak{g}$ es un álgebra de Lie de dimensión finita, existe $\mathcal{R} \in \mathcal{E}$ de dimensión máxima, es decir,

$$\text{dím } \mathcal{R} \geq \text{dím } I, \text{ para todo ideal } I \in \mathcal{E},$$

de la Proposición anterior se tiene

$$I + \mathcal{R} \in \mathcal{E}, \text{ para todo } I \in \mathcal{E},$$

luego dím $\mathcal{R} \leq$ dím $(I+\mathcal{R}) \leq$ dím $\mathcal{R}$, es decir, dím $(I+\mathcal{R}) =$ dím $\mathcal{R}$, así que $I+\mathcal{R} = \mathcal{R}$, por tanto, $I \subseteq \mathcal{R}$, para todo ideal $I \in \mathcal{E}$. Por último, la unicidad de $\mathcal{R}$ es evidente. □

Definición 1.13 (**Radical y álgebra semisimple**)**.** Sea $\mathfrak{g}$ un álgebra de Lie de dimensión finita. El radical de $\mathfrak{g}$, denotado por $rad\mathfrak{g}$, es el único ideal soluble $\mathcal{R}$ de $\mathfrak{g}$ que contiene a todos los ideales solubles de $\mathfrak{g}$. Además, se dice que $\mathfrak{g}$ es semisimple, si $rad\mathfrak{g} = \{\mathbf{0}\}$.

Proposición 1.10. Si $\mathfrak{g}$ es un álgebra de Lie de dimensión finita, entonces $\dfrac{\mathfrak{g}}{rad\mathfrak{g}}$ es un álgebra de Lie semisimple.

Demostración. Sean $\mathcal{R} = rad\mathfrak{g}$, $\overline{\mathcal{J}}$ un ideal soluble de $\dfrac{\mathfrak{g}}{\mathcal{R}}$ y considere el epimorfismo canónico $\pi : \mathfrak{g} \longrightarrow \dfrac{\mathfrak{g}}{\mathcal{R}}$, a continuación se probará que $\overline{\mathcal{J}} = \{\mathcal{R}\}$. Para comenzar, observe que el Teorema (1.2) garantiza que $\mathfrak{s} = \pi^{-1}(\overline{\mathcal{J}})$ es un ideal de $\mathfrak{g}$ que contiene a $\mathcal{R}$, además, tomando $x, y \in \mathfrak{s}$, se tiene

$$\pi([x,y]) = [\pi(x), \pi(y)] \in [\overline{\mathcal{J}}, \overline{\mathcal{J}}],$$

luego $[\mathfrak{s}, \mathfrak{s}] \subseteq \pi^{-1}([\overline{\mathcal{J}}, \overline{\mathcal{J}}])$. De forma similar se prueba que

$$\mathfrak{s}^{(n)} \subseteq \pi^{-1}(\overline{\mathcal{J}}^{(n)}), \text{ para todo entero positivo } n.$$

Dado que $\overline{\mathcal{J}}$ es soluble, existe un entero positivo m, tal que $\overline{\mathcal{J}}^{(m)} = \{\mathcal{R}\}$, entonces

$$\mathfrak{s}^{(m)} \subseteq \pi^{-1}(\{\mathcal{R}\}) = \mathcal{R},$$

pero $\mathcal{R}$ es soluble, luego $\mathfrak{s}^{(m)}$ es soluble, en consecuencia $\mathfrak{s}$ es un ideal soluble de $\mathfrak{g}$. Cuando el radical de un álgebra de Lie contiene a todos sus ideales solubles, se tiene $\mathfrak{s} \subseteq \mathcal{R}$. Pero

$\mathfrak{s}$ es un ideal de $\mathfrak{g}$ que contiene a $\mathcal{R}$, luego

$$\mathcal{R} = \mathfrak{s} = \pi^{-1}(\overline{\mathcal{J}}).$$

Así que $\overline{\mathcal{J}} = \{\mathcal{R}\}$, por tanto, $rad\left(\dfrac{\mathfrak{g}}{\mathcal{R}}\right) = \{\mathcal{R}\}$, es decir, el álgebra $\dfrac{\mathfrak{g}}{\mathcal{R}}$ es semisimple. $\square$

Definición 1.14 (Serie central descendente y álgebra nilpotente). Sea $\mathfrak{g}$ un álgebra de Lie. La serie central descendente de $\mathfrak{g}$ es la cadena

$$\mathfrak{g} = \mathfrak{g}^0 \supseteq \mathfrak{g}^1 \supseteq \cdots \supseteq \mathfrak{g}^r \supseteq \cdots,$$

en la cual $\mathfrak{g}^0 = \mathfrak{g}$, y para cada entero positivo r, se define $\mathfrak{g}^r = \left[\mathfrak{g}, \mathfrak{g}^{r-1}\right]$. Además, se dice que $\mathfrak{g}$ es nilpotente si existe un entero positivo r, tal que $\mathfrak{g}^r = \{\mathbf{0}\}$.

Observación 1.10. Para todo entero positivo r se cumple

$$\mathfrak{g}^{(r)} = [\mathfrak{g}^{(r-1)}, \mathfrak{g}^{(r-1)}] \subseteq [\mathfrak{g}, \mathfrak{g}^{r-1}] = \mathfrak{g}^r,$$

por tanto, toda álgebra de Lie nilpotente es soluble. Sin embargo, existen álgebras de Lie solubles no nilpotentes. De lo expuesto el Ejemplo (1.21), el álgebra de Lie τ_n es soluble, pero no es nilpotente porque $\tau_n^1 = [\tau_n, \tau_n] = span\left\{E_{ij} : 1 \leq i < j \leq n\right\}$, entonces

$$E_{12} = [E_{11}, E_{12}] \in \left[\tau_n, \tau_n^1\right] = \tau_n^2,$$

$$E_{12} = [E_{11}, E_{12}] \in \left[\tau_n, \tau_n^2\right] = \tau_n^3,$$

de hecho, para todo entero positivo r, se tiene $E_{12} \in \tau_n^r$. Por tanto, τ_n es un álgebra de Lie soluble no nilpotente.

Por su parte, un procedimiento similar al utilizado en el Ejemplo (1.21) le permite al lector mostrar que el álgebra de Lie $\mathfrak{g} = span\left\{E_{ij} : 1 \leq i < j \leq n\right\}$ es nilpotente.

Lema 1.1. Sea $\mathfrak{g}$ un álgebra de Lie

1. Si $\mathfrak{g}$ es nilpotente, entonces toda subálgebra de $\mathfrak{g}$ es nilpotente.
2. Si $\mathfrak{g}$ es nilpotente, entonces toda imagen homomorfa de $\mathfrak{g}$ es nilpotente.
3. Si $\dfrac{\mathfrak{g}}{Z(\mathfrak{g})}$ es nilpotente, entonces $\mathfrak{g}$ es nilpotente.

Demostración. El procedimiento de prueba de los primeros dos enunciados es similar al utilizado en la demostración de la Proposición (1.8). Para mostrar el tercer enunciado sea

r un entero positivo, tal que $\left(\dfrac{\mathfrak{g}}{Z(\mathfrak{g})}\right)^r = \{\mathbf{0}\}$. Por un razonamiento similar al utilizado en la Proposición (1.8) se tiene $\pi(\mathfrak{g}^r) = \{Z(\mathfrak{g})\}$, en la que $\pi : \mathfrak{g} \longrightarrow \dfrac{\mathfrak{g}}{Z(\mathfrak{g})}$ es la proyección canónica. Luego $\mathfrak{g}^r \subseteq Z(\mathfrak{g})$, entonces

$$\mathfrak{g}^{r+1} = [\mathfrak{g}, \mathfrak{g}^r] \subseteq [\mathfrak{g}, Z(\mathfrak{g})] = \{\mathbf{0}\}.$$

□

Definición 1.15 (ad-nilpotente). Sean $\mathfrak{g}$ un álgebra de Lie y x un elemento de $\mathfrak{g}$. Se dice que x es ad-nilpotente si la transformación ad_x es un endomorfismo nilpotente, es decir, existe un entero positivo n, tal que

$$(ad_x)^n = \underbrace{ad_x \cdots ad_x}_{n \text{ veces}} = \mathcal{O},$$

en el que $\mathcal{O}$ es la transformación nula de $\mathfrak{gl}(\mathfrak{g})$.

Lema 1.2. Sean V un espacio vectorial y $\mathfrak{g}$ una subálgebra de $\mathfrak{gl}(V)$. Si $x, y \in \mathfrak{g}$, entonces para todo entero positivo n, se tiene

$$(ad_x)^n(y) \in span\{x^{n-i}yx^i : i = 0, 1, \cdots, n\}.$$

Demostración. La prueba se hará por inducción sobre n. Para comenzar, dado un entero positivo n sea $W_n = span\{x^{n-i}yx^i : i = 0, 1, \cdots, n\}$. De la definición de ad_x, se tiene

$$ad_x(y) = [x, y] = xy - yx \in W_1.$$

Suponga que el enunciado se cumple para algún entero positivo n, entonces deben existir escalares $a_0, a_1, \ldots, a_n \in \mathbb{C}$, tales que

$$(ad_x)^n(y) = \sum_{i=0}^{n} a_i x^{n-i}yx^i \in W_n,$$

luego

$$(ad_x)^{n+1}(y) = ad_x((ad_x)^n(y)) = ad_x\left(\sum_{i=0}^{n} a_i x^{n-i}yx^i\right),$$

pero

$$ad_x\left(x^{n-i}yx^i\right) = x\left(x^{n-i}yx^i\right) - \left(x^{n-i}yx^i\right)x = x^{n-i+1}yx^i - x^{n-i}yx^{i+1}$$

entonces
$$(ad_x)^{n+1}(y) = \sum_{i=0}^{n} a_i \left(x^{n-i+1} y x^i - x^{n-i} y x^{i+1} \right) \in W_{n+1}.$$

□

Teorema 1.5. Sean V un espacio vectorial y $\mathfrak{g}$ una subálgebra de $\mathfrak{gl}(V)$. Si $x \in \mathfrak{g}$ es nilpotente, entonces x es ad-nilpotente.

Demostración. Dado que x es nilpotente, existe un entero positivo n, tal que $x^n = \mathcal{O}$, en el cual $\mathcal{O}$ es la transformación nula de $\mathfrak{gl}(V)$. Ahora sea $y \in \mathfrak{g}$, por el Lema anterior existen escalares $a_0, a_1, \ldots, a_{2n} \in \mathbb{C}$ tales que
$$(ad_x)^{2n}(y) = \sum_{i=0}^{2n} a_i x^{2n-i} y x^i.$$

Observe que para toda $i \in \{0, 1, ..., 2n\}$ se debe tener $i \geq n$ o $2n - i \geq n$, luego
$$x^{2n-i} = \mathcal{O}, \quad \text{o} \quad x^i = \mathcal{O}.$$

Por tanto,
$$(ad_x)^{2n}(y) = \sum_{i=0}^{2n} a_i x^{2n-i} y x^i = \mathcal{O},$$

es decir, x es ad-nilpotente. □

Teorema 1.6. Sea V un $\mathbb{C}$-espacio vectorial no trivial. Si $\mathfrak{g}$ es una subálgebra de $\mathfrak{gl}(V)$ y todo endomorfismo de $\mathfrak{g}$ es nilpotente, entonces existe un vector no nulo $v \in V$, tal que $x(v) = \mathbf{0}$ para todo $x \in \mathfrak{g}$.

Demostración. La prueba se realizará aplicando el principio de inducción fuerte sobre la dimensión del álgebra $\mathfrak{g}$. Si dím $\mathfrak{g} = 1$ y todo endomorfismo de $\mathfrak{g}$ es nilpotente, entonces $\mathfrak{g} = span\{x\}$, para algún endomorfismo nilpotente $x \neq \mathcal{O}$. Sea $r > 1$ el menor entero, tal que $x^r = \mathcal{O}$, entonces $x^{r-1} \neq \mathcal{O}$ y debe existir un vector no nulo $v \in V$, tal que $x^{r-1}(v) \neq \mathbf{0}$ y $x^r(v) = \mathbf{0}$. Tomando $w = x^{r-1}(v) \in V$ y un endomorfismo $\alpha x \in \mathfrak{g}$, con $\alpha \in \mathbb{C}$, se tiene
$$\alpha x(w) = \alpha x(x^{r-1}(v)) = \alpha x^r(v) = \mathbf{0}.$$

Ahora suponga que el enunciado es válido para cualquier subálgebra de endomorfismos nilpotentes $\mathfrak{h}$, con dím $\mathfrak{h} \leq n$, para algún entero positivo n, y suponga que dím $\mathfrak{g} = n+1$. Para continuar, sea $\mathcal{N}$ la colección de subálgebras propias de $\mathfrak{g}$, y note que $\mathcal{N} \neq \emptyset$, porque todo subespacio 1-dimensional contenido en $\mathfrak{g}$ es un elemento de $\mathcal{N}$. Escoja $\mathfrak{h} \in \mathcal{N}$ de dimensión maximal y para cada $y \in \mathfrak{h}$ considere la aplicación $f_y : \frac{\mathfrak{g}}{\mathfrak{h}} \to \frac{\mathfrak{g}}{\mathfrak{h}}$ definida por

$$f_y(w + \mathfrak{h}) = [y, w] + \mathfrak{h}, \text{ para toda } w \in \mathfrak{g}.$$

Note que f_y está bien definida, porque dados $w, z \in \mathfrak{g}$, tales que $w - z \in \mathfrak{h}$, se tiene

$$f_y(z + \mathfrak{h}) = [y, z] + \mathfrak{h} = ([y, z] + [y, w - z]) + \mathfrak{h} = [y, w] + \mathfrak{h} = f_y(w + \mathfrak{h}).$$

La bilinealidad del corchete implica que $f_y \in \mathfrak{gl}\left(\frac{\mathfrak{g}}{\mathfrak{h}}\right)$, además, el Teorema (1.5) garantiza que todo endomorfismo de $\mathfrak{h}$ es ad-nilpotente, en consecuencia f_y es nilpotente. Ahora, sea $\mathcal{H} = \left\{f_y : y \in \mathfrak{h}\right\}$, utilizando la identidad de Jacobi se puede comprobar que para toda $f_x, f_y \in \mathcal{H}$, se tiene

$$\left[f_x, f_y\right] = f_x f_y - f_y f_x = f_{[x,y]} \in \mathcal{H},$$

esto significa que $\mathcal{H}$ es una subálgebra de endomorfismos nilpotentes de $\mathfrak{gl}\left(\frac{\mathfrak{g}}{\mathfrak{h}}\right)$, además, dím $\mathcal{H} \leq$ dím $\mathfrak{h} \leq n$. Por hipótesis de inducción, debe existir $w + \mathfrak{h} \in \frac{\mathfrak{g}}{\mathfrak{h}}$, con $w + \mathfrak{h} \neq \mathfrak{h}$, tal que

$$f_y(w + \mathfrak{h}) = [y, w] + \mathfrak{h} = \mathfrak{h}, \text{ para toda } f_y \in \mathcal{H},$$

es decir, $w \notin \mathfrak{h}$ y $[y, w] \in \mathfrak{h}$, para toda $y \in \mathfrak{h}$. De la definición (1.4), $w \in N_{\mathfrak{g}}(\mathfrak{h})$, y dado que $\mathfrak{h}$ es una subálgebra propia de dimensión maximal en $\mathfrak{g}$, se deduce que $N_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g}$, en consecuencia $\mathfrak{h}$ es un ideal de $\mathfrak{g}$. Por lo anterior, se tiene el epimorfismo canónico de álgebras de Lie $\pi : \mathfrak{g} \longrightarrow \frac{\mathfrak{g}}{\mathfrak{h}}$. Dado que $\mathfrak{h}$ es una subálgebra propia de $\mathfrak{g}$, es posible elegir un vector no nulo $w + \mathfrak{h} \in \frac{\mathfrak{g}}{\mathfrak{h}}$, luego $\bar{\mathfrak{s}} = span\{w + \mathfrak{h}\}$ es una subálgebra no trivial de $\frac{\mathfrak{g}}{\mathfrak{h}}$, entonces $\pi^{-1}(\bar{\mathfrak{s}})$ es una subálgebra de $\mathfrak{g}$, que contiene propiamente a $\mathfrak{h}$. Por la maximalidad de la dimensión de $\mathfrak{h}$ en $\mathcal{N}$ se tiene que $\pi^{-1}(\bar{\mathfrak{s}}) = \mathfrak{g}$, entonces

$$\bar{\mathfrak{s}} = \pi\left(\pi^{-1}(\bar{\mathfrak{s}})\right) = \pi(\mathfrak{g}) = \frac{\mathfrak{g}}{\mathfrak{h}}.$$

Por ende

$$\text{dím } \mathfrak{g} = \text{dím } \mathfrak{h} + \text{dím } \bar{\mathfrak{s}} = \text{dím } \mathfrak{h} + 1.$$

Así que, $\mathfrak{g} = \mathfrak{h} \oplus span\{z\}$ para algún vector z de $\mathfrak{g}$ que no pertenece a $\mathfrak{h}$. Por hipótesis de inducción existe un vector no nulo $u \in V$, tal que $h(u) = \mathbf{0}$ para todo endomorfismo $h \in \mathfrak{h}$. Sea W el subespacio de V dado por

$$W = \{v \in V : h(v) = \mathbf{0}, \text{ para todo } h \in \mathfrak{h}\} \neq \{\mathbf{0}\}$$

En seguida, se probará que W es $\mathfrak{g}$-invariante, en efecto, sea $x = h + \alpha z \in \mathfrak{g}$, en la cual $h \in \mathfrak{h}$ y $\alpha z \in span\{z\}$, y sea $v \in W$, se tiene

$$x(v) = (h + \alpha z)(v) = h(v) + \alpha z(v) = \mathbf{0} + \alpha z(v) = \alpha z(v),$$

resta probar que $yz(v) = \mathbf{0}$, para todo endomorfismo $y \in \mathfrak{h}$. Para esto, recuerde que $[y, z] = yz - zy$, entonces

$$yz(v) = [y, z](v) + zy(v),$$

pero anteriormente se probó que $\mathfrak{h}$ es un ideal de $\mathfrak{g}$, luego $[y, z] \in \mathfrak{h}$, en consecuencia

$$yz(v) = \cancelto{\mathbf{0}}{[y, z](v)} + zy(v) = z(\mathbf{0}) = \mathbf{0}.$$

Esto prueba que W es $\mathfrak{g}$-invariante, por ende la restricción $z\,|_W \colon W \longrightarrow W$ es un endomorfismo nilpotente en $gl(W)$, entonces debe existir un vector no nulo $w \in W$, tal que $z(w) = z\,|_W\,(w) = \mathbf{0}$. Así, para toda $h \in \mathfrak{h}$ y toda $\alpha z \in span\{z\}$ se tiene

$$(h + \alpha z)(w) = \cancelto{\mathbf{0}}{h(w)} + \cancelto{\mathbf{0}}{\alpha z(w)} = \mathbf{0}.$$

Por tanto, todo endomorfismo de $\mathfrak{g}$ se anula en el vector no nulo w. □

Teorema 1.7 (Teorema de Engel). Sea $\mathfrak{g}$ un álgebra de Lie. Si todo elemento de $\mathfrak{g}$ es ad-nilpotente, entonces $\mathfrak{g}$ es nilpotente.

Demostración. Preste atención a la siguiente prueba por inducción sobre la dimensión del álgebra $\mathfrak{g}$. Si dím $\mathfrak{g} = 1$, el resultado es inmediato porque $\mathfrak{g}$ es abeliana. Suponga que el enunciado se satisface para toda álgebra de Lie $\mathfrak{a}$ de elementos ad-nilpotentes con dím $\mathfrak{a} \leq n$, para algún entero positivo n y sea $\mathfrak{g}$ un álgebra de Lie de elementos ad-nilpotentes de dimensión $n + 1$. Luego $ad_{\mathfrak{g}} = \{ad_x : x \in \mathfrak{g}\}$ es una subálgebra de endomorfismos nilpotentesde contenida en $\mathfrak{gl}(\mathfrak{g})$. Por Teorema (1.6), existe un vector no nulo $x \in \mathfrak{g}$, tal que

$$ad_y(x) = [y, x] = \mathcal{O}, \text{ para todo endomorfismo } y \in \mathfrak{g},$$

así $Z(\mathfrak{g}) \neq \{\mathcal{O}\}$, entonces dím $\dfrac{\mathfrak{g}}{Z(\mathfrak{g})} < n$. Además, dados $\overline{x}, \overline{y} \in \dfrac{\mathfrak{g}}{Z(\mathfrak{g})}$, se tiene

$$(ad_{\overline{x}})^n(\overline{y}) = (ad_x)^n(y) + Z(\mathfrak{g}), \text{ para todo entero positivo } n.$$

Pero x es una ad-nilpotente, luego $\overline{x}$ es ad-nilpotente, así que, $\dfrac{\mathfrak{g}}{Z(\mathfrak{g})}$ es un álgebra de Lie que consta de elementos ad-nilpotentes y dím $\left(\dfrac{\mathfrak{g}}{Z(\mathfrak{g})}\right) \leq n$. Por hipótesis de inducción, $\dfrac{\mathfrak{g}}{Z(\mathfrak{g})}$ es nilpotente y del Lema (1.1), se deduce que $\mathfrak{g}$ es nilpotente. $\square$

Al cierre de este capítulo se presenta el Teorema de Lie para álgebras de Lie solubles. Este teorema es un resultado fundamental en la teoría de álgebras de Lie y de aquí se deduce que cualquier representación finita de una $\mathbb{C}$-álgebra de Lie soluble $\mathfrak{g}$ contiene una base en la que cada elemento de $\mathfrak{g}$ es representado por una matriz triangular superior.

Teorema 1.8 (**Teorema de Lie**). Si V es un espacio vectorial no trivial de dimensión finita sobre el cuerpo $\mathbb{C}$ y $\mathfrak{g}$ es una subálgebra soluble contenida en $\mathfrak{gl}(V)$, entonces existe $v \in V$, tal que v es un vector propio para todos los endomorfismos de $\mathfrak{g}$.

Demostración. La demostración se hará por inducción en la dimensión de $\mathfrak{g}$. Para el caso en que dím $\mathfrak{g} = 1$ el resultado es obvio, porque el cuerpo $\mathbb{C}$ es algebraicamente cerrado. Ahora, suponga que el enunciado se satisface para toda subálgebra soluble $\mathfrak{h}$ contenida en $\mathfrak{gl}(V)$, con dím $\mathfrak{h} \leq n$, para algún entero positivo n, y suponga que $\mathfrak{g}$ es una subálgebra soluble contenida en $\mathfrak{gl}(V)$, con dím $\mathfrak{g} = n + 1$. Note que $[\mathfrak{g}, \mathfrak{g}]$ es un ideal propio de $\mathfrak{g}$, asimismo, el álgebra cociente $\mathcal{H} = \dfrac{\mathfrak{g}}{[\mathfrak{g}, \mathfrak{g}]}$ es abeliana, porque dados $x, y \in \mathfrak{g}$, se tiene

$$[x + [\mathfrak{g}, \mathfrak{g}], y + [\mathfrak{g}, \mathfrak{g}]] = [x, y] + [\mathfrak{g}, \mathfrak{g}] = [\mathfrak{g}, \mathfrak{g}].$$

Sea $\mathcal{W}$ un subespacio de $\mathcal{H}$, con dím $\mathcal{W} =$ dím $\mathcal{H} - 1$. Note que $\mathcal{W}$ es un ideal de $\mathcal{H}$, pues $\mathcal{H}$ es abeliana. Considere el epimorfismo canónico $\pi : \mathfrak{g} \longrightarrow \mathcal{H}$, entonces $\mathfrak{s} = \pi^{-1}(\mathcal{W})$ es un ideal propio de $\mathfrak{g}$, luego

$$\text{dím } \mathfrak{s} \leq \text{dím } \mathfrak{g} - 1 = n.$$

En el caso dím $\mathfrak{s} < n$, existe un subespacio $\mathcal{J} \subset \mathfrak{g}$, tal que $\mathfrak{s} \subsetneq \mathcal{J} \subsetneq \mathfrak{g}$, y se tiene

$$\mathcal{W} = \pi(\mathfrak{s}) \subsetneq \pi(\mathcal{J}),$$

pero dím $\mathcal{W} =$ dím $\mathcal{H} - 1$, entonces

$$\pi(\mathcal{J}) = \mathcal{H} = \pi(\mathfrak{g}),$$

así, para cada $x \in \mathfrak{g}$ existe $j \in \mathcal{J}$, tal que $\pi(x) = \pi(j)$, es decir

$$x - j \in Ker(\pi) \subseteq \pi^{-1}(\mathcal{W}) \subsetneq \mathcal{J},$$

esto implica que $x \in \mathcal{J}$, por tanto $\mathcal{J} = \mathfrak{g}$, que contradice el hecho de que $\mathcal{J}$ es un subespacio propio de $\mathfrak{g}$. En consecuencia, dím $\mathfrak{s} = n =$ dím $\mathfrak{g} - 1$ y debe existir un endomorfismo $z \in \mathfrak{g} \setminus \mathfrak{s}$, tal que $\mathfrak{g} = \mathfrak{s} \oplus span\{z\}$. Ahora, por la hipótesis de inducción es posible escoger un vector $v \in V$ que es autovector para todo endomorfismo de $\mathfrak{s}$, es decir, dado $x \in \mathfrak{s}$ existe un escalar $\lambda_x \in \mathbb{C}$, tal que $x(v) = \lambda_x v$. Fijando este vector propio común v se tiene la aplicación $\mathbb{C}$-lineal $\lambda : \mathfrak{s} \longrightarrow \mathbb{C}$ definida por $\lambda(x) = \lambda_x$. Considere el subconjunto W definido por

$$W = \{w \in V : x(w) = \lambda_x w, \text{ para todo endomorfismo } x \in \mathfrak{s}\},$$

note que $v \in W$ y de hecho W es un subespacio de V. En la Proposición (A.1) de los anexos (capítulo A) se prueba que W es $\mathfrak{g}$-invariante, esto implica que se puede ver a z como un endomorfismo de $gl(W)$ y como $\mathbb{C}$ es algebraicamente cerrado, el endomorfismo z tiene un vector propio $w_0 \in W$. Para finalizar, sea $y \in \mathfrak{g}$, entonces existen $x \in \mathfrak{s}$ y $\alpha \in \mathbb{C}$, tales que $y = x + \alpha z$, luego $y(w_0) = x(w_0) + \alpha z(w_0)$. Pero $z(w_0) = \beta w_0$ para algún $\beta \in \mathbb{C}$, así que $y(w_0) = (\lambda_x + \alpha\beta)w_0$. Por tanto, w_0 es un vector propio común para todo $y \in \mathfrak{g}$. □

Corolario 1.2. Sea V un $\mathbb{C}$-espacio vectorial no trivial de dimensión finita. Si $\mathfrak{g}$ es una subálgebra soluble de $\mathfrak{gl}(V)$, entonces existe una base de V, en la cual cada elemento de $\mathfrak{g}$ es representado por una matriz triangular superior.

Demostración. Se probará por inducción en la dimensión de V. En el caso dím $V = 1$ se cumple el enunciado, porque dado un vector no nulo $v \in V$ se tiene que $B = \{v\}$ es una base de V y la matriz $[x]_B$ del endomorfismo $x \in \mathfrak{gl}(V)$, en la base B, es un escalar. Ahora suponga que el enunciado se cumple para todo $\mathbb{C}$-espacio vectorial de dimensión n, para algún entero positivo n y sea V un $\mathbb{C}$-espacio vectorial de dimensión $n+1$. Escoja una subálgebra soluble $\mathfrak{g}$ contenida en $\mathfrak{gl}(V)$, por el Teorema de Lie, existe $v_1 \in V$, tal que v_1 es un vector propio común para todo endomorfismo $x \in \mathfrak{g}$. Considere el subespacio $U = span\{v_1\} \subseteq V$, entonces el espacio cociente V/U tiene dimensión n y por la hipótesis de inducción se satisface el enunciado de este corolario. Ahora, para cada endomorfismo $x \in \mathfrak{g}$ considere la función $\overline{x} : V/U \longrightarrow V/U$, definida por

$$\overline{x}(w + U) = x(w) + U, \text{ para todo } w + U \in V/U.$$

A continuación se probará que $\overline{x} \in \mathfrak{gl}(V/U)$. Primero observe que $\overline{x}$ está bien definida, pues si $w + U = t + U$, entonces $w = t + \beta v_1$, para algún escalar $\beta \in \mathbb{C}$. Luego

$$\overline{x}(w + U) = x(t + \beta v_1) + U = (x(t) + \beta\lambda_x v_1) + U = x(t) + U = \overline{x}(t + U).$$

La linealidad de $\overline{x}$ se obtiene de la linealidad del endomorfismo x, en consecuencia, $\overline{x}$ es un endomorfismo de $\mathfrak{gl}(V/U)$. Ahora considere la subálgebra soluble

$$\overline{\mathfrak{g}} = \{\overline{x} : x \in \mathfrak{g}\} \subseteq \mathfrak{gl}(V/U),$$

por el Teorema de Lie existe una base $\overline{B} = \{\overline{v}_2, \ldots, \overline{v}_n\}$ del espacio cociente V/U en la cual cada endomorfismo de $\overline{\mathfrak{g}}$ se representa por una matriz triangular superior. Observe que $B = \{v_1, v_2, \ldots, v_n\}$ es una base de V, y a continuación se mostrará que para todo $x \in \mathfrak{g}$ la matriz $[x]_B$ del endomorfismo x es la base B es triangular superior. Para cada $j = 1, \ldots, n$ existen escalares $\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}$, tales que

$$x(v_j) = \alpha_{1j} v_1 + \alpha_{2j} v_2 + \cdots + \alpha_{nj} v_n.$$

Entonces

$$\overline{x}(\overline{v_j}) = \big(\alpha_{1j} v_1 + \alpha_{2j} v_2 + \cdots + \alpha_{nj} v_n\big) + U,$$

y dado que $v_1 \in U$, se obtiene

$$\overline{x}(\overline{v_j}) = \alpha_{2j} \overline{v_2} + \cdots + \alpha_{jj} \overline{v_j} + \cdots + \alpha_{nj} \overline{v_n}.$$

Pero la matriz $[\overline{x}]_{\overline{B}}$ del endomorfismo $\overline{x} \in gl\,(V/U)$ en la base $\overline{B}$ es triangular superior, en consecuencia,

$$\alpha_{kj} = 0, \text{ para todo } k = j+1, \ldots, n.$$

Luego,

$$x(v_j) = \alpha_{1j} v_1 + \alpha_{2j} v_2 + \cdots + \alpha_{jj} v_j.$$

Por tanto,

$$[x]_B = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1j} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2j} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \cdots & \alpha_{jj} & \cdots & \alpha_{jn} \\ \vdots & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & \alpha_{nn} \end{pmatrix},$$

lo que termina la prueba. $\square$

CAPÍTULO 2

Filtraciones y envolvente universal

2.1 Anillos graduados

El estudio de las representaciones (o módulos) de álgebras de Lie se puede realizar por medio de los módulos sobre su correspondiente álgebra envolvente universal y en esta conexión las álgebras graduadas emergen como una herramienta poderosa para entender y describir la complejidad de estas estructuras. En esta sección se presenta una rápida introducción a los anillos graduados y al concepto de filtración, el cual es particularmente relevante en la construcción del álgebra envolvente universal $U(\mathfrak{g})$ de una álgebra de Lie $\mathfrak{g}$ de dimensión finita. El álgebra $U(\mathfrak{g})$ tiene una filtración natural y el álgebra graduada asociada a esta filtración es el álgebra simétrica $S(\mathfrak{g})$ que es fundamental para estudiar las representaciones del álgebra de Lie $\mathfrak{g}$. El lector que desee profundizar en el tema de anillos graduados puede consultar Oystaeyen y Nastasescu (2004), Matsumura (1987) o

Hazrat (2016).

Definición 2.1 (Anillos G-graduadas). Sea $(G,\cdot)$ un monoide conmutativo con elemento identidad 1. Un anillo A junto con una descomposición de A, como suma directa de subgrupos aditivos $A = \bigoplus_{g\in G} A_g$, se denomina anillo G-graduado, si para todo par de elementos $g, h \in G$ se cumple $A_g A_h \subseteq A_{gh}$.

Sea A un anillo G-graduado. Dado que $A_e A_e \subseteq A_e$, entonces A_e es un subanillo de A. Además, para cada elemento no cero $x \in A$ existen elementos homogéneos únicos $x_1, \ldots, x_r$, con $x_i \in A_{g_i}$, tales que

$$x = x_1 + \cdots + x_r,$$

en este caso, los elementos x_i se denominan **componentes homogéneas de** x.

Ejemplo 2.1. A continuación se presentan algunos ejemplos de anillos graduados.

1. Sea G un monoide conmutativo con elemento identidad 1. Todo anillo A tiene una estructura trivial de anillo G-graduado llamando $A_1 = A$ y $A_g = \{0\}$, para todo elemento $g \in G - \{1\}$.

2. El anillo de polinomios en la indeterminada X, con coeficientes en un anillo A, es $\mathbb{N}$-graduado, porque al definir $A_0 = A$ y $A_i = \left\{aX^i : a \in A\right\}$, para cada $i > 0$, se obtiene la descomposición de $A[X]$ como suma directa de subgrupos aditivos $A[X] = \bigoplus_{i\in\mathbb{N}} A_i$. Además, $A_i A_j = A_{i+j}$, para todo par $i, j \in \mathbb{N}$.

3. Sea A un anillo y sea $B = A[X_1, \ldots, X_r]$ el anillo de polinomios en las indeterminadas $X_1, \ldots, X_r$ con coeficientes en A. Note que B es un anillo $\mathbb{N}$-graduado. En efecto, sea $B_0 = A$ y para cada $n > 0$, defina

$$B_n = \left\{ \sum_{i=1}^{m} a_i X_1^{n_{i_1}} \cdots X_r^{n_{i_r}} : m, n_{i_1}, \ldots, n_{i_r} \in \mathbb{Z}^+, a_i \in A \text{ y } n_{i_1} + \cdots + n_{i_r} = n \right\},$$

es decir, B_n es el grupo aditivo de los polinomios homogéneos de grado n en el anillo B. Entonces, se tiene la descomposición de B como suma directa de subgrupos aditivos $B = \bigoplus_{n\in\mathbb{N}} B_n$, y dados $f = aX_1^{n_{i_1}} \cdots X_r^{n_{i_r}} \in B_n$ y $g = bX_1^{m_{i_1}} \cdots X_r^{m_{i_r}} \in B_m$, se tiene

$$fg = abX_1^{n_{i_1}+m_{i_1}} \cdots X_r^{n_{i_r}+m_{i_r}}$$

en el cual, $(n_{i_1} + m_{i_1}) + \cdots + (n_{i_r} + m_{i_r}) = n + m$. En consecuencia, para todo par

$n, m \in \mathbb{N}$, se cumple $B_n B_m \subseteq B_{n+m}$.

4. Sea $B = A[X_1, \ldots, X_r]$ el anillo de polinomios en las indeterminadas $X_1, \ldots, X_r$ con coeficientes en un anillo A. Considere el monoide conmutativo
$$\mathbb{N}^r = \{(\alpha_1, \ldots, \alpha_r) : \alpha_i \in \mathbb{N}\},$$
con elemento identidad $(0, \ldots, 0)$. Para cada $k > 0$ sea
$$\mathbb{N}^r(k) = \{(\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r : \alpha_1 + \cdots + \alpha_r = k\},$$
y dado $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, denote $X^\alpha = X_1^{\alpha_1} \cdots X_r^{\alpha_r}$. Llamando $B_0 = A$ y para cada $k > 0$, defina
$$B_k = \left\{ \sum_{i=1}^{m} a_i X^\alpha : m \in \mathbb{Z}^+, a_i \in A, \alpha \in \mathbb{N}^r(k) \right\}.$$
Entonces B es un anillo $\mathbb{N}^r$-graduado, porque el anillo B descompone como suma directa de subgrupos aditivos como $B = \bigoplus_{k\in\mathbb{N}} B_k$ y de forma similar al ejemplo del ítem anterior se obtiene $B_k B_t \subseteq B_{k+t}$, para todo par $k, t \in \mathbb{N}$.

Definición 2.2 (Ideal graduado). Sea $A = \bigoplus_{g\in G} A_g$ un anillo G-graduado. Un ideal J de A es G-graduado si $J = \bigoplus_{g\in G} J \cap A_g$ es una G-graduación de J.

Ejemplo 2.2. Suponga que $A = \bigoplus_{g\in G} A_g$ es un anillo G-graduado. Si J es un ideal de A generado por elementos homogéneos de A, entonces J es un ideal G-graduado. En efecto, sea S un subconjunto no vacío de elementos homogéneos, es decir
$$\emptyset \neq S \subseteq \bigcup_{g\in G} A_g,$$
y sea $J = \langle S \rangle$. Para cada $x \in J$, existen elementos $\alpha_1, \ldots, \alpha_r$ del anillo A y elementos homogéneos $x_1, \ldots, x_r \in J$, tales que
$$x = \alpha_1 x_1 + \cdots + \alpha_r x_r.$$
Suponga que para cada $i = 1, \ldots, r$, las componentes homogéneas de α_i son $\alpha_{i1}, \ldots, \alpha_{is_i}$, esto significa que
$$\alpha_i = \alpha_{i1} + \cdots + \alpha_{is_i},$$

luego,

$$x = \left(\sum_{j=1}^{s_1} \alpha_{1j} \right) x_1 + \cdots + \left(\sum_{j=1}^{s_r} \alpha_{rj} \right) x_r,$$

dado que los x_i son homogéneos, entonces la igualdad anterior es la representación de x como suma de sus componentes homogéneas. Pero todos los $\alpha_{ij}x_i$ están en el ideal J, en consecuencia, todas las componentes homogéneas de los elementos de J están en J. Por tanto, $J = \bigoplus\limits_{g\in G} \left(J \cap A_g\right)$ y J es un ideal G-graduado del anillo A.

No obstante, no todos los ideales de un anillo graduado son ideales graduados. Por ejemplo, el anillo $B = A[X, Y]$ de polinomios en las indeterminadas X e Y con coeficientes en un anillo A es $\mathbb{N}$-graduado. En efecto, llamando $B_0 = A$, y para $n > 0$ defina

$$B_n = \left\{ \sum_{i=0}^{n} a_i X^{n-i} Y^i : a_i \in A \right\},$$

entonces $B = \bigoplus\limits_{n\in\mathbb{N}} B_n$. Ahora considere el ideal $J = \left\langle X + Y^2 \right\rangle$, note que para todo $n \in \mathbb{N}$, se cumple

$$(J \cap B_n) \cap \left\{ X, Y^2, X + Y^2 \right\} = \emptyset,$$

y dado que $X + Y^2 \in J$, se obtiene $J \neq \bigoplus\limits_{n\in\mathbb{N}} (J \cap B_n)$.

Observación 2.1. Sea $A = \bigoplus\limits_{g\in G} A_g$ un anillo G-graduado. Si J es un ideal G-graduado de A, entonces el anillo cociente $\dfrac{A}{J}$ es G-graduado, con graduación dada como sigue

$$\frac{A}{J} = \bigoplus_{g\in G} \frac{A_g}{J \cap A_g}$$

Definición 2.3 (Filtración). Sea A un anillo. **Una filtración de** A es una cadena descendente de ideales

$$\cdots \subseteq J_{k+1} \subseteq J_k \subseteq \cdots \subseteq J_1 \subseteq J_0 = A,$$

tal que para todo par $m, n \in \mathbb{N}$ se cumple $J_m J_n \subseteq J_{m+n}$.

Teorema 2.1. Toda filtración de un anillo A define un anillo $\mathbb{N}$-graduado.

Demostración. Sea A un anillo con filtración

$$\cdots \subseteq J_{k+1} \subseteq J_k \subseteq \cdots \subseteq J_1 \subseteq J_0 = A. \tag{2.1}$$

Para cada $n \in \mathbb{N}$ sea $B_n = \dfrac{J_n}{J_{n+1}}$ y considere el grupo abeliano $B = \bigoplus_{n\in\mathbb{N}} B_n$. Ahora, para $x \in J_m$ e $y \in J_n$ defina la multiplicación como sigue

$$(x + J_{m+1})\,(y + J_{n+1}) = xy + J_{m+n+1}.$$

Se mostrará que esta multiplicación está bien definida. En efecto, sean $x, y \in J_m$ y $w, z \in J_n$, tales que

$$x + J_{m+1} = y + J_{m+1} \quad \text{y} \quad w + J_{n+1} = z + J_{n+1},$$

entonces existen $a \in J_{m+1}$ y $b \in J_{n+1}$, tales que

$$x = y + a \quad \text{y} \quad w = z + b.$$

Luego,

$$xw - yz = (y + a)(z + b) - yz = yb + az + ab \in J_{m+n+1}.$$

Así que

$$(x + J_{m+1})\,(w + J_{n+1}) = (y + J_{m+1})\,(z + J_{n+1})\,.$$

En consecuencia, la multiplicación está bien definida y se tiene

$$B_n B_m \subseteq B_{n+m}.$$

Por tanto, B es un anillo $\mathbb{N}$-graduado. $\square$

El anillo B de la prueba anterior se denomina **graduación asociada a la filtración** (2.1) y se denota $B = gr(A)$.

Ejemplo 2.3. Sean A un anillo y J un ideal de A. Para un entero $k > 0$, con J^k se denota el ideal de A generado por todos los productos de la forma $a_1 \cdots a_k$, en las que todas las $a_i \in J$, es decir,

$$J^k = \langle a_1 \cdots a_k : a_i \in J \rangle\,.$$

de la definición se obtiene la filtración

$$\cdots \subseteq J^k \subseteq J^{k-1} \subseteq \cdots \subseteq J^2 \subseteq J \subseteq J^0 = A.$$

La graduación asociada a esta filtración es el anillo

$$B = gr_J(A) = \bigoplus_{k\in\mathbb{N}} \frac{J^k}{J^{k+1}}.$$

En este caso $B_0 = \dfrac{A}{J}$ y $B_k = \dfrac{J^k}{J^{k+1}}$, para todo entero $k > 0$. Un elemento $w \in B_k$ es de la forma $w = a + J^{k+1}$, para algún elemento $a \in J^k$, pero esto significa que a es una suma de productos de la forma $\alpha a_1 \cdots a_k$, en la cual $\alpha \in A$ y los $a_i \in J$. Por la forma como se definió la multiplicación en la graduación B, se tiene

$$(\alpha a_1 \cdots a_k) + J^{k+1} = (\alpha + J)\left(a_1 + J^2\right) \cdots \left(a_k + J^2\right),$$

en la que $\alpha + J \in B_0$ y los $a_i + J^2 \in B_1$, en consecuencia, cada elemento $w \in B_k$ es combinación lineal de productos de k factores de B_1 con coeficientes en el anillo B_0. En particular, si $J = \langle a_1, \ldots, a_r\rangle$ y se denota $\delta_i = a_i + J^2$, para $i = 1, \ldots, r$, entonces cada elemento $w \in B_k$ es de la forma

$$w = \sum_{t=1}^{m} \alpha_t \delta_1^{t_1} \cdots \delta_r^{t_r},$$

en el cual m y todos los t_i son enteros positivos, además, $t_1 + \cdots + t_r = k$, para toda $t = 1, \ldots, m$ y los α_t son elementos del anillo B_0. Considere el polinomio homogéneo f de grado k, dado por

$$f = \sum_{t=1}^{m} \alpha_t X_1^{t_1} \cdots X_r^{t_r} \in \frac{A}{J}[X_1, \ldots, X_r],$$

entonces, $w = f(\delta_1, \ldots, \delta_r)$. Por tanto, llamando $\mathcal{P}_k$ al conjunto de los polinomios homogéneos de grado k en el anillo $\dfrac{A}{J}[X_1, \ldots, X_r]$ se tiene el epimorfismo de grupos aditivos $\varepsilon_\delta : \mathcal{P}_k \longrightarrow B_k$, definido por

$$\varepsilon_\delta(f) = f(\delta_1, \ldots, \delta_r), \text{ para todo polinomio } f \in \mathcal{P}_n.$$

Una colección especialmente importante de anillos $\mathbb{N}$- graduados en álgebra conmutativa y geometría algebraica es la clase de los anillos Noetherianos $\mathbb{N}$-graduados. El siguiente teorema caracteriza los anillo Notherianos $\mathbb{N}$-graduados, y su prueba se puede consultar en Matsumura (1987) página 93.

Teorema 2.2. Un anillo $\mathbb{N}$-graduado $A = \bigoplus_{n\in\mathbb{N}} A_n$ es Notheriano, si y solo si, el grupo aditivo A_0 es Notheriano y A es un anillo finitamente generado sobre A_0.

2.2 Álgebra envolvente universal

El álgebra envolvente universal de una $\mathbb{C}$-álgebra de Lie de dimensión finita es una construcción algebraica importante en la teoría de álgebras de Lie. Esta construcción juega un papel crucial en el estudio de las representaciones del álgebras de Lie y en otras áreas de la matemática y la física. En esta sección se presentan sin demostración las ideas básicas que permiten construir el álgebra envolvente universal de una $\mathbb{C}$-álgebra de Lie de dimensión finita. El lector que desee profundizar en esta temática puede consultar Humphreys (1997) y SanMartin (1999).

Álgebra tensorial

Sea $\mathfrak{g}$ un $\mathbb{C}$-álgebra de Lie de dimensión finita. Sea $T^0\mathfrak{g} = \mathbb{C}$ y para cada entero $n > 0$ considere el $\mathbb{C}$-espacio vectorial

$$T^n\mathfrak{g} = \underbrace{\mathfrak{g} \otimes \cdots \otimes \mathfrak{g}}_{n \text{ veces}}.$$

El álgebra tensorial de $\mathfrak{g}$ es el $\mathbb{C}$-espacio vectorial

$$T(\mathfrak{g}) = \bigoplus_{n \in \mathbb{N}} T^n\mathfrak{g},$$

con multiplicación asociativa definida por concatenación de tensores, esto significa que

$$\underbrace{(x_1 \otimes \cdots \otimes x_m)}_{\in T^m\mathfrak{g}} \underbrace{(y_1 \otimes \cdots \otimes y_n)}_{\in T^n\mathfrak{g}.} = x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n \in T^{m+n}\mathfrak{g}$$

Se sabe que $T(\mathfrak{g})$ es una $\mathbb{C}$-álgebra asociativa unitaria y $\mathbb{N}$-graduada que contiene el álgebra de Lie $\mathfrak{g}$ como subespacio vectorial. Además, el álgebra tensorial es finitamente generada sobre $\mathbb{C}$, porque al escoger una $\mathbb{C}$-base B del álgebra de Lie $\mathfrak{g}$, todo elemento de $T(\mathfrak{g})$ es una combinación lineal de tensores de la forma $x_1 \otimes \cdots \otimes x_r$, con los $x_i \in B$.

El álgebra tensorial es universal, en el siguiente sentido: Si A es un álgebra asociativa unitaria que contiene a $\mathfrak{g}$ como subespacio vectorial y $\delta : \mathfrak{g} \longrightarrow A$ es una aplicación $\mathbb{C}$-lineal, entonces existe un único homomorfismo de $\mathbb{C}$-álgebras asociativas $\psi : T(\mathfrak{g}) \longrightarrow A$ tal que $\psi(1) = 1$ y $\psi \circ i = \delta$, es decir, el siguiente diagrama conmuta:

$$
\begin{tikzcd}
\mathfrak{g} \arrow[rr, "\overset{\text{aplicación inclusión}}{i}"] \arrow[ddrr, "\delta"'] & & T(\mathfrak{g}) \arrow[dd, "\psi"] \\
& \arrow[ur, phantom, "\circlearrowright"] & \\
& & A
\end{tikzcd}
$$

Álgebra simétrica

En el estudio de las representaciones de un álgebra de lie $\mathfrak{g}$, es importante considerar álgebras de la forma $\dfrac{T(\mathfrak{g})}{\mathcal{I}}$, en la cual $\mathcal{I}$ es un ideal bilateral del álgebra tensorial $T(\mathfrak{g})$. Una de estas es el **álgebra simétrica**, la cual actúa como un espacio de funciones polinómicas sobre el espacio dual del álgebra de Lie $\mathfrak{g}$, y permite estudiar las representaciones de manera algebraica y geométrica.

Observación 2.2. Suponga que $\mathfrak{g}$ es una $\mathbb{C}$-álgebra de Lie de dimensión finita y sea $J = \langle x \otimes y - y \otimes x : x, y \in \mathfrak{g} \rangle$. Note que J es un ideal bilateral, $\mathbb{N}$-graduado del álgebra tensorial $T(\mathfrak{g})$. En efecto,

$$J = \bigoplus_{n \geq 2} \left(J \cap T^n \mathfrak{g} \right).$$

Definición 2.4 (Álgebra simétrica). Sean $\mathfrak{g}$ un álgebra de Lie de dimensión finita y J el ideal de $T(\mathfrak{g})$ presentado en la Observació anterior. El álgebra cociente $S(\mathfrak{g}) = \dfrac{T(\mathfrak{g})}{J}$ se denomina **álgebra simétrica** del algebra de Lie $\mathfrak{g}$.

Por definición el álgebra $S(\mathfrak{g})$ es conmutativa y las componentes homogéneas de cualquier elemento no cero de J tienen grado mayor o igual a 2, entonces el homomorfismo canónico $\pi : T(\mathfrak{g}) \longrightarrow S(\mathfrak{g})$ es inyectivo cuando se restringue al subespacio $\mathbb{C} \otimes \mathfrak{g}$, así que $\mathfrak{g} \cong \pi(\mathfrak{g})$ como $\mathbb{C}$-espacios vectoriales, y se puede ver a $\mathfrak{g}$ como un subespacio de $S(\mathfrak{g})$. Además, por la Observación (2.1), $S(\mathfrak{g})$ es un álgebra $\mathbb{N}$-graduada. El álgebra simétrica es universal en el siguiente sentido: Si A es una $\mathbb{C}$-álgebra asociativa, unitaria, conmutativa y $\delta : \mathfrak{g} \longrightarrow A$ es una aplicación $\mathbb{C}$-lineal, entonces existe un único homomorfismo de $\mathbb{C}$-álgebras asociativas $\psi : S(\mathfrak{g}) \longrightarrow A$, tal que $\psi(1) = 1$ y el siguiente diagrama conmuta:

$$
\begin{tikzcd}
\mathfrak{g} \arrow[r, "i"] \arrow[dr, "\delta"'] \arrow[dr, phantom, shift left=3ex, "\circlearrowright\ \delta = \psi \circ i"] & S(\mathfrak{g}) \arrow[d, "\psi"] \\
 & A
\end{tikzcd}
$$

Si el álgebra de Lie $\mathfrak{g}$ es de dimensión finita y $B = \{e_1, \ldots, e_r\}$ es una $\mathbb{C}$-base de $\mathfrak{g}$, entonces los vectores de $S(\mathfrak{g})$ son combinaciones lineales de clases de equivalencia de la forma

$$e_1^{n_1} \otimes \cdots \otimes e_r^{n_r} + J, \text{ donde los } n_{i_j} \in \mathbb{N}.$$

De aquí se tiene el isomomorfismo $\phi : \mathbb{C}[X_1, \ldots, X_r] \longrightarrow S(\mathfrak{g})$ de $\mathbb{C}$-álgebras asociativas, conmutativas y unitarias definido por

$$\phi\left(X_1^{n_1} \cdots X_r^{n_r}\right) = e_1^{n_1} \otimes \cdots \otimes e_r^{n_r} + J.$$

Por tanto, el álgebra simétrica $S(\mathfrak{g})$ de un álgebra de Lie compleja $\mathfrak{g}$ de dimensión r es isomorfa al álgebra de polinomios $\mathbb{C}[X_1, \ldots, X_r]$.

Álgebra envolvente universal

Definición 2.5 (Álgebra envolvente universal). Sea $\mathfrak{g}$ un álgebra de Lie compleja. **Un álgebra envolvente universal** de $\mathfrak{g}$ es un par (U, i), en la que U es un álgebra asociativa unitaria e $i : \mathfrak{g} \longrightarrow U$ es una aplicación $\mathbb{C}$-lineal inyectiva que satisface las condiciones siguientes:

1. Para todo par de elementos $x, y \in \mathfrak{g}$ se cumple
$$i\left([x, y]\right) = i(x)i(y) - i(y)i(x).$$
2. El álgebra U es generada por $i\left(\mathfrak{g}\right) = \{i(x) : x \in \mathfrak{g}\}$.
3. Si $\mathcal{U}$ es una $\mathbb{C}$-álgebra asociativa unitaria y $\delta : \mathfrak{g} \longrightarrow \mathcal{U}$ es una aplicación $\mathbb{C}$-lineal, entonces existe un único homomorfismo de $\mathbb{C}$-álgebras asociativas $\psi : U \longrightarrow \mathcal{U}$ tal que $\psi(1) = 1$ y $\delta = \psi \circ i$.

De la definición se desprende que el álgebra envolvente universal es única, salvo isomorfismo; en efecto, suponga que (U, i) y $(\mathcal{U}, j)$ son dos álgebras envolventes universales de $\mathfrak{g}$, entonces existen homomorfismos de $\mathbb{C}$-álgebras asociativas únicos $\psi : U \longrightarrow \mathcal{U}$ y $\gamma : \mathcal{U} \longrightarrow U$ tales que
$$j = \psi \circ i \quad \text{e} \quad i = \gamma \circ j.$$
Luego, $i = \gamma \circ \psi \circ i$ y dado que U es generada como álgebra por la imagen $i\left(\mathfrak{g}\right)$, entonces cada $u \in U$ es combinación lineal de productos de la forma
$$i\left(x_1\right) \cdots i\left(x_r\right), \text{ con los } x_k \in \mathfrak{g},$$
pero γ y ψ son homomorfismos de álgebras asociativas, así que
$$\gamma \circ \psi \left(\prod_{k=1}^{r} i\left(x_k\right) \right) = \prod_{k=1}^{r} \gamma \circ \psi \circ i\left(x_k\right) = \prod_{k=1}^{r} i\left(x_k\right),$$
por tanto $\gamma \circ \psi(u) = u$, para todo $u \in U$, esto significa que $\gamma \circ \psi = id_U$ y de forma similar se tiene $\psi \circ \gamma = id_{\mathcal{U}}$, por tanto $U \cong \mathcal{U}$.

Para construir un álgebra envolvente universal de un álgebra de Lie $\mathfrak{g}$ considere el álgebra tensorial $T\left(\mathfrak{g}\right)$, y sea K el ideal bilateral de $T\left(\mathfrak{g}\right)$ dado por
$$K = \langle x \otimes y - y \otimes x - [x, y] : x, y \in \mathfrak{g} \rangle .$$
Ahora sea $U\left(\mathfrak{g}\right) = \dfrac{T\left(\mathfrak{g}\right)}{K}$ y sea $i : \mathfrak{g} \longrightarrow U\left(\mathfrak{g}\right)$ la restricción del homomorfismo canónico $\pi : T\left(\mathfrak{g}\right) \longrightarrow U\left(\mathfrak{g}\right)$. Una consecuencia del famoso Teorema de **Poincaré-Birkhoff-Witt** (PBW), que el lector puede consultar en el capítulo V de Humphreys (1997), es que el

par $(U(\mathfrak{g}), i)$ es un álgebra envolvente universal de $\mathfrak{g}$. El Teorema PBW es fundamental en la teoría de álgebras de Lie y establece un puente esencial entre la teoría de álgebras de Lie y la teoría de álgebras asociativas unitarias. Una importante consecuencia de este teorema es que $U(\mathfrak{g})$ tiene una filtración natural y la graduación asociada a esta filtración es isomorfa al álgebra simétrica $S(\mathfrak{g})$. Esto implica que se puede identificar el anillo de polinomios $\mathbb{C}[X_1, \ldots, X_r]$ con la graduación asociada al álgebra envolvente universal $U(\mathfrak{g})$ de una $\mathbb{C}$-álgebra de Lie $\mathfrak{g}$ de dimensión r.

CAPÍTULO 3

Geometría algebraica

3.1 Topología del espacio afín

En esta sección se hace una introducción a los conceptos y resultados básicos de la geometría algebraica, necesarios para entender los avances a cerca de subálgebras de Mishchenko-Fomenko, que serán expuestos en el capítulo final de este texto. Para entender los temas que aquí se exponen, es necesario que el lector tenga conocimientos de la teoría básica de anillos. En lo que sigue, el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en el cuerpo $\mathbb{F}$ se denota con $\mathbb{F}[X_1, \ldots, X_n]$.

Definición 3.1 (Espacio afín y variedad algebraica afín). El *espacio afín* de dimensión n, sobre un cuerpo $\mathbb{F}$, denotado $A^n_{\mathbb{F}}$, es el conjunto de n-uplas ordenadas de escalares en el cuerpo $\mathbb{F}$, es decir

$$A^n_{\mathbb{F}} = \{(a_1, \ldots, a_n) : a_i \in \mathbb{F}\}.$$

Cuando se trabaje con el cuerpo $\mathbb{C}$ de los números complejos, se denotará el espacio afín con A^n, en lugar de $A^n_{\mathbb{C}}$.

Dado un subconjunto no vacío $E \subseteq \mathbb{F}[X_1, \ldots, X_n]$, el conjunto de puntos del espacio afín $A^n_{\mathbb{F}}$ que anulan a todos los polinomios de E, se denota por $\mathcal{V}(E)$, y se denomina *variedad algebraica afín determinada por E sobre $\mathbb{F}$* (o simplemente *variedad*), es decir

$$\mathcal{V}(E) = \{P \in A^n_{\mathbb{F}} : f(P) = 0, \text{ para todo } f \in E\}$$

Ejemplo 3.1. Las rectas y las curvas cónicas como las circunferencia, parábolas, elipses e hipérbolas son variedades del espacio afín $A^2_{\mathbb{R}}$. Los planos y las superficies cuádricas como las esferas, elipsoides, conos y cilindros son variedades del espacio afín $A^3_{\mathbb{R}}$. Aunque todos los resultados que se presentan en este capítulo son válidos cuando el cuerpo $\mathbb{F}$ es algebraicamente cerrado, en lo que sigue se utilizará como cuerpo base el cuerpo $\mathbb{C}$ de los números complejos.

Proposición 3.1. Si E es un subconjunto del anillo de polinomios $\mathbb{C}[X_1, \ldots, X_n]$ y $J = \langle E \rangle$ es el ideal de $\mathbb{C}[X_1, \ldots, X_n]$ generado por E, entonces $\mathcal{V}(E) = \mathcal{V}(J)$.

Demostración. Sea $P \in \mathcal{V}(J)$, entonces $f(P) = 0$, para todo polinomio $f \in J$. Pero $E \subseteq J$, luego

$$f(P) = 0, \text{ para todo polinomio } f \in E,$$

en consecuencia, $P \in \mathcal{V}(E)$. Por otro lado, sean $P \in \mathcal{V}(E)$ y $f \in J$, entonces existen polinomios $f_1, \ldots, f_r \in E$ y $g_1, \ldots, g_3 \in \mathbb{C}[X_1, \ldots, X_n]$, tales que

$$f = g_1 f_1 + \cdots + g_r f_r,$$

luego, $f(P) = \sum_{i=1}^{r} g_i(P) f_i(P) = 0$, por que $f_i(P) = 0$, para toda $i = 1, \ldots, r$. Entonces $P \in \mathcal{V}(J)$, por tanto $\mathcal{V}(E) = \mathcal{V}(J)$. □

El Teorema de la base de Hilbert es un resultado fundamental de la teoría de anillos conmutativos, con importantes aplicaciones en el campo de la geometría algebraica. Este teorema garantiza que todos los anillos de polinomios $\mathbb{F}[X_1, \ldots, X_n]$, con coeficientes en un cuerpo $\mathbb{F}$, son noetherianos. Esto significa que cualquier ideal del anillo de polinomios $\mathbb{F}[X_1, \ldots, X_n]$ es finitamente generado. Una prueba de este teorema se puede consultar en Matsumura (1987), página 16.

Teorema 3.1 (Teorema de la base de Hilbert). Si A es un anillo Noetheriano, entonces el anillo de polinomios $A[X]$ es Noetheriano.

Ejemplo 3.2. Sea $E = \{Xf : f \in \mathbb{R}[X,Y]\}$, se quiere determinar $\mathcal{V}(E)$.

Por la Proposición (3.1), $\mathcal{V}(E) = \mathcal{V}(J)$, en la cual $J = \langle E \rangle$, y por el Teorema de la base de Hilbert, el ideal J es finitamente generado, de hecho $J = \langle X \rangle$, entonces

$$\mathcal{V}(E) = \mathcal{V}(\langle X \rangle) = \{(0,a) : a \in \mathbb{R}\}.$$

Geométricamente $\mathcal{V}(E)$ es el eje Y en $\mathbb{R}^2$.

Lema 3.1. En el espacio afín A^n se tienen los siguientes enunciados:

1. Si $\mathcal{I}$ y J son dos ideales de $\mathbb{C}[X_1,\ldots,X_n]$, con $\mathcal{I} \subseteq J$, entonces $\mathcal{V}(J) \subseteq \mathcal{V}(\mathcal{I})$.
2. A^n y $\emptyset$ son variedades.
3. Si $V_1,\ldots,V_k$ son variedades, entonces $V_1 \cup \cdots \cup V_k$ también es una variedad.
4. Si $\{V_j\}_{j\in\mathcal{J}}$ es una colección arbitraria de variedades, entonces $\bigcap\limits_{j\in\mathcal{J}} V_j$ también es una variedad.
5. Si $\mathcal{I}$ es un ideal de $\mathbb{C}[X_1,\ldots,X_n]$, entonces $\mathcal{V}(\mathcal{I}) = \mathcal{V}(\sqrt{\mathcal{I}})$, donde $\sqrt{\mathcal{I}}$ denota el ideal radical de $\mathcal{I}$, definido por

$$\sqrt{\mathcal{I}} = \left\{ f \in \mathbb{C}[X_1,\ldots,X_n] : f^m \in \mathcal{I}, \text{ para algún } m \in \mathbb{Z}^+ \right\}.$$

Demostración. Para el primer enunciado, sean $P \in \mathcal{V}(J)$ y f un polinomio del ideal $\mathcal{I}$. Dado que $\mathcal{I} \subseteq J$, se deduce que $f \in \mathcal{V}(J)$, luego $f(P) = 0$. Por tanto $P \in \mathcal{V}(\mathcal{I})$.

El siguiente enunciado es válido, porque $A^n = \mathcal{V}(0)$ y $\emptyset = \mathcal{V}(1)$.

Para el tercer enunciado, sean $\mathcal{I}_1,\ldots,\mathcal{I}_k$ ideales de $\mathbb{C}[X_1,\ldots,X_n]$, tales que $V_j = \mathcal{V}(\mathcal{I}_j)$, para toda $j = 1,\ldots,k$. Se mostrará que

$$V_1 \cup \cdots \cup V_k = \mathcal{V}(\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_k). \tag{3.1}$$

En efecto, si P es un elemento de alguna variedad $V_j = \mathcal{V}(\mathcal{I}_j)$, entonces $f(P) = 0$, para todo polinomio $f \in \mathcal{I}_j$, y dado que $\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_k \subseteq \mathcal{I}_j$, se tiene $P \in \mathcal{V}(\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_k)$. Ahora, si $P \notin V_1 \cup \cdots \cup V_k$, entonces para cada $j = 1,\ldots,k$ existe un polinomio $f_j \in \mathcal{I}_j$, tal que $f_j(P) \neq 0$. Luego, el producto $f_1 \cdots f_k$ es un polinomio del ideal $\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_k$, y se tiene

$$(f_1 \cdots f_k)(P) = f_1(P) \cdots f_k(P) \neq 0,$$

luego, $P \notin \mathcal{V}(\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_k)$, y esto implica la igualdad dada en la ecuación (3.1).

A fin de mostrar el cuarto enunciado, para cada $j \in \mathcal{J}$ sea $\mathcal{I}_j$ el ideal del anillo $\mathbb{C}[X_1,\ldots,X_n]$, tal que $V_j = \mathcal{V}\left(\mathcal{I}_j\right)$ y sea

$$\mathcal{I} = \left\{ \sum_{j \in \mathcal{J}} f_j : f_j \in \mathcal{I}_j \text{ y } f_j \neq 0 \text{ para a lo mas un número finito de términos} \right\}.$$

No es dificil verificar que $\mathcal{I}$ es un ideal de $\mathbb{C}[X_1, \ldots, X_n]$. En seguida se probará que

$$\bigcap_{j \in \mathcal{J}} \mathcal{V}\left(\mathcal{I}_j\right) = \mathcal{V}(\mathcal{I}).$$

El Teorema de la base de Hilbert, presentado en (3.1), garantiza que existen polinomios $f_1, \ldots, f_r \in \mathcal{I}$, tales que

$$\mathcal{I} = \langle f_1, \ldots, f_r \rangle.$$

Sean $P \in \bigcap_{j \in \mathcal{J}} \mathcal{V}\left(\mathcal{I}_j\right)$ y f un polinomio de $\mathcal{I}$, entonces existen polinomios $g_1, \ldots, g_r$ en $\mathbb{C}[X_1, \ldots, X_n]$, tales que

$$f = g_1 f_1 + \cdots + g_r f_r,$$

note que $f_i(P) = 0$, para toda $i = 1, \ldots, r$, entonces

$$f(P) = g_1(P) f_1(P) + \cdots + g_r(P) f_r(P) = 0,$$

es decir, $\bigcap_{j \in \mathcal{J}} \mathcal{V}\left(\mathcal{I}_j\right) \subseteq \mathcal{V}(\mathcal{I})$. Para la otra contenencia observe que para cada $j \in \mathcal{J}$ se tiene $\mathcal{I}_j \subseteq \mathcal{I}$, esto junto con el primer enunciado implica que $\mathcal{V}(\mathcal{I}) \subseteq \mathcal{V}\left(\mathcal{I}_j\right)$, entonces $\mathcal{V}(\mathcal{I}) \subseteq \bigcap_{j \in \mathcal{J}} \mathcal{V}\left(\mathcal{I}_j\right)$ y la prueba está completa.

Para finalizar, de la definición de ideal radical se obtiene $\mathcal{I} \subseteq \sqrt{\mathcal{I}}$, luego $\mathcal{V}\left(\sqrt{\mathcal{I}}\right) \subseteq \mathcal{V}(\mathcal{I})$. Para la otra contenencia, sean $P \in \mathcal{V}(\mathcal{I})$ y $f \in \sqrt{\mathcal{I}}$, luego $f^m \in \mathcal{I}$, para algún entero $m > 0$. En consecuencia, $f^m(P) = 0$ y dado que un cuerpo no tiene divisores de cero se desprende que $f(P) = 0$, por tanto, $P \in \mathcal{V}\left(\sqrt{\mathcal{I}}\right)$. □

Ejemplo 3.3. A continuación se van a determinar todas las variedades del espacio afín A^1. Del Lema (3.1) se sabe que A^1 y $\emptyset$ son variedades. Sea $\{a_1, \ldots, a_t\} \subseteq A^1$ y considere el polinomio $f = (X - a_1) \cdots (X - a_t)$, entonces

$$\mathcal{V}(f) = \{a_1, \ldots, a_t\}.$$

Finalmente si V es una variedad infinita contenida en A^1, entonces $V = \mathcal{V}(\mathcal{I})$, para algún ideal $\mathcal{I} \subseteq \mathbb{C}[X]$. Como $\mathcal{V}(\mathbb{C}[X]) = \mathcal{V}(\langle 1 \rangle) = \emptyset$ y $\mathbb{C}[X]$ es un DIP, se obtiene que $\mathcal{I} = \langle f \rangle$, para algún polinomio $f \in \mathbb{C}[X]$. Si f es de grado positivo t, entonces f tiene exactamente

t raíces en el cuerpo $\mathbb{C}$ y en este caso $\mathcal{V}(\mathcal{I})$ es finito. En consecuencia $\mathcal{I} = \{0\}$, y se tiene

$$V = \mathcal{V}\left(\{0\}\right) = A^1.$$

Por tanto, las variedades del espacio afín A^1 son A^1 y los conjuntos de cardinalidad finita.

La siguiente observación presenta algunas propiedades fundamentales de las variedades algebraicas, cuya demostración se propone como ejercicio para el lector:

Observación 3.1. En el espacio afín A^n se satisfacen las siguientes igualdades:

1. Si $f_1, \ldots, f_r$ son polinomios del anillo $\mathbb{C}\left[X_1, \ldots, X_n\right]$, entonces
$$\mathcal{V}\left(f_1, \ldots, f_r\right) = \bigcap_{i=1}^{r} \mathcal{V}\left(f_i\right).$$
2. Para todo polinomio $f \in \mathbb{C}\left[X_1, \ldots, X_n\right]$ y todo escalar no cero λ se tiene $\mathcal{V}\left(\lambda f\right) = \mathcal{V}\left(f\right)$.
3. Si f, g y h son polinomios de $\mathbb{C}\left[X_1, \ldots, X_n\right]$, entonces

   a) $\mathcal{V}(f, fg \pm h) = \mathcal{V}(f, h)$.

   b) $\mathcal{V}(f, gh) = \mathcal{V}(f, g) \cup \mathcal{V}(f, h)$.

   c) $\mathcal{V}(f - g,\ hf) = \mathcal{V}(f - g, hg)$.

   d) $\mathcal{V}(f - g, h \pm f) = \mathcal{V}(f - g, h \pm g)$.

Teorema 3.2. Sean $X_1, \ldots, X_r$ indeterminadas conmutativas. Si para $i = 1, \ldots, r$ el polinomio $f_i \in \mathbb{C}\left[X_1, \ldots, X_r\right]$ es la suma de los $\begin{pmatrix} r \\ i \end{pmatrix}$ monomios de grado i de la forma $X_{j_1} \cdots X_{j_i}$, con $j_1 < \cdots < j_i$, entonces

$$\mathcal{V}\left(f_1, \ldots, f_r\right) = \mathcal{V}\left(X_1, \ldots, X_r\right).$$

Demostración. El caso $r = 1$ es inmediato. Ahora, note que

$$\begin{aligned} f_1 &= X_1 + \cdots + X_r. \\ f_2 &= \sum_{i=1}^{r-1} \sum_{j=i+1}^{r} X_i X_j. \\ f_3 &= \sum_{i=1}^{r-2} \sum_{j=i+1}^{r-1} \sum_{k=j+1}^{r} X_i X_j X_k. \\ &\ \vdots \\ f_r &= X_1 \cdots X_r. \end{aligned} \tag{3.2}$$

La prueba se realizará por inducción sobre el número r de indeterminadas. Para $r = 2$ se tienen los polinomios

$$f_1 = X_1 + X_2 \quad \text{y} \quad f_2 = X_1 X_2.$$

Los enunciados de la Observación anterior implican

$$\mathcal{V}(f_1, f_2) = \mathcal{V}(X_1 + X_2, X_1 X_2) = \mathcal{V}(X_1 + X_2, X_1) \cup \mathcal{V}(X_1 + X_2, X_2).$$

Pero

$$\mathcal{V}(X_1 + X_2, X_1) = \mathcal{V}(X_1, X_2) = \mathcal{V}(X_1 + X_2, X_2),$$

entonces $\mathcal{V}(f_1, f_2) = \mathcal{V}(X_1, X_2)$. Ahora suponga que el enunciado es válido para anillos de polinomios en $r-1$ indeterminadas conmutativas y considere los r polinomios referidos en (3.2). Dado que $f_r = X_1 \cdots X_{r-1} X_r$ se tiene

$$\mathcal{V}(f_1, \ldots, f_r) = \bigcup_{i=1}^{r} \mathcal{V}(f_1, \ldots, f_{r-1}, X_i). \tag{3.3}$$

Note que un punto $(a_1, \ldots, a_r) \in A^r$ está en $\mathcal{V}(f_1, \ldots, f_{r-1}, X_i)$, si y solo si, $a_i = 0$ y el punto $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_r) \in A^{r-1}$ anula a los $r-1$ polinomios $g_1, \ldots, g_{r-1}$ definidos por

$$g_j = f_j (X_i = 0), \text{ para } j = 1, \ldots, r-1.$$

No es dificil verificar que los polinomio $g_1, \ldots, g_{r-1}$ tienen la forma de los polinomios de la lista (3.2) en el anillo $\mathbb{C}[X_1, \ldots, X_{i-1}, X_{i+1}, X_r]$, y por la hipótesis de inducción se tiene

$$\mathcal{V}(g_1, \ldots, g_{r-1}) = \mathcal{V}(X_1, \ldots, X_{i-1}, X_{i+1}, X_r).$$

Dado que $\mathcal{V}(f_1, \ldots, f_{r-1}, X_i) = \mathcal{V}(g_1, \ldots, g_{r-1}) \cap \mathcal{V}(X_i)$, se concluye que

$$\mathcal{V}(f_1, \ldots, f_{r-1}, X_i) = \mathcal{V}(X_1, \ldots, X_{i-1}, X_{i+1}, X_r) \cap \mathcal{V}(X_i) = \mathcal{V}(X_1, \ldots, X_r).$$

Sustituyendo en la igualdad (3.3), se obtiene el resultado deseado. □

Proposición 3.2 (Ideal asociado). Si B es un subconjunto no vacío de A^n, entonces el conjunto de polinomios del anillo $\mathbb{C}[X_1, \ldots, X_n]$ que se anulan en todos los puntos de B es un ideal de $\mathbb{C}[X_1, \ldots, X_n]$ denominado *ideal asociado al subconjunto B* y se denota por $J(B)$. Además, se define $J(\emptyset) = \mathbb{C}[X_1, \ldots, X_n]$.

Demostración. Según el enunciado anterior

$$J(B) = \{f \in \mathbb{C}[X_1, \ldots, X_n] : f(P) = 0, \text{ para todo } P \in B\}.$$

Claramente el polinomio $0 \in J(B)$. Ahora, si $P \in B$, los polinomios f y g están en $J(B)$

y $h \in \mathbb{C}[X_1, \ldots, X_n]$, se tiene

$$(f-g)(P) = f(P) - g(P) = 0 \quad \text{y} \quad (fh)(P) = f(P)h(P) = 0.$$

Por tanto, $f - g \in J(B)$ y $fh \in J(B)$. $\square$

Lema 3.2. Sean B y D dos subconjuntos del espacio A^n, se cumplen los siguientes enunciados

1. Si $B \subseteq D$, entonces $J(D) \subseteq J(B)$.
2. $J(B \cup D) = J(B) \cap J(D)$.
3. $\sqrt{J(B)} = J(B)$.

Demostración. El primer enunciado es claramente válido cuando $B = \emptyset$. Suponga que $B \neq \emptyset$ y sean P un punto de B y f un polinomio de $J(D)$, luego $P \in D$, y de ahí que $f(P) = 0$. Por tanto $f \in J(B)$.

Para el segundo enunciado, sea $f \in J(B \cup D)$ y escoja un punto $P \in B$. Dado que $B \subseteq B \cup D$, se tiene $f(P) = 0$, luego $f \in J(B)$ y, similarmente, se obtiene $f \in J(D)$, en consecuencia, $f \in J(B) \cap J(D)$. Ahora, sea f un polinomio de $J(B) \cap J(D)$ y sea P un punto de $B \cup D$. En cualquiera de los dos casos $P \in B$ o $P \in D$, se obtiene $f(P) = 0$. Por tanto, $f \in J(B \cup D)$.

Para finalizar, sean $f \in \sqrt{J(B)}$ y $P \in B$, entonces $f^r \in J(B)$, para algún entero $r > 0$. Luego, $f^r(P) = 0$ y dado que $f(P) \in \mathbb{C}$, se sigue que $f(P) = 0$, por tanto $f \in J(B)$. La otra inclusión siempre es válida. $\square$

Lema 3.3. Para todo entero positivo n, se tiene $J(A^n) = \{0\}$.

Demostración. Por inducción en n, para $n = 1$, se obtiene $A^1 = \mathbb{C}$ y sea $f \in \mathbb{C}[X]$ un polinomio no constante. Dado que $\mathbb{C}$ es un cuerpo algebaicamente cerrado, existen escalares $c_1, \ldots, c_r, a_r \in \mathbb{C}$, con $a_r \neq 0$, tales que

$$f = a_r (X - c_1) \cdots (X - c_r)$$

Luego, $f(z) \neq 0$, para todo complejo $z \notin \{c_1, \ldots, c_r\}$, en consecuencia $f \notin J(A^1)$. Además los polinomios constantes no cero no tienen raíces, por tanto, $J(A^1) = \{0\}$. Ahora suponga que el enunciado es válido para algún entero positivo n y sea f un polinomio en $J(A^{n+1})$. Si $f \neq 0$, entonces existen polinomios $g_0, g_1, \ldots, g_r \in \mathbb{C}[Y_1, \ldots, Y_n]$, con $g_r \neq 0$, tales que

$$f = g_0 + g_1 X + \cdots + g_r X^r,$$

Dado que $J(A^n) = \{0\}$ se sigue que $g_r \notin J(A^n)$, luego

$$g_r(P) \neq 0, \text{ para algún punto } P \in A^n,$$

entonces $h = g_0(P) + g_1(P)X + \cdots + g_r(P)X^r$ es un polinomio no cero en $\mathbb{C}[X]$, esto implica que existe un $z \in \mathbb{C}$, tal que

$$h(z) = g_0(P) + g_1(P)z + \cdots + g_r(P)z^r \neq 0.$$

En consecuencia, el punto (z, P) está en el espacio afín A^{n+1} y $f(z, P) = h(z) \neq 0$, lo que contradice $f \in J\left(A^{n+1}\right)$. Por tanto $f = 0$. $\square$

Observación 3.2. Si P es un punto de un conjunto $B \subseteq A^n$, entonces para cualquier polinomio $f \in J(B)$ se tiene $f(P) = 0$, luego $P \in \mathcal{V}(J(B))$. Además

$$\mathcal{V}(J(\emptyset)) = \mathcal{V}(\mathbb{C}[X_1, \ldots, X_n]) = \emptyset.$$

Por tanto, para todo $B \subseteq A^n$ se cumple $B \subseteq \mathcal{V}(J(B))$. El lector puede comprobar que la igualdad $B = \mathcal{V}(J(B))$ es válida, si y solo si, B es una variedad algebraica.

Ejemplo 3.4. Si $P = (a_1, \ldots, a_n)$ es un punto del espacio afín A^n, probar que el ideal $\mathfrak{m}_P = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ es maximal en el anillo de polinomios $\mathbb{C}[X_1, \ldots, X_n]$.

Demostración. Sea $\varepsilon_P : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}$, definido por

$$\varepsilon(f) = f(P), \text{ para todo polinomio } f \in \mathbb{C}[X_1, \ldots, X_n],$$

es decir, ε_P es el homomorfismo de evaluación en P. Se puede comprobar que dado un polinomio f existen polinomios $g_1, \ldots, g_n \in \mathbb{C}[X_1, \ldots, X_n]$ y un escalar $b \in \mathbb{C}$, tales que

$$f = g_1(X_1 - a_1) + \cdots + g_n(X_n - a_n) + b.$$

Así que,

$$f \in Ker(\varepsilon_P), \text{ si y solo si, } b = 0, \text{ si y solo si, } f \in \mathfrak{m}_P = \langle X_1 - a_1, \ldots, X_n - a_n \rangle,$$

esto implica que $Ker(\varepsilon_P) = \mathfrak{m}_P$. Pero el homomorfismo ε_P es claramente sobreyectivo, entonces

$$\frac{\mathbb{C}[X_1, \ldots, X_n]}{\mathfrak{m}_P} \cong \mathbb{C}.$$

Dado que $\mathbb{C}$ es un cuerpo, se sigue que $\mathfrak{m}_P$ es un ideal maximal del anillo de polinomios $\mathbb{C}[X_1, \ldots, X_n]$. $\square$

Teorema 3.3 (**Teorema de los ceros de Hilbert**)**.** Sean $\mathfrak{m}$ e $\mathcal{I}$ dos ideales del anillo de polinomios $\mathbb{C}[X_1, \ldots, X_n]$. Los siguientes enunciados son verdaderos:

1. $\mathfrak{m}$ es máximal, si y solo si, existe un punto $P = (a_1, \ldots, a_n) \in A^n$, tal que
$$\mathfrak{m} = \mathfrak{m}_P = \langle X_1 - a_1, \ldots, X_n - a_n \rangle .$$
2. Si $\mathcal{I}$ es un ideal propio, entonces $\mathcal{V}(\mathcal{I}) \neq \emptyset$.
3. $J(\mathcal{V}(\mathcal{I})) = \sqrt{\mathcal{I}}$.

Demostración. Para mostrar el primer enunciado, recuerde que el Ejemplo (3.4) establece que en el anillo $\mathbb{C}[X_1, \ldots, X_n]$, todo ideal de la forma $\mathfrak{m}_P = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$, es maximal. Ahora, suponga que $\mathfrak{m} \subset \mathbb{C}[X_1, \ldots, X_n]$ es un ideal máximal y considere el cuerpo $K = \dfrac{\mathbb{C}[X_1, \ldots, X_n]}{\mathfrak{m}}$ junto con el homomorfismo de anillos $\delta : \mathbb{C} \longrightarrow K$ definido por
$$\delta(a) = a + \mathfrak{m}, \text{ para toda } a \in \mathbb{C}.$$
Dado que $\mathfrak{m}$ es máximal se sigue que $\mathbb{C} \cap \mathfrak{m} = \{0\}$, luego
$$a \in Ker(\delta), \text{ si y sólo si, } a \in \mathfrak{m}, \text{ si y sólo si, } a = 0.$$
entonces δ es un homomorfismo inyectivo y se tiene la extensión de cuerpos $K|\mathbb{C}$. Por lo expuesto en la sección (A.2) de los anexos, se sigue que la extensión $K|\mathbb{C}$ es de tipo finito con generadores $X_1 + \mathfrak{m}, \ldots, X_n + \mathfrak{m}$. Por el Lema de Zariski, presentado en (A.3), todo elemento en K es algebraico sobre $\mathbb{C}$, y dado que $\mathbb{C}$ es algebraicamente cerrado se sigue que $\mathbb{C} \cong \delta(\mathbb{C}) = K$. Lo anterior implica que para cada $i = 1, \ldots, n$ existe un único complejo a_i tal que
$$X_i + \mathfrak{m} = \delta(a_i) = a_i + \mathfrak{m},$$
entonces
$$X_i - a_i \in \mathfrak{m}, \text{ para toda } i = 1, \ldots, n.$$
Por ende,
$$\mathfrak{m}_P = \langle X_1 - a_1, \ldots, X_n - a_n \rangle \subseteq \mathfrak{m},$$
pero el ideal $\mathfrak{m}_P$ es máximal, por tanto $\mathfrak{m}_P = \mathfrak{m}$.

Para el siguiente enunciado sea $\mathfrak{m}$ un ideal máximal de $\mathbb{C}[X_1, \ldots, X_n]$ tal que $\mathcal{I} \subseteq \mathfrak{m}$. Por el Lema (3.1) se sigue que $\mathcal{V}(\mathfrak{m}) \subseteq \mathcal{V}(\mathcal{I})$ y dado que $\mathfrak{m} = \mathfrak{m}_P$, para algún punto $P \in A^n$, se tiene $\mathcal{I} \neq \emptyset$, porque
$$\{P\} = \mathcal{V}(\mathfrak{m}) \subseteq \mathcal{V}(\mathcal{I}).$$
Para probar el último enunciado sea f un polinomio de $\sqrt{\mathcal{I}}$ y sea P un punto de la variedad $\mathcal{V}(I)$, entonces $f^m \in \mathcal{I}$, para algún entero $m > 0$, y se tiene
$$(f(P))^m = f^m(P) = 0, \text{ luego, } f(P) = 0.$$

Esto significa que $\sqrt{\mathcal{I}} \subseteq J(\mathcal{V}(\mathcal{I}))$. Mostrar la otra contenencia presenta mayor dificultad y en el proceso de prueba se utilizará una técnica elegante en álgebra conmutativa que permite identificar los ideales del anillo de polinomios que son radicales y las variedades algebriacas. Esta técnica conocida como **el truco de Rabinowitsch** fue descrita por Rabinowitsch (1930).

Por el Teorema de la base de Hilbert (3.1), todo ideal de $\mathbb{C}[X_1,\ldots,X_n]$ es finitamente generado, luego existen polinomios $f_1,\ldots,f_m$, tales que $\mathcal{I}=\langle f_1,\ldots,f_m\rangle$. Sea Y una nueva indeterminada y para cada polinomio no nulo $f\in J(\mathcal{V}(\mathcal{I}))$, considere el ideal

$$\widehat{\mathcal{I}}_f=\langle f_1,\ldots,f_m, Yf-1\rangle \subseteq \mathbb{C}[X_1,\ldots,X_n,Y].$$

Observe que dado un punto $P\in\mathcal{V}(\mathcal{I})$ y cualquier $a\in\mathbb{C}$, se tiene

$$(Yf-1)(P,a)=Y(P,a)f(P,a)-1=a0-1\neq 0,$$

esto implica que $\mathcal{V}\left(\widehat{\mathcal{I}}_f\right)=\emptyset$ y por el enunciado anterior $\widehat{\mathcal{I}}_f=\mathbb{C}[X_1,\ldots,X_n,Y]$. Luego, existen polinomios $g_1,\ldots,g_n,g\in\mathbb{C}[X_1,\ldots,X_n,Y]$, tales que

$$g_1f_1+\cdots+g_nf_n+g\,(Yf-1)=1.$$

Ahora, para cada $i=1,\ldots,n$ sea t_i el mayor exponente de la indeterminada Y en el polinomio g_i y sea $T=t_1+\cdots+t_n$. Haciendo $Y=\dfrac{1}{f}$, se obtiene

$$f^T\left(g_1f_1+\cdots+g_nf_n+g\left(\frac{1}{f}f-1\right)\right)=f^T,$$

entonces

$$\sum_{i=1}^{n} f^{T-t_i}\left(f^{t_i}g_i\right)f_i=f^T.$$

Note que $f^{t_i}g_i\in\mathbb{C}[X_1,\ldots,X_n]$, para toda $i=1,\ldots,n$, en consecuencia $f^T\in\mathcal{I}$. Por tanto, $f\in\sqrt{\mathcal{I}}$ y la prueba está completa. $\square$

3.2 Componentes irreducibles

Para presentar los avances a cerca de la regularidad de secuencias de Mischenko-Fomenko es necesario justificar que toda variedad algebraica se puede expresar de forma única como unión de variedades irreducibles. En seguida se presenta la teoría que sustenta este resultado.

Definición 3.2 (**Variedad Irreducible**)**.** Una variedad V del espacio afín A^n es irreducible si para todo par de variedades V_1 y V_2 tales que $V = V_1 \cup V_2$, se tiene $V = V_1$ o $V = V_2$. En caso contrario, V se denomina reducible.

Ejemplo 3.5. De la definición anterior, es claro que la variedad $\mathcal{V}(1) = \emptyset$ es irreducible. Por el Ejemplo (3.3), el espacio afín A^1 es irreducible, porque dadas dos variedades V_1 y V_2, tales que $A^1 = V_1 \cup V_2$, con $A^1 \neq V_1$, se sigue que V_1 es finita y V_2 es infinta. Por tanto $A^1 = V_2$.

La variedad $\mathcal{V}(X) = \{(0, a) : a \in \mathbb{C}\} \subseteq A^2$ es irreducible. En efecto, sean V_1 y V_2 dos variedades, tales que $\mathcal{V}(X) = V_1 \cup V_2$, y suponga que $\mathcal{V}(X) \neq V_1$. Sean R y S dos ideales del anillo $\mathbb{C}[X, Y]$, para los cuales se cumple

$$\mathcal{V}(R) = V_1 \quad \text{y} \quad \mathcal{V}(S) = V_2.$$

Luego, existe un polinomio $f \in R$ que no se anula en algún punto de $\mathcal{V}(X)$ y dado un polinomio arbitrario $g \in S$, se tiene $fg \in R \cap S$. El Lema (3.1) garantiza que

$$\mathcal{V}(X) = V_1 \cup V_2 = \mathcal{V}\left(R \cap S\right),$$

y del Teorema de los ceros de Hilbert (3.3) se obtiene

$$\sqrt{\langle X \rangle} = J\left(\mathcal{V}(X)\right) = J\left(\mathcal{V}(R \cap S)\right) = \sqrt{R \cap S},$$

entonces

$$fg \in R \cap S \subseteq \sqrt{R \cap S} = \sqrt{\langle X \rangle}.$$

Pero $\langle X \rangle$ es un ideal primo, porque el cociente $\dfrac{\mathbb{C}[X, Y]}{\langle X \rangle} \cong \mathbb{C}[Y]$ es un dominio entero. En consecuencia, $\sqrt{\langle X \rangle} = \langle X \rangle$ y se obtiene $fg \in \langle X \rangle$. Pero $f \notin \langle X \rangle$, porque f no se anula en algún punto de $\mathcal{V}(X)$. De aquí se deduce que $g \in \langle X \rangle$ y se tiene $S \subseteq \langle X \rangle$, luego

$$\mathcal{V}(X) \subseteq \mathcal{V}(S) = V_2 \subseteq \mathcal{V}(X).$$

Por tanto $\mathcal{V}(X) = V_2$ y se ha demostrado que la variedad $\mathcal{V}(X)$ es irreducible.

El ejemplo anterior es una situación particular del siguiente teorema:

Teorema 3.4. Una variedad no vacía $V \subseteq A^n$ es irreducible, si y solo si, el ideal $J(V)$ es primo.

Demostración. Para iniciar suponga que la variedad no vacía V es irreducible. Por uno de los enunciados del Teorema de los ceros de Hilbert (3.3), se sigue que $J(V)$ es un ideal propio del anillo de polinomios $\mathbb{C}[X_1, \ldots, X_n]$. Sean f y g dos polinomios, tales que $fg \in J(V)$, por la Observación (3.2) y las propiedades expuestas en el Lema (3.1), se tiene

$$V = \mathcal{V}(J(V)) \subseteq \mathcal{V}(fg) = \mathcal{V}(f) \cup \mathcal{V}(g).$$

Pero V es irreducible, luego no se pierde generalidad en suponer que $V = \mathcal{V}(f)$, y de aquí se tiene

$$f \in J(\mathcal{V}(f)) = J(V),$$

por tanto $J(V)$ es primo. Recíprocamente, suponga que $J(V)$ es un ideal primo del anillo $\mathbb{C}[X_1, \ldots, X_n]$. Por contradicción suponga que V es reducible, luego existen dos ideales R y S, tales que

$$V = \mathcal{V}(R) \cup \mathcal{V}(S) = \mathcal{V}(R \cap S),$$

con $V \neq \mathcal{V}(R)$ y $V \neq \mathcal{V}(S)$. Entonces se pueden elegir dos polinomios $f \in R$ y $g \in S$ tales que ni f ni g pertenecen a $J(V)$. Del hecho que $J(V)$ es primo se sigue $fg \notin J(V)$, luego

$$f(P)g(P) \neq 0, \text{ para algun punto } P \in V = \mathcal{V}(R \cap S),$$

pero esto contradice que $fg \in R \cap S$. Por tanto la variedad V es irreducible. □

Ejemplo 3.6. Para todo entero $n > 0$, el espacio afín A^n es una variedad irreducible porque $J(A^n) = \{0\}$, que es un ideal primo.

Del Ejemplo (3.3), las variedades del espacio afín A^1 son: A^1 y los subconjuntos finitos de A^1. Por lo anterior, A^1 es una variedad irreducible y se sabe que la variedad vacía también es irreducible. Además, para cada $a \in \mathbb{C}$, se tiene $J(a) = \langle X - a \rangle$, que es un ideal máximal y, en consecuencia, primo en el anillo $\mathbb{C}[X]$, así que $\{a\}$ es una variedad irreducible. Pero si V es una variedad finita de cardinal mayor que dos, entonces V es reducible. Por tanto, en A^1 las variedades irreducibles son A^1, $\emptyset$ y las variedades que tienen un único punto.

Proposición 3.3. Sean m y n dos enteros positivos, con $m \leq n$. Si $a_1, \ldots, a_m \in \mathbb{C}$, entonces la variedad $\mathcal{V}(\langle X_1 - a_1, \ldots, X_m - a_m \rangle) \subseteq A^n$ es irreducible.

Demostración. Sean $D = \mathbb{C}[X_1, \ldots, X_n]$ y $\mathcal{J} = \langle X_1 - a_1, \ldots, X_m - a_m \rangle$. Si $m = n$, el ideal $\mathcal{J}$ es máximal y, por tanto, la variedad $\mathcal{V}(\mathcal{J})$ es irreducible. Ahora suponga que $m < n$ y considere el homomorfismo de anillos $\psi : \mathbb{C}[X_{m+1}, \ldots, X_n] \longrightarrow \dfrac{D}{\mathcal{J}}$, definido por

$$\psi(h) = h + \mathcal{J}, \text{ para todo polinomio } h \in \mathbb{C}[X_{m+1}, \ldots, X_n].$$

Note que para cada polinomio $f \in D$, existen polinomios $g_1, \ldots, g_m \in D$ y un polinomio

$h \in \mathbb{C}[X_{m+1}, \ldots, X_n]$, tales que

$$f = g_1 (X_1 - a_1) + \cdots + g_m (X_m - a_m) + h,$$

luego $\psi(h) = f + \mathcal{J}$, y esto implica que ψ es un isomorfismo de anillos. Entonces, $\dfrac{D}{\mathcal{J}}$ es un dominio entero, por tanto, $\mathcal{V}(\mathcal{J})$ es una variedad irreducible. $\square$

Lema 3.4. Una variedad $V \subseteq A^n$ es irreducible, si y solo si, dadas dos variedades V_1 y V_2 contenidas propiamente en V, se tiene $(V - V_1) \cap (V - V_2) \neq \emptyset$.

Demostración. Primero suponga que V es irreducible, y por contradicción considere como cierto que existen variedades V_1 y V_2 contenidas propiamente en V, tales que

$$(V - V_1) \cap (V - V_2) = \emptyset,$$

entonces,

$$V = V - \emptyset = V - ((V - V_1) \cup (V - V_2)) = V_1 \cup V_2.$$

Dado que V es irreducible, entonces $V = V_1$ o $V = V_2$ pero esto contradice el hecho que las dos variedades están contenidas propiamente en V, en consecuencia

$$(V - V_1) \cap (V - V_2) \neq \emptyset.$$

Para el recírpoco, sean V_1 y V_2 dos variedades tales que $V = V_1 \cup V_2$, se tiene

$$(V - V_1) \cap (V - V_2) = V - (V_1 \cup V_2) = \emptyset.$$

Lo anterior, junto con la hipótesis, implican que alguna de las variedades V_1 o V_2 no es un subconjunto propio de V, es decir, $V = V_1$ o $V = V_2$, por tanto V es irreducible. $\square$

Proposición 3.4. Toda colección no vacía de variedades algebraicas de A^n tiene un elemento minimal.

Demostración. Suponga que el enunciado es falso y escoja una colección no vacía $\mathcal{F}$ de variedades de A^n, tal que $\mathcal{F}$ no tiene elemento minimal. Seleccione una variedad $V_0 \in \mathcal{F}$, dado que V_0 no es minimal en $\mathcal{F}$, existe $V_1 \in \mathcal{F}$, tal que $V_0 \supset V_1$. Ahora, V_1 no es minimal en $\mathcal{F}$, luego existe $V_2 \in \mathcal{F}$, tal que $V_0 \supset V_1 \supset V_2$. Dado que $\mathcal{F}$ no tiene elemento minimo, este proceso no termina y se construye la cadena infinita estrictamente decreciente

$$V_0 \supset V_1 \supset \cdots \supset V_m \supset V_{m+1} \supset \cdots$$

En consecuencia, se tiene la siguiente cadena creciente de ideales del anillo $\mathbb{C}[X_1, \ldots, X_n]$

$$J(V_0) \subseteq J(V_1) \subseteq \cdots \subseteq J(V_m) \subseteq J(V_{m+1}) \subseteq \cdots$$

Dado que $\mathbb{C}[X_1, \ldots, X_n]$ es un anillo Noetheriano, la cadena anterior estabiliza, lo cual significa que existe un entero positivo k, tal que

$$J(V_k) = J(V_t) \text{ para todo entero } t \geq k,$$

en particular, $J(V_k) = J(V_{k+1})$. Pero de aquí se obtiene la contradicción

$$V_k = \mathcal{V}(J(V_k)) = \mathcal{V}(J(V_{k+1})) = V_{k+1} \neq V_k.$$

Por tanto, la colección $\mathcal{F}$ tiene un elemento minimal. □

Teorema 3.5. Si V es una variedad de A^n, entonces existen variedades irreducibles $V_1, \ldots, V_m$, tales que $V = V_1 \cup \cdots \cup V_m$. Además, las variedades irreducibles se pueden seleccionar de tal manera que ninguna de las V_i esté contenida en la unión de las demás, es decir, para toda $i = 1, \ldots, m$ se cumple

$$V_i \nsubseteq \bigcup_{\substack{j=1 \\ j\neq i}}^{m} V_j.$$

Demostración. El enunciado es claramente válido cuando V es irreducible, entonces resta probar que el teorema se cumple para variedades reducibles. Por contradicción, suponga que la colección $\mathcal{F}$ de variedades del espacio afín A^n que son reducibles y no se pueden expresar como unión finita de variedades irreducibles, es no vacía. De acuerdo con la Proposición (3.4), la colección $\mathcal{F}$ tiene un elemento minimal V que es reducible, luego existen variedades V_1 y V_2 contenidas propiamente en V, tales que $V = V_1 \cup V_2$. Por la minimalidad de V en la colección $\mathcal{F}$ se sigue que las variedades V_1 y V_2 no están en $\mathcal{F}$, y se deben poder expresar como unión finita de variedades irreducibles; pero esto implica que la variedad V es unión finita de variedades irreducibles y se contradice el hecho de que $V \in \mathcal{F}$. Por tanto, la colección $\mathcal{F}$ es vacía y toda variedad V del espacio afín A^n se puede expresar como unión finita de variedades irreducibles. Para continuar, suponga que $V_1, \ldots, V_k$ son variedades irreducibles, tales que

$$V = V_1 \cup \cdots \cup V_k.$$

Si alguna de las variedades V_i está contenida en la unión de las demás, entonces eliminando V_i y haciendo una nueva numeración de las variedades restantes, se obtiene

$$V = V_1 \cup \cdots \cup V_{k-1},$$

esta acción se repite siempre que una de las variedades V_i esté contenida en la unión de las demás. El proceso es finito, en consecuencia, existen variedades irreducibles $V_1 \cup \cdots \cup V_m$, tales que $V = V_1 \cup \cdots \cup V_m$, y para toda $i = 1, \ldots, m$ se cumple

$$V_i \nsubseteq \bigcup_{\substack{j=1 \\ j \neq i}}^{m} V_j.$$

□

Corolario 3.1. Sea V una variedad de A^n. Las variedades irreducibles garantizadas en el Teorema (3.5) son únicas, salvo permutación de las V_i, y se denominan **componentes irreducibles** para V.

Demostración. Primero note que dadas las variedades $W, V_1, \ldots, V_m$, con W irreducible, la igualdad

$$W = V_1 \cup \cdots \cup V_m.$$

implica $W = V_i$, para alguna $i = 1, \ldots, m$. Ahora, sean $\{V_1, \ldots, V_m\}$ y $\{W_1, \ldots, W_k\}$ dos colecciones de variedades irreducibles en A^n que satisfacen el Teorema (3.5) para V. Sin pérdida de generalidad suponga que $m \leq k$, entonces

$$V_1 \subseteq V = W_1 \cup \cdots \cup W_k.$$

De aquí se obtiene

$$V_1 = V_1 \cap (W_1 \cup \cdots \cup W_k) = (V_1 \cap W_1) \cup \cdots \cup (V_1 \cap W_k).$$

Por lo expuesto al principio de esta demostración, se sigue que $V_1 = V_1 \cap W_i$, para alguna $i = 1, \ldots, k$, y salvo una nueva numeración de los W_i, se puede suponer que $V_1 = V_1 \cap W_1$, esto implica que $V_1 \subseteq W_1$. De forma similar se puede deducir que $W_1 \subseteq V_i$, para alguna $i = 1, \ldots, m$. De ahí que $V_1 \subseteq W_1 \subseteq V_i$, sin embargo,

$$V_1 \nsubseteq V_2 \cup \cdots \cup V_m,$$

de modo que $V_i = V_1$, entonces $V_1 = W_1$, y se tiene

$$V_2 \cup \cdots \cup V_m = W_2 \cup \cdots \cup W_k.$$

Repitiendo el proceso anterior, se sigue que $V_i = W_i$, para toda $i = 1, \ldots, m$. Note que en el caso $m < k$, se tendría

$$W_{m+1} \cup \ldots \cup W_k = \emptyset,$$

y se obtiene la contradicción

$$W_{m+1} = \emptyset \subseteq \bigcup_{\substack{j=1\\ j\neq m+1}}^{k} W_j.$$

Por tanto, $m = k$ y la prueba está completa. $\square$

Ejemplo 3.7. En seguida se determinan las componentes irreducibles de la variedad

$$V = \mathcal{V}(X+Y+Z, XY+XZ+YZ, XYZ) \subseteq A^3.$$

Note que el Teorema (3.2) garantiza que en el espacio afín A^3, se cumple

$$V = \mathcal{V}(X, Y, Z) = \{(0,0,0)\}.$$

Luego, V es una variedad irreducible del espacio afín A^3, y por tanto $V = \{(0,0,0)\}$ es su única componente irreducible.

Ejemplo 3.8. Encontrar las componentes irreducibles de la variedad $V = \mathcal{V}\left(X^2Y^2+1\right)$, contenida en el espacio afín A^2.

Solución: Note que

$$\mathcal{V}\left(X^2Y^2+1\right) = \mathcal{V}((XY+i)(XY-i)) = \mathcal{V}(XY+i) \cup \mathcal{V}(XY-i).$$

Pero los polinomios $f = XY + i$ y $g = XY - i$ son irreducibles sobre $\mathbb{C}$, pues la única posible factorización de f (similarmente para g) es de la forma

$$f = (X-a)(Y-b),$$

pero esto implica $a = b = 0$ y $ab = i$, lo cual es imposible. De modo que los ideales $\langle XY+i\rangle$ y $\langle XY-i\rangle$ son primos. Por ende las componentes irreducibles de la variedad $V = \mathcal{V}\left(X^2Y^2+1\right)$ son $V_1 = \mathcal{V}(XY+i)$ y $V_2 = \mathcal{V}(XY-i)$.

3.3 Variedades isomorfas

El concepto de isomorfismo es fundamental, porque permite clasificar variedades en clases de equivalencia, en las cuales las variedades isomorfas se consideran esencialmente iguales desde el punto de vista algebraico y geométrico. En muchos casos, utilizar variedades algebraicas isomorfas consigue simplificar problemas complejos mediante la utilización de variedades más sencillas. En este punto se presenta la definición de **isomorfismo de variedades algebraicas afines** junto con algunos ejemplos de este importante concepto.

Definición 3.3 (**Anillo de coordenadas**). Sea V una variedad algebraica contenida en el espacio afín A^n. **El anillo de coordenada afín** asociado a la variedad V es el anillo cociente

$$\mathbb{C}[V] = \frac{\mathbb{C}\left[X_1, \ldots, X_n\right]}{J(V)}.$$

Ejemplo 3.9. A continuación, se procederá a identificar el anillo de coordenadas de la variedad $V = \mathcal{V}(XY) \subseteq A^2$.

Por el Teorema de los ceros de Hilbert se tiene

$$J(V) = \sqrt{\langle XY \rangle} = \left\{ f \in \mathbb{C}[X, Y] : f^m \in \langle XY \rangle, \text{ para algún entero } m > 0 \right\}.$$

Primero se comprobará que $\sqrt{\langle XY \rangle} = \langle XY \rangle$. En efecto, sea $f \in \sqrt{\langle XY \rangle}$, entonces para algún entero $m > 0$, se tiene

$$f^m \in \langle XY \rangle = \langle X \rangle \cap \langle Y \rangle.$$

en consecuencia

$$f^m \in \langle X \rangle \quad \text{y} \quad f^m \in \langle Y \rangle.$$

Pero $\langle X \rangle$ y $\langle Y \rangle$ son ideales primos del anillo $\mathbb{C}[X, Y]$, entonces

$$f \in \langle X \rangle \cap \langle Y \rangle = \langle XY \rangle.$$

Por tanto, $J(V) = \langle XY \rangle$, y se tiene

$$\mathbb{C}[V] = \frac{\mathbb{C}\left[X, Y\right]}{J(V)} = \frac{\mathbb{C}\left[X, Y\right]}{\langle XY \rangle} = \left\{ f + g + \langle XY \rangle : f \in \mathbb{C}[X], g \in \mathbb{C}[Y] \right\}.$$

Observación 3.3. Sea V una variedad algebraica del espacio afín A^n. Cada clase lateral $\overline{f}$ del anillo $\mathbb{C}[V]$ se puede visualizar como la función $\overline{f} : V \longrightarrow \mathbb{C}$ dada por

$$\overline{f}(P) = f(P), \text{ para todo punto } P \in V.$$

La función $\overline{f}$ esta bien definida, porque no depende del representante de la clase lateral $\overline{f}$. En efecto, la igualdad $\overline{f} = \overline{g}$ es válida en $\mathbb{C}[V]$, si y solo si, $f - g \in J(V)$, entonces para todo punto $P \in V$, se cumple

$$\overline{f}(P) = f(P) = (f - g)(P) + g(P) = 0 + g(P) = g(P) = \overline{g}(P).$$

Por tanto, $\mathbb{C}[V]$ se puede ver como **el anillo de funciones polinomiales definidas en la variedad** V.

Observación 3.4. Por el Teorema (3.4), una variedad algebraica no vacía $V \subseteq A^n$ es irreducible, si y solo si, el ideal $J(V)$ es primo, o de forma equivalente, el anillo de coordenadas $\mathbb{C}[V]$ es un dominio entero. En este caso existe el cuerpo de cocientes de $\mathbb{C}[V]$ que se denotará $\mathbb{C}(V)$, y está dado por $\mathbb{C}(V) = \left\{ \frac{\overline{f}}{\overline{g}} : g \notin J(V) \right\}$. Ahora, cada elemento $\frac{\overline{f}}{\overline{g}}$ del cuerpo $\mathbb{C}(V)$ determina una función $\frac{\overline{f}}{\overline{g}} : D \longrightarrow \mathbb{C}$, con dominio $D = \{P \in V : g(P) \neq 0\}$, y definida por

$$\frac{\overline{f}}{\overline{g}}(P) = \frac{f(P)}{g(P)}.$$

La función $\frac{\overline{f}}{\overline{g}}$ está bien definida, porque la igualdad $\frac{\overline{f}}{\overline{g}} = \frac{\overline{h}}{\overline{t}}$ es válida en el cuerpo $\mathbb{C}(V)$, si y solo si, $\overline{f}\ \overline{t} = \overline{g}\ \overline{h}$. De modo que el polinomio $ft - gh \in J(V)$. Esto implica que para todo punto $P \in D \subseteq V$, se cumple $f(P)t(P) = g(P)h(P)$. Por tanto,

$$\frac{\overline{f}}{\overline{g}}(P) = \frac{f(P)}{g(P)} = \frac{h(P)}{t(P)} = \frac{\overline{h}}{\overline{t}}(P).$$

La función $\frac{\overline{f}}{\overline{g}}$ se denomina **función racional** y el cuerpo de cocientes $\mathbb{C}(V)$ es el **cuerpo de funciones racionales de la variedad algebraica irreducible** V.

Definición 3.4 (**Aplicación polinomial**). Sean $V \subseteq A^n$ y $W \subseteq A^m$ dos variedades algebraicas no vacías. Una **aplicación polinomial** de la variedad V en la variedad W es una función $F : V \longrightarrow W$ definida por funciones polinomiales, esto significa que existen polinomios $f_1, \ldots, f_m \in \mathbb{C}[X_1, \ldots, X_n]$, tales que

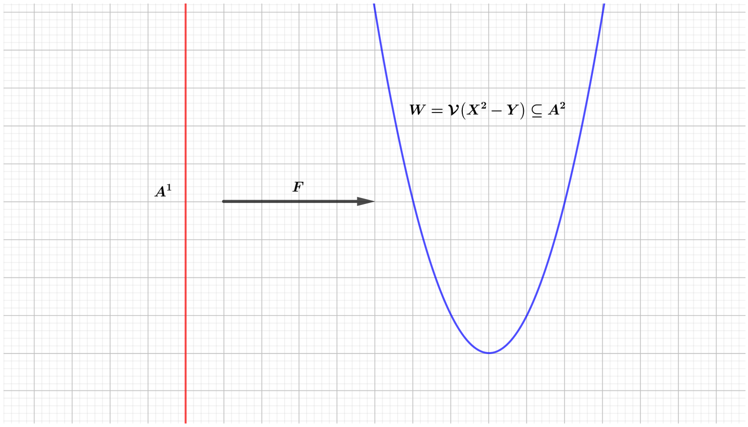
$$F(P) = (f_1(P), \ldots, f_m(P)), \text{ para todo punto } P \in V.$$

La aplicación polinomial F se denota $F = (f_1, \ldots, f_m)$.

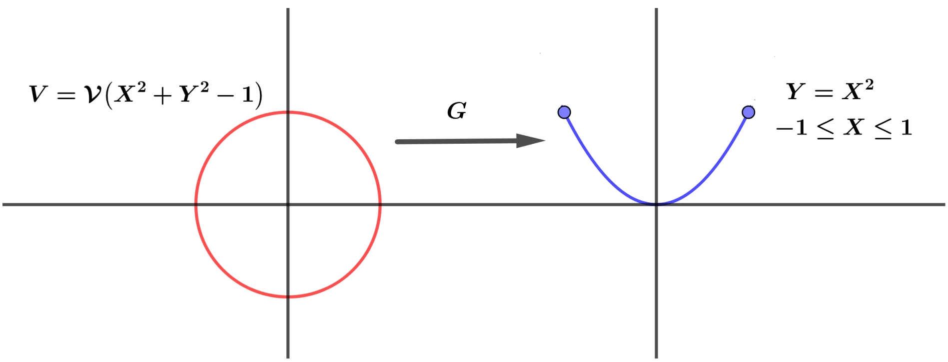
Por ejemplo, si $V \subseteq A^n$la es una variedad algebraica no vacía, entonces la función idéntidad $id_V : V \longrightarrow V$ es una aplicación polinomial, porque $id_V = \left(\overline{X_1}, \ldots, \overline{X_n}\right)$, en la cual $\overline{X_i}$ es la función polinomial en $\mathbb{C}[V]$, dada por $\overline{X_i}\,(a_1, \ldots, a_n) = a_i$, para toda $i = 1, \ldots, n$.

Ejemplo 3.10. Sea $W = \mathcal{V}\left(Y - X^2\right) \subseteq A^2$. La aplicación polinomial $F : A^1 \longrightarrow W$, definida por $F(t) = \left(t, t^2\right)$, para todo $t \in A^1$, transforma la recta afín A^1 en la parábola

$Y = X^2$ del plano cartesiano.



Ejemplo 3.11. Considere la variedad $V = \mathcal{V}\left(X^2 + Y^2 - 1\right)$ del espacio afín A^2. La aplicación polinomial $G : V \longrightarrow A^2$, definida por $G(a, b) = \left(a, 1 - b^2\right)$, para todo punto $(a, b) \in V$, transforma la circunferencia $X^2 + Y^2 = 1$ en la porción de la parábola $Y = X^2$ limitada por $-1 \leq X \leq 1$.



Proposición 3.5. Sean $V \subseteq A^n$ y $W \subseteq A^m$ dos variedades algebraicas no vacías. Si $F = (f_1, \ldots, f_m)$ es una aplicación polinomial de la variedad V en la variedad W y $\overline{g} \in \mathbb{C}[W]$, entonces $\overline{g} \circ F$ es una función polinomial del anillo $\mathbb{C}[V]$.

Demostración. Dado que $\overline{g} \in \mathbb{C}[W]$, entonces g es un polinomio del anillo $\mathbb{C}\left[Y_1, \ldots, Y_m\right]$. Sea $h = g\left(f_1, \ldots, f_m\right)$ el polinomio del anillo $\mathbb{C}\left[X_1, \ldots, X_n\right]$ que se obtiene al sustituir en g la indeterminada Y_j por el polinomio f_j, para toda $j = 1, \ldots, m$. Por la Observación

(3.3) se tiene la función polinomial $\overline{h} : V \longrightarrow \mathbb{C}$. Entonces para cada punto $P \in V$ se cumple

$$\overline{g} \circ F(P) = \overline{g}\,(F(P)) = \overline{g}\,(f_1(P), \ldots, f_m(P)) = \overline{h}(P).$$

Por tanto, $\overline{g} \circ F = \overline{h} \in \mathbb{C}[V]$. □

Definición 3.5 (Variedades isomorfas). Dos variedades algebraicas no vacías $V \subseteq A^n$ y $W \subseteq A^m$ son **isomorfas**, lo que se denota por $V \cong W$, si existen aplicaciones polinomiales $F : V \longrightarrow W$ y $G : W \longrightarrow V$, tales que

$$id_V = G \circ F \quad \text{y} \quad id_W = F \circ G.$$

Además, cada una de las aplicaciones polinomiales F y G se denomina **isomorfismo de variedades algebraicas afines**.

Ejemplo 3.12. Las variedades $V = A^1$ y $W = \mathcal{V}\left(Y - X^2\right) \subseteq A^2$ son isomorfas. En efecto, por el Ejemplo (3.10), se sabe que la aplicación polinomial $F : V \longrightarrow W$, definida por $F(t) = \left(t, t^2\right)$ transforma la recta afín A^1 en la parábola $Y = X^2$. Ahora considere la aplicación polinomial $G : W \longrightarrow V$, definida por

$$G(a, b) = a, \text{ para todo punto } (a, b) \in W.$$

Entonces, para cada $t \in V$, se tiene

$$G \circ F(t) = G(F(t)) = G(t, t^2) = t = id_V(t),$$

además, para cada punto $(a, b) \in W$, se cumple

$$F \circ G(a, b) = F(G(a, b)) = F(a) = (a, a^2) = (a, b) = id_W(a, b).$$

Por tanto,

$$A^1 \cong \mathcal{V}\left(Y - X^2\right).$$

Por definición, los isomorfismos de variedades algebraicas afines son funciones biyectivas. La aplicación polinomial del Ejemplo (3.11) no es inyectiva, por ende, esta aplicación no es un isomorfismo de variedades algebraicas afines.

Ejemplo 3.13. Para cada permutación $\sigma \in S_n$ considere el automorfismo de $\mathbb{C}$-álgebras $\sigma^* : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$, definido por

$$\sigma^*(X_i) = X_{\sigma(i)}, \text{ para toda } i = 1, \ldots, n.$$

Ahora, considere los polinomios $f_1, \ldots, f_r$ del anillo $\mathbb{C}[X_1, \ldots, X_n]$, entonces las variedades

$V = \mathcal{V}(f_1, \ldots, f_r)$ y $W = \mathcal{V}(\sigma^*(f_1), \ldots, \sigma^*(f_r))$ son isomorfas, porque la aplicación polinomial

$$F = \left(X_{\sigma(1)}, \ldots, X_{\sigma(r)}\right) : V \longrightarrow W,$$

es un isomorfismo de variedades algebraicas afines. En particular, la variedad

$$V = \mathcal{V}(X_1 + X_2, X_1X_3 + X_2) \subseteq A^3$$

es isomorfa a la variedad $W = \mathcal{V}(X_1 + X_2, X_2X_3 + X_1)$, porque tomando la permutación $\sigma = (1, 2) \in S_3$, se tiene

$$\sigma^*(X_1 + X_2) = X_2 + X_1 \quad \text{y} \quad \sigma^*(X_1X_3 + X_2) = X_2X_3 + X_1.$$

Teorema 3.6. Si las variedades algebraicas no vacías $V \subseteq A^n$ y $W \subseteq A^m$ son isomorfas, entonces los respectivos anillos de coordenadas son $\mathbb{C}$-álgebras isomorfas.

Demostración. Para iniciar suponga que $F = (f_1, \ldots, f_m) : V \longrightarrow W$ es un isomorfismo de variedades algebraicas. Por la Proposición (3.5), si $\overline{g} \in \mathbb{C}[W]$, entonces $\overline{g} \circ F \in \mathbb{C}[V]$ y se tiene la correspondencia $F^* : \mathbb{C}[W] \longrightarrow \mathbb{C}[V]$, definida por

$$F^*(\overline{g}) = \overline{g} \circ F.$$

En seguida se demuestra que F^* es un isomorfismo de $\mathbb{C}$-álgebras. Para comprobar que F^* esta bien definida, suponga que $\overline{g} = \overline{h}$ en $\mathbb{C}[W]$, entonces $g - h \in J(W)$, pero esto implica que $\overline{g - h}$ es la función polinomial nula en $\mathbb{C}[W]$. Luego, para todo punto $P \in V$, se tiene $F(P) \in W$, y

$$\left(\overline{g} \circ F - \overline{h} \circ F\right)(P) = \left(\overline{g} - \overline{h}\right)(F(P)) = \overline{g - h}(F(P)) = 0.$$

En consecuencia, $\overline{g} \circ F - \overline{h} \circ F$ es la función nula en $\mathbb{C}[V]$, por tanto

$$F^*(\overline{g}) = \overline{g} \circ F = \overline{h} \circ F = F^*\left(\overline{h}\right).$$

Es decir, F^* está bien definida. Ahora, sean $\overline{g}$ y $\overline{h}$ dos clases laterales del anillo $\mathbb{C}[W]$ y sean $a, b \in \mathbb{C}$, entonces

$$F^*\left(a\overline{g} + b\overline{h}\right) = \left(a\overline{g} + b\overline{h}\right) \circ F = a(\overline{g} \circ F) + b\left(\overline{h} \circ F\right) = aF^*(g) + bF^*(h).$$

Además,

$$F^*\left(\overline{g}\,\overline{h}\right) = F^*\left(\overline{gh}\right) = \overline{gh} \circ F,$$

pero dado un punto arbitrario $P \in V$, se cumple

$$\left(\overline{gh} \circ F\right)(P) = \overline{gh}(F(P)) = \overline{g}(F(P))\,\overline{h}(F(P)) = (\overline{g} \circ F)\left(\overline{h} \circ F\right)(P),$$

por ende, $\overline{gh} \circ F = (\overline{g} \circ F)\left(\overline{h} \circ F\right)$, y se tiene

$$F^*\left(\overline{g}\;\overline{h}\right) = \overline{gh} \circ F = (\overline{g} \circ F)\left(\overline{h} \circ F\right) = F^*(g)F^*(h).$$

Por tanto, F^* es un homomorfismo de $\mathbb{C}$-álgebras. Para probar que F^* es inyectivo, sea $\overline{g} \in Ker\,(F^*)$, entonces

$$\overline{g} \circ F = F^*\left(\overline{g}\right) = \overline{0},$$

luego $\overline{g} \circ F$ es la función nula en $\mathbb{C}[V]$, y esto implica

$$\overline{g}(W) = \overline{g}\,(F(V)) = \overline{g} \circ F(V) = \{0\}.$$

Así que $\overline{g}$ es la función nula en $\mathbb{C}[W]$; en consecuencia, $Ker\,(F^*) = \{\overline{0}\}$. Para mostrar que F^* es sobreyectivo, sea $\overline{t} \in \mathbb{C}[V]$ y sea $G = (g_1, \ldots, g_n) : W \longrightarrow V$ la aplicación polinomial que satisface

$$id_V = G \circ F \quad \text{y} \quad id_W = F \circ G.$$

Entonces, $\overline{t} \circ G$ es una función polinomial del anillo $\mathbb{C}[W]$, y se sigue

$$F^*\left(\overline{t} \circ G\right) = \left(\overline{t} \circ G\right) \circ F = \overline{t} \circ (G \circ F) = \overline{t} \circ id_V = \overline{t}.$$

Por tanto, F^* es un isomorfismo de $\mathbb{C}$-álgebras y la prueba está completa. $\square$

Corolario 3.2. Sean $V \subseteq A^n$ y $W \subseteq A^m$ dos variedades algebraicas isomorfas no vacías. Entonces, la variedad V es irreducible, si y solo si, la variedad W es irreducible y, en este caso, los cuerpos de funciones racionales $\mathbb{C}(V)$ y $\mathbb{C}(W)$ son $\mathbb{C}$-álgebras isomorfas.

Demostración. Por el Teorema (3.6), los anillos $\mathbb{C}[V]$ y $\mathbb{C}[W]$ son $\mathbb{C}$-álgebras asociativas isomorfas. Entonces, $\mathbb{C}[V]$ es un dominio entero, si y solo si, $\mathbb{C}[W]$ es un dominio entero, en consecuencia, V es irreducible, si y solo si, W es irreducible. Finalmente, todo isomorfismo de $\mathbb{C}$-álgebras $\psi : \mathbb{C}[V] \longrightarrow \mathbb{C}[W]$ extiende al isomorfismo $\psi^* : \mathbb{C}(V) \longrightarrow \mathbb{C}(W)$, definido por $\psi^*\left(\dfrac{\overline{f}}{\overline{g}}\right) = \dfrac{\psi\left(\overline{f}\right)}{\psi\left(\overline{g}\right)}$. $\square$

Ejemplo 3.14. La variedad algebraica $\mathcal{V}\left(Y - X^2\right) \subseteq A^2$ es irreducible. En efecto, del Ejemplo (3.6) se garantiza que la recta afín A^1 es una variedad irreducible y del Ejemplo (3.12) se sabe que y $A^1 \cong \mathcal{V}\left(Y - X^2\right)$.

El ejemplo anterior es un caso particular de una situación general que se enuncia en la siguiente proposición:

> **Proposición 3.6.** Si f es un polinomio del anillo $\mathbb{C}\left[X_1, \ldots, X_n\right]$, entonces que la variedad $W = \mathcal{V}\left(Y - f\right) \subseteq A^{n+1}$ es irreducible.

Demostración. Considere la aplicación polinomial $F = (X_1, \ldots, X_n, f) : A^n \longrightarrow A^{n+1}$. Note que los puntos de la variedad W son de la forma

$$(P, b), \text{ donde } P \in A^n, b \in \mathbb{C} \text{ y } b = f(P).$$

Luego, para cada punto $P \in A^n$, se tiene $F(P) = (P, f(P)) \in W$, entonces $F\left(A^n\right) \subseteq W$. Ahora, sea $G = (X_1, \ldots, X_n) : W \longrightarrow A^n$. Entonces, para todo punto $P \in A^n$, se cumple $G \circ F(P) = G\left(P, f(P)\right) = P$, además, $F \circ G\left(P, f(P)\right) = F\left(P\right) = \left(P, f(P)\right)$. Así que,

$$G \circ F = id_{A^n} \quad \text{y} \quad F \circ G = id_W.$$

Por tanto, $A^n \cong W$, y dado que A^n es una variedad irreducible, se sigue que W es irreducible. $\square$

3.4 Dimensión de variedades afines

La dimensión es una característica importante de una variedad algebraica afín, porque cuantifica el número de parámetros independientes necesarios para describir un punto en la variedad. El concepto de dimensión influye en la estructura topológica de la variedad algebraica y su cálculo se basa en herramientas sofisticadas, como la teoría de ideales y la dimensión de Krull. Este concepto se puede abordar de varias maneras, pero el interés en esta sección es presentar la definición de dimensión aprovechando la conexión existente entre una variedad algebraica afín V y el anillo de coordenadas $\mathbb{C}\left[V\right]$, tomando distancia del lenguaje técnico de la estructura de espacio topológico del espacio afín A^n.

Para comenzar, recuerde que una variedad algebraica $V \subseteq A^n$ es irreducible, si y solo si, su anillo de coordenadas $\mathbb{C}[V]$ es un dominio entero y existe el cuerpo de funciones racionales $\mathbb{C}(V)$, que es una extensión del cuerpo de los números complejos. En este caso, tiene sentido hablar del grado de trascendencia de la extensión $\mathbb{C}(V)\,|\mathbb{C}$, concepto que se puede consultar en la sección (A.3) de los anexos.

Definición 3.6 (**Dimensión de una variedad algebraica irreducible**). Sea V una variedad algebraica irreducible del espacio afín A^n. La dimensión de V, denotada por $dimV$, es el grado de trascendencia del cuerpo $\mathbb{C}(V)$ sobre $\mathbb{C}$, es decir

$$dimV = grtr_{\mathbb{C}}\mathbb{C}(V).$$

Ejemplo 3.15. De acuerdo con la definición anterior, se tiene

1. $dimA^n = grtr_{\mathbb{C}}\mathbb{C}\,(X_1, \ldots, X_n) = n$.

2. Si $P \in A^n$, entonces $J\,(P)$ es un ideal maximal del anillo $\mathbb{C}\,[X_1, \ldots, X_n]$ y

$$\mathbb{C} = \frac{\mathbb{C}\,[X_1, \ldots, X_n]}{J(P)},$$

   entonces, $dim\mathcal{V}(P) = grtr_{\mathbb{C}}\mathbb{C} = 0$.

3. La variedad algebraica $V = \mathcal{V}\,(X_1, \ldots, X_m) \subseteq A^{m+r}$ es irreducible, porque

$$\mathbb{C}[V] = \frac{\mathbb{C}\,[X_1, \ldots, X_m, Y_1, \ldots, Y_r]}{J(V)} = \mathbb{C}\,[Y_1, \ldots, Y_r]\,,$$

   entonces, $dimV = grtr_{\mathbb{C}}\mathbb{C}\,[Y_1, \ldots, Y_r] = r$.

4. Si $V \subseteq A^n$ y $W \subseteq A^m$ son variedades algebraicas irreducibles isomorfas, entonces

$$dimV = grtr_{\mathbb{C}}\mathbb{C}(V) = grtr_{\mathbb{C}}\mathbb{C}(W) = dimW.$$

   En particular, dado un polinomio $f \in \mathbb{C}\,[X_1, \ldots, X_n]$, por la Proposición (3.6), se obtiene $A^n \cong \mathcal{V}\,(Y - f) \subseteq A^{n+1}$, luego $dim\mathcal{V}\,(Y - f) = dimA^n = n$.

Proposición 3.7. Sean V y W dos variedades afines irreducibles no vacías. Si $V \subseteq W$, entonces $dimV \leq dimW$.

Demostración. Del hecho que $V \subseteq W$, se tiene la inclusión $i : \mathbb{C}[V] \hookrightarrow \mathbb{C}[W]$, definida por $i\left(\overline{f}\right) = \overline{f}$, para toda $\overline{f} \in \mathbb{C}[V]$. La inclusión i está bien definida, porque $J(W) \subseteq J(V)$, y se tiene la extensión de cuerpos $\mathbb{C}(W)\,|\mathbb{C}(V)$. Ahora, sea B una base de trascendencia para $\mathbb{C}(V)$ sobre $\mathbb{C}$, por la Proposición (A.2) de los anexos, existe una base de trascendencia $\overline{B}$ para $\mathbb{C}(W)$ sobre $\mathbb{C}$, tal que $B \subseteq \overline{B}$, por tanto

$$dimV = grtr_{\mathbb{C}}\mathbb{C}[V] = |B| \leq \left|\overline{B}\right| = grtr_{\mathbb{C}}\mathbb{C}[W] = dimW.$$

En particular, si V es una variedad del espacio afín A^n, entonces

$$dimV \leq dimA^n = n.$$

$\square$

Aquí es oportuno ampliar la definición de dimensión para cualquier variedad algebraica afín no vacía. Para esto recuerde que el Corolario (3.1) garantiza que V se puede descomponer de manera única como unión de sus componentes irreducibles.

Definición 3.7 (**Dimensión de una variedad algebraica afín**). Si $V_1, \ldots, V_r$ son las componentes irreducibles de una variedad algebraica afín no vacía V, entonces la dimensión de V, denotada por $dimV$, se define como sigue

$$dimV = \text{máx}\left\{dimV_i : i = 1, \ldots, r\right\}.$$

Además, se dice que la variedad V es equidimensional de dimensión pura s, lo que se denota por $Eqd(s)$, si todas las componentes irreducibles de V tienen dimensión s. Es decir, V es $Eqd(s)$, si y solo si,

$$s = dimV_1 = \cdots = dimV_r.$$

Ejemplo 3.16. Sea f un polinomio del anillo $\mathbb{C}\left[X_1, \ldots, X_n\right]$ y considere la variedad $V = \mathcal{V}\left(X_1(Y - f)\right) \subseteq A^{n+1}$. Se quiere comprobar que $dimV = n$, para esto note que

$$\mathbb{C}\left[V_1\right] \cong \mathbb{C}\left[X_2, \ldots, X_n\right],$$

esto implica que la variedad $V_1 = \mathcal{V}\left(X_1\right)$ es irreducible. Además, por la Proposición (3.6), se conoce que la variedad $V_2 = \mathcal{V}\left(Y - f\right) \cong A^n$, por ende, V_2 también es irreducible. Entonces la descomposición en componentes irreducibles de la variedad V está dada por

$$V = \mathcal{V}\left(X_1(Y - f)\right) = \mathcal{V}\left(X_1\right) \cup \mathcal{V}\left(Y - f\right) = V_1 \cup V_2.$$

Por tanto, $dimV = \text{máx}\left\{dimV_1, dimV_2\right\} = \text{máx}\left\{n - 1, n\right\} = n$.

Ejemplo 3.17. Sean f y g dos polinomios del anillo $\mathbb{C}\left[X_1, \ldots, X_n\right]$ y considere la variedad $V = \mathcal{V}\left(Y^2 + (f + g)Y + fg\right) \subseteq A^{n+1}$. Se quiere comprobar que V es una variedad equidimensional de dimensión pura n. En efecto, primero note que

$$Y^2 + (f + g)Y + fg = \left(Y + f\right)\left(Y + g\right).$$

Entonces la descomposición en componentes irreducibles de la variedad V es como sigue

$$V = \mathcal{V}(Y+f) \cup \mathcal{V}(Y+g),$$

pero $dim\mathcal{V}(Y+f) = dim\mathcal{V}(Y+g) = n$. Por tanto, V es una variedad $Eqd(n)$.

CAPÍTULO 4

Secuencias regulares sobre anillos

4.1 Secuencias regulares

Las secuencias regulares es un concepto fundamental de la teoría de anillos conmutativos con importantes aplicaciones en geometría algebraica. Estas secuencias están relacionadas con la noción de profundidad de un módulo sobre un anillo, lo que es crucial para entender la estructura de los módulos. En geometría algebraica, las secuencias regulares se usan para estudiar la dimensión de variedades y las singularidades. En esta sección se presenta la definición de *secuencia regular* junto con algunos resultados que involucran este concepto, y que se utilizarán en el último capítulo de este texto. Los anillos trabajados en esta sección son conmutativos y unitarios. Para una mayor profundidad en este tema se recomienda consultar el libro de Matsumura (1987).

Definición 4.1 (Elemento regular). Un elemento no cero a de un anillo A se denomina A-**regular** si a no es divisor de cero en A.

Ejemplo 4.1. Según esta definición, se tiene

1. Todo elemento no cero de un dominio entero D es D-regular.

2. Si n es un entero positivo, entonces los elementos $\mathbb{Z}_n$-regulares son las unidades módulo n, es decir, las clases $\overline{r}$ tales que $mcd(n, r) = 1$.

3. En el anillo cociente $A = \dfrac{\mathbb{C}[X, Y]}{\langle XY \rangle}$, la clase $\overline{X+1}$ es A-regular, porque toda clase $\overline{f}$ en A es de la forma
$$\overline{f} = \overline{\alpha + g + h},$$
en la cual α es una constante, $g \in \mathbb{C}[X]$ y $h \in \mathbb{C}[Y]$ son polinomios con término constante cero. Suponiendo que
$$\overline{(X+1)f} = \overline{0},$$
entonces
$$\alpha + \alpha X + g(X+1) + Xh + h \in \langle XY \rangle,$$
De aquí, $\alpha = 0$, $h = 0$ y se obtiene $(X+1)g = 0$. Pero $\mathbb{C}[X, Y]$ no tiene divisores de cero, se sigue $g = 0$. Por tanto, $\overline{f} = \overline{0}$.

Definición 4.2 (Secuencia A-regular). Sea $a_1, \ldots, a_r$ una sucesión de elementos de un anillo A y para $i = 1, \ldots, r$ considere el anillo cociente
$$A_i = \frac{A}{\langle a_1, \ldots, a_i \rangle}.$$
La sucesión $a_1, \ldots, a_r$ es una **secuencia A-regular de longitud** r si cumple

1. El elemento a_1 es A-regular.
2. Para todo $i = 2, \ldots, r$, la clase $\overline{a_i}$ es A_{i-1}-regular.
3. El anillo A_r es no trivial.

Observe que toda unidad es un elemento A-regular, pero una secuencia A-regular no puede terner unidades, porque si alguno de los elementos $a_1, \ldots, a_r$ es una unidad del anillo A, entonces el ideal $\mathcal{I} = \langle a_1, \ldots, a_r \rangle = A$ y el anillo cociente $\dfrac{A}{\mathcal{I}}$ es trivial, por tanto, la secuencia $a_1, \ldots, a_r$ no es A-regular.

Ejemplo 4.2. La definición de secuencia A-regular depende del orden de los elementos; puede suceder que una secuencia sea A-regular y después de una permutación de los elementos la nueva secuencia no sea A-regular. Por ejemplo, considerando los polinomios $f_1 = X$, $f_2 = Y(X-1)$ y $f_3 = Z(X-1)$ del anillo $A = \mathbb{C}[X, Y, Z]$. Con la notación de la definición, se sigue que la secuencia f_1, f_2, f_3 es A-regular, porque el polinomio f_1 es un elemento A-regular. Además, en el anillo A_1 se cumple

$$\overline{Y(X-1)} = \overline{YX} - \overline{Y} = \overline{Y}.$$

Pero A_1 no tiene divisores de cero, ya que $A_1 \cong \mathbb{C}[Y, Z]$ es un dominio entero, entonces $\overline{Y} = \overline{Y(X-1)}$ es un elemento A_1-regular. Para continuar, en el anillo A_2, se tiene la igualdad

$$\overline{Z(X-1)} = \overline{ZX} - \overline{Z} = \overline{Z},$$

Para comprobar que $\overline{Z(X-1)}$ no es divisor de cero en A_2 suponga que h es un polinomio de A, tal que

$$\overline{Z(X-1)h} = \overline{0}, \text{ en el anillo } A_2,$$

entonces

$$Zh \in \langle X, Y(X-1) \rangle = \{Xf + Y(X-1)g : f, g \in A\}.$$

Luego

$$Zh = Xf + Y(X-1)g, \text{ para algunos polinomios } f, g \in A. \tag{4.1}$$

Si $f, g \notin \langle Z \rangle$, no se pierde generalidad en aceptar que $f, g \in \mathbb{C}[X, Y]$, y esto implica que

$$Xf + Y(X-1)g \in \mathbb{C}[X, Y] \cap \langle Z \rangle = \{0\},$$

entonces, $Zh = 0$ y se obtiene $h = 0 \in \langle f_1, f_2 \rangle$. Ahora, si el polinomio f o el polinomio g está en el ideal $\langle Z \rangle$, de la ecuación (4.1), se obtiene que el otro también pertenece a $\langle Z \rangle$, luego

$$Zh = XZq + Y(X-1)Zr, \text{ para algunos polinomios } q, r \in A.$$

Así que

$$h = Xq + Y(X-1)r \in \langle X, Y(X-1) \rangle.$$

Por tanto, la clase $\overline{Z(X-1)}$ es A_2-regular. Finalmente, el anillo A_3 es claramente no trivial. Entonces, la secuencia f_1, f_2, f_3 es A-regular. Ahora, note que la secuencia

$$Y(X-1), Z(X-1), X$$

no es A-regular, porque la clase $\overline{Z(X-1)}$ es un divisor de cero en el anillo $\dfrac{A}{\langle Y(X-1) \rangle}$.

Proposición 4.1. Si a es un elemento A-regular, entonces para todo entero positivo k se tiene que a^k es A-regular.

Demostración. Sea $b \in A$, tal que $a^k b = 0$, entonces $a\left(a^{k-1}b\right) = 0$. Como a no es divisor de cero, se sigue $a^{k-1}b = 0$. Repitiendo este proceso, en una cantidad finita de iteraciones, se obtiene $ab = 0$, lo que implica $b = 0$. Por tanto, a^k es A-regular. $\square$

Proposición 4.2. Suponga que $a_1, \ldots, a_r$ es una secuencia A-regular. Si $b_1, \ldots, b_r$ son elementos del anillo A, tales que

$$a_1 b_1 + \cdots + a_r b_r = 0,$$

entonces todos los b_i están en el ideal $\langle a_1, \ldots, a_r \rangle$.

Demostración. Por inducción, si a_1 es A-regular y $a_1 b_1 = 0$, entonces $b_1 = 0 \in \langle a_1 \rangle$. Ahora suponga que el enunciado se cumple para toda secuencia A-regular con k elementos y sea $a_1, \ldots, a_k, c$ una secuencia A-regular. Si $b_1, \ldots, b_k, d$ son elementos de A, tales que

$$a_1 b_1 + \cdots + a_k b_k + cd = 0,$$

entonces $\overline{cd} = \overline{0}$ en el anillo $\dfrac{A}{\mathcal{I}}$, en el cual $\mathcal{I} = \langle a_1, \ldots, a_k \rangle$. Pero $\overline{c}$ es $\dfrac{A}{\mathcal{I}}$-regular, entonces $\overline{d} = \overline{0}$ en $\dfrac{A}{\mathcal{I}}$. De aquí se sigue que $d \in \mathcal{I}$ y deben existir elementos $s_1, \ldots, s_k \in A$, tales que

$$d = a_1 s_1 + \ldots + a_k s_k,$$

entonces

$$a_1 \left(b_1 + cs_1\right) + \cdots + a_k \left(b_k + cs_k\right) = 0.$$

Pero la secuencia $a_1, \ldots, a_k$ es A-regular, por la hipótesis de inducción se obtiene

$$b_i + cs_i \in \mathcal{I}, \text{ para toda } i = 1, \ldots, k.$$

Por tanto, para toda $i = 1, \ldots, k$

$$b_i \in \mathcal{I} + \langle c \rangle = \langle a_1, \ldots, a_k, c \rangle$$

y esto completa la prueba, porque $d \in \mathcal{I} \subseteq \langle a_1, \ldots, a_k, c \rangle$. $\square$

Teorema 4.1. Si $a_1, a_2, \ldots, a_r$ es una secuencia A-regular, entonces para todo entero $k > 1$ la secuencia $a_1^k, a_2, \ldots, a_r$ es A-regular.

Demostración. Suponga que el enunciado es falso. Luego, existe un entero positivo k, tal que la secuencia $a_1^k, a_2, \ldots, a_r$ no es A-regular y no se pierde generalidad en suponer que

$$k = \text{mín}\left\{s \in \mathbb{Z}^+ : \text{La secuencia } a_1^s, a_2, \ldots, a_r \text{ no es } A\text{-regular}\right\}.$$

Por hipótesis $k \geq 2$ y por la minimalidad del entero k, la secuencia $a_1^{k-1}, a_2, \ldots, a_r$ es A-regular. La Proposición (4.1) garantiza que el elemento a_1^k es A-regular, entonces existe $j \in \{1, 2, \ldots, r-1\}$, tal que la secuencia $a_1^k, a_2, \ldots, a_j$ es A-regular, pero la secuencia $a_1^k, a_2, \ldots, a_j, a_{j+1}$ no lo es. Considere los ideales

$$\mathcal{I} = \left\langle a_1^k, a_2, \ldots, a_j \right\rangle \quad \text{y} \quad J = \left\langle a_1^{k-1}, a_2, \ldots, a_j \right\rangle,$$

entonces $\overline{a_{j+1}}$ debe ser un divisor de cero del anillo $\dfrac{A}{\mathcal{I}}$, esto significa que existe $b \in A - \mathcal{I}$, tal que $a_{j+1}b \in \mathcal{I}$. Luego existen elementos $x \in A$ e $y \in N = \langle a_2, \ldots, a_j \rangle$, de manera que

$$a_{j+1}b = a_1^k x + y = a_1^{k-1}(a_1 x) + y.$$

Pero la secuencia $a_1^{k-1}, a_2, \ldots, a_{j+1}$ es A-regular, entonces $b \in J = \left\langle a_1^{k-1} \right\rangle + N$ y deben existir elementos $w \in A$ y $z \in N$, tales que $b = a_1^{k-1}w + z$, luego

$$a_{j+1}\left(a_1^{k-1}w + z\right) = a_1^{k-1}(a_1 x) + y,$$

de aquí se sigue

$$a_1^{k-1}(a_{j+1}w - a_1 x) + a_{j+1}z - y = 0.$$

Pero $a_{j+1}z - y \in N$, entonces de la Proposición (4.2) se obtiene

$$a_{j+1}w - a_1 x \in J \subseteq \langle a_1, a_2, \ldots, a_j \rangle,$$

en consecuencia, $a_{j+1}w \in \langle a_1, a_2, \ldots, a_j \rangle$, esto junto con la hipótesis implican que w es un elemento del ideal $\langle a_1, a_2, \ldots, a_j \rangle$. Luego existen elementos $p \in A$ y $q \in N$, tales que $w = a_1 p + q$. Por ende,

$$b = a_1^{k-1}w + z = a_1^k p + a_1^{k-1}q + z \in \mathcal{I},$$

pero esto contradice el hecho de que $b \in A - \mathcal{I}$, y la prueba está completa. □

Corolario 4.1. Si $a_1, a_2, \ldots, a_r$ es una secuencia A-regular, entonces para todos los enteros positivos $n_1, n_2, \ldots, n_r$, la secuencia $a_1^{n_1}, a_2^{n_2} \ldots, a_r^{n_r}$ es A-regular.

Demostración. Por el Teorema (4.1), se tiene que la secuencia $a_1^{n_1}, a_2, \ldots, a_r$ es A-regular.

Sea $\mathcal{I} = \left\langle a_1^{n_1} \right\rangle$, entonces $\overline{a_2}, \ldots, \overline{a_r}$ es una secuencia $\dfrac{A}{\mathcal{I}}$-regular y aplicando nuevamente el teorema anterior se obtiene que $\overline{a_2^{n_2}}, \overline{a_3}, \ldots, \overline{a_r}$ es una secuencia $\dfrac{A}{\mathcal{I}}$-regular y esto implica que la secuencia $a_1^{n_1}, a_2^{n_2}, a_3, \ldots, a_r$ es A-regular. Continuando con este proceso, en una cantidad finita de iteraciones, se obtiene el resultado. □

Ejemplo 4.3. Sea a, b una secuencia A-regular. Si f es un polinomio homogéneo de grado positivo en el anillo $A[X, Y]$, tal que $f(a, b) = 0$, probar que todos los coeficientes de f pertenecen al ideal $\mathcal{I} = \langle a, b \rangle$.

Solución: Por inducción sobre el grado del polinomio f. Si $gra(f) = 1$, entonces existen elementos $\alpha, \beta \in A$, tales que $f = \alpha X + \beta Y$, y se tiene $\alpha a + \beta b = 0$, y la Proposición (4.2) implica que $\alpha, \beta \in \mathcal{I}$. Ahora suponga que el enunciado es válido para polinomios homogéneos de grado $n \geq 1$ y escoja un polinomio homogéneo $f \in A[X, Y]$, tal que $gra(f) = n + 1$ y $f(a, b) = 0$. Entonces es posible encontrar un elemento $\alpha \in A$ y un polinomio homogéneo $h \in A[X, Y]$ de grado n, tales que $f = \alpha X^{n+1} + Yh$, luego

$$\alpha a^{n+1} + bh(a, b) = f(a, b) = 0.$$

Por el Teorema (4.1), la secuencia a^{n+1}, b es A-regular, entonces, por un lado se tiene $\alpha \in \mathcal{I}$ y por otro

$$bh(a, b) \in \left\langle a^{n+1} \right\rangle,$$

esto implica que

$$h(a, b) \in \left\langle a^{n+1} \right\rangle \subseteq \langle a^n \rangle,$$

y existe $\delta \in A$, tal que $h(a, b) = \delta a^n$, luego $g = h - \delta X^n$ es un polinomio homogéneo de grado n en el anillo $A[X, Y]$, para el cual se cumple

$$g(a, b) = h(a, b) - \delta a^n = 0.$$

Por la hipótesis de inducción, todos los coeficientes del polinomio g están en $\mathcal{I}$, por tanto, los coeficientes de h pertenecen al ideal $\mathcal{I}$ y la prueba está completa.

Teorema 4.2. Sean m un entero positivo. Si $a_1, \ldots, a_t$ es una secuencia A-regular de longitud $t \geq 1$ y f es un polinomio homogéneo de grado m en el anillo $A\left[X_1, \ldots, X_t\right]$, tal que $f\left(a_1, \ldots, a_t\right) = 0$, entonces todos los coeficientes del polinomio f pertenecen al ideal $\mathcal{I} = \langle a_1, \ldots, a_t \rangle$.

Demostración. Por inducción sobre la longitud t de la secuencia. Para $t = 1$, sean a_1 un elemento A-regular y $f \in A\left[X_1\right]$ un polinomio homogéneo de grado m, tal que $f\left(a_1\right) = 0$, entonces $f = \alpha X_1^m$, para algún $\alpha \in A$, y se tiene $\alpha a_1^m = f\left(a_1\right) = 0$. Pero a_1 no es divisor de cero en el anillo A, entonces $\alpha = 0 \in \langle a_1 \rangle$. Ahora, suponga que el enunciado es válido para todas las secuencias A-regulares de longitud $s \leq t$, y sean $b, a_1, \ldots, a_t$ una secuencia A-regular y $f \in A[Y, X_1, \ldots, X_t]$ un polinomio homogéneo de grado m, tal que $f(b, a_1, \ldots, a_t) = 0$. Observe que existen polinomios homogéneos $g_0, g_1, \ldots, g_m$ en el anillo $A[X_1, \ldots, X_t]$, con $gra(g_j) = m - j$, tales que

$$f = g_0 + Yg_1 + \cdots + Y^m g_m.$$

Sea $B_1 = \dfrac{A}{\langle b \rangle}$ y considere el polinomio $f \in B_1[X_1, \ldots, X_t]$. Note que $\overline{a_1}, \ldots, \overline{a_t}$ es una secuencia B_1-regular de longitud t, además,

$$g_0(\overline{a_1}, \ldots, \overline{a_t}) = \overline{g_0(a_1, \ldots, a_t)} = \overline{f(b, a_1, \ldots, a_t)} = \overline{0}.$$

Por la hipótesis de inducción, todos los coeficientes del polinomio g_0 pertenecen al ideal $\overline{\mathcal{I}} = \langle \overline{a_1}, \ldots, \overline{a_t} \rangle$. Pero no es difícil comprobar que

$$\overline{w} \in \overline{\mathcal{I}}, \text{ si y solo si, } w \in \langle b, a_1, \ldots, a_t \rangle.$$

En consecuencia, todos los coeficientes del polinomio g_0 están en el ideal $\mathcal{I} = \langle b, a_1, \ldots, a_t \rangle$. Para continuar, suponga que todos los coeficientes de los polinomios $g_0, \ldots, g_{i-1}$ están en el ideal $\mathcal{I}$. De acuerdo con lo expuesto en el Ejemplo (2.3), existen polinomios homogéneos $h_0, h_1, \ldots, h_{i-1}$ en el anillo $A[X_1, \ldots, X_t]$, tales que para toda $j = 0, 1, \ldots, i-1$ se cumple $gra(h_j) = gra(g_j) - (i - j)$, además

$$g_j(a_1, \ldots, a_t) = h_j(a_1, \ldots, a_t).$$

Entonces el polinomio

$$h = h_0 + bh_1 + \cdots + b^{i-1}h_{i-1} + b^i g_i \in A[X_1, \ldots, X_t],$$

es homogéneo de grado $m - i$ y en el anillo $B_{i+1} = \dfrac{A}{\langle b^{i+1} \rangle}$, satisface

$$h(\overline{a_1}, \ldots, \overline{a_t}) = b^i g_i(\overline{a_1}, \ldots, \overline{a_t}) + \sum_{j=0}^{i-1} b^j h_j(\overline{a_1}, \ldots, \overline{a_t}) = \overline{f(b, a_1, \ldots, a_t)} = \overline{0}.$$

Por el Teorema (4.1), la secuencia $b^{i+1}, a_1, \ldots, a_t$ es A-regular, y de aquí se deduce que la secuencia $\overline{a_1}, \ldots, \overline{a_t}$ es B_{i+1}-regular. De la hipótesis de inducción, se obtiene que todos los coeficientes del polinomio h, vistos en el anillo B_{i+1}, están en el ideal $\overline{\mathcal{I}} = \langle \overline{a_1}, \ldots, \overline{a_t} \rangle$. En particular, si α es un coeficiente del polinomio g_i, entonces

$$\overline{b^i \alpha} \in \langle \overline{a_1}, \ldots, \overline{a_t} \rangle.$$

Luego, existen elementos $\delta, \beta_1, \ldots, \beta_t \in A$, tales que

$$b^i\alpha = \delta b^{i+1} + \beta_1 a_1 + \cdots + \beta_t a_t,$$

así que

$$b^i(\delta b - \alpha) + \beta_1 a_1 + \cdots + \beta_t a_t = 0,$$

pero la secuencia $b^i, a_1, \ldots, a_t$ es A-regular, entonces

$$\delta b - \alpha \in \left\langle b^i, a_1, \ldots, a_t \right\rangle \subseteq \langle b, a_1, \ldots, a_t \rangle = \mathcal{I}.$$

En consecuencia, $\alpha \in \mathcal{I}$, es decir, los coeficientes del polinomio g_i están en el ideal $\mathcal{I}$. Por tanto, todos los coeficientes de los polinomios $g_0, g_1, \ldots, g_m$ están en el ideal $\mathcal{I}$ y la prueba está completa. $\square$

Definición 4.3 (Secuencia casi regular). Sea $J = \langle a_1, \ldots, a_r \rangle$ un ideal propio de un anillo A. La secuencia $a_1, \ldots, a_r$ se llama A-**casi regular** si dado cualquier polinomio homogéneo $f \in A[X_1, \ldots, X_r]$ de grado m, tal que $f(a_1, \ldots, a_r) \in J^{m+1}$, entonces todos los coeficientes de f pertenecen al ideal J.

La definición de secuencia regular depende del orden de los elementos en la secuencia, como se mostró en el Ejemplo (4.2), pero la noción de casi regular es independiente de este orden, esto significa que cualquier permutación de una secuencia casi regular, también es casi regular.

Observación 4.1. En la definición de secuencia A-casi regular, la condición $f(a_1, \ldots, a_r) \in J^{m+1}$, implica que existe un polinomio homogéneo g en el anillo $A[X_1, \ldots, X_r]$, de grado $m+1$, tal que

$$f(a_1, \ldots, a_r) = g(a_1, \ldots, a_r).$$

Pero el polinomio g se puede expresar como $g = \sum_{i=1}^{r} X_i g_i$, en la cual, los g_i son polinomios homogéneos de grado m, entonces el polinomio $h = f - \sum_{i=1}^{r} a_i g_i$ es homogéneo de grado m, y satisface $h(a_1, \ldots, a_r) = 0$. Luego, en la definición de secuencia casi regular, la condición $f(a_1, \ldots, a_r) \in J^{m+1}$, se puede sustituir por $f(a_1, \ldots, a_r) = 0$.

Proposición 4.3. Toda secuencia regular es casi regular.

Demostración. En efecto, sea $a_1, \ldots, a_r$ una secuencia A-regular y escoja un polinomio homogéneo $f \in A[X_1, \ldots, X_r]$, de grado m, tal que $f(a_1, \ldots, a_r) \in J^{m+1}$. Dado que $J^{m+1} \subseteq J^m$, entonces existe un polinomio homogéneo $g \in A[X_1, \ldots, X_r]$ de grado m, tal que $f(a_1, \ldots, a_r) = g(a_1, \ldots, a_r)$. Así, el polinomio $h = f - g$ es homogéneo de grado m, y satisface

$$h(a_1, \ldots, a_r) = f(a_1, \ldots, a_r) - g(a_1, \ldots, a_r) = 0.$$

De acuerdo con el Teorema (4.2), todos los coeficientes del polinomio h pertenecen al ideal $J = \langle a_1, \ldots, a_r \rangle$, y esto implica que todos los coeficientes de f también pertenecen al ideal $J = \langle a_1, \ldots, a_r \rangle$. □

El ejemplo siguiente, aparece en la publicación de Kim (2024), y presenta una secuencia A-casi regular que no es A-regular

Ejemplo 4.4. Sea k un cuerpo y denote con $B = k[X, Y_1, Y_2, \ldots, Y_r, \ldots]$ al anillo de polinomios en infinitas indeterminadas conmutativas, con coeficientes en el cuerpo k. Ahora, sea $f_1 = XY_1$, y para cada entero $n \geq 2$ sea $f_n = XY_n - Y_{n-1}$. Considere el ideal $\mathcal{I} = \left\langle f_n : n \in \mathbb{Z}^+ \right\rangle$ y el anillo cociente $A = \dfrac{B}{\mathcal{I}}$, y observe que los polinomios no cero en $\mathcal{I}$ tienen grado mayor que 1, entonces $X + \mathcal{I}$ y $Y_1 + \mathcal{I}$ son dos clases no cero en A. Sin embargo,

$$(X + \mathcal{I})(Y_1 + \mathcal{I}) = XY_1 + \mathcal{I} = \mathcal{I},$$

esto significa que $X + \mathcal{I}$ es un divisor de cero en A, y por ende, $X + \mathcal{I}$ no es un elemento A-regular. Por otro lado, en el anillo A se cumple

$$Y_{n-1} + \mathcal{I} = XY_n + \mathcal{I} \in \langle X + \mathcal{I} \rangle, \text{ para todo } n \geq 2,$$

entonces

$$A = \{h + Y_1 g + \mathcal{I} : h \in k[X], g \in k[Y_1]\},$$

Sea $J = \langle X + \mathcal{I} \rangle$, por el Ejemplo (2.3), se tiene la graduación $gr_J(A)$, y el lector puede comprobar que

$$gr_J(A) = \bigoplus_{k \in \mathbb{N}} \frac{J^k}{J^{k+1}} \cong k[X].$$

Esto implica que $X + \mathcal{I}$ es A-casi regular, es decir, $X + \mathcal{I}$ es un ejemplo de una secuencia que es A-casi regular, pero no es A-regular. Otras ejemplos de secuencias casi regulares que no son regulares se puede consultar en Cherrabi (2010).

En anillos Noetherianos $\mathbb{N}$-graduados el Teorema 16.3 de Matsumura (1987), garantiza que toda secuencia casi regular de elementos homogéneos, es una secuencia regular.

Teorema 4.3. Sea A un anillo Noetheriano $\mathbb{N}$-graduado. Si la secuencia $a_1, \ldots, a_r$ es A-casi regular y cada a_i es homogéneo de grado positivo, entonces $a_1, \ldots, a_r$ es una secuencia A-regular.

Este teorema, junto con el hecho que las secuencias A-casi regulares son independientes del orden de los elementos, garantiza que en el anillo de polinomios $A = \mathbb{C}[X_1, \ldots, X_r]$, cualquier permutación de una secuencia A-regular, formada por polinomios homogéneos de grado positivo, también es A-regular. Por medio de secuencias regulares de polinomios homogéneos de grado positivo, es posible estudiar la dimensión de las variedades de Mishchenko-Fomenko, que se presentarán en el siguiente capítulo.

Regularidad y dimensión de una variedad

Estudiar las secuencias regulares en anillos de polinomios tiene importantes aplicaciones en geometría algebraica. Por ejemplo, el Teorema de Nagata-Auslander-Buchsbaum Auslander y Buchsbaum (1959) implica que en un anillo local A la longitud máxima de una secuencia regular, en el ideal maximal del anillo, es igual a la dimensión de A.

Definición 4.4. Sea $V = \mathcal{V}(f_1, \ldots, f_r)$ una variedad del espacio afín A^n. Se dice que V es una **intersección completa** si $dim(V) = n - r$.

Observación 4.2. Si $V = \mathcal{V}(f_1, \ldots, f_r)$ es una intersección completa y W es una componente irreducible de V, se tiene

$$n - r \leq dim(W) \leq dim(V) = n - r,$$

luego, $dim(W) = n - r$, y por la Definición (3.7), la variedad V es $Eqd(n - r)$.

El siguiente teorema relaciona los conceptos de intersección completa y secuencia regular en el álgebra de polinomios $\mathbb{C}[X_1, \ldots, X_r]$. Los detalles de la prueba se pueden consultar en el libro de Matsumura (1987) y el artículo de Futorny y Ovsienko. (2005)

Teorema 4.4. Sea $f_1, \ldots, f_r$ una secuencia del algebra $A = \mathbb{C}[X_1, \ldots, X_r]$. Entonces

1. La variedad $V = \mathcal{V}(f_1, \ldots, f_r)$ es una intersección completa, si y solo si, V es $Eqd(n - r)$.
2. La secuencia $f_1, \ldots, f_r$ es A-regular, si y solo si, la variedad $\mathcal{V}(f_1, \ldots, f_i)$ es $Eqd(n - i)$, para toda $i = 1, \ldots, r$.
3. Si $V = \mathcal{V}(f_1, \ldots, f_r)$ es una intersección completa y los polinomios f_i son homogéneos de grado positivo, entonces cualquier subvariedad de V es una intersección completa.

Observación 4.3. En las $\mathbb{C}$-álgebras de polinomios $A = \mathbb{C}[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$ y $B = \mathbb{C}[Y_1, \ldots, Y_n]$ considere los polinomios $F_1, \ldots, F_r \in A$. Ahora, para cada $i = 1, \ldots, r$ sea f_i el polinomio que resulta de cancelar en F_i todos los monomios que sean producto de alguna de las indeterminadas $X_1, \ldots, X_m$, es decir,

$$f_i = F_i (X_1 = \cdots = X_m = 0) \in B.$$

Entonces, el segundo enunciado del Teorema (4.4) garantiza que la secuencia $X_1, \ldots, X_m, F_1, \ldots, F_r$ es A-regular, si y solo si, la secuencia $f_1, \ldots, f_r$ es B-regular.

CAPÍTULO 5

Subálgebras de Mishchenko-Fomenko

El álgebra envolvente universal $U(\mathfrak{g})$ de un álgebra de Lie $\mathfrak{g}$, junto con el Teorema PBW, que el lector puede consultar en el capítulo V de Humphreys (1997), permiten enlazar la teoría de álgebras de Lie y la teoría de álgebras asociativas, lo cual proporciona un camino para estudiar representaciones del álgebra de Lie $\mathfrak{g}$, por medio de las representaciones de su envolvente universal $U(\mathfrak{g})$.

En este contexto, es importante determinar subálgebras conmutativas B, contenidas en el álgebra envolvente universal $U(\mathfrak{g})$, tal que $U(\mathfrak{g})$ sea un B-módulo libre. A partir de estas condiciones, toda representación irreducible del álgebra B se puede visualizar como una representación irreducible sobre $U(\mathfrak{g})$, y por ende, como una representación del álgebra de Lie $\mathfrak{g}$. Desde esta perspectiva, el famoso Teorema de Kostant (2009) afirma que el álgebra envolvente universal $U(\mathfrak{g})$, de un álgebra de Lie semisimple compleja $\mathfrak{g}$, es un módulo libre sobre su centro. Para el caso del álgebra de Lie $\mathfrak{gl}_n$, de las matrices cuadradas de orden n con componentes complejas, el resultado principal de Ovsienko (2003) establece que $U(\mathfrak{gl}_n)$ es un módulo libre sobre la subálgebra de Gelfand-Tsetlin.

Sea A una subálgebra conmutativa del álgebra envolvente universal $U(\mathfrak{gl}_n)$. En general $U(\mathfrak{gl}_n)$ no es un A-módulo libre, sin embargo, por el resultado principal de Futorny y Ovsienko (2003) se conoce que $U(\mathfrak{gl}_n)$ es un A-módulo libre cuando la graduación de A es generada por una intersección completa en $S(\mathfrak{gl}_n)$, de hecho, ellos prueban el teorema siguiente:

> **Teorema 5.1.** Sea U un álgebra filtrada especial sobre un cuerpo $\mathbb{F}$. Si $g_1, \ldots, g_t$ es una secuencia de elementos que conmutan, cuyas imágenes forman una intersección completa en el álgebra graduada asociada $gr(U)$, entonces el álgebra U es un $\mathbb{F}[g_1, \ldots, g_t]$-módulo libre a izquierda (o derecha).

Un resultado conocido en la teoría de álgebras de Lies es que el álgebra envolvente universal $U(\mathfrak{g})$, de un álgebra de Lie $\mathfrak{g}$ de dimensión finita, es filtrada especial. Este hecho, junto con el Teorema (4.4), motivan el estudio de subálgebras del álgebra simétrica $S(\mathfrak{gl}_n)$, las cuales son generadas por una secuencia $S(\mathfrak{gl}_n)$-regular de polinomios. Este proyecto de investigación analizó una colección especial de subálgebras conmutativas del álgebra simétrica $S(\mathfrak{gl}_n)$, denominadas **subálgebras de Mishchenko-Fomenko**. A su vez, estas subálgebras juegan un papel crucial en teoría de sistemas integrables y en representaciones de álgebras de Lie. Cada vez que se escoja un parámetro $\mu \in \mathfrak{gl}_n$, con el proceso de "deslizamiento de argumento" se obtiene una subálgebra de Mishchenko-Fomenko $\overline{A}_\mu$. Para estas subálgebras, se tiene la conjetura dada a continuación.

Conjetura 5.1. Para todo parámetro $\mu \in \mathfrak{gl}_n$, la subálgebra de Mishchenko-Fomenko $\overline{A}_\mu$ es generada por una secuencia $S(\mathfrak{gl}_n)$-regular.

En lo que sigue se presentan las subálgebras de Mishchenko-Fomenko en el álgebra de Lie $\mathfrak{gl}_n$ junto con los resultados más importantes sobre la $S(\mathfrak{gl}_n)$-regularidad de la secuencia de polinomios que las generan.

5.1 Subálgebras de Mishchenko-Fomenko

Las subálgebras de Mishchenko-Fomenko, obtenidas mediante el método de modificar o "deslizar los argumentos" (o parámetros) de los generadores del álgebra simétrica, son subálgebras conmutativas del álgebra simétrica de un álgebra de Lie, las cuales aparecen en el estudio de las representaciones del álgebra de Lie. Los detalles teóricos del método de deslizamiento de argumento desbordan el interés de este texto, pero el lector puede consultarlos en Mishchenko y Fomenko (1978). En el resultado principal del artículo Futorny y Molev (2014), se presenta un procedimiento que permite elegir un conjunto de polinomios algebraicamente independientes que generan las subálgebras de Mischenko-

Fomenko, contenidas en el álgebra simétrica $S(\mathfrak{gl}_n)$. Cada conjunto de generadores está asociado a una forma canónica de Jordan $\mu \in \mathfrak{gl}_n$, y en la investigación se estudiaron los generadores presentados en este artículo, para determinar si forman una secuencia $S(\mathfrak{gl}_n)$-regular. Aunque no fue posible dar respuesta positiva a esta problemática, se estudió la subálgebra de Mishchenko-Fomenko asociada a un parámetro particular y se logró comprobar que, en este caso, la variedad se puede expresar como unión de tres subvariedades donde dos de estas son isomorfas. Esto, en teoría, permitirá simplificar los cálculos necesarios en la búsqueda de la solución general del problema.

5.1.1. Generadores de las Subálgebras de Mishchenko-Fomenko

El siguiente procedimiento descrito en Futorny y Molev (2014) permite escoger un conjunto de polinomios algebraicamente independientes, que generan las subálgebras de Mishchenko-Fomenko.

Para cada matriz $E = (e_{ij}) \in \mathfrak{gl}_n$ y cada par de subconjuntos $I = \{i_1 < \cdots < i_t\}$ y $J = \{j_1 < \cdots < j_t\}$, contenidos en $[1, n] = \{1, \ldots, n\}$, con $E(I, J)$, se denota el siguiente determinante:

$$E(I, J) = \det \begin{pmatrix} e_{i_1 j_1} & e_{i_1 j_2} & \cdots & e_{i_1 j_t} \\ e_{i_2 j_1} & e_{i_2 j_2} & \cdots & e_{i_2 j_t} \\ \vdots & \vdots & \ddots & \vdots \\ e_{i_t j_1} & e_{i_t j_2} & \cdots & e_{i_t j_t} \end{pmatrix}$$

Además, por definición $E(\emptyset, \emptyset) = 1$. Ahora, sea $\mu \in \mathfrak{gl}_n$ y suponga que los diferentes valores propios de μ son $\lambda_1, \ldots, \lambda_s$. Si el valor propio λ_i tiene asociado k bloques de Jordan de tamaños $r_{i1} \geq r_{i2} \geq \cdots \geq r_{ik}$, con $J(r_{ij}, \lambda_i)$ se denotará el bloque de Jordan de tamaño $r_{ij} \times r_{ij}$, asociado al valor propio λ_i, esto significa que en la forma canónica de Jordan asociada a μ, los bloques de Jordan correspondientes al valor propio λ_i tienen la forma

$$J_\mu(\lambda_i) = \begin{pmatrix} J(r_{i1}, \lambda_i) & & & \\ & J(r_{i2}, \lambda_i) & & \\ & & \ddots & \\ & & & J(r_{ik}, \lambda_i) \end{pmatrix}.$$

Así, la forma canónica de Jordan de μ se puede expresar como

$$J_\mu = J_\mu(\lambda_1) \oplus \cdots \oplus J_\mu(\lambda_s).$$

Ahora, con $\alpha(\lambda_i)$ denote el diagrama Young [1] que tiene r_{ij} cajas en la j-ésima fila, y sea $|\alpha(\lambda_i)|$ el número total de cajas en este diagrama. Entonces,

$$|\alpha(\lambda_i)| = r_{i1} + \cdots + r_{ik}.$$

Para continuar, considere otro diagrama de Young γ, tal que el número de cajas de la t-ésima fila de γ sea el número total de cajas que están estrictamente por debajo de la t-ésima fila en todos los diagramas $\alpha(\lambda_i)$ y denote este número con γ_t, es decir

$$\gamma_t = \sum_{i=1}^{s} \left(\sum_{j \geq t+1} r_{ij} \right).$$

Ahora, sean M un conjunto finito y k un entero, tal que $0 \leq k \leq |M|$. Con $\mathcal{P}(M,k)$, denote la colección de subconjuntos de cardinal k, contenidos en M. En particular, para enteros positivos $k \leq m$, se utiliza la notación $\mathcal{P}(n,k) = \mathcal{P}(\{1,2,\ldots,n\},k)$. Además, sea $\left\{X_{ij} : i,j \in A\right\}$ un conjunto de n^2 indeterminadas conmutativas y considere la matriz E cuya ij-ésima componente es la indeterminada X_{ij}. Para enteros k y m, tales que $0 \leq k < m \leq n$, se define el polinomio $\overline{\phi}_m^{(k)}$ como sigue

$$\overline{\phi}_m^{(k)} = \sum_{J \in \mathcal{P}(n,m)} \left(\sum_{B,C \in \mathcal{P}(J,k)} (\mathrm{sgn}\sigma)\mu\,(B,C)\,E\,(J-B,J-C) \right), \tag{5.1}$$

en el cual sgnσ denota el signo de la permutación $\sigma = \begin{pmatrix} B & J-B \\ C & J-C \end{pmatrix}$. A continuación, para $i,j = 1,\ldots,n$, en la ij-ésima caja del diagrama de Young $\mathit{\Gamma} = (n, n-1, \ldots, 1)$ escriba el polinomio $\overline{\phi}_{n-j+1}^{(n-i-j+1)}$, como se presenta en seguida

$$\mathit{\Gamma} = \begin{array}{ccccc} \overline{\phi}_n^{(n-1)} & \overline{\phi}_{n-1}^{(n-2)} & \cdots & \overline{\phi}_2^{(1)} & \overline{\phi}_1^{(0)} \\ \overline{\phi}_n^{(n-2)} & \overline{\phi}_{n-1}^{(n-3)} & \cdots & \overline{\phi}_2^{(0)} & \\ \vdots & \vdots & & & \\ \overline{\phi}_n^{(1)} & \overline{\phi}_{n-1}^{(0)} & & & \\ \overline{\phi}_n^{(0)} & & & & \end{array}$$

Se puede considerar el diagrama $\mathit{\Gamma}/\gamma$ que resulta cuando se eliminan del diagrama $\mathit{\Gamma}$ las cajas que están en el diagrama γ. El resultado que se presenta en seguida puede ser consultado en Futorny y Molev (2014), y es particularmente importante en el desarrollo

[1] Diagrama de Young es una organización de cajas, en filas, de modo que el número de cajas de una fila no excede al número de cajas de la fila anterior.

de investigaciones sobre las álgebras de Mishchenko-Fomenko en $S(\mathfrak{gl}_n)$.

Teorema 5.2. Para cada parámetro $\mu \in \mathfrak{gl}_n$, los polinomios $\overline{\phi}_m^{(k)}$ correspondientes a cajas del diagrama Γ/γ son generadores algebraicamente independientes de la subálgebra de Mishchenko-Fomenko $\overline{A}_\mu$ en $S(\mathfrak{gl}_n)$.

Ejemplo 5.1. Sea $\mu \in \mathfrak{gl}_n$ una forma canónica de Jordan que consta de n bloques de Jordan de orden 1, todos asociados al mismo valor propio λ. Luego μ es de la forma

$$\mu = \underbrace{(\lambda) \oplus \ldots \oplus (\lambda)}_{n \text{ veces}} .$$

En este caso, el diagrama de Young $\gamma = (n-1, n-2, \ldots, 1)$, y al aplicar el Teorema (5.2), se obtiene que la subálgebra de Mishchenko-Fomenko $\overline{A}_\mu$ es generada por los polinomios

$$\overline{\phi}_m^{(0)} = \sum_{I \in \mathcal{P}(n,m)} (\text{sgn}\sigma)\mu(\emptyset, \emptyset)\, E(I, I) = \sum_{I \in \mathcal{P}(n,m)} E(I, I),$$

en la que $m = 1, \ldots, n$. En particular,

$$\overline{\phi}_1^{(0)} = \sum_{I \in \mathcal{P}(n,1)} E(I, I) = \sum_{i=1}^{n} X_{ii}.$$

Mientras que

$$\overline{\phi}_n^{(0)} = \det E = \det \begin{pmatrix} X_{11} & X_{12} & \ldots & X_{1n} \\ X_{21} & X_{22} & \ldots & X_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ X_{n1} & X_{n2} & \ldots & X_{nn} \end{pmatrix}.$$

Ejemplo 5.2. Sea $\mu \in \mathfrak{gl}_n$ una forma canónica de Jordan que consta de $n-2$ bloques de Jordan de orden 1 y un bloque de Jordan de orden 2, todos asociados al mismo valor propio λ. Así que μ es de la forma

$$\mu = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \oplus \underbrace{(\lambda) \oplus \ldots \oplus (\lambda)}_{n-2 \text{ veces}} .$$

En este caso, el diagrama de Young $\gamma = (n-2, n-3, \ldots, 1)$, y al aplicar el Teorema

(5.2), se obtiene que la subálgebra $\overline{A}_\mu$ es generada por los polinomios

$$\overline{\phi}_m^{(0)} = \sum_{I\in\mathcal{P}(n,m)} E\left(I,I\right),$$

para $m = 1,\ldots,n$, junto con los polinomios

$$\overline{\phi}_m^{(1)} = \sum_{J\in\mathcal{P}(n,m)} \sum_{B,C\in\mathcal{P}(J,1)} (\mathrm{sgn}\sigma)\mu\left(B,C\right) E\left(J-B,J-C\right),$$

en la que $m = 2,\ldots,n$. En particular,

$$\overline{\phi}_2^{(1)} = \lambda\left(\sum_{i=1}^{n} X_{ii}\right) - x_{21}.$$

5.1.2. Regularidad de secuencias de Mishchenko-Fomenko

Esta sección expone los avances obtenidos en la búsqueda de solución a la conjetura (5.1). En la tesis doctoral de Mutis (2016) se probó que en el álgebra de Lie $\mathfrak{gl}_3$ las subálgebras de Mishchenko-Fomenko son generadas por una secuencia de polinomios $S\left(\mathfrak{gl}_3\right)$-regular. Igualmente, en esta tesis se logran avances significativos en la problemática para el álgebra de Lie $\mathfrak{gl}_4$. En la presente investigación se estudió el caso general de la subálgebra de Mishchenko-Fomenko en $\mathfrak{gl}_n$, que es generada por una forma canónica de Jordan que tiene un bloque de Jordan de tamaño 2 y $n-2$ bloques de tamaño 1, todos asociados a un mismo valor propio, y en la parte final de este texto se presenta el resultado principal alcanzado en la investigación.

Proposición 5.1. Si $\mu \in gl_2$ está en la forma canónica de Jordan, entonces la subálgebra de Mishchenko-Fomenko A_μ es generada por una secuencia de polinomios $S\left(\mathfrak{gl}_2\right)$-regular.

Demostración. Cualquier forma canónica de Jordan en gl_2 es de una de las siguientes dos posibilidades:

1. $\mu = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$
2. $\mu = \begin{pmatrix} \lambda & 0 \\ 0 & \beta \end{pmatrix}$,

en la que α y β son complejos distintos. Para el primer caso, el álgebra A_μ es generada por la secuencia $f_1 = X_1 + X_2$, $f_2 = X_1X_2 - X_3X_4$ y $f_3 = \lambda\left(X_1+X_2\right) - X_3$. Por la Observación

(3.1), se obtiene

$$V = \mathcal{V}(f_1, f_2, f_3) = \mathcal{V}(f_1, f_2, X_3) = \mathcal{V}(f_1, X_1X_2, X_3)\,\mathcal{V}(X_1, X_2, X_3)\,.$$

Por la Proposición (3.3), la variedad es irreducible, por tanto

$$dimV = grtr_{\mathbb{C}}\frac{\mathbb{C}[X_1, X_2, X_3, X_4]}{\langle X_1, X_2, X_3\rangle} = grtr_{\mathbb{C}}\mathbb{C}[X_4] = 1 = 4 - 3,$$

esto significa que V es $Eqd(4-3)$. Finalmente, del Teorema (4.4), se deduce que la secuencia f_1, f_2, f_3, f_4 es $S(gl_2)$-regular. Para el segundo caso, la subálgebra de Mishchenko-Fomenko es generada por los polinomios f_1 y f_2 del caso anterior, junto con el polinomio $g = \beta X_1 + \lambda X_2$, en el cual $\lambda \neq \beta$. Luego

$$W = \mathcal{V}(f_1, f_2, g) = \mathcal{V}(f_1, f_2, (\lambda - \beta)X_1)\,.$$

Dado que $\lambda - \beta \neq 0$, se sigue

$$W = \mathcal{V}(f_1, f_2, X_1) = \mathcal{V}(X_1, X_2, X_3)\,.$$

Por tanto, W es $Eqd(4-3)$ y la secuencia f_1, f_2, g es $S(gl_2)$-regular. $\square$

En la tesis de Mutis (2016) se prueban los dos teoremas siguientes:

Teorema 5.3. Si $\mu \in gl_3$ una forma canónica de Jordan, entonces la subálgebra de Mishchenko-Fomenko A_μ es generada por una secuencia $S(\mathfrak{gl}_3)$-regular.

Teorema 5.4. Si $\mu \in gl_3$ una forma canónica de Jordan nilpotente, entonces la subálgebra de Mishchenko-Fomenko A_μ es generada por una secuencia $S(\mathfrak{gl}_4)$-regular.

En este punto se presentan los resultados obtenidos durante el trabajo de investigación. Sea $\mathcal{S} = \mathbb{C}\left[X_{ij} : i, j \in [1, n]\right]$ y denote con $\mathcal{V}_{MF}(n)$, la variedad definida por los generadores de la subálgebra de Mischenko-Fomenko en $S(\mathfrak{gl}_n)$, asociada a la forma canónica de Jordan μ, la cual consta de un bloque de Jordan de tamaño 2 y $n-2$ bloques de de tamaño 1, todos asociados a un mismo valor propio λ, es decir, μ tiene la siguiente forma:

$$\mu = \left(\begin{array}{cc|ccc} \lambda & 1 & & 0 & \\ 0 & \lambda & & & \\ \hline & & \lambda & & \\ & 0 & & \ddots & \\ & & & & \lambda \end{array}\right).$$

En este momento es relevante resaltar que de la ecuación (5.1), que define los polinomios $\overline{\phi}_m^{(k)}$, se deduce que estos polinomios son homogéneos de grado $m-k$. De acuerdo con lo expuesto en el Ejemplo (5.2), los polinomios que generan la variedad $\mathcal{V}_{MF}(n)$, son

$$\mathcal{V}_{MF}(n)=\mathcal{V}\left(\left\{\phi_k^{(0)}\right\}_{k=1}^{n}\bigcup\left\{\phi_i^{(1)}\right\}_{i=2}^{n}\right).$$

Además, para cada $k=2,3\dots,n$, se tiene

$$\phi_k^{(1)}=\lambda(n-k+1)\phi_{k-1}^{(0)}-\sum_{\substack{I\subseteq\{1,\dots,n\}\\|I|=k,\{1,2\}\subseteq I}}E\left(I-\{1\},I-\{2\}\right).$$

En particular, para $k=n$, se obtiene $\phi_n^{(1)}=\lambda\phi_{n-1}^{(0)}-E\left([1,n],[1,n]\right)$, en la que el conjunto $[1,n]=\{1,2,\dots,n\}$. Las propiedades para variedades algebraicas expuestas en la Observación (3.1), implican

$$\mathcal{V}_{MF}(n)=\mathcal{V}\left(\left\{\phi_i^{(0)}\right\}_{i=1}^{n}\bigcup\left\{\phi_i^{(1)}\right\}_{i=2}^{n-1}\bigcup\left\{\widehat{\phi_n^{(1)}}\right\}\right),$$

en la cual

$$\widehat{\phi_n^{(1)}}=E\left([1,n],[1,n]\right)=\det\begin{pmatrix} X_{21} & X_{23} & X_{24} & \cdots & X_{2,n-1} & X_{2n}\\ X_{31} & X_{33} & X_{34} & \cdots & X_{3,n-1} & X_{3n}\\ X_{41} & X_{43} & X_{44} & \cdots & X_{4,n-1} & X_{4n}\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ X_{n-1,1} & X_{n-1,3} & X_{n-1,4} & \cdots & X_{n-1,n-1} & X_{n-1,n}\\ X_{n1} & X_{n3} & X_{n4} & \cdots & X_{n,n-1} & X_{nn}\end{pmatrix}.$$

Ahora, para un subconjunto no vacío $\mathbf{X}\subseteq\left\{X_{ij}:i,j\in[1,n]\right\}$ y un polinomio $f\in\mathcal{P}$, con $f^{\mathbf{X}}$ se denota el polinomio que se obtiene de f, igualando a cero todas las indeterminadas del conjunto $\mathbf{X}$. Por ejemplo, si $\mathbf{X}=\{X_{11},X_{22}\}$ y $f=X_{11}+X_{22}+X_{33}$, entonces $f^{\mathbf{X}}=X_{33}$.

Con esta notación, y tomando $\mathbf{X} = \left\{X_{nj}\right\}_{j=3}^{n} \cup \left\{X_{in}\right\}_{i=3}^{n}$, se deduce

$$\begin{aligned}
\left(\widehat{\phi_n^{(1)}}\right)^{\mathbf{X}} &= (-1)^{n+1} X_{n1} \det \begin{pmatrix} X_{23} & X_{24} & \cdots & X_{2,n-1} & X_{2n} \\ X_{33} & X_{34} & \cdots & X_{3,n-1} & 0 \\ X_{43} & X_{44} & \cdots & X_{4,n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ X_{n-1,3} & X_{n-1,4} & \cdots & X_{n-1,n-1} & 0 \end{pmatrix} \\
&= -X_{n1} X_{2n} \det \begin{pmatrix} X_{33} & X_{34} & \cdots & X_{3,n-2} & X_{3,n-1} \\ X_{43} & X_{44} & \cdots & X_{4,n-2} & X_{4,n-1} \\ X_{53} & X_{54} & \cdots & X_{5,n-2} & X_{5,n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ X_{n-1,3} & X_{n-1,4} & \cdots & X_{n-1,n-2} & X_{n-1,n-1} \end{pmatrix} \\
&= -X_{n1} X_{2n} E\left([3, n-1], [3, n-1]\right).
\end{aligned}$$

Por tanto,

$$\mathcal{V}_{MF}(n) \cap \mathcal{V}(\mathbf{X}) = \mathcal{A} \cup \mathcal{B} \cup \mathcal{C},$$

en la cual

$$\begin{aligned}
\mathcal{A} &= \mathcal{V}_{MF}(n) \cap \mathcal{V}(\mathbf{X}) \cap \mathcal{V}(X_{n1}) \\
\mathcal{B} &= \mathcal{V}_{MF}(n) \cap \mathcal{V}(\mathbf{X}) \cap \mathcal{V}(X_{2n}) \\
\mathcal{C} &= \mathcal{V}_{MF}(n) \cap \mathcal{V}(\mathbf{X}) \cap \mathcal{V}\left(E\left([3, n-1], [3, n-1]\right)\right)
\end{aligned}$$

5.1.3. Resultado principal de la investigación

Proposición 5.2. $\mathcal{A} \cong \mathcal{B}$.

Demostración. Considere la transposición $\sigma = (1, 2) \in S_n$ y los isomorfismos de álgebras $\varphi, \psi : \mathcal{S} \longrightarrow \mathcal{S}$, definidos por

$$\varphi(X_{ij}) = X_{\sigma(i)\sigma(j)} \qquad \text{y} \qquad \psi(X_{ij}) = X_{ji}.$$

Se probará que $\psi \circ \varphi$ induce un isomorfismo de variedades algebraicas afínes de $\mathcal{A}$ en $\mathcal{B}$. De hecho, el proceso de demostración se orienta en mostrar que los polinomios que generan la variedad $\mathcal{A}$ se transforman en los que generan la variedad $\mathcal{B}$, vía la función $\psi \circ \varphi$. Sean $\mathbb{X}_1 = \mathbf{X} \cup \{X_{n1}\}$ y $\mathbb{X}_2 = \mathbf{X} \cup \{X_{2n}\}$, para $J = \{j_1 < j_2 < \cdots < j_k\} \subset \{3, \ldots, n\}$, se tiene

$$\psi\varphi\left(E(J, J)\right) = \psi\varphi\left(\det\left(X_{j_r j_s}\right)_{r,s=1}^{k}\right) = \det\left(X_{j_s j_r}\right)_{r,s=1}^{k} = \det\left(\left(X_{j_r j_s}\right)_{r,s=1}^{k}\right)^{T} = E(J, J).$$

Dado que $X_{j_r j_s} \notin \{X_{n1}, X_{2n}\}$, entonces $\psi\varphi\left(E(J,J)\right)^{\mathbb{X}_1} = \left(E(J,J)\right)^{\mathbb{X}_2}$. Ahora, si $j_k < n$, entonces $X_{j_r j_s} \notin \{X_{n1}, X_{2n}\}$, y denotando $C = \{1\} \cup J$ y $D = D$, se tiene

$$\begin{aligned}
\psi\varphi\left(E\left(C,C\right)\right)^{\mathbb{X}_1} &= \psi\varphi\left(\det\begin{pmatrix} X_{11} & X_{1j_2} & \cdots & X_{1j_k} \\ X_{j_2 1} & X_{j_2 j_2} & \cdots & X_{j_2 j_k} \\ \vdots & \vdots & & \vdots \\ X_{j_k 1} & X_{j_k j_2} & \cdots & X_{j_k j_k} \end{pmatrix}^{\mathbb{X}_1}\right) \\
&= \det\begin{pmatrix} X_{22} & X_{j_2 2} & \cdots & X_{j_k 2} \\ X_{2j_2} & X_{j_2 j_2} & \cdots & X_{j_k j_2} \\ \vdots & \vdots & & \vdots \\ X_{2j_k} & X_{j_2 j_k} & \cdots & X_{j_k j_k} \end{pmatrix}.
\end{aligned}$$

Entonces

$$\begin{aligned}
\psi\varphi\left(E\left(C,C\right)\right)^{\mathbb{X}_1} &= \det\begin{pmatrix} X_{22} & X_{2j_2} & \cdots & X_{2j_k} \\ X_{j_2 2} & X_{j_2 j_2} & \cdots & X_{j_2 j_k} \\ \vdots & \vdots & & \vdots \\ X_{j_k 2} & X_{j_k j_2} & \cdots & X_{j_k j_k} \end{pmatrix} \\
&= \left(E\left(D,D\right)\right)^{\mathbb{X}_2}.
\end{aligned}$$

De forma similar, se obtiene

$$\psi\varphi\left(E\left(D,D\right)\right)^{\mathbb{X}_1} = \left(E\left(C,C\right)\right)^{\mathbb{X}_2}.$$

Si $j_k = n$, entonces

$$\psi\varphi\left(E(C,C)\right)^{\mathbb{X}_1} = \psi\varphi\left(\det\begin{pmatrix} X_{11} & X_{1j_2} & \cdots & X_{1j_{k-1}} & X_{1n} \\ X_{j_2 1} & X_{j_2 j_2} & \cdots & X_{j_2 j_{k-1}} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ X_{j_2 1} & X_{j_{k-1} j_2} & \cdots & X_{j_{k-1} j_{k-1}} & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}\right) = 0,$$

además,

$$\left(E(D,D)\right)^{\mathbb{X}_2} = \det\begin{pmatrix} X_{22} & X_{2j_2} & \cdots & X_{2j_{k-1}} & 0 \\ X_{j_2 2} & X_{j_2 j_2} & \cdots & X_{j_2 j_{k-1}} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ X_{j_2 2} & X_{j_{k-1} j_2} & \cdots & X_{j_{k-1} j_{k-1}} & 0 \\ X_{n2} & 0 & \cdots & 0 & 0 \end{pmatrix} = 0.$$

es consecuencia,

$$\psi\varphi\left(E(C,C)\right)^{\mathbb{X}_1} = 0 = \left(E(D,D)\right)^{\mathbb{X}_2}.$$

También

$$\begin{aligned}
\psi\varphi\left(E(D,D)\right)^{\mathbb{X}_1} &= \psi\varphi\left(\det\begin{pmatrix} X_{22} & X_{2j_2} & \cdots & X_{2j_{k-1}} & X_{2n} \\ X_{j_2 2} & X_{j_2 j_2} & \cdots & X_{j_2 j_{k-1}} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ X_{j_2 2} & X_{j_{k-1} j_2} & \cdots & X_{j_{k-1} j_{k-1}} & 0 \\ X_{n2} & 0 & \cdots & 0 & 0 \end{pmatrix}\right), \\
&= \det\begin{pmatrix} X_{11} & X_{j_2 1} & \cdots & X_{j_{k-1} 1} & X_{n1} \\ X_{1j_2} & X_{j_2 j_2} & \cdots & X_{j_{k-1} j_2} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ X_{1j_{k-1}} & X_{j_2 j_{k-1}} & \cdots & X_{j_{k-1} j_{k-1}} & 0 \\ X_{1n} & 0 & \cdots & 0 & 0 \end{pmatrix}, \\
&= \det\begin{pmatrix} X_{11} & X_{1j_2} & \cdots & X_{1j_{k-1}} & X_{1n} \\ X_{j_2 1} & X_{j_2 j_2} & \cdots & X_{j_2 j_{k-1}} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ X_{j_{k-1} 1} & X_{j_{k-1} j_2} & \cdots & X_{j_{k-1} j_{k-1}} & 0 \\ X_{n1} & 0 & \cdots & 0 & 0 \end{pmatrix}, \\
&= \left(E(C,C)\right)^{\mathbb{X}_2}.
\end{aligned}$$

En el caso $j_k = n$, y denotando $G = \{1,2\} \cup J$, se obtiene

$$\psi\varphi\left(E(G,G)\right)^{\mathbb{X}_1} = \psi\varphi\left(\det\begin{pmatrix} X_{11} & X_{12} & X_{1j_3} & \cdots & X_{1j_{k-1}} & X_{1n} \\ X_{21} & X_{22} & X_{2j_3} & \cdots & X_{2j_{k-1}} & X_{2n} \\ X_{j_3 1} & X_{j_3 2} & X_{j_3 j_3} & \cdots & X_{j_3 j_{k-1}} & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ X_{j_{k-1} 1} & X_{j_{k-1} 2} & X_{j_{k-1} j_3} & \cdots & X_{j_{k-1} j_{k-1}} & 0 \\ 0 & X_{n2} & 0 & \cdots & 0 & 0 \end{pmatrix}\right).$$

Luego,

$$
\begin{aligned}
\psi\varphi\left(E(G,G)\right)^{\mathbb{X}_1} &= \det\begin{pmatrix}
X_{22} & X_{12} & X_{j_3 2} & \cdots & X_{j_{k-1}2} & X_{n2}\\
X_{21} & X_{11} & X_{j_3 1} & \cdots & X_{j_{k-1}1} & X_{n1}\\
X_{2j_3} & X_{1j_3} & X_{j_3 j_3} & \cdots & X_{j_{k-1}j_3} & 0\\
\vdots & \vdots & \vdots & & \vdots & \vdots\\
X_{2j_{k-1}} & X_{1j_{k-1}} & X_{j_3 j_{k-1}} & \cdots & X_{j_{k-1}j_{k-1}} & 0\\
0 & X_{1n} & 0 & \cdots & 0 & 0
\end{pmatrix},\\
&= -\det\begin{pmatrix}
X_{21} & X_{11} & X_{j_3 1} & \cdots & X_{j_{k-1}1} & X_{n1}\\
X_{22} & X_{12} & X_{j_3 2} & \cdots & X_{j_{k-1}2} & X_{n2}\\
X_{2j_3} & X_{1j_3} & X_{j_3 j_3} & \cdots & X_{j_{k-1}j_3} & 0\\
\vdots & \vdots & \vdots & & \vdots & \vdots\\
X_{2j_{k-1}} & X_{1j_{k-1}} & X_{j_3 j_{k-1}} & \cdots & X_{j_{k-1}j_{k-1}} & 0\\
0 & X_{1n} & 0 & \cdots & 0 & 0
\end{pmatrix},\\
&= \det\begin{pmatrix}
X_{11} & X_{21} & X_{j_3 1} & \cdots & X_{j_{k-1}1} & X_{n1}\\
X_{12} & X_{22} & X_{j_3 2} & \cdots & X_{j_{k-1}2} & X_{n2}\\
X_{1j_3} & X_{2j_3} & X_{j_3 j_3} & \cdots & X_{j_{k-1}j_3} & 0\\
\vdots & \vdots & \vdots & & \vdots & \vdots\\
X_{1j_{k-1}} & X_{2j_{k-1}} & X_{j_3 j_{k-1}} & \cdots & X_{j_{k-1}j_{k-1}} & 0\\
X_{1n} & 0 & 0 & \cdots & 0 & 0
\end{pmatrix},\\
&= \det\begin{pmatrix}
X_{11} & X_{12} & X_{1j_3} & \cdots & X_{1j_{k-1}} & X_{1n}\\
X_{21} & X_{22} & X_{2j_3} & \cdots & X_{2j_{k-1}} & 0\\
X_{j_3 1} & X_{j_3 2} & X_{j_3 j_3} & \cdots & X_{j_3 j_{k-1}} & 0\\
\vdots & \vdots & \vdots & & \vdots & \vdots\\
X_{j_{k-1}1} & X_{j_{k-1}2} & X_{j_{k-1}j_3} & \cdots & X_{j_{k-1}j_{k-1}} & 0\\
X_{n1} & X_{n2} & 0 & \cdots & 0 & 0
\end{pmatrix}^{T}\\
&= \left(E(G,G)\right)^{\mathbb{X}_2}.
\end{aligned}
$$

Ahora, si $j_k < n$, entonces $X_{j_r j_s} \notin \{X_{n1}, X_{2n}\}$, y se tiene

$$
\psi\varphi\left(E(G,G)\right)^{\mathbb{X}_1} = \psi\varphi\left(\det\begin{pmatrix}
X_{11} & X_{12} & X_{1j_3} & \cdots & X_{1j_k}\\
X_{21} & X_{22} & X_{2j_3} & \cdots & X_{2j_k}\\
X_{j_3 1} & X_{j_3 2} & X_{j_3 j_3} & \cdots & X_{j_3 j_k}\\
\vdots & \vdots & \vdots & & \vdots\\
X_{j_k 1} & X_{j_k 2} & X_{j_k j_3} & \cdots & X_{j_k j_k}
\end{pmatrix}\right),
$$

entonces

$$
\begin{aligned}
\psi\varphi\left(E(G,G)\right)^{\mathbb{X}_1} &= \det\begin{pmatrix} X_{22} & X_{12} & X_{j_3 2} & \cdots & X_{j_k 2} \\ X_{21} & X_{11} & X_{j_3 1} & \cdots & X_{j_k 1} \\ X_{2 j_3} & X_{1 j_3} & X_{j_3 j_3} & \cdots & X_{j_k j_3} \\ \vdots & \vdots & \vdots & & \vdots \\ X_{2 j_k} & X_{1 j_k} & X_{j_3 j_k} & \cdots & X_{j_k j_k} \end{pmatrix}, \\
&= -\det\begin{pmatrix} X_{21} & X_{11} & X_{j_3 1} & \cdots & X_{j_k 1} \\ X_{22} & X_{12} & X_{j_3 2} & \cdots & X_{j_k 2} \\ X_{2 j_3} & X_{1 j_3} & X_{j_3 j_3} & \cdots & X_{j_k j_3} \\ \vdots & \vdots & \vdots & & \vdots \\ X_{2 j_k} & X_{1 j_k} & X_{j_3 j_k} & \cdots & X_{j_k j_k} \end{pmatrix}, \\
&= \det\begin{pmatrix} X_{11} & X_{21} & X_{j_3 1} & \cdots & X_{j_k 1} \\ X_{12} & X_{22} & X_{j_3 2} & \cdots & X_{j_k 2} \\ X_{1 j_3} & X_{2 j_3} & X_{j_3 j_3} & \cdots & X_{j_k j_3} \\ \vdots & \vdots & \vdots & & \vdots \\ X_{1 j_k} & X_{2 j_k} & X_{j_3 j_k} & \cdots & X_{j_k j_k} \end{pmatrix}, \\
&= \det\begin{pmatrix} X_{11} & X_{12} & X_{1 j_3} & \cdots & X_{1 j_k} \\ X_{21} & X_{22} & X_{2 j_3} & \cdots & X_{2 j_k} \\ X_{j_3 1} & X_{j_3 2} & X_{j_3 j_3} & \cdots & X_{j_3 j_k} \\ \vdots & \vdots & \vdots & & \vdots \\ X_{j_k 1} & X_{j_k 2} & X_{j_k j_3} & \cdots & X_{j_k j_k} \end{pmatrix}^T, \\
&= \left(E(G,G)\right)^{\mathbb{X}_2}.
\end{aligned}
$$

Ahora, note que

$$
\psi\varphi\left(\phi_1^{(0)}\right)^{\mathbb{X}_1} = \psi\varphi\left(\sum_{j=1}^{n-1} X_{jj}\right) = \sum_{j=1}^{n-1} X_{jj} = \left(\sum_{j=1}^{n} X_{jj}\right)^{\mathbb{X}_2} = \left(\phi_1^{(0)}\right)^{\mathbb{X}_2}.
$$

Para $i = 2, \ldots, n$, se tiene

$$
\phi_i^{(0)} = \sum_{J\in\mathcal{P}([3,n],i)} E(J,J) + \sum_{J\in\mathcal{P}([3,n],i-2)} E(G,G) + \sum_{J\in\mathcal{P}([3,n],i-1)} \left(E(C,C)+E(D,D)\right),
$$

y por los cálculos anteriores, se obtiene

$$\psi\varphi\left(\sum_{J\in\mathcal{P}([3,n],i)} E(J,J)\right)^{\mathbb{X}_1} = \left(\sum_{J\in\mathcal{P}([3,n],i)} E(J,J)\right)^{\mathbb{X}_2}$$

$$\psi\varphi\left(\sum_{J\in\mathcal{P}([3,n],i-1)} E(C,C)\right)^{\mathbb{X}_1} = \left(\sum_{J\in\mathcal{P}([3,n],i-1)} E(D,D)\right)^{\mathbb{X}_2}$$

$$\psi\varphi\left(\sum_{J\in\mathcal{P}([3,n],i-1)} E(D,D)\right)^{\mathbb{X}_1} = \left(\sum_{J\in\mathcal{P}([3,n],i-1)} E(C,C)\right)^{\mathbb{X}_2}$$

$$\psi\varphi\left(\sum_{J\in\mathcal{P}([3,n],i-2)} E(G,G)\right)^{\mathbb{X}_1} = \left(\sum_{J\in\mathcal{P}([3,n],i-2)} E(G,G)\right)^{\mathbb{X}_2}.$$

Por lo tanto,

$$\psi\varphi\left(\phi_i^{(0)}\right)^{\mathbb{X}_1} = \psi\varphi\left(\phi_i^{(0)}\right)^{\mathbb{X}_2}, \text{ para toda } i = 1, \ldots, n.$$

Ahora, para $i = 2, \ldots, n$, considere el conjunto $\mathcal{J}_i = \{\{1, 2, j_3, \ldots, j_i\} : 3 \leq j_3 < \cdots < j_i \leq n\}$, luego

$$\left(\widehat{\phi_i^{(1)}}\right)^{\mathbb{X}_1} = \left(\sum_{\substack{J\in\mathcal{J}_i \\ j_i\neq n}} E\left(J-\{1\}, J-\{2\}\right)\right)^{\mathbb{X}_1} + \left(\sum_{\substack{J\in\mathcal{J}_i \\ j_i=n}} E\left(J-\{1\}, J-\{2\}\right)\right)^{\mathbb{X}_1},$$

si $j_i \neq n$, entonces

$$\left(E\left(J-\{1\}, J-\{2\}\right)\right)^{\mathbb{X}_1} = \det\begin{pmatrix} X_{21} & X_{2j_3} & \cdots & X_{2j_i} \\ X_{j_31} & X_{j_3j_3} & \cdots & X_{j_3j_i} \\ \vdots & \vdots & & \vdots \\ X_{j_i1} & X_{j_ij_3} & \cdots & X_{j_ij_i} \end{pmatrix},$$

y en el caso $j_i = n$, se tiene

$$\begin{aligned}
\left(E\left(J-\{1\}, J-\{2\}\right)\right)^{\mathbb{X}_1} &= \det\begin{pmatrix} X_{21} & X_{2j_3} & \cdots & X_{2j_{i-1}} & X_{2n} \\ X_{j_31} & X_{j_3j_3} & \cdots & X_{j_3j_{i-1}} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ X_{j_{i-1}1} & X_{j_{i-1}j_3} & \cdots & X_{j_{i-1}j_{i-1}} & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} = 0 \\
&= \left(E\left(J-\{1\}, J-\{2\}\right)\right)^{\mathbb{X}_2}.
\end{aligned}$$

Luego,

$$\begin{aligned}
\psi\varphi\left(\widehat{\phi_i^{(1)}}\right)^{\mathbb{X}_1} &= \sum_{\substack{J\in\mathcal{J}_i \\ j_i\neq n}} \det\begin{pmatrix} X_{21} & X_{j_31} & \cdots & X_{j_i1} \\ X_{2j_3} & X_{j_3j_3} & \cdots & X_{j_ij_3} \\ \vdots & \vdots & & \vdots \\ X_{2j_i} & X_{j_3j_i} & \cdots & X_{j_ij_i} \end{pmatrix} \\
&= \sum_{\substack{J\in\mathcal{J}_i \\ j_i\neq n}} \det\begin{pmatrix} X_{21} & X_{2j_3} & \cdots & X_{2j_i} \\ X_{j_31} & X_{j_3j_3} & \cdots & X_{j_3j_i} \\ \vdots & \vdots & & \vdots \\ X_{j_i1} & X_{j_ij_3} & \cdots & X_{j_ij_i} \end{pmatrix}^T \\
&= \left(\sum_{\substack{J\in\mathcal{J}_i \\ j_i\neq n}} E\left(J-\{1\}, J-\{2\}\right)\right)^{\mathbb{X}_2} = \left(\widehat{\phi_i^{(1)}}\right)^{\mathbb{X}_2}.
\end{aligned}$$

Por tanto, $\mathcal{A} \cong \mathcal{B}$. $\square$

APÉNDICE A

Complementos

A.1 Sobre el Teorema de Engel

Proposición A.1. Con las condiciones del Teorema (1.8), el subespacio

$$W = \{w \in V : x(w) = \lambda_x w, \text{ para todo endomorfismo } x \in \mathfrak{s}\}$$

es $\mathfrak{g}$-invariante.

Sea w un vector de W y escoja un endomorfismo $y \in \mathfrak{g}$, se mostrará que dado un endomorfismo $x \in \mathfrak{s}$, se cumple $x(y(w)) = \lambda_x y(w)$. Note que esta igualdad es clara para $w = \mathbf{0}$, entonces se puede aceptar $w \neq \mathbf{0}$. Dado que $\mathfrak{s}$ es un ideal de $\mathfrak{g}$, se tiene $[x, y] \in \mathfrak{s}$, y esto implica

$$xy(w) = yx(w) + [x, y](w) = \lambda_x y(w) + \lambda_{[x,y]} w. \tag{A.1}$$

El enunciado de esta proposición se obtiene con $\lambda_{[x,y]} = 0$. Para ello, se mostrará que a todo endomorfismo $x \in \mathfrak{s}$ se le puede asociar un subespacio x-invariante $M \subseteq W$ y una base B de M, tal que la matriz $[x]_B$, del endomorfismo x en la base B, es triangular superior con entradas de la diagonal principal todas iguales al escalar λ_x. Sea

$$k = \text{máx } \left\{ t \in \mathbb{Z}^+ : w, y(w), \ldots, y^t(w) \text{ son linealmente independientes} \right\},$$

y considere el conjunto linealmente independiente $B = \{w, y(w), \ldots, y^k(w)\}$, luego B es una base para el subespacio $M = span(B) \subseteq W$. Para cada entero $j \geq 0$, considere los subespacios

$$M_j = span \left\{ w, y(w), \ldots, y^j(w) \right\},$$

observe que

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M_j = M, \text{ para todo entero } j \geq k.$$

además,

$$y\left(M_j\right) \subseteq span \left\{ w, y(w), \ldots, y^{j+1}(w) \right\} \subseteq M_{j+1}. \tag{A.2}$$

Ahora se probará por inducción que para cada entero positivo j existe un vector $u_j \in M_{j-1}$, tal que

$$xy^j(w) = \lambda_x y^j(w) + u_j \in M_j.$$

La ecuación (A.1), implica que existe un vector $u_1 \in M_0$, tal que

$$xy(w) = \lambda_x y(w) + u_1 \in M_1.$$

Suponga que $n \in \mathbb{Z}^+$, y que el enunciado es válido para todo entero positivo $j \leq n$, entonces

$$xy^{n+1}(w) = xy\left(y^n(w)\right) = \left(yx + [x, y]\right)\left(y^n(w)\right) = y\left(xy^n(w)\right) + [x, y]y^n(w),$$

por hipótesis de inducción

$$y\left(xy^n(w)\right) = y\left(\lambda_x y^n(w) + u_n\right) = \lambda_x y^{n+1}(w) + y\left(u_n\right),$$

para algún vector $u_n \in M_{n-1}$, luego

$$xy^{n+1}(w) = \lambda_x y^{n+1}(w) + y\left(u_n\right) + [x, y]y^n(w). \tag{A.3}$$

Observe que $y\left(u_n\right) \in M_n$. Sea $z_0 = x$ y para cada entero $j \geq 1$, considere el endomorfismo $z_j = \left[z_{j-1}, y\right] \in \mathfrak{s}$. Recuerde que todo endomorfismo en $\mathfrak{s}$ actúa como el producto por un escalar sobre cada vector de W, entonces

$$z_1 y(w) = (yz_1 + z_2)(w) = \lambda_{z_1} y(w) + \lambda_{z_2} w \in M_1.$$

También,

$$z_1 y^2(w) = (yz_1 + z_2)\, y(w) = y\,(z_1 y(w)) + yz_2(w) + z_3(w) \in M_2.$$

Al continuar con esta recurrencia, se obtiene

$$[x, y]y^n(w) = z_1 y^n(w) \in M_n.$$

Entonces el vector $u_{n+1} = y\,(u_n) + [x, y]y^n(w)$ está en M_n, y sustituyendo en la igualdad (A.3), se deduce que

$$xy^{n+1}(w) = \lambda_x y^{n+1}(w) + u_{n+1} \in M_{n+1}.$$

En consecuencia, el subespacio M es x-invariante, y la matriz $[x]_B$ del endomorfismo x en la base B de M es triangular superior, además, todas las entradas de la diagonal principal de $[x]_B$ son iguales al escalar λ_x. Dado que $z_1 = [x, y] \in \mathfrak{s}$, se obtiene $tr([z_1]_B) = n\lambda_{[x,y]}$. Las propiedades de la traza implican

$$tr([z_1]_B) = tr([xy]_B) - tr([yx]_B) = 0.$$

Es decir, $n\lambda_{[x,y]} = 0$, de aquí se obtiene, $\lambda_{[x,y]} = 0$. Por tanto, W es $\mathfrak{g}$-invariante.

A.2 Extensiones de cuerpos

El propósito de esta sección es presentar la prueba del **Lema de Zariski**, que se utiliza en la demostración del **Teorema de los ceros de Hilbert** (3.3). Se asume que el lector está familiarizado con los conceptos y resultados fundamentales de la teoría de anillos conmutativos, como son: dominio entero, dominio de ideales principales (DIP), dominio de factorización única (DFU), cuerpo, elemento irreducible, entre otros.

Definición A.1 (Extensiones de cuerpo). Sean K y k dos cuerpos.

1. Se dice que K es una **extensión** de k, si existe un subcuerpo $\widehat{\mathrm{k}}$, contenido en K, tal que $\widehat{\mathrm{k}} \cong \mathrm{k}$. En este caso, se puede ver a k como un subcuerpo de K y se denota con $K|\mathrm{k}$.
2. La extensión $K|\mathrm{k}$ se denomina de **tipo finito** si existen $b_1, \ldots, b_n \in K$, tales que cada elemento $a \in K$, se puede expresar en la forma $f\,(b_1, \ldots, b_n) = a$, para algún polinomio $f \in \mathrm{k}\,[X_1, \ldots, X_n]$. Para denotar que la extensión $K|\mathrm{k}$

es de tipo finito, se escribe $K = \mathrm{k}[b_1, \ldots, b_n]$, y los elementos $b_1, \ldots, b_n$ se denominan **generadores** de K sobre k.

3. Si $K|\mathrm{k}$, entonces K tiene una estructura natural de espacio vectorial sobre el cuerpo k. La dimensión de K sobre k es el **grado de la extensión** y se denota $[K : \mathrm{k}]$. La extensión $K|\mathrm{k}$ es finita si $[K : \mathrm{k}] < \infty$, caso contrario, la extensión es infinita.
4. Considere la extensión $K|\mathrm{k}$ y sea b un elemento de K. Se dice que b es **algebraico** sobre k si existe un polinomio no nulo $f \in \mathrm{k}[X]$, tal que $f(b) = 0$. Si b no es algebraico, se dice que b es **trascendente** sobre k. La extensión $K|\mathrm{k}$ es **algebraica** si todo elemento de K es algebraico sobre el cuerpo k, caso contrario, se dice que la extensión $K|\mathrm{k}$ es trascendente.
5. Considere la extensión $K|\mathrm{k}$ y sean $b_1, \ldots, b_n \in K$. Con $\mathrm{k}(b_1, \ldots, b_n)$ se denota el menor subcuerpo de K que es extensión de k y contiene a todos los b_i. Es decir, si F es un subcuerpo de K, los elementos $b_1, \ldots, b_n \in F$ y $F|\mathrm{k}$, entonces $\mathrm{k}(b_1, \ldots, b_n) \subseteq F$. La extensión $K|\mathrm{k}$ se denomina **simple** si $K = \mathrm{k}(b)$, para algún elemento $b \in K$.

Ejemplo A.1. Con base en las definiciones anteriores, se tiene

1. La extensión $\mathbb{C}|\mathbb{R}$ es finita porque $\{1, i\}$ es una base de $\mathbb{C}$ sobre $\mathbb{R}$.

2. Todo elemento $a \in \mathrm{k}$ es algebraico sobre k, porque es un cero del polinomio $X - a$.

3. El número $\sqrt{2} \in \mathbb{R}$ es algebraico sobre el cuerpo $\mathbb{Q}$ de los números racionales, porque es una raíz del polinomio $X^2 - 2 \in \mathbb{Q}[X]$.

4. Dado cualquier polinomio no cero $f \in \mathbb{Q}[X]$, se sabe que $f(\pi) \neq 0$, por tanto el número real π es trascendente sobre $\mathbb{Q}$.

5. Si $b_1, \ldots, b_n \in \mathrm{k}$, entonces $\mathrm{k}(b_1, \ldots, b_n) = \mathrm{k}$, por esta razón, cuando se utiliza la extensión $\mathrm{k}(b_1, \ldots, b_n)$ se asume que $b_1, \ldots, b_n \notin \mathrm{k}$.

Teorema A.1. Toda extensión finita es de tipo finito y algebraica.

Demostración. Suponga que $K|\mathrm{k}$ es finita de grado n y sea $\{b_1, \ldots, b_n\}$ una base de K sobre k. Entonces para cada $c \in K$ existen escalares $a_1, \ldots, a_n \in \mathrm{k}$, tales que

$$c = a_1 b_1 + \cdots + a_n b_n,$$

esto implica que el polinomio $f = a_1X_1 + \cdots + a_nX_n$ está en el anillo $\mathrm{k}[X_1, \ldots, X_n]$, y

$$f(b_1, \ldots, b_n) = a_1b_1 + \cdots + a_nb_n = c.$$

Por tanto, $K|\mathrm{k}$ es de tipo finito. Por otro lado, el conjunto $\{1, c, \ldots, c^n\}$ es linealmente dependiente sobre k, entonces debe existir $c^t \in span\left\{1, c, \ldots, c^{t-1}\right\}$, es decir

$$a_0 + a_1c + \cdots + a_{r-1}c^{t-1} = c^t.$$

para algunos escalares $a_0, a_1, \ldots, a_{t-1} \in \mathrm{k}$. En consecuencia, c es una raíz del polinomio no nulo

$$f = X^r - a_{r-1}X^{r-1} - \cdots - a_1X - a_0 \in \mathrm{k}[X],$$

por tanto, c es algebraico sobre k. $\square$

Observación A.1. La extensión $\mathbb{R}|\mathbb{Q}$ no es algebraica, porque $\pi \in \mathbb{R}$ es trascendente sobre $\mathbb{Q}$. Por el Teorema (A.1), el cuerpo $\mathbb{R}$ es un $\mathbb{Q}$-espacio vectorial de dimensión infinita.

Considere la extensión $K|\mathrm{k}$, y para cada $b \in K$ sea $\varepsilon_b : \mathrm{k}[X] \longrightarrow K$ el homomorfismo de evaluación en b, definido por

$$\varepsilon_b(f) = f(b).$$

Por definición, b es algebraico sobre k, si y solo si, $Ker(\varepsilon_b) \neq \{0\}$. Dado que $\mathrm{k}[X]$ es un DIP, existe un polinomio irreducible $f \in \mathbb{K}[X]$, tal que $Ker(\varepsilon_b) = \langle f \rangle$. En este caso, $Ker(\varepsilon_b)$ es un ideal maximal del anillo $\mathrm{k}[X]$, y se tiene el siguiente enunciado: Un elemento $b \in K$ es algebraico sobre el cuerpo k, si y solo si, el anillo cociente $\dfrac{\mathrm{k}[X]}{Ker(\varepsilon_b)}$ es un cuerpo. También, si a es el coeficiente principal del polinomio f, entonces $f_{b,\mathrm{k}} = \dfrac{1}{a}f$ es un polinomio mónico irreducible sobre k, tal que $Ker(\varepsilon_b) = \langle f_{b,\mathrm{k}} \rangle$. Se puede probar que el polinomio $f_{b,\mathrm{k}}$ es único y se denomina el **polinomio minimal** de b sobre k. Por ejemplo

$$f_{\sqrt{2},\mathbb{Q}} = X^2 - 2 \quad \text{y} \quad f_{\sqrt{2},\mathbb{R}} = X - \sqrt{2}.$$

Cuando no haya ambigüedad sobre el cuerpo base k, se utilizará la notación f_b en lugar de $f_{b,\mathrm{k}}$.

Ejemplo A.2. Sea $K|\mathrm{k}$ una extensión de tipo finito con un único generador, probar que $K|\mathrm{k}$ es finita.

Demostración. Sea b el generador, luego todo elemento de K se puede expresar como un polinomio en b, con coeficientes en el cuerpo k, entonces

$$K = \{f(b) : f \in \mathbb{K}[X]\} = \mathrm{k}[b].$$

Note que b es trascendente sobre k, si y solo si, $Ker\,(\varepsilon_b) = \{0\}$, y en este caso $\mathrm{k}[b]$ es un dominio entero, pero no un cuerpo. Así que b debe ser algebraico sobre k, por ende existe el polinomio minimal $f_{b,\mathrm{k}}$. Suponga que

$$f_{b,\mathrm{k}} = a_0 + a_1 X + \cdots a_{n-1} X^{n-1} + X^n,$$

entonces

$$b^n = -\left(a_0 + a_1 b + \cdots a_{n-1} b^{n-1}\right) \in span\left\{1, b, \ldots, b^{n-1}\right\}.$$

Luego,

$$b^{n+1} = bb^n \in span\left\{b, \ldots, b^{n-1}, b^n\right\} \subseteq span\left\{1, b, \ldots, b^{n-1}\right\}.$$

Lo anterior implica que

$$b^r \in span\left\{1, b, \ldots, b^{n-1}\right\}, \text{ para todo entero } r \geq 0.$$

De aquí, se obtiene

$$K = \mathrm{k}\,[b] = span\left\{1, b, \ldots, b^{n-1}\right\}.$$

Dado que el polinomio $f_{b,\mathrm{k}}$ es irreducible de grado n, se sigue que $\left\{1, b, \ldots, b^{n-1}\right\}$ es linealmente independiente sobre k, por tanto $[K : \mathrm{k}] = n$. □

Sea D un dominio entero, el **cuerpo de cocientes** del dominio D es el menor cuerpo que contiene a D, y está dado por

$$\mathrm{k} = \left\{\frac{a}{b} : a, b \in D, b \neq 0\right\}.$$

Sean D y R dos dominios, con $D \subseteq R$. Un elemento $b \in R$ es **entero** sobre D si existe un polinomio mónico $f \in D[X]$, tal que $f(b) = 0$. Si $b, c \in R$ son enteros sobre D, se puede probar que $b \pm c$ y bc también son enteros sobre D.

Ejemplo A.3. Sea D un DFU con cuerpo de cocientes K. Si $x \in K$ es entero sobre D, probar que $x \in D$.

Demostración. El enunciado es claramente válido cuando $x = 0$, así que, puede suponer que $x \neq 0$, y escoja un polinomio mónico $f = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} + X^n \in D[X]$, de grado n, tal que $f(x) = 0$. Como K es el cuerpo de cocientes del DFU D, se tiene

$$x = \frac{a}{b}, \text{ para algún par de coprimos } a, b \in D.$$

Luego

$$a^n = -b\left(c_0 b^{n-1} + c_1 b^{n-2} a + \cdots + c_{n-2} b a^{n-2} + c_{n-1} a^{n-1}\right),$$

en consecuencia, $b \mid a^n$. Note que si p es irreducible y $p \mid b$, entonces $p \mid a$ y esto contradice el hecho de que a y b son coprimos. Lo anterior implica que b no tiene factores irreducibles, por tanto b debe ser una unidad en D, y se obtiene $x = \frac{a}{b} = ab^{-1} \in D$. □

Teorema A.2. Sea D un dominio entero con cuerpo de cocientes k. Si $K|$k y $s \in K$ es algebraico sobre k, entonces existe un elemento no cero $r \in D$, tal que rs es entero sobre D.

Demostración. Sea $f_s = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n$ el polinomio minimal de s sobre el cuerpo k, entonces

$$a_0 + a_1 s + \cdots + a_{n-1} s^{n-1} + s^n = 0.$$

Como k es el cuerpo de cocientes del dominio entero D y los a_i son elementos de k, entonces para cada a_i existe un $r_i \in D$, con $r_i \neq 0$, tal que $r_i a_i \in D$. Tomando el elemento no cero $r = r_0 r_1 \cdots r_{n-1} \in D$, se tiene

$$r^n\left(a_0 + a_1 s + \cdots + a_{n-1} s^{n-1} + s^n\right) = 0.$$

Para cada $i = 0, 1, \ldots, n-1$ sea $c_i = r^{n-i} a_i \in D$, se sigue que

$$c_0 + c_1 (rs) + \cdots + c_{n-1} (rs)^{n-1} + (rs)^n = 0,$$

entonces $f = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} + X^n$ es un polinomio mónico de $D[X]$ y se cumple $f(rs) = 0$. □

Teorema A.3 (Lema de Zariski). Si $K|$k es una extensión de tipo finito, entonces $K|$k es algebraica.

Demostración. Por inducción sobre el número n de generadores. El caso $n = 1$ se presentó en el Ejemplo (A.2). Suponga que el enunciado es válido para extensiones de tipo finito con máximo $n - 1$ generadores, y sea $K|$k una extensión de tipo finito con n generadores $b_1, \ldots, b_n$, es decir, todo elemento de K se puede expresar como un polinomio en los b_i, con coeficientes en k. Se probará que todos los b_i son algebraicos sobre k, para ello, suponga lo contrario, y sin pérdida de generalidad considere que b_1 es uno de los generadores trascendentes sobre k. Luego, $\mathrm{k}\left[b_1\right] = \left\{f\left(b_1\right) : f \in \mathrm{k}[X]\right\}$, es un dominio entero y $\mathrm{k}\left(b_1\right) = \left\{\dfrac{f\left(b_1\right)}{g\left(b_1\right)} : f, g \in \mathrm{k}[X], g\left(b_1\right) \neq 0\right\}$ es su cuerpo de cocientes. Entonces, la extensión $K\left|\mathrm{k}\left(b_1\right)\right.$ es de tipo finito con generadores $b_2, \ldots, b_n$, y por la hipótesis de inducción, esta extensión es algebraica. Por el Teorema (A.2), para cada $i = 2, \ldots, n$ existe un elemento no cero $r_i \in \mathrm{k}\left[b_1\right]$, tal que $r_i b_i$ es entero sobre $\mathrm{k}\left[b_1\right]$. Ahora, sea $r = r_2 \cdots r_n \in D$ y escoja un elemento no cero $a \in K$, entonces existe un polinomio no nulo $f \in \mathrm{k}\left[X_1, X_2, \ldots, X_n\right]$, tal que $f\left(b_1, b_2 \cdots b_n\right) = a$. Suponga que N es el grado absoluto del polinomio f, y denote con $\mathcal{L} = a_j X_1^{t_1} X_2^{t_2} \cdots X_n^{t_n}$ a uno de los monomios en f, se tiene

$$r^N \mathcal{L}\left(b_1, b_2 \cdots b_n\right) = r^N a_j b_1^{t_1} \prod_{i=2}^{n} b_i^{t_i} = a_j \left(\prod_{i=2}^{n} r_i^{N-t_i}\right) b_1^{t_1} \prod_{i=2}^{n} \left(r_i b_i\right)^{t_i}.$$

Dado que

$$a_j \left(\prod_{i=2}^{n} r_i^{N-t_i}\right) b_1^{t_1} \in \mathrm{k}\left[b_1\right] \quad \text{y} \quad \prod_{i=2}^{n} \left(r_i b_i\right)^{t_i} \text{ es entero sobre k,}$$

se sigue que $r^N \mathcal{L}\left(b_1, b_2 \cdots b_n\right)$ es entero sobre k. Esto implica que $r^N a$ es entero sobre k, en particular, para el elemento $\dfrac{1}{b_1} \in \mathrm{k}\left(b_1\right) \subseteq K$ existe un entero $m > 0$, tal que $\dfrac{r^m}{b_1}$ es entero sobre $\mathrm{k}\left[b_1\right]$. Pero $\mathrm{k}\left[b_1\right]$ es un DFU, de lo expuesto en el Ejemplo (A.3), se deduce que $\dfrac{r^m}{b_1} \in \mathrm{k}\left[b_1\right]$. Luego, existen elementos $c_0, c_1, \ldots, c_t \in \mathrm{k}$, tales que

$$c_0 + c_1 b_1 + \cdots + c_t b_1^t = \frac{r^m}{b_1}.$$

Esto implica que b_1 es una raíz del polinomio no nulo

$$g = -r^m + c_0 X + c_1 X^2 + \cdots + c_t X^{t+1} \in \mathrm{k}[X],$$

lo que es imposible, porque b_1 es trascendente sobre k. Por tanto, los elementos $b_1, b_2, \ldots, b_n$ son algebraicos sobre k, y dado que la suma y multiplicación de elementos algebraicos es también algebraico, entonces la extención $K|\mathrm{k}$ es algebraica. □

A.3 Grado de trascendencia de una extensión

El grado de trascendencia de una extensión de cuerpos es un concepto fundamental del álgebra abstracta que permite estudiar la dimensión de una variedad algebraica afín, concepto relevante para clasificar y entender las variedades desde un punto de vista teórico, además de tener aplicaciones prácticas en áreas como la teoría de números, la física teórica y la computación algebraica.

Definición A.2 (**Independencia algebraica**). Sea $K|\mathrm{k}$ una extensión trascendente de cuerpos. Un conjunto no vacío $A \subseteq K$ es **algebraicamente independiente** sobre k si para cualquier selección de elementos $a_1, \ldots, a_n \in A$, el homomorfismo de k-álgebras $\varphi : \mathrm{k}[X_1, \ldots, X_n] \longrightarrow K$ definido por

$$\varphi(f) = f(a_1, \ldots, a_n),$$

es inyectivo. Caso contrario, se dice que A es **algebraicamente dependiente** sobre el cuerpo k.

Ejemplo A.4. Sea $K|\mathrm{k}$ una extensión de cuerpos, se tiene

1. El conjunto unitario $\{a\} \subseteq K$ es algebraico sobre el cuerpo k, si y solo si, existe un polinomio no nulo $f \in \mathrm{k}[Y]$, tal que $f(a) = 0$. En consecuencia, f es un polinomio no nulo de $\mathrm{k}[Y, X_1, \ldots, X_n]$, y dados elementos arbitrarios $b_1, \ldots, b_n \in K$, se deduce que $f(a, b_1, \ldots, b_n) = f(a) = 0$, y esto implica que el conjunto $\{a, b_1, \ldots, b_n\} \subseteq K$ es algebraicamente dependiente sobre k.

   Por lo anterior, si el conjunto $\{a_1, \ldots, a_n\} \subseteq K$ es algebraicamente independiente sobre k, entonces los elementos $a_1, \ldots, a_n$ son trascendentes sobre el cuerpo k. En ese sentido, es válido presentar un contraejemplo del recíproco de esta implicación.

2. Los números reales π y π^2 son trascendentes sobre el cuerpo $\mathbb{Q}$ de los números racionales. Sin embargo, no son algebraicamente independientes sobre $\mathbb{Q}$, porque existe el polinomio no nulo $f = X^2 - Y \in \mathbb{Q}[X, Y]$, tal que

$$f\left(\pi, \pi^2\right) = \pi^2 - \pi^2 = 0.$$

Definición A.3 (**Base de trascendencia**). Sea $K|\mathrm{k}$ una extensión trascendente de cuerpos. Una **base de trascendencia** para K sobre el cuerpo k es un conjunto $B \subseteq K$ que satisface las dos condiciones siguientes:

1. El conjunto B es algebraicamente independiente sobre k.
2. El cuerpo K es una extensión algebraica del cuerpo $\mathrm{k}(B)$.

Ejemplo A.5. El conjunto $\{\pi\}$ es una base de trascendencia para $\mathbb{Q}\left(\sqrt{2},\pi\right)$ sobre el cuerpo $\mathbb{Q}$, porque π es trascendente sobre $\mathbb{Q}$ y la extensión $\mathbb{Q}\left(\sqrt{2},\pi\right)|\mathbb{Q}(\pi)$ es algebraica.

Teorema A.4. Toda extensión trascendente contiene una base de trascendencia.

Demostración. Sea $K|\mathrm{k}$ una extensión trascendente. Luego, existe un elemento $b \in K$, trascendente sobre k, esto implica que el conjunto $\{b\}$ es algebraicamente independiente sobre el cuerpo k. Por ende, la colección $\mathcal{F}$ de subconjuntos de K, que son algebraicamente independientes sobre k, es no vacía. Sea

$$A_1 \subseteq \cdots \subseteq A_k \subseteq A_{k+1} \subseteq \cdots$$

una cadena de elementos de $\mathcal{F}$, y considere el subconjunto

$$A = \bigcup_{i=1}^{\infty} A_i \subseteq K.$$

Note que A es algebraicamente independiente sobre k, porque al escoger los elementos arbitrarios $a_1, \ldots, a_n \in A$, existe un entero $t > 0$, tal que $a_1, \ldots, a_n \in A_t$, y dado que A_t es algebraicamente independiente, se sigue que

$$f\left(a_1, \ldots, a_n\right) \neq 0, \text{ para todo polinomio } f \in \mathrm{k}\left[X_1, \ldots, X_n\right].$$

En consecuencia, $A \in \mathcal{F}$ y por el Lema de Zorn existe un elemento maximal $B \in \mathcal{F}$. Ahora, suponga que B no es una base de trascendencia para K sobre k, entonces la extensión $K|\mathrm{k}(B)$ es trascendente y debe existir un elemento $b \in K$ que es trascendente sobre el cuerpo $\mathrm{k}(B)$. Dado que todo cuerpo es una extensión algebraica sobre sí mismo, se deduce que $b \notin \mathrm{k}(B)$. Seleccione elementos $b_1, \ldots, b_m \in B$, y considere el homomorfismo de k-álgebras $\varphi : \mathrm{k}\left[X_1, \ldots, X_m, Y\right] \longrightarrow K$, definido por

$$\varphi(f) = f\left(b_1, \ldots, b_m, b\right).$$

Dado un polinomio $f \in \mathrm{k}\left[X_1, \ldots, X_m, Y\right]$, se infiere que existen polinomios $g_0, g_1, \ldots, g_r$ del anillo $\mathrm{k}\left[X_1, \ldots, X_m\right]$, tales que f se puede expresar de la forma

$$f = g_0 + g_1 Y + \cdots + g_r Y^r.$$

Para $i = 0, 1, \ldots, r$, sea $c_i = g_i\left(b_1, \ldots, b_m\right) \in \mathrm{k}(B)$, entonces $h = c_0 + c_1 Y + \cdots + c_r Y^r$ es un polinomio del anillo $\mathrm{k}\left(b_1, \ldots, b_m\right)[Y]$, y se tiene

$$h(b) = f\left(b_1, \ldots, b_m, b\right).$$

En particular, si $f \in Ker(\varphi)$, se garantiza $h(b) = f\left(b_1, \ldots, b_m, b\right) = 0$. Del hecho que b

es trascendente sobre el cuerpo $\mathrm{k}(B)$, se obtiene $h = 0$, luego

$$c_0 = c_1 = \cdots = c_r = 0,$$

por ende,

$$g_i(b_1, \ldots, b_m) = c_i = 0, \text{ para toda } i = 0, 1, \ldots, r.$$

Pero B es algebraicamente independiente sobre el cuerpo k y cada uno de los polinomios g_i está en el anillo $\mathrm{k}[X_1, \ldots, X_m]$, entonces $g_i = 0$, para toda $i = 0, 1 \ldots, r$. Luego

$$f = g_0 + g_1 Y + \cdots + g_m Y^m = 0,$$

y esto significa que el homomorfismo φ es inyectivo, es decir, $B \cup \{b\}$ es un subconjunto de K, algebraicamente independiente sobre k. Entonces, $B \cup \{b\}$ es un elemento de la colección $\mathcal{F}$, pero esto es una contradicción, porque B es un elemento maximal de la colección $\mathcal{F}$ y $b \notin B$. Por tanto, B es una base de trascendencia para K sobre k. $\square$

Proposición A.2. Sea $K|\mathrm{k}$ una extensión trascendente de cuerpos. Si $L \subseteq K$ es un conjunto algebraicamente independiente sobre k, entonces existe una base de trascendencia B para K sobre el cuerpo k, tal que $L \subseteq B$.

Demostración. Considere la colección

$$\mathcal{F} = \{A \subseteq K : L \subseteq A \text{ y } A \text{ es algebraicamente independiente sobre k}\}.$$

Claramente $\mathcal{F} \neq \emptyset$, porque $L \in \mathcal{F}$ y por el Lema de Zorn la colección $\mathcal{F}$ tiene un elemento maximal B. Entonces $L \subseteq B$, y de forma similar al proceso de prueba del Teorema (A.4), se obtiene que B es una base de trascendencia para K sobre el cuerpo k. $\square$

Corolario A.1. Sea $K|\mathrm{k}$ una extensión trascendente y sea B un subconjunto de K. El conjunto B es una base de trascendencia para K sobre el cuerpo k, si y solo si, B es un conjunto algebraicamente independiente maximal.

Demostración. Primero acepte que B es una base de trascendencia para K sobre k. Por la proposición anterior existe un conjunto algebraicamente independiente maximal $\widehat{B}$, tal que $B \subseteq \widehat{B}$. Por contradicción suponga que $\widehat{B} \neq B$, entonces es posible escoger un elemento $a \in \widehat{B} - B$. Dado que la extensión $K|\mathrm{k}(B)$ es algebraica, existen elementos $b_1, \ldots, b_n \in B$ y un polinomio no nulo $f \in \mathrm{k}(b_1, \ldots, b_n)[Y]$, tales que $f(a) = 0$. Luego f es de la forma

$$f = \sum_{i=0}^{t} \frac{g_i(b_1, \ldots, b_n)}{h_i(b_1, \ldots, b_n)} Y^i,$$

en la cual los g_i y los h_i son polinomios del anillo $\mathrm{k}[X_1, \ldots, X_n]$. Ahora, considere el polinomio no nulo $H = h_0 h_1 \cdots h_t$, y para cada $i = 0, 1, \ldots, t$ defina los polinomios $\widehat{H}_i$ como sigue

$$\widehat{H}_i = \frac{H g_i}{h_i} \in \mathrm{k}[X_1, \ldots, X_n].$$

Note que algún $\widehat{H}_i \neq 0$, porque $f \neq 0$, y se tiene el polinomio no nulo

$$F = \sum_{i=0}^{t} \widehat{H}_i Y^i \in \mathrm{k}[X_1, \ldots, X_n, Y],$$

tal que

$$F(b_1, \ldots, b_n, a) = \sum_{i=0}^{t} \widehat{H}_i (b_1, \ldots, b_n) a^i = H(b_1, \ldots, b_n) f(a) = 0.$$

Pero esto es imposible porque $\{b_1, \ldots, b_n, a\} \subseteq \widehat{B}$ y $\widehat{B}$ es algebraicamente independiente sobre k. Por tanto, B es un conjunto algebraicamente independiente maximal. El recíproco se deduce inmediatamente de la Proposición (A.2). □

Teorema A.5. Sea $K|\mathrm{k}$ una extensión trascendente de cuerpos. Si existe una base de trascendencia finita para K sobre k, entonces todas las bases de trascendencia para K sobre k son finitas y tienen la misma cantidad de elementos.

Demostración. Sea $B = \{b_1, \ldots, b_n\}$ una base de trascendencia para K sobre k, y suponga que A es otra base de trascendencia. Entonces la extensión $K|\mathrm{k}(b_1, \ldots, b_n)$ es algebraica y para cada elemento $a_1 \in A$ debe existir un polinomio no nulo $f \in \mathrm{k}(b_1, \ldots, b_n)[Y]$, tal que $f(a_1) = 0$. Luego f es de la forma

$$f = \sum_{i=0}^{t} \frac{g_i(b_1, \ldots, b_n)}{h_i(b_1, \ldots, b_n)} Y^i,$$

donde los g_i y los h_i son polinomios del anillo $\mathrm{k}[X_1, \ldots, X_n]$. Al igual que el Corolario (A.1), llamando $\widehat{H}_i$ al polinomio del anillo $\mathrm{k}[X_1, \ldots, X_n]$, definido por

$$\widehat{H}_i = (h_0 h_1 \cdots h_t) \frac{g_i}{h_i}, \text{ para toda } i = 0, 1, \ldots, t,$$

se tiene el polinomio no nulo

$$F = \sum_{i=0}^{t} \widehat{H}_i Y^i \in \mathrm{k}[X_1, \ldots, X_n, Y],$$

tal que $F(b_1, \ldots, b_n, a_1) = 0$. Dado que a_1 es trascendente sobre el cuerpo k, entonces el polinomio F debe ser de grado positivo con respecto de alguna de las variables X_i, y salvo una nueva numeración de las variables, se puede suponer que F es de grado positivo respecto de la variable X_1. Entonces existen polinomios $F_0, F_1, \ldots, F_r \in \mathrm{k}[X_2, \ldots, X_n, Y_1]$, tales que

$$F = F_0 + F_1X_1 + \ldots + F_rX_1^r,$$

así que

$$\widehat{F} = \sum_{i=0}^{r} F_i(b_2, \ldots, b_n, a_1) X_1^i$$

es un polinomio no nulo del anillo $\mathrm{k}(b_2, \ldots, b_n, a_1)[X_1]$, tal que

$$\widehat{F}(b_1) = \sum_{i=0}^{r} F_i(b_2, \ldots, b_n, a_1) b_1^i = F(b_1, \ldots, b_n, a_1) = 0,$$

esto significa que b_1 es algebraico sobre el cuerpo $\mathrm{k}(b_2, \ldots, b_n, a_1)$; por ende, la extensión $K\,|\mathrm{k}(b_2, \ldots, b_n, a_1)$ es algebraica. Además el conjunto $\{b_2, \ldots, b_n, a_1\}$ es algebraicamente independiente, porque en caso contrario existe un polinomio no nulo $f \in \mathrm{k}[X_2, \ldots, X_n, Y_1]$, tal que $f(b_2, \ldots, b_n, a_1) = 0$. Dado que a_1 es un elemento trascendente sobre el cuerpo k, entonces existen polinomios $f_0, f_1, \ldots, f_s \in \mathrm{k}[X_2, \ldots, X_n]$, en el que alguno de los f_j tiene grado absoluto positivo, tales que

$$f = f_0 + f_1Y_1 + \cdots + f_sY_1^s,$$

y se tiene el polinomio no nulo

$$\widehat{f} = f_0 + a_1f_1 + \cdots + a_1^sf_s \in \mathrm{k}[X_2, \ldots, X_n],$$

el cual satisface $\widehat{f}(b_2, \ldots, b_n) = 0$, pero esto es imposible, porque B es algebraicamente independiente. Por tanto, $\{b_2, \ldots, b_n, a_1\}$ es una base de transcendencia para K sobre k. Ahora suponga que para algún entero positivo t se han seleccionado elementos $a_1, \ldots, a_t$ de la base A, tales que el conjunto

$$C = (B - \{b_1, \ldots, b_t\}) \cup \{a_1, \ldots, a_t\}$$

es una base de trascendencia para K sobre el cuerpo k. Si $C \cap B \neq \emptyset$, entonces el Corolario (A.1) garantiza que $A - \{a_1, \ldots, a_t\} \neq \emptyset$, además, debe existir un elemento $a_{t+1} \in A - C$. Dado que la extensión $K\,|\mathrm{k}(C)$ es algebraica, entonces al aplicar un proceso similar al presentado en la prueba del colorario (A.1) se garantiza que existen polinomios $g_0, g_1, \cdots, g_s$ en el anillo $\mathrm{k}[X_{t+1}, \ldots, X_n, Y_1, \ldots, Y_t]$, tales que el polinomio

$$G = g_0 + g_1Y_{t+1} + \cdots + g_sY_{t+1}^s$$

es no nulo y satisface $G(b_{t+1}, \ldots, b_n, a_1, \ldots, a_t, a_{t+1}) = 0$. Observe que ninguno de los polinomios g_i puede tener grado positivo respecto de alguna de las variables Y_j, porque en el caso de que alguno de los g_i tenga grado positivo respecto de la variable Y_j, entonces al evaluar el polinomio G en el punto $P = \left(b_{t+1}, \ldots, b_n, a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_t\right)$, se obtiene el polinomio no nulo

$$G(P) = g_0(P) + g_1(P)Y_{t+1} + \cdots + g_s(P)Y_{t+1}^s,$$

con $G(P) \in \mathrm{k} \in \left[Y_j, Y_{t+1}\right]$, porque todos los $g_i(P) \in \mathrm{k}\left[Y_j\right]$. Además,

$$G(P)\left(a_j, a_{t+1}\right) = G\left(b_{t+1}, \ldots, b_n, a_1, \ldots, a_t, a_{t+1}\right) = 0.$$

Pero esto contradice el hecho de que A es algebraicamente independiente. Por tanto, todos los polinomios g_i pertenecen al anillo $\mathrm{k}\left[X_{t+1}, \ldots, X_n\right]$. Por lo expuesto en la parte inicial de esta prueba, se deduce que el conjunto $\left(C \cup \{a_{t+1}\}\right) - \{b_{t+1}\}$ es una base de trascendencia para K sobre el cuerpo k. El proceso de intercambiar elementos de B por elementos de la base A, termina cuando se haya formado una nueva base de trascendencia $\widehat{C} = \{a_1, \ldots, a_n\}$ contenida en A, y del hecho de que las bases de trascendencia son conjuntos algebraicamente independientes maximales se sigue que $A = \widehat{C}$, por tanto $|A| = |B|$. $\square$

Observación A.2. Sea $K|\mathrm{k}$ una extensión trascendente de cuerpos. Si una base de trascendencia para K sobre k es infinita, entonces toda base de trascendencia para K sobre k es infinita.

Ejemplo A.6. El conjunto de variables $\{X_1, \ldots, X_n\}$ es una base de trascendencia para el cuerpo $\mathrm{k}(X_1, \ldots, X_n)$ de funciones racionales, definido por

$$\mathrm{k}(X_1, \ldots, X_n) = \left\{\frac{f}{g} : f, g \in \mathrm{k}[X_1, \ldots, X_n], g \neq 0\right\}.$$

Definición A.4 (Grado de trascendencia). Sea $K|\mathrm{k}$ una extensión de cuerpos. El grado de trascendencia de K sobre k, denotado $grtr_{\mathrm{k}}K$, se define de la siguiente forma

1. Si la extensión $K|\mathrm{k}$ es algebraica, entonces $grtr_{\mathrm{k}}K = 0$.
2. Si la extensión $K|\mathrm{k}$ es trascendente y K contiene una base de trascendencia finita con n elementos, entonces $grtr_{\mathrm{k}}K = n$.
3. Si la extensión $K|\mathrm{k}$ es trascendente y K contiene una base de trascendencia infinita, entonces $grtr_{\mathrm{k}}K = \infty$.

Ejemplo A.7. El lector puede verificar que

1. La extención $\mathbb{C}\,|\mathbb{R}$ es algebraica, luego $grtr_{\mathbb{R}}\mathbb{C} = 0$.

2. El conjunto $B = \{\pi\}$ es una base de trascendencia para $\mathbb{Q}\left(\sqrt{2}, \pi\right)$ sobre el cuerpo $\mathbb{Q}$ de los números racionales, entonces $grtr_{\mathbb{Q}}\mathbb{Q}\left(\sqrt{2}, \pi\right) = 1$.

3. El conjunto $B = \{X_1, \ldots, X_n\}$ es una base de trascendencia para el cuerpo de funciones racionales $\mathrm{k}(X_1, \ldots, X_n)$, entonces
$$grtr_{\mathrm{k}}\mathrm{k}(X_1, \ldots, X_n) = |B| = n.$$

4. El Teorema de **Lindemann–Weierstrass** es un resultado fundamental en la teoría de números, y establece que si los reales $\alpha_1, \ldots, \alpha_n$ son algebaicos y linealmente independientes sobre $\mathbb{Q}$, entonces $e_1^{\alpha}, \ldots, e_n^{\alpha}$ son algebraicamente independientes sobre $\mathbb{Q}$. Sea $\overline{\mathbb{Q}}$ la clausura algebraica de $\mathbb{Q}$ en $\mathbb{R}$, es decir
$$\overline{\mathbb{Q}} = \{r \in \mathbb{R} : r \text{ es algebraico sobre } \mathbb{Q}\}.$$
No es difícil notar que la extensión $\overline{\mathbb{Q}}|\mathbb{Q}$ es infinita, luego existe un conjunto infinito B linealmente independiente sobre $\mathbb{Q}$, y esto implica que el conjunto
$$\widehat{B} = \left\{e^r : r \in \overline{\mathbb{Q}}\right\} \subseteq \mathbb{R},$$
es infinito y algebraicamente independiente. Por tanto, $grtr_{\mathbb{Q}}\mathbb{R} = \infty$.

Bibliografía

Auslander y Buchsbaum, D. (1959). Unique factorization in regular local rings. *National Academy of Sciences of the USA*, 45:733–734.

Cherrabi, A. (2010). Quasi-regular sequences and regular sequences. *Communications in Algebra - COMMUN ALGEBRA*, 39:184–188.

Futorny, V. y Molev, A. (2014). Quantization of the shift of argument subalgebras in type a. *Advances in Mathematics*, 285:1358–1375.

Futorny, V. y Ovsienko, S. (2003). Kostant's theorem for special filtered algebras. *Bulletin of the London Mathematical Society*, 37:187–199.

Futorny, V. y Ovsienko., S. (2005). Kostant's theorem for special filtered algebras. *Bulletin of the London Mathematical Society*, 37:187–199.

Hazrat, R. (2016). *Graded rings and graded Grothendieck groups*. Cambridge University Press. Cambridge University Press.

Humphreys, J. E. (1997). *Introduction to Lie Algebras and Representation Theory*. Springer-Verlag. Springer International Edition.

Kim, H. (6 de septiembre de 2024). *Regular sequences and regular rings*. https://sites.math.duke.edu/ ezra/358/regSeq.pdf.

Kostant, B. (2009). *Lie Group Representations On Polynomial Rings*, volumen 69, pp. 309–317.

Matsumura, H. (1987). *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics. Cambridge Studies in Advanced Mathematics.

Mishchenko, A. S. y Fomenko, A. T. (1978). Euler equations on finite dimensional lie groups. *Mathematics of the USSR-Izvestiya*, 12(2):371–389.

Mutis, W. (2016). Subalgebras de mishchenko-fomenko em s(gln) e sequências regulares.

Ovsienko, S. (2003). Strongly nilpotent matrices and gelfand–zetlin modules. *Linear Algebra and Its Applications - LINEAR ALGEBRA APPL*, 365:349–367.

Oystaeyen, F. y Nastasescu, C. (2004). *Methods of Graded Rings*. Springer-verlag.

Rabinowitsch, J. L. (1930). Zum hilbertschen nullstellensatz. *Mathematische Annalen*, 102:520–520.

SanMartin, L. (1999). *Álgebras de Lie*. Editora da Unicamp. Editora da Unicamp.

êditorial
Universidad de **Nariño**

Fecha de publicación: de 2025
San Juan de Pasto - Nariño - Colombia

La teoría de álgebras de Lie, cuyo desarrollo comenzó gracias a los trabajos de Sophus Lie en el siglo XIX, ocupa un lugar de importancia en la matemática moderna. La comprensión de esta teoría puede ser desafiante incluso para matemáticos experimentados, debido a la complejidad conceptual de sus temáticas y el requisito de tener conocimientos básicos de otras áreas como la geometría, el álgebra y la topología. El primer propósito de este texto es ofrecer una introducción comprensiva a las álgebras de Lie y sus representaciones, combinando rigor matemático con un enfoque didáctico, con el cual se espera que el lector alcance un mejor entendimiento de los temas que se exponen. El otro propósito es presentar, por un lado, las subálgebras de Mishchenko-Fomenko y, por otro, exponer el problema de determinar si estas subálgebras son generadas por una secuencia regular de polinomios.

El texto se estructura en cinco capítulos. El primero ofrece los fundamentos básicos de la teoría de álgebras de Lie. El segundo aborda una introducción general a las álgebras graduadas y filtradas haciendo énfasis en el álgebra envolvente universal de un álgebra de Lie de dimensión finita. El tercero elabora una sencilla pero rigurosa introducción a la geometría algebraica. El cuarto está dedicado a desarrollar el concepto de secuencias regulares en anillos conmutativos. El último capítulo desarrolla una presentación no rigurosa de las subálgebras de Mishchenko-Fomenko en S *(gl_n)*.

9 786287 771307

Universidad de Nariño
FUNDADA EN 1904

ai
Universidad de Nariño
ACREDITADA EN ALTA CALIDAD
RESOLUCIÓN MEN 000022 - ENERO 11 DE 2023

120 Años
Universidad de Nariño

editorial
Universidad de Nariño