UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

SECCIÓN DE MATEMÁTICA.

TEMA:

INTRODUCCIÓN A LAS ÁLGEBRAS DE LIE

PRESENTADO POR:

LUIS ALEXANDER FUENTES

VICTOR EDGARDO LÓPEZ SANDOVAL

ASESOR DIRECTOR:

LIC. JOSÉ FREDY VÁSQUEZ

ASESOR METODOLÓGICO:

LIC. JOSÉ ENRY GARCÍA

PARA OPTAR AL TITULO DE:

LICENCIADO EN MATEMÁTICA

CIUDAD UNIVERSITARIA DE ORIENTE, SAN MIGUEL,
EL SALVADOR, CENTRO AMÉRICA, AGOSTO DE 2013

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

SECCIÓN DE MATEMÁTICA.

TEMA:

INTRODUCCIÓN A LAS ÁLGEBRAS DE LIE

PRESENTADO POR:

LUIS ALEXANDER FUENTES

VICTOR EDGARDO LÓPEZ SANDOVAL

ASESOR DIRECTOR:

LIC. JOSÉ FREDY VÁSQUEZ

ASESOR METODOLÓGICO:

LIC. JOSÉ ENRY GARCÍA

PARA OPTAR AL TITULO DE:

LICENCIADO EN MATEMÁTICA

CIUDAD UNIVERSITARIA DE ORIENTE, SAN MIGUEL,

EL SALVADOR, CENTRO AMÉRICA, AGOSTO DE 2013

UNIVERSIDAD DE EL SALVADOR.

MSC. MARIO ROBERTO NIETO LOVO
RECTOR

MSC. ANA MARIA GLOWER
VICERRECTORA ACADÉMICA

MSC. MARIO ROBERTO NIETO LOVO
VICERRECTOR ADMINISTRATIVO EN FUNCIONES

DRA. ANA LETICIA ZABALETA DE AMAYA
SECRETARIA GENERAL

LIC. FRANCISCO CRUZ LETONA
FISCAL GENERAL

FACULTAD MULTIDISCPLINARIA ORIENTAL

LIC. CRISTOBAL HERNÁN RÍOS
DECANO

LIC. CARLOS ALEXANDER DÍAZ
VICE DECANO

LIC. JORGE ALBERTO ORTÉZ
SECRETARIO

MSC.EDWIND JEOVANNY TREJOS CABRERA
ADMINISTRADOR ACADÉMICO

LIC. JOSÉ ENRY GARCÍA
JEFE DEL DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

ING. DOLORES BENEDICTO SARAVIA
COORDINADOR DE LA SECCIÓN DE MATEMÁTICA

LIC. OSCAR ULISES LIZAMA VIGIL
COORDINADOR DE PROCESOS DE GRADUACIÓN
DEPTO. DE CIENCIAS NATURALES Y MATEMÁTICA

TRABAJO DE GRADUACIÓN APROBADO POR:

_____

Lic. Oscar Ulises Lizama Vigil
Coordinador de Procesos de Graduación
Depto. Ciencias Naturales y Matemática.

_____

Lic. José Fredy Vásquez.
Asesor Director.

_____

Lic. José Enry García
Asesor Metodológico

AGRADECIMIENTOS

Por Luis Alexander Fuentes:

A mi familia por su apoyo en cada etapa de mi formación, en especial a mi madre **Martha Lilian Fuentes**, y mi tío **Juan Pedro Fuentes** quienes depositaron en mi toda su confianza y acompañaron cada una de mis decisiones académicas y personales, son personas con cualidades ejemplares y han sido un modelo para mi en todo momento.

A la memoria de mi abuela **Simona Lilian Álvarez**, quien no puede estar presente para el cierre de mi carrera pero siempre mantuvo la alegría e ilusión de verme triunfando. Me enseño en gran parte a tener un buen criterio entre muchas otras cosas que hicieron de mi un hombre de bien.

Al Consejo de Becas Estudiantiles que con los beneficios otorgados fue muy importante y determinante en muchas etapas de la carrera.

Al licenciado José Fredy Vásquez por su paciencia, sus conocimientos y sobre todo su exigencia y profesionalismo como catedrático y asesor.

A todos los docentes que me brindaron sus conocimientos, y por la exigencia que mantuvieron hacia mi, en especial al lic. Marcelino Mejía que sin duda trascendió para que no sea un profesional conformista, sino hambriento de éxito.

Por Victor Edgardo López Saldoval:

A mi **madre Rosa María Sandoval** y mi **padre Jaime Romualdo López** por brindarme su apoyo incondicional, por su sudor y lágrimas al formarme, por todos sus años de dedicación y trabajo para regalarme el tesoro de la educación, por su comprensión y amor, por ser verdaderos luchadores y mostrarme bajo el ejemplo el valor de la perseverancia y por iluminarme el camino a seguir a fuerza de consejos.

A mi **hija Patricia Yossibeth López Ventura** por convertirse en la fuerza impulsadora de mis sueños.

A mi **familia, compañeros y amigos** por estar presentes en momentos de felicidad y tristeza, por potenciar mis cualidades, por haber colaborado de incontables maneras para que culmine mi carrera y por haberme brindado en todo momento la fuerza necesaria para seguir adelante.

A nuestros asesores **Lic. José Fredy Vásquez y Lic. José Enry García** por corregir nuestros errores con modestia, por haber contribuido con su experiencia y conocimiento al desarrollo de nuestro trabajo de graduación, por su comprensión y paciencia al asesorarnos.

A todos los **docentes** que contribuyeron a mi educación y formación, por toda su dedicación y esfuerzo al enseñarme y por toda su paciencia al soportar mis arrebatos.

Una dedicatoria especial a la memoria de mi hermana **Karla Tatiana López Sandoval** cuya partida marcará por siempre mis días, le estaré por siempre agradecido por toda la alegría y felicidad que nos transmitió durante su corta estancia en este mundo, a pesar de que no está presente físicamente, su sonrisa la hizo inmortal.

CONVENCIÓN

La álgebra se refiere al objeto matemático

El álgebra se refiere a la rama de la matemática

ÍNDICE DE CONTENIDOS

BREVE DESCRIPCIÓN DE LA INVESTIGACIÓN

Éste trabajo está estructurado por tres capítulos, en los cuales se pretende abordar y desglosar la teoría necesaria para el desarrollo sistemático de la investigación, comenzando desde una introducción de la teoría básica del álgebra abstracta, hasta llegar a los resultados buscados en las álgebras de Lie.

CAPÍTULO UNO: En el primer capítulo se presentan los conceptos, definiciones y resultados básicos del álgebra abstracta que son necesarios para poder abordar las álgebras de Lie, se presentan resultados interesantes que posteriormente serán de gran utilidad para obtener conclusiones importantes en el área desarrollada. Partimos inicialmente del concepto de *grupo*, se muestran algunas características de éstos y algunos grupos especiales, trabajamos con *homomorfismos de grupos* y se muestran algunas propiedades de los homomorfismos, se define lo que son *permutaciones* y se presenta un grupo especial el cual es el *grupo simétricos*. También se abordan los *anillos*, dónde se hace un estudio análogo al primer apartado, se define una clase especial de anillo el cual es el concepto de *dominio*, se define lo que es un *campo*, lo que es un *ideal*, los *homomorfismos sobre anillos* y por último se trabaja sobre *anillos de polinomios*. Se sigue recalcando que aquí se aborda la teoría básica y necesaria para desarrollar toda la investigación.

CAPÍTULO DOS: En éste capítulo se trabaja el álgebra lineal pero desde un enfoque abstracto, de manera que se acople más a la línea de nuestro trabajo de investigación, se comienza definiendo un *espacio vectorial* y algunas de sus propiedades importantes. Se presenta la definición y propiedades de las *sumas directas* y *espacio cociente* para

posteriormente analizar un poco sobre el *álgebra bilineal*. Es en esta parte también se aborda la importantísima definición de *transformación lineal*.

Con esto ya se tienen los elementos necesarios para definir formalmente una *álgebra* como objeto matemático. A su alrededor se analiza un marco teórico de definiciones, proposiciones y resultados importantes que incluyen *subalgebras, ideales, homomorfismos y las álgebras simples.* Se concluye el capítulo con el análisis del *álgebra de transformaciones lineales* y también se trabaja con los inversos de una álgebra y se domina a este apartado *inversión.*

Nótese que hasta esta parte no se ha definido una álgebra de Lie.

CAPÍTULO TRES: En éste capitulo se da el clímax de la investigación, en el cual se presentan los resultados obtenidos sobre el estudio de las álgebras de Lie. Iniciamos éste último capítulo definiendo formalmente una *álgebra de Lie* y ejemplos que ilustran sus características y diversidad de contextos, asimismo algunos resultados demostrados. Posteriormente se estudian *ideales* y *homomorfismos* sobre estas álgebras. Se presentan unos casos especiales de álgebras de Lie como lo son las *álgebras de Lie nilpotentes* y *las álgebras de Lie resolubles*. Se termina la temática abordando las *álgebras de Lie semisimples* y presentando resultados importantes sobre ellas. Finalizando el capítulo con una aplicación a la economía y finanzas

INTRODUCCIÓN

En el presente trabajo se abordan y analizan las álgebras de Lie, abriendo por este medio una ventana hacia el genial trabajo del matemático Sophus Lie. Aunque vale la pena aclarar que los conceptos que aquí se estudiarán no son en ninguna medida obvios, razón por la cual el análisis de dicha teoría genera un tanto de inquietud en el lector dado que requiere estudios previos sobre álgebra abstracta.

La aportación de Sophus Lie a las matemáticas requiere un esfuerzo para poder entenderla, por su complejidad y la novedad que encierra en su interior. Aun sigue siendo una teoría de vanguardia y visionaria, por la gran extensión de aplicaciones que tiene en las diferentes ramas de la ciencia contemporánea.

Esta teoría se centra fundamentalmente en el campo del álgebra abstracta, rama a la que Lie dió un impulso casi definitivo. En matemática, los grandes progresos siempre han estado ligados a progresos en la capacidad de escalar un poco más en el campo de la abstracción. En particular, para darnos una idea de la importancia que tiene la teoría de las algebras de Lie, basta recordar lo que Albert Einstein llegó a afirmar: *"sin sus descubrimientos no habría sido posible el nacimiento de la Teoría de la Relatividad".* Por otro lado, este trabajo no ambiciona ser una biografía de este matemático, eso ya sería tema para historiadores. Lo que realmente se pretende, es presentar un trabajo sobre su obra relacionado a las álgebras, de manera que se alcance una mayor comprensión sobre ésta temática, a la vez que sea utilizado como una herramienta de estudio.

Por otro lado, no debemos olvidar que una característica distintiva de la matemática es su gran unidad, es decir, es imposible hablar de áreas que evolucionen de manera aislada, o como lo dice David Hilbert: "*La matemática es en mi opinión un todo indivisible, un organismo cuya vitalidad está condicionada por la conexión de sus partes…*". Por lo tanto, el desarrollo de una área necesariamente marca su impacto en las otras y todas se retroalimentan entre sí. En particular, el álgebra no es ajena a esta tendencia y a lo largo de su desarrollo es posible observar su influencia en otras ramas de la matemática y como se ha visto beneficiada por los desarrollos de éstas. Sin embargo, a pesar que sería muy fructífero asomarnos un poco a este proceso, no es posible revisar en su totalidad en este documento esas conexiones del álgebra con otras áreas y sólo le pedimos al lector tener en cuenta que el álgebra no ha evolucionado de forma aislada y es posible notar su presencia en toda la matemática.

NOTA HISTÓRICA

En su época, Sophus Lie era considerado por casi todos como el arquetipo de personaje de un drama teatral, el prototipo de rubio nórdico. Era conocido en toda Europa como el gran gigante germano, una fuerza primordial, un titán lleno de ansias de vivir con objetivos audaces y una fuerza de voluntad indomable. Era descrito como altamente comprometido e innovador, alguien con la resistencia necesaria para superar la mayoría de los obstáculos. Es de destacar que Lie es considerado uno de los matemáticos más prolíficos que han existido. De hecho, el volumen de sus publicaciones es comparable incluso al de los propios Euler y Gauss, por ejemplo.

En el año de 1873, Sophus Lie dio origen a las ideas que conformaron, la hoy denominada *teoría de Lie*, con aportes posteriores de Weyl, Cartan, Chevalley, Killing, Serre, Harishchandra y otros. En los primeros trabajos de Lie, la idea subyacente era construir una teoría de "grupos continuos", que complementara la ya existente teoría de grupos discretos. La aplicación inicial que Lie tenía en mente era en ecuaciones diferenciales. El objetivo era desarrollar una teoría capaz de unificar el estudio de las simetrías en el área de las ecuaciones diferenciales ordinarias. Si bien continúo su desarrollo en otra dirección, la teoría de Lie juega un papel fundamental en el álgebra contemporánea.

Lie observó que las simetrías de una ecuación diferencial daban lugar a grupos con parámetros (que hoy consideraríamos un grupo de Lie). El grupo de Lie que dejaba invariante una ecuación diferencial actúa sobre el conjunto de soluciones de dicha ecuación.

Los "grupos" y conjuntos con los que Lie trabajaba en general, no eran grupos de Lie en realidad, dado que la estructura de grupo estaba definida sólo localmente cerca de la

identidad. De todos modos, todo grupo local admite un álgebra de Lie, que a su vez se integra a un grupo global. Fue Weyl (1924) quien por primera vez estudió sistemáticamente grupos definidos globalmente.

Los aportes fundamentales que realizó Lie fueron el asociar a cada grupo de transformaciones continuas una álgebra de Lie y el definir una aplicación del álgebra de Lie al grupo de Lie por medio de grupos monoparamétricos.

JUSTIFICACIÓN

Es difícil hablar de una justificación para el estudio de las álgebras de Lie, sería más conveniente hablar de justificaciones por las múltiples aplicaciones que puede tener en la ciencia moderna.

Como ya se ha indicado anteriormente, entendemos que la enorme trascendencia de la obra de Lie, tanto sobre los fundamentos de la Matemática actual como por su extensa aplicación a otras ciencias, tales como Física, Ingenierías y economía y finanzas por ejemplo, le hacen merecedora de ser un poco más conocida y estudiada.

Como una muestra de la aplicación del trabajo de Lie a la Física Moderna, queremos destacar que los grupos y las álgebras de Lie son muy utilizadas actualmente como herramientas en el estudio de las simetrías, no sólo de las clásicas en el espacio-tiempo, sino en las nuevas asociadas con los grados de libertad interna de las partículas y de los campos, así como también en la moderna teoría de las súper-cuerdas.

El matemático francés Jean Dieudonné dijo: *"La teoría de Lie está en proceso de convertirse en la parte más importante de la Matemática. Poco a poco se ha hecho obvio que las teorías más inesperadas, desde Aritmética hasta Física Cuántica, han venido a rodear este campo de Lie como a un gran eje gigante".*

Sophus Lie proporcionó la fundación ideológica que, en gran medida, marcó el desarrollo de las Matemáticas modernas y de la construcción de modelos matemáticos. El método de Lie para resolver ecuaciones diferenciales fue importante para los cálculos inmersos en la Teoría General de la Relatividad de Einstein. La Teoría de Lie también fue

indispensable para la formulación fundamental de las leyes naturales y del entendimiento de las estructuras internas del átomo. Cabe señalar que Sophus Lie ya había previsto este hecho en vida cuando dijo: *"Estoy seguro, absolutamente seguro de que estas teorías serán reconocidas como fundamentales en algún momento del futuro"*.

He aquí, unas cuantas de las muchas razones por las cuales se vuelve importante el estudio de la teoría de Lie y de sus álgebras en particular. Podemos considerar toda esta teoría como la cima del pensamiento matemático en la actualidad.

OBJETIVOS

GENERALES:

- Elaborar un material bibliográfico sobre las álgebras de Lie que muestre los fundamentos de dicha teoría y presente los conceptos que son necesarios para su comprensión.
- Analizar las álgebras de Lie para fomentar su estudio y reconocer su utilidad en las ciencias modernas.

ESPECÍFICOS:

- Estimular el interés de la Teoría de álgebras de Lie a estudiantes y catedráticos en ciencias naturales y matemática.
- Mostrar una base de conceptos necesarios para comprender los principios de la teoría de Lie.
- Documentar de forma introductoria la teoría de álgebras de Lie para mostrar su importancia y existencia de aplicaciones.
- Elaborar un texto introductorio sobre la Teoría de álgebras de Lie para estudiantes de la Licenciatura en Matemática.

CAPÍTULO I:

ELEMENTOS INTRODUCTORIOS DE ÁLGEBRA ABSTRACTA

SECCIÓN 1: ELEMENTOS DE TEORIA DE GRUPOS

1.1 GRUPOS

DEFINICIÓN (GRUPO) 1.1.1

Se dice que un conjunto no vacío *G* es un *grupo* si en él hay definida una operación * tal que:

a) $a, b \in G$ implica que $a * b \in G$.

b) Dados $a, b, c \in G$ se tiene que $a * (b * c) = (a * b) * c$.

c) Existe un elemento especial $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$ (e se llama *elemento identidad* o *unidad* de G).

d) Para todo $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$ *(a^{-1} se llama elemento inverso de a).*

DEFINICIÓN (GRUPO ABELIANO) 1.1.2

Se dice que un grupo *G* es *abeliano* si $a * b = b * a$ para todo $a, b \in G$.

A partir de aquí se entenderá la operación $a * b = ab$, y se comprenderá como *producto*.

LEMA 1.1.3

Si *G* es un grupo, entonces:

a) Su elemento *identidad* es *único.*

b) Todo $a \in G$ tiene un inverso único $a^{-1} \in G$.

c) Si $a \in G, (a^{-1})^{-1} = a$.

d) Para $a,\ b\ \in G, (ab)^{-1} = b^{-1}a^{-1}$.

e) Si $a,\ b,\ c\ \in G$

   i. $ab = ac,$ entonces $b = c$.

   ii. $ba = ca,$ entonces $b = c$.

DEFINICIÓN (ORDEN) 1.1.4

- El orden de un grupo finito *G* es su *cardinalidad*, es decir, el número de sus elementos y es denotado por $o(G)$.
- El orden de un elemento *a* de un grupo *G* es el más pequeño entero positivo *m* tal que $a^m = e$, donde e es el elemento identidad de *G.*

1.2 SUBGRUPOS

DEFINICIÓN (SUBGRUPO) 1.2.1

Un subconjunto no vacío *H* de un grupo *G* se llama *subgrupo* de *G*, si *H* mismo forma un grupo relativo al producto de *G*.

LEMA 1.2.2

Un subconjunto no vacío *H* del grupo *G* es un subgrupo de *G* si y solo si

i. $a, b \in H$ implica que $ab \in H$.

ii. $a \in H$ implica que $a^{-1} \in H$.

1.3 SUBGRUPOS NORMALES

DEFINICIÓN (CLASES LATERALES) 1.3.1

Si *G* es un grupo y *H* es un subgrupo de *G* y g es un elemento de *G*, entonces

i. $gH = \{gh : h\ un\ elemento\ de\ H\}$ es una *clase lateral izquierda* de *H* en *G*.

ii. $Hg = \{hg : h\ un\ elemento\ de\ H\}$ es una *clase lateral derecha* de *H* en *G*.

DEFINICIÓN (SUBGRUPO NORMAL) 1.3.2

Se dice que un subgrupo *N* de *G* es un *subgrupo normal* de *G* si $a^{-1}Na \subset N$ para todo $a \in G$.

Se expresa "*N* es un subgrupo normal de *G*" mediante el símbolo abreviado $N \lhd G$.

TEOREMA 1.3.3

$N \lhd G$ si y solo si toda clase lateral izquierda de *N* en *G* es una clase lateral derecha de *N* en *G*.

COROLARIO 1.3.4

Si H y K son subgrupos de un grupo abeliano G, entonces $HK = \{hk : h\ es\ un\ elemento\ de\ H\ y\ k\ es\ un\ elemento\ de\ K\}$ es un subgrupo de G.

LEMA 1.3.5

Un subgrupo N de G es un subgrupo normal de G si y sólo si $(Na)(Nb) = Nab$. $a, b \in G$.

Se denota por *G/N* la colección de las clases laterales derechas de *N* en *G* (Es decir, los elementos de *G/N* son ciertos subconjuntos de *G*). Se denomina *Grupo factor o grupo cociente.*

DEFINICIÓN (GRUPO COCIENTE) 1.3.6

Si *G* es un grupo y *N* un subgrupo normal de *G*, entonces *G/N* es también un grupo. Se le llama grupo cociente o grupo factor de *G* por *N*.

La operación de grupo en *G/N* es definida por

$(aN)(bN) = (ab)N, aN\ y\ bN \in G/N.$

1.4 HOMOMORFISMOS DE GRUPOS

DEFINICIÓN (HOMOMORFISMO DE GRUPOS) 1.4.1

Sean G, $G´$ dos grupos; entonces una aplicación $\varphi: G \to G´$ es un *homomorfismo* si $\varphi(ab) = \varphi(a)\,\varphi(b)$ para todo $a, b \in G$.

Se utilizara el apocope *sobre* para hacer referencia a sobreyectividad.

LEMA 1.4.2

Si φ es un homomorfismo de G en $G´$, entonces:

a) $\varphi(e) = e´, e´$ el elemento unidad de G´.

b) $\varphi(a^{-1}) = \varphi(a)^{-1}$ para todo $a \in G$.

LEMA 1.4.3

Si φ es un homomorfismo de G en $G´$, entonces la imagen de de φ es un subgrupo de $G´$.

LEMA 1.4.4

Supóngase que G es un grupo y que N es un subgrupo normal de G; definamos la aplicación $\varphi(a) = Na$ para todo $a \in G$. Entonces, φ es un homomorfismo de G sobre G/N.

DEFINICIÓN (KERNEL) 1.4.5

Si φ es un homomorfismo de grupos G en G', entonces el *kernel* o *núcleo* de $\varphi, K(\varphi)$, se define por $K(\varphi) = \{a \in G \mid \varphi(a) = e'\}$.

TEOREMA 1.4.6

Sea φ un homomorfismo de G sobre G' con núcleo K. Entonces G/K es isomorfo a G'.

APLICACIÓN 1 (TEOREMA DE CAUCHY PARA GRUPOS ABELIANOS)

Supongamos que G es un grupo abeliano finito y que $p|o(G)$, donde p es un número primo. Entonces hay un elemento $a \neq e$ $(a, e \in G)$ tal que $a^p = e$.

APLICACIÓN 2 (TEOREMA DE SYLOW PARA GRUPOS ABELIANOS)

Si G es un grupo abeliano de orden $o(G)$, y si p es un número primo tal que $p^\alpha | o(G)$, $p^{\alpha+1} \nmid o(G)$, entonces G tiene un subgrupo de orden p^α, $\alpha \in \mathbb{N}$.

LEMA 1.4.7

Sea φ un homomorfismo de G sobre G' de núcleo K. Para un subgrupo H' de G' sea H el subconjunto de G definido por $H = \{x \in G | \varphi(x) \in H'\}$. Entonces H es un subgrupo de G y $H \supset K$; si H' es normal en G', entonces H es normal en G. Por otra parte, esta asociación establece una aplicación biyectiva del conjunto de todos los subgrupos de G' sobre el conjunto de todos los subgrupos de G que contienen a K.

TEOREMA 1.4.8

Sea φ un homomorfismo de *G* sobre *G´* de núcleo *K*, y sea *N´* un subgrupo normal de *G´* y $N = \{x \in G | \varphi(x) \in N'\}$. Entonces *G/N* es isomorfo a *G´/N´*, o lo que es equivalente, *G/N* es isomorfo a (*G/K*)/(*N/K*).

SECCIÓN 2: ELEMENTOS DE TEORÍA DE ANILLOS

1.5 ANILLOS

Hay ciertos sistemas algebraicos que sirven como los bloques de construcción de las estructuras del álgebra moderna. Ya se ha aprendido algo de uno de ellos, los grupos. Ahora el propósito es introducir y estudiar un segundo de tales bloques, el constituido por los llamados anillos. El concepto abstracto de grupo tiene su origen en el conjunto de aplicaciones o permutaciones de un conjunto sobre sí mismo. En contraste, los anillos nacen de otra fuente bastante familiar, el conjunto de los enteros. Se observará que están caracterizados de acuerdo a los aspectos algebraicos de los enteros ordinarios de los que pueden considerarse una generalización.

En el próximo párrafo se aclarará que un anillo es completamente diferente de un grupo, ya que es un sistema bioperacional, en el que hay definidas dos operaciones; estas operaciones comúnmente se llaman adición y multiplicación. Sin embargo, a pesar de las diferencias, el análisis de los anillos seguirá el esquema que fue establecido para los grupos. Se tendrán los análogos de los homomorfismos, de los subgrupos normales, etc.

Ahora se presenta una definición formal de anillo:

DEFINICIÓN (ANILLO) 1.5.1

Un conjunto no vacío *R* se dice que es un *anillo* si en *R* están definidas dos operaciones, denotadas por "+" y "·" respectivamente tales que para cualesquiera *a, b, c* de *R*:

1) $a + b$ está en R $\forall a, b \in R$.
2) $a + b = b + a$ $\forall a, b \in R$.
3) $a + (b + c) = (a + b) + c$ $\forall a, b, c \in R$.
4) Existe un elemento 0 en R tal que $a + 0 = a$ $\forall a \in R$.
5) Existe un elemento $-a$ en R tal que $a + (-a) = 0$ $\forall a \in R$.
6) $a \cdot b$ está en R $\forall a, b \in R$.
7) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ $\forall a, b, c \in R$.
8) $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$ (las dos leyes distributivas) $\forall a, b, c \in R$.

Los axiomas del (1) al (5) simplemente afirman que *R* es un grupo abeliano bajo la operación + a la que se llamará adición. Los axiomas (6) y (7) nos dicen que *R* es cerrado bajo una operación asociativa · a la que llamamos multiplicación. El axioma (8) sirve para correlacionar las dos operaciones de *R*.

Siempre que se hable de anillo se entenderá es de un anillo asociativo. Los anillos no asociativos, es decir aquellos en los que no se identifican los axiomas (3) y (7), se presentan en matemáticas y son objeto de estudio, pero aquí no se tendrá ocasión para considerarlos.

Puede o no suceder que exista un elemento 1 en R tal que $a \cdot 1 = 1 \cdot a = a$ para toda a en R; si tal elemento existe diremos que R es un *anillo con elemento unitario.*

Si en la multiplicación en R se cumple que $a \cdot b = b \cdot a$ para todos a, b que pertenecen a R, entonces se llama a R *anillo conmutativo.*

Antes de comenzar a estudiar algunas propiedades de los anillos, se hará una pausa para examinar algunos ejemplos. Motivándose en ellos se definirán varios casos especiales de anillos que son de importancia.

EJEMPLO:

R es el conjunto de los enteros positivos, negativos y el cero; + es la adición usual y · la multiplicación usual de los enteros. Es un anillo conmutativo con elemento unitario.

EJEMPLO:

R es el conjunto de los enteros pares bajo las operaciones habituales de adición y multiplicación. R es un anillo conmutativo, pero no tiene elemento unitario.

PROPIEDADES DE ANILLOS 1.5.2

Si R es un anillo, entonces para todo $a, b \in R$

1) $a \cdot 0 = 0 \cdot a = 0$.

2) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

3) $(-a) \cdot (-b) = a \cdot b$.

Si además, *R* tiene elemento unitario, 1, entonces

4) $(-1) \cdot a = -a$.

5) $(-1) \cdot (-1) = 1$.

1.6 DOMINIOS

Los ejemplos que se estudiaron en la sección anterior claramente indican que aunque los anillos son una generalización directa de los enteros, ciertos hechos aritméticos a los que se está acostumbrado en el anillo de los enteros no tienen forzosamente que tener validez en los anillos en general. Por ejemplo, se ha visto la posibilidad de que $a \cdot b = 0$ sin que ni *a* ni *b* sean cero. Existen también ejemplos muy naturales en que $a \cdot b \neq b \cdot a$. Todas estas cosas van en contra de la experiencia previa.

Por simplicidad en la expresión, se prescindirá de aquí en adelante del punto en $a \cdot b$ y escribiremos simplemente este producto como *ab*.

DEFINICIÓN (DIVISOR DE CERO) 1.6.1

Si R es un anillo conmutativo entonces, si $a \in R$ y además $a \neq 0$ se dice que a es *un divisor de cero* si existe un b que pertenece a R, $b \neq 0$, tal que $ab = 0$.

Con el concepto anterior ya es posible dar una definición sobre un dominio, que no es más que una clase especial de anillo.

DEFINICIÓN (DOMINIO) 1.6.2

Un anillo conmutativo es un *dominio entero* si no tiene divisores de cero.

El anillo de los enteros es un ejemplo de dominio entero.

1.7 CAMPOS

Para definir el concepto de campo, previamente se debe definir un concepto necesario, así como se definió un dominio entero.

DEFINICIÓN (ANILLO CON DIVISIÓN) 1.7.1

Un anillo se dice que es un *anillo con división* si sus elementos distintos de cero forman un grupo bajo la multiplicación.

El elemento unidad bajo la multiplicación se escribirá como 1, y el inverso de un elemento *a* bajo la multiplicación se denotará como a^{-1}.

Se presenta finalmente la definición del importante objeto matemático conocido como campo.

DEFINICIÓN (CAMPO) 1.7.2

Un *campo* es un anillo conmutativo con división.

Para la mayoría de lectores el concepto de anillo constituía un terreno desconocido: en cambio, el concepto de campo está más relacionado con la experienciam, mientras que el único anillo que se pudiera haberse considerado en la enseñanza elemental era el anillo de los enteros, se tenía más experiencia trabajando con los números racionales, los reales y en algunos casos, los números complejos al resolver ecuaciones lineales y cuadráticas. La capacidad de dividir entre elementos diferentes de cero proporcionó cierta libertad de acción para resolver una amplia variedad de problemas, la cual podría no haberse tenido con los enteros.

De modo que a primera vista, cuando se empieza a trabajar con campos se siente como en casa. Los campos desempeñan un papel importante en la geometría, la teoría de

las ecuaciones y en ciertas áreas muy importantes de la teoría de los números. Se denotará un campo en general con la letra *F*. Ahora bien, se presentan algunos ejemplos clásicos de campos.

EJEMPLOS:

1) $\mathbb{Q}$, el campo de los números racionales.
2) $\mathbb{R}$, el campo de los números reales.
3) $\mathbb{C}$, el campo de los números complejos.
4) Sea $F = \{a + bi | a, b \in \mathbb{Q}\}$. Se verifica solamente que si $a + bi \neq 0$ está en F, entonces $(a + bi)^{-1}$ también está en F. Pero, ¿a qué es igual $(a + bi)^{-1}$? Simplemente es:

$$\frac{a}{(a^2 + b^2)} - \frac{bi}{(a^2 + b^2)}.$$

Y puesto que $a^2 + b^2 \neq 0$ y es racional entonces $a/(a^2 + b^2)$ y $b/(a^2 + b^2)$ son también racionales, por lo tanto $(a + bi)^{-1}$ está efectivamente en F.

Se podría seguir viendo más ejemplos de campos, pero los anteriores muestran una cierta variedad de campos y se observa que no es muy difícil encontrase con ellos.

DEFINICIÓN (CARACTERÍSTICA DE UN CAMPO) 1.7.3

Se dice que un campo *F* tiene (o es de) *característica* $p \neq 0$ si para cierto entero positivo p, $px = 0$ para todo $x \in F$, y ningún entero positivo menor que p goza de esta propiedad.

Si un campo *F* no es de característica $p \neq 0$ para ningún entero positivo p, se le llama campo de *característica* 0. De esta forma $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son campos de característica 0.

En la definición anterior, el uso de la letra p para definir la característica de un campo es altamente sugestivo, ya que siempre se acostumbra utilizar p para denotar un número primo. En realidad, como se observa en el teorema siguiente, este empleo de p resulta consistente.

TEOREMA 1.7.4

La característica de un campo es cero o bien un número primo.

1.8 HOMOMORFISMOS DE ANILLOS

Al estudiar los grupos se observó que el concepto de homomorfismo resultaba ciertamente fructífero. Esto parece sugerir que apropiadamente un análogo para anillos llevaría también hasta importantes ideas. Recuérdese que para los grupos un homomorfismo se definió como una aplicación tal que $\varphi(ab) = \varphi(a)\varphi(b)$. Como un anillo tiene dos operaciones, ¿Qué podría ser una extensión más natural de este tipo de fórmula que la representa en la siguiente definición?.

DEFINICIÓN (HOMOMORFISMO) 1.8.1

Una aplicación φ del anillo R en el anillo R' se dice que es un *homomorfismo* si para cualesquiera $a, b \in R$ se cumple

1) $\varphi(a + b) = \varphi(a) + \varphi(b)$,
2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Como en el caso de los grupos, observemos que en los miembros izquierdos de las relaciones (1) y (2) las operaciones pertenecen a R mientras que el $+$ y el $\cdot$ que aparecen el lado derecho son las de R'.

Una útil observación es la que un homomorfismo de un anillo R en un anillo R' es: si se ignora totalmente la multiplicación en ambos anillos, resulta al menos un homomorfismo de R en R' cuando los consideramos como grupos abelianos bajo las respectivas adiciones. Por tanto en cuanto a la adición concierne, todas las propiedades

acerca de los homomorfismos de grupos se verifican aquí también. También es posible mencionar las siguientes propiedades:

PROPIEDADES DE HOMOMORFISMOS 1.8.2

Si φ es un homomorfismo de *R* en *R'*, entonces:

1) $\varphi(0) = 0$.
2) $\varphi(-a) = -\varphi(a)$ para toda $a \in R$.

Ahora bien, en el caso de los grupos, dado un homomorfismo, se asocia con este homomorfismo cierto subconjunto del grupo que es llamado núcleo del homomorfismo. ¿Cuál deberá ser la definición apropiada del núcleo de un homomorfismo entre anillos? Después de todo, los anillos tienen dos operaciones, adición y multiplicación, y podría ser natural preguntar cuál de éstas dos debe singularizarse como base para la definición. Pero la elección es clara. Dentro de la definición de cualquier grupo arbitrario está la condición de que el anillo forme un grupo abeliano bajo la adición. La multiplicación del anillo se dejó con muchas menos restricciones, y por ello, en cierto sentido, mucho menos bajo nuestro control que la adición. Es por esto que a la adición le da énfasis especial en el anillo, y se presenta la siguiente definición.

DEFINICIÓN (NÚCLEO DE UN HOMOMORFISMO) 1.8.3

Si φ es un homomorfismo de R en R' entonces el *núcleo* de φ, denotado por $K(\varphi)$, es el conjunto de todos los elementos $a \in R$ tales que $\varphi(a) = 0$, el elemento cero en R'.

LEMA 1.8.4

Si φ es un homomorfismo de R en R' con núcleo $K(\varphi)$, entonces:

1) $K(\varphi)$ es un subgrupo de R bajo la adición.
2) Si $a \in K(\varphi)$ y $r \in R$ entonces tanto ar como ra están en $K(\varphi)$.

Examinemos estos conceptos en ciertos ejemplos.

EJEMPLOS:

1) Sean R y R' dos anillos arbitrarios y definamos $\varphi(a) = 0$ para todo $a \in R$. φ es trivialmente un homomorfismo y $K(\varphi) = R$. A φ en este caso se le llama el homomorfismo cero.
2) Sea R un anillo, y sea $R'=R$. Definamos φ por $\varphi(x) = x$ para todo $x \in R$. Claramente φ es un homomorfismo y $K(\varphi)$ consiste solamente en el cero.
3) Sea $J(\sqrt{2})$ el conjunto de todos los números reales de la forma $m + n\sqrt{2}$, donde m y n son enteros. $J(\sqrt{2})$ forma un anillo bajo la adición y la multiplicación usuales de los números reales. Definamos $\varphi : J(\sqrt{2}) \to J(\sqrt{2})$ por $\varphi(m +$

$n\sqrt{2}) = m - n\sqrt{2}$. φ es un homomorfismo de $J(\sqrt{2})$ sobre $J(\sqrt{2})$ y su núcleo $K(\varphi)$ consiste solamente en el cero.

1.9 IDEALES

Una vez que se han establecido las ideas de homomorfismo y su núcleo para anillos, basadas ambas en la experiencia con los grupos, parece que ha der ser fructuoso establecer también para anillos algo análogo al concepto de subgrupo normal. Una vez logrado esto puede esperarse que este análogo conduzca a una construcción sobre anillos semejante a la del grupo cociente de un grupo por un subgrupo normal. Finalmente, si alguien fuera optimista, esperaría que los teoremas sobre homomorfismos sobre grupos se pudieran aplicar íntegramente a los anillos.

Afortunadamente, todo esto puede hacerse proveyéndose con ello de una técnica incisiva para el análisis de los anillos.

La primera tarea parece ser definir un concepto adecuado de "subgrupo normal" para anillos. Con un poco de intuición esto no resulta tan difícil. Recordar que los subgrupos normales resultaban no ser otra cosa en el último término que núcleos de homomorfismos, aunque en sus primeras condiciones definitorias no aparecieran los homomorfismos para nada. Entonces, ¿Por qué usar esta observación como clave de nuestra definición para anillos?.

El lema 1.8.4 nos ha proporcionado ya algunas condiciones de las que un subconjunto de anillo debe cumplir para que pueda ser el núcleo de un homomorfismo. Se toma ahora el punto de vista de que ya al menos al presente no tenemos ninguna otra información de que disponer, se harán de las conclusiones del lema 1.8.4 el punto de partida para la tarea, por lo que se define:

DEFINICIÓN (IDEAL) 1.9.1

Un subconjunto no vacío *U* de *R*, donde *R* es un anillo, se dice que es un *ideal* (bilateral) de *R* si:

1) *U* es un subgrupo de *R* bajo la adición.
2) Para todo $u \in U$ y $r \in R$ tanto *ur* como *ru* están en *U*.

La condición (2) afirma que *U* "absorbe" la multiplicación a la derecha y a la izquierda por elementos arbitrarios del anillo. Por esta razón *U* comúnmente se llama ideal bilateral. Como no se tendrá ninguna ocasión de usar algún otro concepto de ideal, solo se utilizará la palabra ideal en lugar de ideal bilateral en todo lo que sigue. Se denotarán a los ideales por *I.*

EJEMPLOS:

1) Se utilizará el anillo de los enteros como primer ejemplo. Sea $n > 1$ un entero fijo e I_n el conjunto de los múltiplos de *n*; entonces I_n es un ideal de el anillo de los enteros.
2) Sea *F* un campo; ¿Cuáles pueden ser los ideales de *F?* supóngase que $I \neq \{0\}$ es un ideal de *F*; sea $a \neq 0 \in I$. Entonces dado que *I* es un ideal de *F*, $1 = aa^{-1} \in I$; pero entonces puesto que $1 \in I, r1 = r \in I$, para todo $r \in F$. En forma breve $I = F$. De manera que *F* tiene solamente los ideales triviales $\{0\}$ y el propio *F*.

1.10 ANILLOS DE POLINOMIOS

En la educación matemática se introdujo muy pronto –generalmente en los primeros años de secundaria- al estudio de los polinomios. Durante una temporada que parecía no tener fin, se obligaba hasta el aburrimiento insoportable de factorizarlos, multiplicarlos, dividirlos y simplificarlos. La facilidad en factorizar un polinomio cuadrático se interpretaba como una muestra de genuino talento matemático.

Posteriormente, en los primeros años de universidad, los polinomios hacen de nuevo aparición en un marco algo distinto. Ahora son funciones con sus valores, y nos preocupan su continuidad, sus derivadas, sus integrales y sus máximos y mínimos.

También aquí es importante interesarse por los polinomios, pero desde un punto de vista cualquiera de los que se han mencionado, por siempre, los polinomios eran

simplemente elementos de un cierto anillo, y lo que interesará son las propiedades algebraicas de ese anillo.

DEFINICIÓN (ANILLO DE POLINOMIOS) 1.10.1

Sea F un campo; el *anillo de polinomios en x sobre F*, que siempre se expresará como $F[x]$, es el conjunto de todas las expresiones formales $p(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n$, donde $n \in N$ y los a_i, llamados *coeficientes* del *polinomio p(x)*, están en F. En $F[x]$ se definen la igualdad, suma y producto de dos polinomios para hacer de $F[x]$ un anillo conmutativo como sigue:

1) **IGUALDAD:** Se dice que $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ y $q(x) = b_0 + b_1 x + \ldots + b_m x^m$ son *iguales* si y sólo si sus coeficientes correspondientes son iguales, es decir, si y sólo si $a_i = b_i$ para todo $i \geq 0$.

2) **ADICIÓN:** Si $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ y $q(x) = b_0 + b_1 x + \ldots + b_m x^m$, entonces se define $p(x) + q(x) = c_0 + c_1 x + \ldots + c_s x^s$, donde para cada $i = 1,2, \ldots, s$ $c_i = a_i + b_i$, y además s será el *máx(m,n)* cuando $n \neq m$.

3) **MULTIPLICACIÓN:** Si $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ y $q(x) = b_0 + b_1 x + \ldots + b_m x^m$, entonces se define $p(x)\, q(x) = c_0 + c_1 x + \ldots +$

$c_k x^{n+m}$, donde c_i para $i = 1, 2, \ldots, k$ se determinan multiplicando la expresión formalmente (es decir, en cuanto a la forma), utilizando las leyes distributivas y las reglas de los exponentes $x^u\, x^v = x^{u+v}$, y reuniendo términos. De manera más formal:

$c_i = a_i b_0 + a_{i-1} b_1 + \ldots + a_1 b_{i-1} + a_0 b_i$, para todo i.

La primera observación que se hace (la cual no se verifica) es que $F[x]$ es un anillo conmutativo. El examinar al fondo los detalles de comprobación de los axiomas de un anillo conmutativo, es una tarea sencilla pero laboriosa y se omitirá.

LEMA 1.10.2

$F[x]$ es un anillo conmutativo con unidad.

Estas definiciones de las operaciones en $F[x]$ no dice más que para multiplicar dos polinomios se multiplican los símbolos formalmente, se usa la relación $x^\alpha x^\beta = x^{\alpha+\beta}$ y se reducen los términos semejantes. Por lo tanto nuestra definición de suma y multiplicación son las mismas que el lector ya conocía. Sin más exámenes afirmamos que $F[x]$ es un anillo bajo estas operaciones, que su multiplicación es conmutativa y que tiene un elemento unitario. La verificación de todas estas afirmaciones se las dejamos al lector.

DEFINICIÓN (GRADO DE UN POLINOMIO) 1.10.3

Si $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ y Si $a_n \neq 0$, entonces el *grado* de $p(x)$, denotado por $grd\ p(x)$, es *n.*

LEMA 1.10.4

Si $p(x)$, $q(x)$ son elementos de $F[x]$ distintos de cero, entonces $grd\ \big(p(x)q(x)\big) = grd\ p(x) + grd\ q(x)$.

LEMA 1.10.5

Si $p(x), q(x) \in F[x]$ y $p(x) + q(x) \neq 0$, entonces

$$grd\ \big(p(x) + q(x)\big) \leq máx\ \big(grd\ p(x),\ grd\ q(x)\big).$$

LEMA 1.10.6

$F[x]$ es un dominio entero.

TEOREMA (ALGORITMO DE LA DIVISIÓN) 1.10.7

Dados los polinomios $f(x),\ g(x) \in F[x],$ donde $g(x) \neq 0,$ se cumple entonces que:

$$f(x) = q(x)g(x) + r(x).$$

Donde $q(x),\ r(x) \in F[x]$ y $r(x) = 0$ ó bien $grd\ r(x) < grd\ g(x)$.

El algoritmo de la división tiene una aplicación inmediata: permite determinar la naturaleza de todos los ideales de $F[x]$. Como se ve en el siguiente teorema, un ideal de $F[x]$ debe consistir simplemente de todos los múltiplos, por elementos de $F[x]$, de cierto polinomio *fijo*.

TEOREMA 1.10.8

Si $I \neq (0)$ es un ideal de $F[x]$, entonces $I = \{f(x)g(x)|f(x) \in F[x]\}$; es decir, I consiste de todos los múltiplos del polinomio fijo $g(x)$ por los elementos de $F[x]$.

DEFINICIÓN (DOMINIO DE IDEALES PRINCIPALES) 1.10.9

Un dominio integral R se llama *dominio de ideales principales* si todo ideal I en R es de la forma $I = \{xa|x \in R\}$ para algún $a \in I$.

El Teorema 1.11.8 se puede expresar como: $F[x]$ *es un dominio de ideales principales*.

Si se considera el *ideal generado por un polinomio dado*, $g(x)$, a saber $\{f(x)g(x)|f(x) \in F[x]\}$, se expresará como $\big(g(x)\big)$.

DEFINICIÓN (POLINOMIO MÓNICO) 1.10.10

$f(x) \in F[x]$ es un *polinomio Mónico* si el coeficiente de su potencia más alta es 1.

Es decir, $f(x)$ es mónico si:

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0.$$

DEFINICIÓN (DIVISIBILIDAD ENTRE POLINOMIOS) 1.10.11

Si $f(x)$ y $g(x) \neq 0 \in F[x]$, entonces se dice que $g(x)$ divide a $f(x)$, expresado como $g(x)|f(x)$, si $f(x) = a(x)g(x)$ para algún $a(x) \in F[x]$.

DEFINICIÓN (MÁXIMO COMÚN DIVISOR) 1.10.12

Se dice que el polinomio $d(x) \in F[x]$ es el *máximo común divisor* de los polinomios $f(x), g(x) \in F[x]$ [donde no son a la vez $f(x) = 0$ y $g(x) = 0$] si $d(x)$ es un polinomio mónico tal que:

(a) $d(x)|f(x)$ y $d(x)|g(x)$.

(b) Si $h(x)|f(x)$ y $h(x)|g(x)$, entonces $h(x)|d(x)$.

Aunque se ha definido el máximo común divisor de dos polinomios, no se sabe hasta ahora, que existe, ni cuál puede ser su forma. Se podría haber definido de otra manera, equivalente como el *polinomio mónico de grado más alto que divide tanto a* $f(x)$ *como a* $g(x)$. Si asi se hiciera, su existencia sería automática, pero no se conocería su forma.

TEOREMA 1.10.13

Dados $f(x)$ y $g(x) \neq 0$ en $F[x]$, entonces su máximo común divisor $d(x) \in F[x]$ existe; además, $d(x) = a(x)f(x) + b(x)g(x)$ para ciertos $a(x), b(x) \in F[x]$.

LEMA 1.10.14

Si $f(x) \neq 0$, $g(x) \neq 0$ están en $F[x]$ y $f(x)|g(x)$ y $g(x)|f(x)$, entonces $f(x) = ag(x)$, done $a \in F$.

LEMA 1.10.15

Se dice que dos polinomios $f(x)$, $g(x)$ en $F[x]$ son *primos entre sí* si su máximo común divisor es 1.

Aunque el siguiente teorema es simplemente un caso muy especial del Teorema 1.10.13, para ponerlo en relieve y tenerlo de referencia, se presenta:

TEOREMA 1.10.16

Si $f(x)$, $g(x) \in F[x]$ son relativamente primos, entonces $a(x)f(x) + b(x)g(x) = 1$ para ciertos $a(x)$, $b(x) \in F[x]$. A la inversa, si $a(x)f(x) + b(x)g(x) = 1$ para ciertos $a(x)$, $b(x) \in F[x]$, entonces $f(x)$ y $g(x)$ son primos entre sí.

Como con los enteros se tiene:

TEOREMA 1.10.17

Se sabe que, si $q(x)$ y $f(x)$ son primos entre sí y si $q(x)|f(x)g(x)$, entonces $q(x)|g(x)$ ó $q(x)|f(x)$.

Es posible sentirse ahora preparados para destacar la importante clase de polinomios que desempeñaran el mismo papel como objetos primos en $F[x]$ que desempeñaron los números primos en $\mathbb{Z}$.

DEFINICIÓN (POLINOMIO IRREDUCIBLE) 1.10.18

Un polinomio $p(x) \in F[x]$ de grado positivo es *irreducible* en $F[x]$ si, dado cualquier polinomio $f(x)$ en $F[x]$, entonces ya sea que $p(x)|f(x)$ o bien $p(x)$ es primo respecto a $f(x)$.

Resulta inmediato que si $p(x)$ es irreducible en $F[x]$, entonces $p(x)$ *no puede ser factorizado* de una manera no trivial en $F[x]$. Dicho en otras palabras, si $p(x) = a(x)b(x)$, donde $a(x)$ y $b(x)$ están en $F[x]$, entonces una de dos se cumple, $a(x)$ es una constante ó $b(x)$ es una constante (constante = elemento de F).

Obsérvese que la irreducibilidad de un polinomio depende del campo F. Por ejemplo, el polinomio $x^2 - 2$ es irreducible en $\mathbb{Q}[x]$, donde $\mathbb{Q}$ es el campo de los números racionales; pero $x^2 - 2$ no es irreducible en $\mathbb{R}[x]$, donde $\mathbb{R}$ es el campo de los números reales, ya que en $\mathbb{R}[x]$:

$$x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right).$$

COROLARIO 1.10.19

Si$p(x)$es irreducible en $F[x]$ y $p(x)|a_1(x)a_2x \ \ldots \ a_k(x)$, donde $a_1(x)$, ... , $a_k(x)$ están en $F[x]$, entonces $p(x)|a_i(x)$ para algún i.

TEOREMA 1.10.20

Si $p(x) \in F[x]$, entonces el ideal $(p(x))$ generado por $p(x)$ en $F[x]$, es un ideal máximo de $F[x]$ si y sólo si $p(x)$ es irreducible en $F[x]$.

TEOREMA 1.10.21

Sea $f(x) \in F[x]$ de grado positivo. Entonces $f(x)$ es irreducible en $F[x]$ o bien $f(x)$ es el producto de polinomios irreducibles en $F[x]$. En efecto se tiene entonces que:

$$f(x) = ap_1(x)^{m_1}p_2(x)^{m_2} \ \ldots \ p_k(x)^{m_k} ,$$

donde a es el coeficiente de la potencia más alta de $f(x)$, $p_1(x), \ldots , p_k(x)$ son mónicos e irreducibles en $F[x]$, $m_i > 0$ para $i = 1,2, \ldots, k$ y dicha factorización en tal forma es única excepto por el orden de los $p_i(x)$.

Se ha hecho notar cuán semejante es la situación de los $\mathbb{Z}$ y el anillo de polinomios $F[x]$. Esto sugiere que debe haber una cantidad más amplia de anillos, de la cual los dos ejemplos $\mathbb{Z}$ y $F[x]$ son casos especiales, para los que gran parte de la argumentación es válida. Fue válida para $\mathbb{Z}$ y $F[x]$ porque en estos anillo se tenía una

medida de magnitud, ya sea por el tamaño de un entero o por el grado de un polinomio. Dicha medida de magnitud fue tal que permitió la validez de un algoritmo de tipo euclidiano.

Lo anterior conduce a definir una clase de anillos, los *anillos euclidianos.*

DEFINICIÓN (ANILLO EUCLIDIANO) 1.10.22

Un dominio entero R es un *anillo euclidiano* si existe una función d de los elementos distintos de cero de R a los enteros no negativos que satisface:

(a) Para $a \neq 0$, $b \neq 0 \in R$, $d(a) \leq d(ab)$.

(b) Dados $a \neq 0$, $b \neq 0$, existen q y $r \in R$, tales que $b = qa + r$, donde $r = 0$ ó $d(r) < d(a)$.

Los enteros podrían servir como un ejemplo de un anillo euclidiano, definiendo $d(a)$ como la función valor absoluto de *a*.

Como $F[x]$ es un dominio entero, a la luz del lema 1.11.6 es posible construir por ello su campo de cocientes. Este campo se compone simplemente de todos los cocientes de polinomios y se llama campo de las *funciones racionales* en x sobre *F*.

La función $grd\ f(x)$ definida para todos los polinomios $f(x) \neq 0$ en $F[x]$ tiene las siguientes propiedades:

1) $grd\ f(x)$ es un entero no negativo.
2) $grd\ f(x) \leq grd\ f(x)g(x)$ para todo $g(x) \neq 0$ en $F[x]$.

Para que $F[x]$ sea un anillo euclidiano con la función de grado actuando como la *d*-función de un anillo euclidiano, auxiliándose del algoritmo de la división (teorema 1.11.7) para asegurar que dadas dos funciones $f(x)$ y $g(x)$ que están en $F[x]$, existen funciones $t(x)$ y $r(x)$ también en $F[x]$ tal que: $f(x) = t(x)g(x) + r(x)$, con $r(x) = 0$ ó $grd\ r(x) < g(x)$. Con esto se llenan todos los requisitos para afirmar que $F[x]$ es un anillo euclidiano.

DEFINICIÓN (EXTENSIÓN DE UN CAMPO) 1.10.23

Sean *K* y *F* campos. Decimos que *F* es una *extensión* de *K* (o equivalentemente, que *K* es un *subcampo* de *F*) si $K \subseteq F$ y *K* hereda la suma y la multiplicación de F.

Con esto se concluye el estudio de conceptos básicos y necesarios sobre la teoría de grupos y teoría de anillos, no es posible obviar que estos elementos son solo una parte de dicha teoría y que en este momento no es el objeto de estudio, sin embargo es necesario su análisis y presentación como base para la formulación y construcción de teorías algebraicas que lleven hasta la definición y estructuración de las algebras de Lie.

CAPITULO II:

ÁLGEBRA LINEAL Y ELEMENTOS DE TEORÍA DE ÁLGEBRAS EN GENERAL

SECCIÓN 1: ÁLGEBRA LINEAL Y ESPACIOS VECTORIALES

2.1 ESPACIOS VECTORIALES

Como insumo fundamental para el estudio de las álgebras iniciamos definiendo y analizando resultados y aplicaciones trascendentales de los espacios vectoriales, como no es un objeto desconocido para el lector, nos limitaremos a profundizar solo lo necesario.

Además, utilizaremos las matrices como objetos matemáticos pero desde un punto de vista abstracto es decir se consideran los elementos de la matriz como elementos de un campo F. Se asume que el lector domina la teoría básica del álgebra lineal y todo lo concerniente a matrices. Todas las propiedades de matrices en $\mathbb{R}$ se heredan para matrices en un campo F en general.

Ya previamente se definieron estructuras algebraicas muy importantes como los grupos, anillos y campos. A continuación se estudiara otra estructura importante: los espacios vectoriales.

DEFINICIÓN (ESPACIO VECTORIAL) 2.1.1

Un *espacio vectorial* sobre un campo *F*, es un conjunto $V \neq \emptyset$; sobre el que hay definidas dos operaciones:

1. **Suma:**

$$+: V \times V \to V$$

$$(\boldsymbol{u}, \boldsymbol{v}) \to \boldsymbol{u} + \boldsymbol{v}$$

Verificando las siguientes propiedades:

a) Conmutativa: $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}, \forall \boldsymbol{u}, \boldsymbol{v} \in V$.

b) Asociativa: : $(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w}), \forall \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$.

c) Elemento neutro: Existe $0 \in V$ tal que $\boldsymbol{u} + 0 = 0 + \boldsymbol{u} = \boldsymbol{u} \ \forall \boldsymbol{u} \in V$.

d) Elemento opuesto: Para todo $\boldsymbol{u} \in V$ existe $-\boldsymbol{u} \in V$ tal que

$$\boldsymbol{u} + (-\boldsymbol{u}) = (-\boldsymbol{u}) + \boldsymbol{u} = \boldsymbol{0}.$$

2. **Producto por un escalar:**

$$\cdot : F \times V \to V$$

$$(\gamma, \boldsymbol{v}) \to \gamma \cdot \boldsymbol{v}$$

Verificando las siguientes propiedades:

a) $1 \cdot \boldsymbol{u} = \boldsymbol{u} \quad \forall \boldsymbol{u} \in V.$

b) $\gamma \cdot (\mu \cdot \boldsymbol{u}) = (\gamma \cdot \mu) \cdot \boldsymbol{u} \quad \forall \boldsymbol{u} \in V \quad \forall \gamma, \mu \in F.$

c) $(\gamma + \mu) \cdot \boldsymbol{u} = \gamma \cdot \boldsymbol{u} + \mu \cdot \boldsymbol{u} \quad \forall \boldsymbol{u} \in V \quad \forall \gamma, \mu \in F.$

d) $\gamma \cdot (\boldsymbol{u} + \boldsymbol{v}) = \gamma \cdot \boldsymbol{u} + \gamma \cdot \boldsymbol{v} \quad \forall \boldsymbol{u}, \boldsymbol{v} \in V \quad \forall \gamma \in F.$

Los elementos de un espacio vectorial los llamaremos *vectores*.

DEFINICIÓN (SUBESPACIO) 2.1.2

Un subconjunto $W \subseteq V$ es llamado *subespacio* de V si $\alpha_1 w_1 + \alpha_2 w_2 \in W$ para todo $w_1, w_2 \in W$ y $\alpha_1, \alpha_2 \in F$. Los subespacios también son espacios vectoriales.

DEFINICIÓN (COMBINACIÓN LINEAL) 2.1.3

Supongamos que V es un espacio vectorial sobre un campo F y que $\mathfrak{B} \subseteq V$ es un subconjunto no vacío. Una ***combinación lineal*** de vectores $v_1, v_2, \ldots, v_k \in \mathfrak{B}$ donde k es un entero positivo, es un vector de la forma $\sum_{i=1}^{k} \alpha_i v_i$ para algunos $\alpha_1, \alpha_2, \ldots, \alpha_k \in F$.

DEFINICIÓN (EXTENSIÓN) 2.1.4

El conjunto formado por todas las combinaciones lineales de elementos de $\mathfrak{B}$ es un subespacio de V llamado **extensión** de V y lo denotaremos por $E(\mathfrak{B}_F)$.

DEFINICIÓN (INDEPENDENCIA LINEAL) 2.1.5

Los elementos de un subconjunto no vacío $\mathfrak{B} \subseteq V$ son ***linealmente independientes*** si, para k vectores distintos $v_1, v_2, \dots, v_k \in \mathfrak{B}$, la ecuación $\sum_{i=1}^{k} \alpha_i v_i = 0$ se cumple sólo si cada $\alpha_i = 0$.

DEFINICIÓN (BASE) 2.1.6

Un subconjunto no vacío $\mathfrak{B} \subseteq V$ es llamado una ***base*** de V si los elementos de $\mathfrak{B}$ son vectores linealmente independientes y si $E(\mathfrak{B}_F) = V$.

El primer teorema importante álgebra lineal básica establece que si en un espacio de vectores V, la base más pequeña es finita, entonces toda base de V es finita y toda base de V tiene igual número de elementos, este número es llamado dimensión de V. Al espacio de vectores $V = \{0\}$ se le asigna la dimensión 0. Así podemos definir formalmente la dimensión de un espacio vectorial.

DEFINICIÓN (DIMENSIÓN) 2.1.7

Si $\mathfrak{B}$ es una base de un espacio vectorial *V*, entonces la dimensión de *V* es el número de elementos de la base, es decir la cardinalidad de $\mathfrak{B}$.

Si $V = \{0\}$ o si V tiene una base finita $\mathfrak{B}$, entonces V es llamado un espacio de vectores ***finito-dimensional***, de igual forma un espacio de vectores que tiene una base infinita es llamado espacio de vectores ***infinito-dimensional***.

Un ***espacio de vectores simple*** es el espacio F^n formado por todas las *n*-uplas de elementos de un campo *F*. Se adopta convencionalmente que los elementos de F^n son vectores columnas, es decir, si $\xi \in F^n$, entonces existen $\xi_1, \ldots, \xi_n \in F$ tales que:

$$\xi = \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}.$$

Otro espacio de vectores que nos resulta familiar es $\mathcal{M}_{m\times n}(F)$, el espacio de matrices de $m \times n$, donde sus entradas son elementos de un campo F. Con frecuencia los elementos de $\mathcal{M}_{m\times n}(F)$ son vistos como una transformación lineal de F^m a F^n. Se recuerda que:

DEFINICIÓN (TRANSFORMACIÓN LINEAL) 2.1.8

Si *V* y *W* son espacios vectoriales cualesquiera sobre un campo *F*, entonces una función $T: V \to W$ es llamada una ***transformación lineal*** si para todo $\alpha \in F$ y todo $v, v_1, v_2 \in V$, $T(\alpha v) = \alpha T v$ y $T(v_1 + v_2) = T(v_1) + T(v_2)$.

Relacionados con *T* existen dos subespacios:

i. El kernel o núcleo de *T* es el subespacio $\ker T \subseteq V$ de todo $v \in V$ para el cual $T(v) = 0$, y

ii. El rango de T es el subespacio $ran\, T \subseteq W$ de todos los vectores $w \in W$ de la forma $w = T(v)$ para algún $v \in V$.

Si ocurre que una transformación lineal $T: V \to W$ es una biyección, entonces los espacios de vectores *V* y *W* son llamados ***isomorfos*** y esto lo denotamos por $V \cong W$.

El conjunto $\mathfrak{L}(V, W)$, formado por todas las transformaciones lineales $V \to W$, por sí mismo tiene una estructura de espacio vectorial natural. Supongamos que $\alpha \in F$ y $A, A_1, A_2 \in \mathfrak{L}(V, W)$, entonces definimos las transformaciones lineales αA y $A_1 + A_2$ de *V* a *W* por las ecuaciones:

$$(\alpha A)v = \alpha(Av), \quad (A_1 + A_2)v = A_1 v + A_2 v, \quad \forall v \in V.$$

Con estas operaciones, $\mathfrak{L}(V, W)$ es un espacio vectorial. Observe que debido a que las transformaciones lineales son funciones, dos transformaciones lineales *A* y *B* son iguales si y sólo si $Av = Bv$ para todo $v \in V$. Por otro lado, si $V = W$, entonces podemos "componer" dos transformaciones lineales, digamos *S* y *T* en *V*, para producir una tercera transformación, denotémosla por *ST*, donde la acción sobre *V* está definida por $(ST)v = S(Tv), \forall v \in V$. La multiplicación usual de matrices en $\mathcal{M}_{m\times n}(F)$, es un ejemplo concreto de de composición de transformaciones lineales sobre F^n.

Toda transformación lineal de un espacio de vectores finito-dimensional puede ser representada por una matriz. Supongamos que *V* y *W* son espacios vectoriales finito-dimensionales sobre un campo *F*, y $\mathfrak{B}_v$ y $\mathfrak{B}_w$ las bases de *V* y *W* respectivamente. Sean:

$$\mathfrak{B}_v = \{v_1, v_2, \dots, v_n\}$$

$$\mathfrak{B}_w = \{w_1, w_2, \dots, w_m\}.$$

Y además $A \in \mathfrak{L}(V, W)$ una transformación lineal arbitraria. Entonces para cada $j = 1, \dots, n$, el vector Av_j es un elemento de W, y es representado únicamente como una combinación lineal de $w_1, w_2, \dots, w_m$, en otras palabras, existan escalares $\alpha_{ij}, \dots, \alpha_{mj} \in F$ tal que:

$$Av_j = \sum_{i=1}^{m} \alpha_{ij} w_i \qquad \forall j = 1, .., n. \qquad (\dagger)$$

Ahora asociamos con la transformación lineal $A: V \to W$ una matriz $\mathcal{A}$ de $m \times n$ cuyas entradas son elementos que pertenecen a F, donde las (i, j)-entradas de la matriz están dadas por α_{ij}. El rango de la matriz está dado por el tamaño de las columnas de la matriz; igualmente, el rango de nuestra transformación lineal A es la dimensión de los vectores $Av_1, Av_2, \dots, Av_n \in W$. Así la j-ésima columna de la matriz $\mathcal{A}$ puede consistir de vectores Av_j en esta representación como un vector en F^m con respecto a la base $\mathfrak{B}_w$, realmente, Av_j es el vector columna:

$$\begin{bmatrix} \alpha_{ij} \\ \vdots \\ \alpha_{mj} \end{bmatrix} \in F^m.$$

Por lo tanto, para toda transformación lineal $A: V \to W$, la ecuación (†) es la matriz representación de A, con sus respectivas bases $\mathfrak{B}_v$ y $\mathfrak{B}_w$, es:

$$\mathcal{A} = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \vdots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{bmatrix}.$$

Nota: teniendo en cuenta que nuestro objetivo final es estudiar álgebras, vamos a adoptar el hábito de designar a la transformación de identidad $v \mapsto v$ en un espacio vectorial V por 1. En esta notación, la Matriz identidad de $\mathcal{M}_{m\times n}(F)$, también se escribe como 1.

DEFINICIÓN (ESPACIO DUAL) 2.1.9

El ***espacio dual*** V^* de un espacio vectorial V es el espacio vectorial formado por las transformaciones lineales $V \to F$, dónde F es un campo. A una transformación lineal $\varphi: V \to F$ se le llama ***función lineal*** sobre V. El siguiente resultado afirma que $V^* \cong V$ para todo espacio vectorial V finito-dimensional.

PROPOSICIÓN 2.1.10

Para toda base $\mathfrak{B} = \{\mathrm{v}_1, \mathrm{v}_2, \dots, \mathrm{v}_\mathrm{n}\}$ de V le corresponde una base $\mathfrak{B}^* = \{\varphi_1, \varphi_2, \dots, \varphi_\mathrm{n}\}$ de V^*con la propiedad que $\varphi_\mathrm{i}(\mathrm{v}_\mathrm{j}) = 0$, si $\mathrm{i} \neq \mathrm{j}$, y que $\varphi_\mathrm{j}(\mathrm{v}_\mathrm{j}) = 1$ para todo j.

Demostración:

Todo vector $v \in V$determina una única n-upla de escalares $\alpha_i, \dots, \alpha_n \in F$, es decir, las coordenadas de v con respecto a la base $\mathfrak{B}$, tal que:

$$v = \alpha_1 v_1 + \cdots + \alpha_n v_n. \qquad (2.1)$$

Por lo tanto. Para cada $j = 1, \ldots, n$, la función $\varphi_j : V \to F$ definida por $\varphi_j(v) = \alpha_j$, donde α_j es el único escalar que multiplica a v_j que aparece en la ecuación (2.1), está bien definida. Por otra parte, cada φ_j tiene la propiedad que $\varphi_i(v_j) = 0$ cuando $i \neq j$ y $\varphi_j(v_j) = 1$. Se debe verificar que cada φ_j es una transformación lineal. Para esto, supongamos que $v, w \in V$. Entonces

$$v = \alpha_1 v_1 + \cdots + \alpha_n v_n$$

$$w = \beta_1 w_1 + \cdots + \beta_n w_n$$

Para algunos escalares $\alpha_k, \beta_k \in F$. Así,

$$\varphi_j(v + w) = \varphi_j[(\alpha_1 + \beta_1)v_1 + \cdots + (\alpha_n + \beta_n)v_n]$$

$$= \alpha_j + \beta_j$$

$$= \varphi_j(v) + \varphi_j(w).$$

De forma análoga se puede mostrar que $\varphi_j(\alpha v) = \alpha \varphi_j(v)$. Así, para cada j, φ_j es una función lineal sobre *V*.

Ahora, se muestra que $\varphi_1, \ldots, \varphi_n$ son linealmente independientes. Bueno, supongamos que $\gamma_1, \ldots, \gamma_n \in F$ tal que

$$\sum_{j=1}^{n} \gamma_j \varphi_j = 0.$$

Pero entonces, para cualquier $k \in \{1, 2, \dots, n\}$,

$$0 = \left(\sum_{j=1}^{n} \gamma_j \varphi_j \right) v_k = \sum_{j=1}^{n} \gamma_j \varphi_j \, (v_k) = \gamma_k.$$

Puesto que $\varphi_1, \dots, \varphi_n$ son linealmente independientes. Solo restaría verificar que $\varphi_1, \dots, \varphi_n$ efectivamente se encuentra en V^*, lo cual resulta obvio ya que $\varphi_1, \dots, \varphi_n$ son funciones lineales de *V* en *F*.

■

EJEMPLO:

(El dual de F^n). Por conveniencia, cuando consideramos un campo *F* como un espacio de vectores sobre sí mismo, llamamos {1} la base estándar para *F*. para comenzar, *F* y F^n tienen sus respectivas bases estándar. A partir de nuestro análisis anterior, sabemos que cualquier función lineal $\varphi: F^n \to F$ tiene una matriz $1 \times n$, representemos ésta matriz por $\Phi = (\vartheta_1, \vartheta_2, \dots, \vartheta_n)$, donde cada $\vartheta_k \in F$. En este sentido, el espacio dual de F^n puede ser representado por $(F^n)^t$, es decir, puede ser representado por la transpuesta de F^n.

Así, mientras los elementos de F^n, son vectores columna, los elementos de $(F^n)^t$ son representados por vectores fila. Ahora bien, ¿Cuál es la representación matricial de los vectores base duales? Bueno, haciendo una analogía del dual para F^n, puede ser razonable esperar que cada vector base $\varphi_j \in (F^n)^*$ pueda tener una representación matricial de la forma $\Phi_j = e_j^t$. En efecto, este es el caso. Continuando con la analogía, uno puede suponer que la función lineal $\varphi = \sum_{j=1}^n \vartheta_j \varphi_j \in (F^n)^*$ tiene una representación matricial de la forma $\Phi = (\vartheta_1, \vartheta_2, \dots, \vartheta_n)$. En efecto, con $v = \sum_{j=1}^n \xi_k e_k \in F^n$, así tenemos por un lado:

$$\varphi(v) = \sum_{j=1}^{n} \vartheta_j \varphi_j(v) = \sum_{j=1}^{n} \vartheta_j \varphi_j \left(\sum_{k=1}^{n} \xi_k e_k \right)$$

$$= \sum_{j=1}^{n} \sum_{k=1}^{n} \vartheta_j \xi_k \varphi_j(e_k) = \sum_{j=1}^{n} \vartheta_j \xi_j.$$

Y por otro lado:

$$\Phi v = (\vartheta_1, \vartheta_2, \dots, \vartheta_n) \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix} = \sum_{j=1}^{n} \vartheta_j \xi_j.$$

Así, $\varphi(v)$ es el "producto punto", en realidad el producto matricial Φv.

Ahora bien, ¿Cómo calcular la base dual de $(F^n)^*$ a partir de la base de F^n? Supongamos que $v_1, v_2, \dots, v_n \in F^n$ forma una base para F^n. Observamos una base dual,

pero a partir de lo anterior sabemos que el espacio dual es simplemente la transpuesta de F^n; así, vemos *n* vectores $w_1, w_2, \dots, w_n \in F^n$ tal que:

$$w_i^t v_i = 1 \text{ para cada } i \text{ y } w_i^t v_j = 0 \text{ siempre que } i \neq j.$$

Este es realmente un problema de inversión de matrices. Sea $A \in \mathcal{M}_{n\times n}(F)$ la matriz con columnas $v_1, v_2, \dots, v_n$, y sea $B \in \mathcal{M}_{n\times n}(F)$ la matriz con filas $w_1^t, \dots, w_n^t$; entonces $\{w_1^t, \dots, w_n^t\}$ forma una base dual si y sólo si

$$BA = 1, \text{ la matriz identidad.}$$

Así, para obtener la base dual de $v_1, v_2, \dots, v_n$ tomamos las filas $w_1^t, \dots, w_n^t$ de la inversa de la matriz *A* que tiene columnas $v_1, v_2, \dots, v_n$. ✧

2.2 SUMAS DIRECTAS Y ESPACIOS COCIENTES

DEFINICIÓN (SUMA Y SUMA DIRECTA) 2.2.1

Sean *L* y *M* subespacios de un espacio vectorial *V*.

1. El subespacio $L + M$ denota el conjunto de todos los vectores de la forma $f + g$, donde $f \in L$ y $g \in M$, este subespacio es llamado la ***suma*** de *L* y *M*.
2. El subespacio $L \oplus M$ denota $L + M$ en el caso particular cuando $L \cap M = \{0\}$. El subespacio $L \oplus M$ es llamado la ***suma directa*** de *L* y *M*.

Observe que cada $z \in L \oplus M$ tiene una descomposición única como $z = v + w$ para algún $v \in L$ y algún $w \in M$, a continuación se verifica este hecho.

Supongamos que $z \in L \oplus M$ y además supongamos que a *z* lo podemos descomponer de dos formas diferentes, es decir $z = v_1 + w_1 = v_2 + w_2$ para algunos $v_1, v_2 \in L$ y $w_1, w_2 \in M$, entonces $v_1 - v_2 = w_2 - w_1 \in L \cap M = \{0\}$, esto implica que $v_1 - v_2 = 0$ y $w_2 - w_1 = 0$, por lo tanto $v_1 = v_1$ y $w_1 = w_2$.

Si *V* y *W* son espacios vectoriales sobre un campo *F*, entonces el producto Cartesiano

$$V \times W = \{(v, w) : v \in V, w \in W\}$$

tiene una estructura de espacio vectorial dada por

$$(v_1 + w_1) + (v_2 + w_2) = (v_1 + v_2, w_1 + w_2)$$

$$\alpha(v, w) = (\alpha v, \alpha w).$$

El producto Cartesiano $V \times W$, bajo las operaciones de espacio vectorial anteriores, es llamado ***suma directa externa*** de *V* y *W*. La suma directa externa, como la suma directa es denotada por $V \oplus W$.

No hay razón para preocuparse acerca si una suma directa es externa o no, de hecho algunos matemáticos solo mencionan la "suma directa" en general. La razón de esto es que la suma directa externa $V \oplus W$ no es más que la suma directa (interna) de sus

subespacios $V \oplus \{0\}$ y $\{0\} \oplus W$. Pero en la práctica, es conveniente hacer una distinción entre suma directa y suma directa externa.

Ahora pasamos a estudiar los espacios cocientes, pero antes de ello definimos lo que es una clase.

DEFINICIÓN (CLASE) 2.2.2

Supongamos que *W* es un subespacio de un espacio vectorial *V*. Una ***clase*** de *W* es un conjunto de la forma:

$$v + W := \{v + w : w \in W\}.$$

Es importante darse cuenta de que a menos que $W = 0$, cada clase de equivalencia puede tener muchas formas diferentes, en efecto, $v + W = v' + W$ si y sólo si $v - v' \in W$.

DEFINICIÓN (ESPACIO COCIENTE) 2.2.3

El *espacio cociente* denotado por V/W es el conjunto de todas las clases de *W*. El espacio cociente, es un espacio vectorial con la adición definida por:

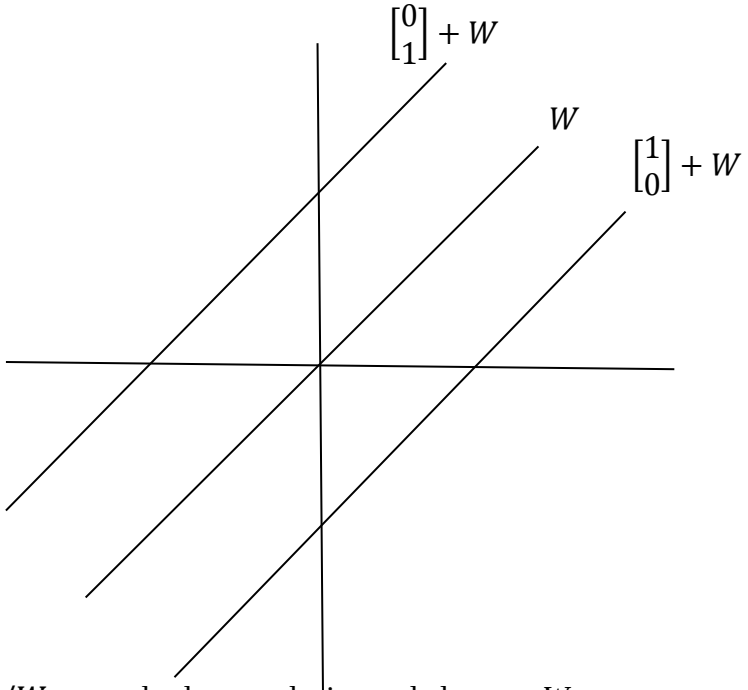
$$(v + W) + (v' + W) = (v + v') + W \quad \forall v, v' \in V$$

Y la multiplicación por un escalar

$$\alpha(v + W) = \alpha v + W \ \ \forall v \in V, \alpha \in F.$$

Falta verificar que estas operaciones están bien definidas, para ello, supongamos que $v + W = v' + W$. Entonces, puesto que $v - v' \in W$, tenemos que $\alpha v - \alpha v' \in W$ para algún escalar $\alpha \in F$, así $\alpha v + W = \alpha v' + W$. Por lo tanto se deduce que las operaciones en efecto, están bien definidas.

El siguiente diagrama muestra los elementos de $\mathbb{R}^2/W$, donde W es el subespacio de $\mathbb{R}^2$ expandido por $\begin{bmatrix}1\\1\end{bmatrix}$:



Las clases de $\mathbb{R}^2/W$ son todas las translaciones de la recta W.

A menudo es útil considerar espacios cocientes cuando se intenta una prueba por inducción sobre la dimensión de un espacio vectorial. En este contexto puede ser útil

saber que si $v_1, v_2, \dots, v_k$ son vectores en *V* tal que las clases $v_1 + W, v_2 + W, \dots, v_k + W$ forman una base para el espacio cociente *V/W*, entonces $v_1, v_2, \dots, v_k$ junto con cualquier base de *W*, forman una base para *V*.

2.3 ALGEBRA BILINEAL

DEFINICIÓN (FORMA BILINEAL) 2.3.1

Una *forma bilineal* sobre *V* es una función

$$(-,-) : V \times V \to F.$$

Tal que

$$(\lambda_1 v_1 + \lambda_2 v_2, w) = \lambda_1 (v_1, w) + \lambda_2 (v_2, w),$$

$$(v, \mu_1 w_1 + \mu_2 w_2) = \mu_1 (v, w_1) + \mu_2 (v, w_2),$$

para todos $v_1, w_i \in V$ y $\lambda_i, \mu_i \in F$.

Por ejemplo, si $F = \mathbb{R}$ y $V = \mathbb{R}^n$, entonces el producto escalar usual es una forma bilineal sobre *V*.

Como para las transformaciones lineales. Podemos representar las formas bilineales mediante matrices. Supongamos que $(-,-)$ es una forma bilineal sobre un espacio de vectores V y que además V tiene como base $\{v_1, \dots, v_n\}$. La matriz de $(-,-)$ con respecto a la base es $A = (a_{ij})$, dónde $a_{ij} = (v_i, v_j)$. Si cambiamos la base, digamos por

$\{w_1, \dots, w_n\}$, entonces la nueva matriz que representa $(-,-)$ es $P^t AP$, donde $P = (p_{ij})$ es la matriz $n \times n$ definida por :

$$w_j = \sum_{i=1}^{n} p_{ij} v_i.$$

Por lo tanto, si existen matrices *A* y *B* que cumplen la relación $B = P^t AP$, decimos que *A* y *B* son ***semejantes***.

Recíprocamente, teniendo una matriz $S = (s_{ij})$, podemos definir una forma bilineal sobre *V* mediante:

$$(v_i, v_j) = s_{ij}.$$

Y extendiéndola "bilinealmente" hacia elementos en $V \times V$. Esto es, si $v = \sum_i \lambda_i v_i$ y $w = \sum_j \mu_j w_j$ con λ_i y μ_j escalares, entonces

$$(v, w) = \sum_{i=1}^{n} \sum_{j=1}^{n} s_{ij} \lambda_i \mu_j \, .$$

La última ecuación puede escribirse en forma matricial como:

$$(v, w) = (\lambda_1 \dots \lambda_n) \begin{pmatrix} s_{11} & \cdots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{n1} & \cdots & s_{nn} \end{pmatrix} \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}.$$

SECCIÓN 2: INTRODUCCIÓN A LA TEORÍA DE ALGEBRAS

En la presente sección se aborda elementos de teoría de álgebras desde su definición, propiedades y ejemplos hasta teoremas que serán sin duda de suma importancia para el estudio de las Álgebras de Lie.

2.4 ÁLGEBRAS

DEFINICIÓN (ÁLGEBRAS) 2.4.1

Una *álgebra* sobre un campo F es un espacio vectorial A sobre F junto con una operación binaria definida entre vectores:

$$A \times A \to A, \qquad (x, y) \to xy.$$

(Decimos que xy es el producto entre x y y) Tal que es bilineal y distributiva respecto a la suma, es decir que para todo $x, y, z \in A$, $\lambda \in F$:

1. $x(y + z) = xy + xz.$
2. $(x + y)\mathrm{z} = xz + yz.$
3. $x(\lambda y) = (\lambda x)y = \lambda(xy).$

La álgebra se dice que es *asociativa* si:

$$(xy)z = x(yz) \qquad \text{para todo } x, y, z \in A.$$

DEFINICIÓN (ÁLGEBRA UNITAL) 2.4.2

La álgebra *A* se dice que es *unital* si existe un elemento 1 en el álgebra con la propiedad

$$1a = a1 = a \qquad \text{para todo } a \in A.$$

EJEMPLO:

Si *E* es un campo de extensión de un campo *F*, entonces $A = E$ es una álgebra asociativa sobre *F*, donde la suma y la multiplicación de elementos de *A* son la suma y la multiplicación del campo en *E*, y la multiplicación del campo *E* y la multiplicación de un escalar por un elemento de *F* es, de nuevo la multiplicación del campo *E*. Para comprobarlo. Sea $x, y, z \in A$, $\lambda \in F$

1. $x(y + z) = xy + xz$ Por ser un campo.
2. $(x + y)\text{z} = z(x + y) = zx + zy = xz + yz$. Recuérdese que un campo cumple con ser un anillo conmutativo.
3. $x(\lambda y) = (x\lambda)y = (\lambda x)y = \lambda(xy)$. Obsérvese que un campo es cerrado bajo la multiplicación, por lo que el producto de $\lambda \in F$ con cualquier elemento de *E* permanece en E. De esta forma, se ha probado que es una algebra.

EJEMPLO:

Para cualquier grupo *G* y cualquier campo *F*, el álgebra definida por $F(G)$, donde $F(G)$ es el conjunto de todas las sumas formales es un álgebra asociativa sobre *F*.

Antes de comprobar que es un álgebra estudiaremos la definición de $F(G)$:

La operación de división en álgebras realmente no existe en general. Sin embargo nos interesaremos en elementos particulares que pueden ser invertibles.

Un elemento $a \in A$ es *invertible* en una algebra unital A si existe un elemento $b \in A$ para el cual $ab = ba = 1$. Este elemento b si existe, es único; b es denotado por a^{-1} y es llamado inverso de a.

DEFINICIÓN (ÁLGEBRA DE DIVISIÓN) 2.4.3

Una álgebra A sobre un campo F es una *álgebra de división* sobre F si A tiene unitario para la multiplicación y contiene un inverso multiplicativo para cada elemento distinto de cero. (Nótese que no se supone la asociatividad de la multiplicación).

EJEMPLO (MUY IMPORTANTE):

La algebra de matrices cuadradas $M_n(F)$ consiste en todas las matrices A $n \times n$ cuyos elementos pertenecen a un campo F y la suma y multiplicación de matrices son las usuales. Si $n > 1$, entonces la algebra de matrices cuadradas es no conmutativa. La matriz unitaria estándar de $M_n(F)$ es, para todos los valores de i, j en $\{1, \dots, n\}$, las matrices denotadas por $E_{i,j} \in M_n(F)$, cada elemento de la matriz es cero excepto para la (i, j) −entrada $(i = j)$, siendo este elemento el unitario del campo F. El conjunto de las matrices unitarias estándar (referidas a las matrices cuya única entrada distinta de cero está en la diagonal, y es uno) es una base para $M_n(F)$. Los elementos invertibles de $M_n(F)$ son precisamente las matrices con determinantes diferentes de cero.

EJEMPLO:

Un campo de extensión *E* sobre un campo *F*, puede considerarse como un álgebra de división asociativa sobre *F*. En el primer ejemplo de esta sección se probó que en efecto es un álgebra asociativa, por lo que se debe argumentar que es de división. Para ello basta recordar que un campo posee elemento unitario, y cada elemento distinto de cero tiene inverso.

EJEMPLO:

Los *cuaterniones de Hamilton* forman un álgebra de división asociativa sobre $\mathbb{R}$. Procedemos a definirlos. Sea $\mathfrak{Q}$ el conjunto $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Hagamos $I = (1\,,0\,,0\,,0)$, $i = (0\,,1\,,0\,,0)\,,\ j = (0\,,0\,,1\,,0)$, $k = (0\,,0\,,0\,,1)$.

Además, acordamos hacer:

$a_1 = (a_1\,,0\,,0\,,0) \qquad a_2 i = (0\,,a_2\,,0\,,0)$

$a_3 j = (0\,,0\,,a_3\,,0)$ y $a_4 k = (0\,,0\,,0\,,a_4)$

Tenemos:

$(a_1\,,a_2,a_3\,,a_4) = a_1 + a_2 i + a_3 j + a_4 k$

Luego se define la suma:

$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) =$

$(a_1 + b_i) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$

Para definir la multiplicación en $\mathfrak{Q}$, comenzamos definiendo $1a = a1 = a$ para $a \in \mathfrak{Q}$

$i^2 = j^2 = k^2 = -1$ y,

$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad y \ ik = -j,$

Nótese la analogía con los productos de vectores.

Se define el producto como:

$(a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 i + b_3 j + b_4 k) =$

$(a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) i$

$+(a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) j$

$+(a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) k.$

Como se observa a partir de la definición de la suma y de la multiplicación en los cuaterniones, la comprobación que Ω forma un álgebra de división asociativa sobre los números reales resulta tediosa.

El conjugado de un cuaternión $x = a_1 + a_2 i + a_3 j + a_4 k$ es $\bar{x} = a_1 - a_2 i - a_3 j - a_4 k.$

El inverso multiplicativo de un cuaternión x distinto de cero, está dado por:

$(a_1 + a_2 i + a_3 j + a_4 k)^{-1} = \frac{1}{\sum_{j=1}^{4} a_j^2} (a_1 - a_2 i - a_3 j - a_4 k).$

■

COMENTARIO

Los números reales, los números complejos y los cuaterniones son las únicas (salvo isomorfismos) álgebras de división asociativas sobre los números reales (Frobenius. 1878).

.

1.5 SUBALGEBRAS

DEFINICIÓN (SUBALGEBRAS) 2.5.1

Si A es una algebra, entonces una *subalgebra* de A es un conjunto $A_0 \subseteq A$ tal que A_0 por si mismo es una algebra. Si A es una algebra unital, podemos decir que A_0 es una subalgebra unital de A si A_0 es una algebra unital y el elemento identidad 1 de A_0 es el elemento identidad de A. Si $A_0 \neq A$, entonces A_0 es una *subalgebra propia*.

Se debe ser consciente que una subalgebra puede dejar de ser una subalgebra unital, pero persiste como una subalgebra.

Por ejemplo, la algebra:

$$A_0 = \left\{ \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & 0 & 0 \end{pmatrix} : a_{ij} \neq 0 \in F \right\}$$

Es una subalgebra de $A = M_3(F)$, pero no es una algebra unital de $M_3(F)$ porque la identidad 1 de $M_3(F)$ no está en A_0:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \notin A_0$$

DEFINICIÓN (SUBALGEBRA GENERADA) 2.5.2

Supóngase que S es un subconjunto no vacío de una algebra A. La *subalgebra generada* por el conjunto S es denotada por $Alg\, S$ y está definida como la mas pequeña subalgebra de A que contiene al conjunto S. En términos de S:

$$Alg\ S = (\{s_1, \dots, s_n : n \in \mathbb{Z}^+,\ \ s_1, \dots, s_n\ \in S\})$$

En particular, si $S = \{s_1, \dots, s_n\} \subseteq A$, entonces la algebra generada por S es denotada por $Alg\{s, \dots, s_n\}$. Si A es una algebra unital, entonces la *algebra unital generada* por un conjunto no vacío S es $Alg\ \tilde{S}$, donde se define $\tilde{S} = S \cup \{1\}$.

Luego, si A es una algebra unital y si $a \in A$, entonces la subalgebra generada por a es:

$$Alg\ \{a\} = \left\{ \sum_{j=1}^{m} \alpha_j a^j : \alpha_1, \dots, \alpha_m \in F\ \ y\ m \in \mathbb{Z}^+ \right\}.$$

Y la subalgebra unital generada por 1 y a es:

$$Alg\ \{1, a\} = \left\{ \sum_{j=0}^{m} \alpha_j a^j : \alpha_0, \dots, \alpha_m \in F\ \ y\ m \in \mathbb{Z}^+ \right\}.$$

Y una algebra generada por dos elementos se representa en términos generales como:

$$Alg\ \{a, b\} = \left\{ \sum_{j=1}^{m} \alpha_j a^j b^j : \alpha_1, \dots, \alpha_m \in F\ \ y\ m \in \mathbb{Z}^+ \right\}.$$

2.6 IDEALES Y HOMOMORFISMOS DE ÁLGEBRAS Y LAS ÁLGEBRAS SIMPLES

DEFINICIÓN (IDEAL) 2.6.1

Un *ideal* en una algebra A es una subalgebra $\mathcal{I} \subseteq A$ para la cual az y za pertenecen a $\mathcal{I}$ para todo $a \in A$ y $z \in \mathcal{I}$. Un ideal $\mathcal{I}$ es un *ideal propio* si $\mathcal{I} \neq A$.

Análogo a las subalgebras, los ideales pueden ser generados por un conjunto de elementos. El *Ideal generado* por el conjunto $S \subseteq A$ es el ideal mas pequeño $\langle S \rangle$ que contiene a S; estos ideales existen, para $\langle S \rangle$ es simplemente la intersección de todos los ideales de A que contienen a S. Otra forma de caracterizar S es vía:

$$\langle S \rangle = \left\{ \sum_{j=1}^{m} a_j s_j b_j \colon m \in \mathbb{Z}^+, \quad s_j \in S, a_j b_j \in A \right\}$$

En particular, el ideal (a) generado por un elemento a en una algebra unital A contiene a $1ab = ab$ y $ca1 = ca$, para todo $b, c \in A$, y 1 es la identidad multiplicativa de A. Cuando el elemento a es multiplicado a la izquierda y a la derecha por 1, tal que $1a1 = a$, los elementos que se forman a partir de la suma de éstos n veces resulta $1a1 + 1a1 + \cdots + 1a1 = a + a + \cdots + a = na$. Luego, si se multiplica a por la derecha y por la izquierda por $e_j, f_j \in A$ respectivamente, talque ambos son distintos de 1, los elementos en general tendrán la forma $e_j a f_j$, en el caso particular cuando uno de los factores es 1 se obtendrán elementos $e_j a$ y $a f_j$. En general, los elementos del ideal

generado son una combinación de los que acabamos de estudiar, y es posible escribirlo explícitamente como sigue:

$$(a) = \left\{ na + ab + ca + \sum_{j=0}^{m} e_j a f_j : n, m \in \mathbb{Z}^+, \qquad b, c, e_j, f_j \in A \; para \; todo \; j \right\}.$$

La clase de algebras simples es sumamente importante.

DEFINICIÓN (ÁLGEBRA SIMPLE) 2.6.2

Una algebra A es llamada *algebra simple* si:

i. El conjunto de todos los posibles productos ab de elementos arbitrarios $a, b \in A$ no es $\{0\}$, y

ii. El único ideal propio $\mathcal{I}$ de A es $\mathcal{I} = \{0\}$.

DEFINICIÓN (CENTRO DE UNA ÁLGEBRA) 2.6.3

El centro de una algebra A es la subalgebra conmutativa:

$$Z(A) = \{a \in A : ab = ba \; para \; todo \; b \in A\}$$

Una algebra unital es llamada *algebra central* si $Z(A) = \{\lambda 1 : \ \lambda \in F, \ 1 \in A\}$. La algebra unital que es a la vez simple y central es llamada *algebra central simple*.

Para construir una nueva algebra de algebras $A_1, \dots, A_n$ sobre un campo F, una forma de hacerlo es mediante el *producto cartesiano*, que es la algebra

$$A_1 \times \cdots \times A_n = \{(a_1, \dots, a_n) : a_j \in A_j \; para \; todo \; 1 \leq j \leq n\}.$$

Y donde las operaciones de espacio vectorial y de anillos son componente a componente. Si $a = (a_1, \dots, a_n)$, $b = (b_1, \dots, b_n)$ son elementos del producto cartesiano y $\alpha, \beta \in F$, entonces:

$$\alpha a + \beta b = (\alpha a_1 + \beta b_1, \dots, \alpha a_n + \beta b_n)$$

$$ab = (a_1 b_1, \dots, a_n b_n).$$

Observe que en el producto cartesiano $A_1 \times \cdots \times A_n$, cada algebra A_j es identificada fácilmente con el ideal :

$$\mathcal{J}_j = \{(0, 0, \dots, 0, a_j, 0, \dots, 0) : a_j \in A_j\}.$$

Y si $x_i \in \mathcal{J}_i$ y $x_j \in \mathcal{J}_j$ para todo $i \neq j$, entonces $x_i x_j = x_j x_i = 0$.

Esto debido a que al menos el A_j contiene posiblemente elementos distintos de cero, que representa la $j - ésima$ posición de la $n - ada$ del producto cartesiano.

Ahora, se definirá el mapeo de interés en teoría de algebras.

DEFINICIÓN (HOMOMORFISMO) 2.6.4

Si A y B son dos algebras, entonces la función $\varphi: A \to B$ es un *homomorfismo* si φ es una transformación lineal y $\varphi(ab) = \varphi(a)\varphi(b)$ para todo $a, b \in A$.

Si A y B son algebras unitales, entonces un homomorfismo φ es llamado *homomorfismo unital* si $\varphi(1_A) = 1_B$.

Por otra parte, un homomorfismo $\varphi: A \to B$ es

i. Un *isomorfismo* si φ es biyectivo.

ii. Un *automorfismo* si $B = A$ y φ es un isomorfismo.

En caso que exista un isomorfismo $\varphi: A \to B$, se denotará por $A \cong B$.

Todo homomorfismo $\varphi: A \to B$ da lugar a dos subalgebras interesantes:

i. El *kernel* de φ, nombrando al conjunto $ker\ \varphi$ de todos los elementos $a \in A$ los cuales $\varphi(a) = 0$.

ii. El *rango* de φ, el cual es el conjunto $ran\ \varphi$ de todos los $b \in B$ para los cuales existe un elemento $a \in A$ tal que $b = \varphi(a)$.

El kernel de un homomorfismo $\varphi: A \to B$ es además un ideal de A.

Uno de los homomorfismos usados con más frecuencia es el mapeo del *polinomio de cálculo funcional* que se define a continuación.

DEFINICIÓN 2.6.5

Suponga que A es una algebra unital sobre un campo F, y fijemos $a \in A$. Si $f(x) = \sum_{j=0}^{n} \alpha_j x^j \in \mathbb{F}[x]$, $f(a)$ denota el elemento $\sum_{j=0}^{n} \alpha_j a^j \in A$.

De cualquier ideal $\mathcal{I}$ de una algebra A se puede definir una relación de equivalencia en A. Declarando que x es equivalente a y $(x, y \in A)$ si y solo si $x - y \in \mathcal{I}$. Se denota al conjunto de todas las clases de equivalencia de elementos de A por $A/\mathcal{I}$, y la clase de equivalencia (ó cociente) de todo elemento $x \in A$ es indicado por $[x]$; así,

$[x] = \{y \in \mathcal{I}: x - y \in \mathcal{I}\}$.

Como en los anillos cocientes y espacios vectoriales cocientes, el conjunto $A/\mathcal{I}$ de clases de equivalencia es en si misma una álgebra bajo las operaciones

$$[x] + [y] = [x + y]$$

$$\alpha[x] = [\alpha x]$$

$$[x][y] = [xy].$$

La algebra $A/\mathcal{I}$ es llamada *algebra cociente*.

TEOREMA (PRIMER TEOREMA DE ISOMORFISMO) 2.6.6

Si A y B son algebras sobre un campo F, y si $\varphi: A \to B$ es un homomorfismo, entonces $A/\ ker\ \varphi \cong ran\ \varphi$.

Demostración

Sea $\Phi: A/\ ker\ \varphi \to ran\ \varphi$ definida por $\Phi([x]) = \varphi(x)$ para todo $[x] \in A/\ ker\ \varphi$.

Primero se tiene que demostrar que Φ esta bien definida, lo que significa que el valor de Φ en la clase lateral $[x]$ no depende del representante arbitrario x para esa clase lateral. Para este fin, sea $x, x' \in A$ son tal que $[x] = [x']$; queremos probar que $\varphi(x) = \varphi(x')$. Se sabe que si $[x] = [x']$ entonces $[x - x'] = [0]$, por lo que $x - x' \in [0]$, entonces $\varphi(x - x') = 0$ y consecuentemente $x - x' \in ker\ \varphi$; y, por linealidad $\varphi(x) = \varphi(x')$. Por lo que Φ está bien definida.

Probemos que Φ es biyectivo.

Claramente Φ es sobreyectivo, porque si $b \in ran\ \varphi$, entonces existe algún $x \in A$ para el cual $b = \varphi(x)$, y así $b = \Phi([x])$.

Ahora se probará que Φ es inyectivo.

Supóngase que $\Phi([x_1]) = \Phi([x_2])$. Entonces $\varphi(x_1) = \varphi(x_2)$ y así $\varphi(x_1 - x_2) = 0$, lo que implica que $x_1 - x_2 \in ker\,\varphi$. Así, $[x_1] = [x_2]$ y es inyectiva.

Como Φ es biyectivo, es isomorfismo. Lo que completa la prueba

■

2.7 ALGEBRAS DE TRANSFORMACIONES LINEALES

Si A es una algebra y $a \in A$ es un elemento fijo, entonces la multiplicación de elementos arbitrarios $b \in A$ a la izquierda por a tiene como efecto una transformación lineal de A:

$$b \mapsto ab, \quad para\ todo\ b \in A.$$

Esta simple observación prefigura una relación significativa que existe entre algebras en lo abstracto y las algebras de transformaciones lineales. Esto es una de las principales ideas de este capitulo.

TEOREMA 2.7.1

Para toda algebra A existe un espacio vectorial V y una subalgebra A_0 de $\mathfrak{L}(V)$ tal que $A \cong A_0$.

Demostración

Sea $V = A$. Para cada $a \in A$, sea L_a una transformación lineal en V definida por $L_a(b) = ab$, $b \in A$. Ahora sea $\varrho: A \to \mathfrak{L}(V)$ la función $\varrho(a) = L_a$. Para verificar que ϱ es un homomorfismo basta verificar que $\varrho(ab) = \varrho(a)\varrho(b)$ como está definida ϱ es una transformación lineal. Para ello, observaremos el comportamiento de L_a y L_b desde su definición aplicados a un elemento $x \in A$, entonces tenemos:

$$\varrho(ab) = L_{ab}$$

$$\Longrightarrow \quad \varrho(ab)(x) = L_{ab}(x)$$

$$= ab(x)$$

$$= \varrho(a)\varrho(b)(x).$$

Así $\varrho(ab) = \varrho(a)\varrho(b)$ y por tanto ϱ es un homomorfismo. Ahora se probará que ϱ es inyectivo. Basta probar que el núcleo es cero. Si $\varrho(a) = 0$ para algún $a \in A$, entonces L_a es la transformación lineal cero. La acción de L_a en $1 \in V$ permanece, por lo tanto, $0 = L_a(1) = a1 = a$ y ϱ es inyectiva. La prueba de que ϱ es sobreyectivo es trivial, ya que $\mathfrak{L}(V)$ contiene todas las transformaciones lineales sobre $V = A$, y por tanto cada elemento de $\mathfrak{L}(V)$ está relacionado con A porque son elementos del mismo conjunto. Esta prueba de isomorfismo resulta en el caso que A es unital.

Si A no es una algebra unital, entonces considere el espacio vectorial producto cartesiano $A \times F$. Distinto a la manera usual de hacer el producto cartesiano de algebras en algebra, la multiplicación en este espacio vectorial se puede definir de una manera diferente:

$$(a, \alpha) \cdot (b, \beta) = (ab + \beta a + \alpha b + \alpha\beta) \qquad \text{para todo } a, b \in A, \quad \alpha, \beta \in F.$$

Fácilmente se verifica que con esta multiplicación $A \times F$ se convierte en algebra, la que denotaremos por $\tilde{A}$. La identidad multiplicativa de $\tilde{A}$ es $(0,1)$, donde $0 \in A$ y $1 \in F$. Obviamente el mapeo $\pi: A \to \tilde{A}$, donde $\pi(a) = (a, 0)$ para todo a, es un homomorfismo inyectivo que involucra a A como subalgebra (de dimensión 1) de $\tilde{A}$. Ahora sea $\tilde{\varphi}: \tilde{A} \to \mathfrak{L}(\tilde{A})$ el homomorfismo inyectivo descrito en el párrafo anterior, y sea $\varphi = \tilde{\varphi} \circ \pi$, un homomorfismo inyectivo $A \to \mathfrak{L}(A)$, donde $V = \tilde{A}$.

■

El homomorfismo inyectivo $A \to \mathfrak{L}(V)$ del teorema anterior es justamente un ejemplo de representación.

DEFINICIÓN (REPRESENTACIÓN) 2.7.2

Una *representación* de una algebra A en un espacio vectorial $\mathfrak{L}(V)$ es un homomorfismo $\pi: A \to \mathfrak{L}(V)$.

Si una representación es inyectiva, entonces es llamada *representación fiel*. En el caso donde A es una algebra unital.

Ahora se analizarán las propiedades básicas de $\mathfrak{L}(V)$ por si misma. Recordar que en la sección 1 de este capitulo V^* denota el dual de un espacio vectorial V y que los elementos de V^* son llamados funciones lineales.

DEFINICIÓN (RANK) 2.7.3

Sean V y W espacios vectoriales no nulos. Si $T: V \to W$ es una transformación lineal Se define *rank T* como la dimensión de *ran T.*

PROPOSICIÓN 2.7.4

Sean V y W espacios vectoriales no nulos.

1. Si $T: V \to W$ es una transformación lineal de rank 1, entonces existe un vector $w \in W$ y una función lineal $\varphi \in V^*$ tal que $T(v) = \varphi(v)w$ para todo $v \in V$.
2. Si $v \in V$ es diferente de cero, entonces existe alguna función lineal $\varphi \in V^*$ para la cual $\varphi(v) = 1$.

Demostración:

(1) Debido a que el rank de T es 1, existe un vector no nulo $w \in W$ que es base para el rango de T. Así, cada $v \in V$ determina una única $\lambda \in F$ tal que $T(v) = \lambda w$. Denotemos el mapeo $v \mapsto \lambda$ por φ. Para probar que φ es lineal, supóngase que $u, v \in V$ y que $T(u) = \mu w$ y $T(v) = \lambda(w)$. Entonces $T(u + v) = T(u) + T(w) = \mu w + \lambda w = (\mu + \lambda)w$; luego $\varphi(u) = \mu$, $\varphi(v) = \lambda$, y $\varphi(u + v) = \mu + \lambda = \varphi(u) + \varphi(v)$. Un argumento muy similar prueba que $\varphi(\alpha v) = \alpha\varphi(v)$. Así, φ es en efecto lineal.

(2) Se necesita probar que existe alguna función lineal $\varphi \in V^*$, para la cual $\varphi(v) = 1$, para algún $v \in V$. Sea B cualquier base de V que contiene un elemento z. Definamos $\varphi: V \to F$ en los elementos de la base por $\varphi(z) = 1$ y $\varphi(y) = 0$ para los elementos

$y \in B, y \neq z$, para probar que es una transformación lineal considérese en la prueba de (1) $u = y, v = z$, y así, $\varphi \in V^*$ y $\varphi(v) = 1$.

■

DEFINICIÓN (PRODUCTO DIRECTO) 2.7.5

Sea R una transformación lineal en V, $w \in V$ un vector fijo, y $\psi \in V^*$ una función lineal tal que $R(v) = \psi(v)w$ para todo $v \in V$. Se define el *producto directo*

$$w \otimes \psi[z] = \psi(z)w \qquad \text{para todo } z \in V.$$

PROPOSICIÓN 2.7.6

Para todo $n \geq 2$, la algebra $M_n(F)$ es una algebra central simple generada por dos matrices no conmutativas.

Demostración

Como $\mathfrak{L}(F^n) \cong M_n(F)$, el teorema anterior implica que todas las álgebras de matrices son algebras simples centrales. Ahora considere la matriz

$$S = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \qquad \text{y} \qquad S^t = \begin{pmatrix} 0 & 0 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 1 & 0 \end{pmatrix}.$$

Para probar que $M_n(F)$ es generado por S y S^t es suficiente probar que todas las matrices con unidad $E_{u,v}$ pertenecen a $Alg\{S, S^t\}$, donde $E_{u,v}$ es la matriz $n \times n$ y exclusivamente la u, v −entrada es 1 para u, v particulares y todas las demás son cero. Para este fin, obsérvese que:

$$S^{n-k}(S^{n-k})^t = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ \vdots & 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}.$$

Y por lo tanto $S^{n-k}(S^{n-k})^t = E_{11} + \cdots + E_{kk}$, para cada $1 \leq k \leq n-1$.

Por lo tanto, cuando $1 \leq u \leq n-1$

$$E_{uu} = E_{11} + \cdots + E_{uu} - (E_{11} + \cdots + E_{u-1u-1})$$

$$= S^{n-u}(S^{n-u})^t - S^{n-u+1}(S^{n-u+1})^t \in Alg\{S, S^t\}.$$

Para obtener la identidad, se escribe

$$1 = S^tS + E_{11} = S^tS + S^{n-1}(S^{n-1})^t \in Alg\{S, S^t\}.$$

Por sustitución directa

$$E_{nn} = 1 - S^tS = S^tS - SS^t + S^{n-1}(S^{n-1})^t \in Alg\{S, S^t\}.$$

Por último, considere la matriz de diagonal cero cuyos elementos no nulos son 1 Tómese cualquier E_{uv} para $u < v$. Como la $(u, v) - ésima$ de S^{u-v} es 1:

$$E_{uv} = E_{uu}S^{v-u} \in Alg\{S, S^t\}$$

Si $u > v$, entonces, $E_{uv} = E_{uu}(S^{u-v})$. Por lo tanto $M_n(F) = Alg\{S, S^t\}$.

■

2.8 INVERSIÓN

El principal logro que se espera de este contenido es probar que si $a \in A$ es invertible y si A es finito-dimensional, entonces el inverso a^{-1} es determinado por un cierto polinomio f evaluado en a.

Recordemos que una extensión K de un campo F se dice que es algebraica si cada $\zeta \in K$es la raíz de un polinomio $f \in F[x]$, y que un campo F es algebraicamente cerrado si no tiene extensiones algebraicas.

DEFINICIÓN (POLINOMIO ANULADOR) 2.8.1

Sea A un álgebra sobre un campo F, $f \in F[x]$ y $a \in A$. Se dice que f es un *polinomio anulador* de a si $f(a) = 0$.

PROPOSICIÓN 2.8.2

Si A es una algebra unital finito-dimensional, entonces para cada $a \in A$ corresponde un único polinomio mónico $m \in F[x]$ con las siguientes propiedades:

1. m es anulado por a;
2. Si $f \in F[x]$ es anulado por a, entonces $f(x) = q(x)m(x)$ para algún polinomio $q \in F[x]$.

Demostración:

En primer lugar se debe demostrar que existe un polinomio anulador para *a*. Ya que *A* es finito-dimensional y unital, supongamos que la dimensión de *A* es *n*. Entonces los $n+1$ elementos $1, a, a^2, \dots, a^n$ son linealmente dependientes en *A*, propiedad que se demuestra en cursos básicos de álgebra lineal. Así, existen escalares $\alpha_j \in F$, donde al menos uno es diferente de cero, tal que:

$$\sum_{j=0}^{n} \alpha_j a^j = 0$$

entonces tomaremos el polinomio diferente de cero

$$f(x) = \sum_{j=0}^{n} \alpha_j x^j \in F[x]$$

Así, si dividimos $f(x)$ entre el coeficiente α_n, se obtiene un polinomio mónico, el cual es anulado por *a*.

También se observa que este polinomio mónico es único, ya que si suponemos que existen dos polinomios con la misma propiedad, es decir sean $m, m' \in F[x]$ tal que $m(a) = 0$ y $m'(a) = 0$, ya que $0 = 0$, entonces $m(a) = m'(a)$, por lo tanto *m* es único.

Para la segunda parte del teorema, tenemos que $f \in F[x]$ y es grado positivo, entonces por el teorema 1.11.21 $f(x)$ es irreducible o $f(x)$ es el producto de polinomios irreducibles.

En el caso de que $f(x)$ sea irreducible se cumple trivialmente el teorema ya que $f(x) = 1 \cdot f(x)$ y podríamos tomar $q(x) = 1$ y $m(x) = f(x)$. Y si $f(x)$ no es mónico, simplemente se factoriza de la forma usual e coeficiente del termino con mayor grado.

Ahora analicemos el caso de que $f(x)$ no sea irreducible, es posible escribir $f(x)$ como

$$f(x) = cp_1(x) \cdot p_2(x) \cdot \ldots \cdot p_k(x),$$

Donde los $p_1(x), \ldots, p_k(x)$ son polinomios mónicos e irreducibles en $F[x]$ y dicha factorización es única excepto el orden de los $p_i(x)$.

Ahora bien, tomemos a $m(x)$ como el polinomio de menor grado en $p_1(x), \ldots, p_k(x)$, digamos que $m(x) = p_j(x)$ y sea

$$q(x) = \prod_{i=1}^{k} p_i(x)\,; i \neq j.$$

Entonces se puede expresar $f(x)$ en términos de $q(x)$ y $m(x)$ como sigue:

$$f(x) = q(x)m(x).$$

Además, esto se evidencia en el hecho de que $f(a) = 0, m(a) = 0$, entonces de igual forma podemos escribir $f(x) = q(x)m(x)$. Con lo cual se demuestra el teorema.

■

El polinomio $m(x)$ que tomamos en la última parte de la de mostración del teorema anterior es conocido como *polinomio minimal*. Lo definimos formalmente de la siguiente forma:

DEFINICIÓN (POLINOMIO MINIMAL) 2.8.3

Sea A una álgebra y sea $a \in A$. El *polinomio minimal* de a es el polinomio mónico de grado mínimo que es anulado por a a.

En teoría de matrices, la invertibilidad de una matriz es reflejada por el valor del determinante, en una vía análoga, la invertibilidad de un elemento en una algebra es reflejado por los coeficiente en el polinomio minimal anulador.

PROPOSICIÓN 2.8.4

Si $m_\alpha(x) = \sum_{j=0}^{n} \alpha_j x^j$ denota el polinomio minimal anulado por $a \in A$.

i. a es invertible si y solo si $\alpha_0 \neq 0$.

ii. Si a es invertible, entonces $a^{-1} = f(a)$, para algún $f \in F[x]$. Específicamente,

$$a^{-1} = \sum_{j=1}^{n} \left[-(\alpha_0)^{-1}\alpha_j\right] a^{j-1}$$

Demostración:

Se probará ii y la parte "$\Leftarrow$ " de i de una sola vez

Supóngase que el termino constante α_0 del polinomio minimal $m_a(x) = \sum_{j=0}^{n} \alpha_j x^j$ de a es no nulo. De $m_a(a) = 0$ se observa que:

$$m_a(a) = \sum_{j=0}^{n} \alpha_j a^j = 0$$

$$\Longrightarrow \alpha_0 + \alpha_1 x^1 + \cdots + \alpha_n x^n = 0$$

$$\Longrightarrow \qquad \alpha_0 + \sum_{j=1}^{n} \alpha_j a^j = 0$$

$$\Longrightarrow \qquad \alpha_0 = -\sum_{j=1}^{n} \alpha_j a^j$$

$$\Longrightarrow \qquad (\alpha_0)^{-1}(\alpha_0) = (\alpha_0)^{-1}\left(-\sum_{j=1}^{n} \alpha_j a^j\right)$$

$$\Longrightarrow 1 = (\alpha_0)^{-1}\left(-\sum_{j=1}^{n} \alpha_j a^j\right) = (\alpha_0)^{-1}\left(-\sum_{j=1}^{n} \alpha_j a^{j-1}\right)a$$

$$= \left(-\sum_{j=1}^{n} \left[(\alpha_0)^{-1}\left(\alpha_j a^{j-1}\right)\right]\right)a = a\left(\sum_{j=1}^{n} \left[-(\alpha_0)^{-1}\alpha_j\right]a^{j-1}\right).$$

Esto prueba que a^{-1} existe y es igual a $f(a)$, donde

$$f(x) = \sum_{j=1}^{n} \left[-(\alpha_0)^{-1}\alpha_j\right]x^{j-1}$$

"$\Longrightarrow$"

A la inversa, supóngase que $a \in A$ es invertible. Si $a_0 = 0$ en el polinomio minimal de a, entonces:

$$0 = m_a(a) = a\left(\sum_{j=1}^{n} \alpha_j a^{j-1}\right).$$

Por la izquierda multiplicando ambos lados de la ecuación anterior por a^{-1}, se obtiene $q(a) = 0$, donde q es el polinomio $q(x) = \sum_{j=1}^{n} \alpha_j a^{j-1}$. Pero el grado de q es menor que el de m_a, contradiciendo la minimalidad del grado de m_a; por lo tanto debe ser que a_0 es diferente de cero.

■

COROLARIO 2.8.5

Si A_0 es una subalgebra finito-dimensional de una algebra A, y si $a \in A_0$ tiene inverso $a^{-1} \in A$, entonces necesariamente $a^{-1} \in A_0$.

Demostración:

Del teorema anterior se obtiene que el inverso de a es

$$a^{-1} = \sum_{j=1}^{n} \left[-(\alpha_0)^{-1}\alpha_j\right] a^{j-1}.$$

Donde $a^{j-1} \in A_0$ para todo j, y $-(\alpha_0)^{-1}\alpha_j \in F$. Además, A_0 es una álgebra sobre F por lo que cada $\left[-(\alpha_0)^{-1}\alpha_j\right] a^{j-1} \in A_0$ para cada j, por lo tanto $a^{-1} \in A_0$.

■

Un elemento $a \in A$ es *invertible por la izquierda* si existe un elemento $b \in A$ tal que $ba = 1$, y es *invertible por la derecha* si existe un elemento $c \in A$ con $ac = 1$.

Un elemento $a \neq 0 \in A$ se dice que es un *divisor de cero* si existe un elemento distinto de cero $b \in A$ para el cual $ab = 0$.

TEOREMA 2.8.6

Supóngase que A es una algebra unital finito-dimensional.

1. Un elemento $a \in A$ es invertible si y solo si a no es divisor de cero.
2. Si $a \in A$ es invertible por la derecha o por la izquierda, entonces a es invertible.
3. Los siguientes declaraciones son equivalentes para $a, b \in A$

   (i) ab es invertible;

   (ii) a y b son invertibles;

   (iii) ba es invertible.

   Si cualquiera de (i) – (iii) se mantienen, entonces $(ab)^{-1} = b^{-1}a^{-1}$.

Demostración:

Para la prueba de (1), ($\Longrightarrow$) supóngase por contradicción que a es un divisor de cero; así $ab = 0$ para algún elemento b distinto de cero. Si a es invertible, entonces multiplicando la ecuación $ab = 0$ por la izquierda por a^{-1} se llega a la conclusión que $b = 0$, lo que no es verdad; así, a no puede ser invertible. ($\Longleftarrow$) Ahora, en el otro sentido, si a no es invertible (por contradicción) entonces por el teorema anterior, el termino constante en el polinomio minimal de a es cero. Por lo tanto, $m_a(x) = xq(x)$ para algún $q \in F(x)$. Por la minimalidad de $m_a(x)$, el polinomio q no puede ser anulado por a. Entonces, $b = q(a)$ es diferente de cero, y $0 = m_a(a) = aq(a) = ab$. (Observación: El elemento b es un polinomio en a y por lo tanto $ab = ba = 0$).

Demostremos (2). Supongamos que a tiene un inverso por la derecha s. Si a deja de ser invertible, entonces por el argumento en (1) existe un elemento distinto de cero b que conmuta con a tal que $ab = ba = 0$. De multiplicar la ecuación $as = 1$ por la izquierda por b, obtenemos $0 = b$, lo que es imposible; por lo tanto, a debe ser invertible. La prueba en el caso donde a tiene un inverso por la izquierda es similar.

Para probar la parte (3), es trivial que (ii) implica (i) y (iii), y que $(ab)^{-1} = b^{-1}a^{-1}$ y $(ba)^{-1} = a^{-1}b^{-1}$. Asumamos, por lo tanto, que (i) se cumple. Si $z \in A$ es tal que $bz = 0$, entonces $(ab)z = 0$, lo que implica que $z = 0$ y ab es invertible. Por lo tanto, b no es divisor de cero, lo que implica que b es invertible por (1). Entonces $aw = 1$, lo que implica que a es invertible por la izquierda; entonces, a es invertible por (2). Un argumento similar se utiliza para probar que (iii) implica (ii).

■

COROLARIO 2.8.7

Sea A una algebra unital finito-dimensional. Para cualquier $a \in A$ y $\lambda \in F$, $a - \lambda 1$ no es invertible si y solo si λ es una raíz del polinomio minimal de a.

Demostración:

($\Longleftarrow$) Supóngase que λ es una raíz del polinomio minimal $m_a \in F[x]$ de a; asi, $m_a(x) = (x-\lambda)q(x)$, para algún $q \in F[x]$ de grado menor que el grado de m_a. Por la minimalidad de m_a, $q(a)$ es diferente de cero. Entonces,

$$0 = m_a(a) = (a-\lambda 1)q(a), \qquad con\ q(a) \neq 0.$$

entonces, $a - \lambda 1$ es un divisor de cero y por lo tanto no es invertible.

($\Longrightarrow$) Supongamos que $a - \lambda 1$ no es invertible. Entonces existe un elemento distinto de cero $b \in A$ tal que $(a-\lambda 1)b = 0 \Longrightarrow ab - \lambda(1b) = 0 \Longrightarrow ab - \lambda b = 0$; esto es, $ab = \lambda b$. Por lo tanto $f(a)b = f(\lambda)b$ para todos los polinomios $f \in F[x]$, y en particular para $f = m_a$. Entonces, $0 = m_a(\lambda)b$, y porque $b \neq 0$ se deduce que $m_a(\lambda) = 0$.

■

PROPOSICIÓN 2.8.8

Si una algebra A unital finito-dimensional,

$$\sigma(ab) = \sigma(ba).$$

Para todo $a, b \in A$

Demostración:

Podemos asumir sin perder generalidad que F es algebraicamente cerrado.

Primero nuestro objetivo es probar que $\sigma(ab) \setminus \{0\} \subseteq \sigma(ba)$. Para hacer eso probaremos el contrapositivo: si $\lambda \neq 0$ y $\lambda \notin \sigma(ba)$, entonces $\lambda \notin \sigma(ab)$. Para este fin, como $\lambda \notin \sigma(ba)$, el elemento $ba - \lambda 1$ tiene un inverso en A. Sea $z = (ba - \lambda 1)^{-1}$. Entonces

$$\lambda 1 = ab - ab + \lambda 1 = a(ba - \lambda 1)zb + \lambda azb - ab - \lambda azb + \lambda 1$$
$$= abazb - ab - \lambda azb + \lambda 1$$
$$= (ab - \lambda 1)(azb - 1).$$

por lo tanto, $ab - \lambda 1$ es invertible, teniendo el inverso $\lambda^{-1}(azb - 1)$. Esto prueba, por lo tanto, que $\sigma(ab) \setminus \{0\} \subseteq \sigma(ba)$.

Ahora, por el teorema 2.8.6, ab es invertible si y solo si ba es invertible. Por lo tanto, $0 \in \sigma(ab)$ si y solo si $0 \in \sigma(ba)$.

Intercambiando los roles de a y b llevan a la conclusión buscada: $\sigma(ab) = \sigma(ba)$.

■

SECCIÓN 3: ALGEBRAS SEMISIMPLES

En esta sección se introduce el estudio de las algebras semisimples. Dichas algebras son susceptibles a través del análisis y la clasificación, y surgen naturalmente, en donde las álgebras juegan un papel importante.

2.9 ÁLGEBRAS NILPOTENTES Y NIL RADICALES

DEFINICIÓN (ELEMENTO NILPOTENTE) 2.9.1

Un elemento a en una algebra A se dice que es *nilpotente* si $a^k = 0$ para algún entero positivo k.

La noción de nilpotencia aplica igualmente a las algebras. Para tener una idea de A^k, donde A es una algebra y k es un entero positivo, usaremos el "calculo de conjuntos".

Si $S_1, \dots, S_n \subseteq A$ son conjuntos no vacíos de una algebra A, entonces su **suma** y **producto** son los conjuntos

$$S_1 + \cdots + S_n = \{s_1 + \cdots + s_n : s_j \in S_j \text{ para todo } 1 \leq j \leq n\}$$

$$S_1 \cdot \dots \cdot S_n = \left\{ \sum_{i=1}^{m} s_1^{(i)} s_2^{(i)} \dots s_n^{(i)} \ : \ m \in Z_0^+, \quad s_j^{(i)} \in S_j \quad 1 \leq j \leq n \quad 1 \leq i \leq m \right\}.$$

El producto de un conjunto de un solo elemento $\{a\}$ con un conjunto arbitrario S puede denotarse por aS. El producto de S con el mismo k veces es denotado por S^k.

Aunque el cálculo de conjuntos tiene muchas identidades utilizables, solo se necesitarán las siguientes para probar los resultados importantes de esta sección.

LEMA 2.9.2

Sea A una algebra, y supóngase que $a \in A$ y que $J, R \subseteq A$ son ideales de A. Entonces

1. $J \cap R, J + R$, y AaA son ideales de A;
2. J^m es un ideal de A para todo $m \in Z^+$;
3. $(J + R)^m \subseteq J^m + R^m + J \cap R$ para todo $m \in Z^+$;
4. $(AaA)^m \subseteq A(aA)^m$.

Demostración:

Las primeras dos aseveraciones son obvias considerando la definición de suma y producto que ya fueron definidas.

Se probara el enunciado 3). En el caso de, decir $m = 2$ es claro que $(J + R)^2 \subseteq J^2 + JR + RJ + R^2$ y el enunciado sigue de que JR y RJ pertenecen al ideal $J \cap R$. Para grandes valores de m la idea es la misma. Un típico elemento $z \in (J + R)^m$ tiene la forma:

$$z = \sum_{i=1}^{q} \left(x_1^{(i)} + y_1^{(i)}\right)\left(x_2^{(i)} + y_2^{(i)}\right) \cdots \left(x_m^{(i)} + y_m^{(i)}\right).$$

Donde $x_i^{(i)} \in J$ y $y_j^{(i)} \in R$ para todo i, j.

La expansión de cada producto $\left(x_1^{(i)} + y_1^{(i)}\right)\left(x_2^{(i)} + y_2^{(i)}\right) \cdots \left(x_m^{(i)} + y_m^{(i)}\right)$ nos da sumandos $x_1^{(i)} \ldots x_m^{(i)} \in J^m$ y sumandos $y_1^{(i)} \ldots y_m^{(i)} \in R^m$, y el resto de sumandos consiste en términos mixtos, lo que significa que cada uno es el producto de términos $x_j^{(i)}$ y $y_k^{(i)}$ así que la suma de cada término mixto siempre está en el ideal $J \cap R$.

Así, z también pertenece a $J^m + R^m + J \cap R$.

■

Dada cualquier algebra A, se tiene una secuencia

$$A \supset A^2 \supset A^3 \supset \cdots \supset \{0\}$$

Lo importante de esto es que alguna potencia de A llega a cero.

DEFINICIÓN (ÁLGEBRA NILPOTENTE) 2.9.3

Una algebra A se dice que es *nilpotente* (de índice k) si hay un entero positivo k tal que $A^{k-1} \neq \{0\}$ y $A^k = 0$.

Utilizando solamente la definición es difícil determinar cuando una algebra es o no nilpotente. Como sea, hay algo que si es claro: Si una algebra es nilpotente, entonces lo es cada uno de sus elementos individuales. El siguiente resultado resulta de mucha

utilidad, proporciona una prueba de nilpotencia para el algebra a través de sus elementos individuales.

TEOREMA 2.9.4

Si A es una algebra finito-dimensional, entonces A es nilpotente si y solo si cada uno de sus elementos es nilpotente.

Demostración:

" $\Rightarrow$ "

Si A es una algebra nilpotente de índice k, entonces para toda $a \in A, a^k \in A^k = \{0\}$. Por lo tanto, todo elemento de A es nilpotente.

" $\Leftarrow$ "

Para la demostración en el sentido contrario se procederá por inducción sobre la dimensión de la álgebra. Para ello, supóngase que A es 1-dimensional y que cada elemento de A es nilpotente. Entonces A es generada por un elemento nilpotente no nulo $a \in A$. Ahora para cada $m \in Z^+$, A^m es generada por a^m; es decir, que la nilpotencia de a implica la nilpotencia de la algebra A.

Para continuar con el caso general, asumamos que A es una algebra finito-dimensional con la propiedad de que cada uno de sus elementos es nilpotente. Nuestra hipótesis

inductiva es: Si B es una algebra de dimensión $\dim B < \dim A$ y cada elemento $b \in B$ es nilpotente, entonces B es una algebra nilpotente.

Sea $\vartheta: A \to \mathfrak{Q}(A)$ una representación de A, y sea $a \in A$ un elemento arbitrario. Como a es nilpotente, $\vartheta(a)$ es necesariamente una transformación lineal nilpotente en el espacio vectorial finito-dimensional A. Como tal, $\vartheta(a)$ no es invertible y por lo tanto su rank es estrictamente menor que la dimensión de A:

$$\dim(aA) < \dim(a)$$

Donde (a) es el álgebra generada por el elemento a. Todo $z \in (aA)$ esta contenido en A, y así cada elemento (aA) es nilpotente; por la hipótesis inductiva, la algebra (aA) es una algebra nilpotente.

Ahora considere el ideal

$$AaA = \left\{ \sum_j a_1^{(j)} a a_2^{(j)} \quad : \quad a_1^{(j)},\ a_2^{(j)} \in A \text{ para toda } j \right\}$$

Por el lema 2.9.2, $(AaA)^m \subseteq A(aA)^m$; Así el ideal AaA es nilpotente. Para todo $a_1, \dots, a_n \in A$, cada uno de los ideales Aa_jA es nilpotente, como es su suma. En particular, si $\{a_1, \dots, a_n\}$ es una base de A, entonces

$$Aa_1A + Aa_2A + \cdots + Aa_nA = A^3$$

por lo que A^3 es nilpotente, implicando que A si misma es nilpotente.

■

PROPOSICIÓN 2.9.5

Si A es una algebra finito-dimensional, entonces hay un único ideal nilpotente R que contiene a todos los ideales nilpotentes J de A.

Demostración:

Si $\{0\}$ es el único ideal nilpotente de A, entonces la conclusión del teorema es trivial. Supongamos, entonces, que A tiene un ideal nilpotente no nulo; entre todos los ideales nilpotentes no nulos, se elige uno cuya dimensión es el máximo posible y se denotara este ideal por R.

Supóngase ahora que J es un ideal nilpotente arbitrario de A; entonces la intersección $R \cap J$ es un ideal nilpotente por el lema 2.9.2, y además:

$$(J + R)^m \subseteq J^m + R^m + J \cap R \quad \text{para todo } m \in Z^+.$$

Así, para una potencia suficientemente alta de m, $(R + J)^m \subseteq R \bigcap J$, implicando que $(J + R)^m$ es un ideal nilpotente; por lo tanto $R + J$ es nilpotente. Por la maximalidad de la dimensión de R entre ideales nilpotentes, se tiene que

$\dim R \geq \dim(R + J) = \dim R + \dim J - \dim(A \cap J)$.

Dado que $\dim J \leq \dim(A \cap J)$, y así $J \subseteq R$.

■

DEFINICIÓN (NILRADICAL) 2.9.6

El *nil radical* de A es el ideal "más grande" nilpotente de A que contiene todos los ideales nilpotentes de A. El nil radical es denotado por $Rad\ A$.

DEFINICIÓN (PROPIEDAD NILPOTENTE) 2.9.7

Un elemento $a \in A$ se dice que tiene la *propiedad nilpotente* si az es nilpotente para cada $z \in A$.

Observe que si az es nilpotente, entonces lo es za. (Demostración: $(za)^k = z(az)^{k-1}a$ para todo $k \in Z^+$). Nótese que si $a \in A$ tiene la propiedad nilpotente, entonces $a^2 = a \cdot a$ es nilpotente, implicando que a si mismo sea nilpotente.

TEOREMA 2.9.8

Si una algebra A tiene dimensión finita, entonces su nil radical es el conjunto de todos los elementos $a \in A$ con la propiedad nilpotente.

Demostración:

Sea B el conjunto de todos los elementos con la propiedad nilpotente en A. Si $a \in Rad\ A$, entonces $az \in Rad\ A$ para todo $z \in A$; por otra parte, el ideal $Rad\ A$ es

nilpotente, todo elemento de $Rad\ A$ es nilpotente. Por lo tanto, az es nilpotente para todo $z \in A$, probando que $Rad\ A \subseteq B$.

Inversamente, primero tenemos como objetivo probar que el conjunto B de elementos con la propiedad nilpotente es un ideal. Supóngase, por lo tanto, que $a \in B$ y $z \in A$. Para cualquier $w \in A$, $az(w) = a(zw)$ resulta ser nilpotente; por lo tanto az tiene la propiedad nilpotente, que es lo mismo decir que $az \in B$. Por un argumento similar $za \in B$.

Queda por demostrar que $a + b \in B$ para todo $a, b \in B$. En el párrafo previo se demostró que si $a \in B$, entonces az es nilpotente para todo $z \in A$; en otras palabras, la subalgebra aA es nilpotente (Proposición 2.9.5). Usando la relación $(AaA)^m \subseteq A(aA)^m$ (Lema 2.9.2), podemos concluir que el ideal AaA es nilpotente y, entonces, $AaA \subseteq Rad\ A$. Luego, si $a, b \in B$, entonces $a^3, b^3, aba, ab^2, ba^2, bab$ todos se encuentran en $(AaA) \cup (AbA) \subseteq Rad\ A$. Así,

$$a^3 + aba + ab^2 + a^2b + ba^2 + b^2a + bab + b^3 = (a + b)^3 \in Rad\ A.$$

Lo que prueba que $(a + b)^3$ es nilpotente, de donde $a + b$ es nilpotente. En otras palabras, la suma de cualquier dos elementos con la propiedad nilpotente es nilpotente. Pero aun hace falta probar que $a + b$ tiene la propiedad nilpotente. Para es te fin, se toma cualquier $z \in A$ y consideremos $(a + b)z$. Como $(a + b)z = az + bz$ es una suma de dos elementos con la propiedad nilpotente, y como la suma de dos elementos con la

propiedad nilpotente es nilpotente, $(a+b)z$ es nilpotente. Por lo tanto $(a+b) \in B$, lo que completa la prueba que B es un ideal.

Como B es un ideal en el que cada elemento es nilpotente, B es un ideal nilpotente por la proposición 2.9.4. Por la proposición 2.9.5 el nil radical contiene todos los ideales nilpotentes: Por lo tanto $B \subseteq Rad\ A$.

■

Opuestos a los elementos nilpotentes están los idempotentes.

DEFINICIÓN (IDEMPOTENTE) 2.9.9

En una algebra A un elemento e es *idempotente* si $e^2 = e$. Claramente una algebra nilpotente no puede tener un idempotente distinto de cero, pero es verdaderamente interesante que la nilpotencia en una algebra es la única obstrucción para la existencia de elementos idempotentes distintos de cero.

COMENTARIO 2.9.10

Si A es una algebra finito-dimensional que no es nilpotente, entonces A tiene un elemento idempotente distinto de cero.

TEOREMA 2.9.11

Si una algebra A finito-dimensional diferente de cero es tal que $Rad\ A = \{0\}$, entonces A tiene una identidad multiplicativa – es decir, A es una algebra unital.

Demostración:

Como A es una algebra distinta de cero y no nilpotente, hay, por la proposición 2.9.10, un distinto de cero idempotente $e \in A$. Nuestro primer objetivo es demostrar que A posee un e distinto de cero e idempotente tal que el único idempotente $f \in A$ para el cua $ef = fe = 0$ es $f = 0$; idempotentes con esta propiedad son llamados *idempotentes principales*.

Para cualquier idempotente $e \in A$, principal o de otra manera, sea $\mathfrak{L}_e = \{x \in A : xe = 0\}$ y $\mathfrak{R}_e = \{y \in A : ey = 0\}$. Entonces $\mathfrak{L}_e \cap \mathfrak{R}_e$ es el conjunto de todos los $z \in A$ para el cual $ez = ze = 0$ y por lo tanto un idempotente $e \in A$ es un idempotente principal si y solo si $\mathfrak{L}_e \cap \mathfrak{R}_e$ es una algebra nilpotente (posiblemente cero), otra vez por la proposición 2.9.10.

Ahora vamos a probar que A tiene un idempotente principal e. Se elige cualquier idempotente diferente de cero $e_1 \in A$. Si $\mathfrak{L}_{e_1} \cap \mathfrak{R}_{e_1}$ es una subalgebra nilpotente, entonces $e = e_1$ es principal; en otro caso, $\mathfrak{L}_{e_1} \cap \mathfrak{R}_{e_1}$ tiene al menos un idempotente distinto de cero f_1 y, necesariamente, $e_1 f_1 = f_1 e_1 = 0$. Asumiremos esta última

posibilidad. Sea $e_2 = e_1 + f_1$, que es un idempotente porque $e_2^2 = e_1^2 + e_1 f_1 + f_1 e_1 + f_1^2 = e_1 + f_1 = e_2$. Es también cierto que $e_2 \neq 0$, para $e_1 f_1 = f_1 e_1 = 0$ implica que e_1 y f_1 son linealmente independientes. Ahora considere $\mathfrak{L}_{e_2} \cap \mathfrak{R}_{e_2}$. Si esta subalgebra es nilpotente, entonces $e = e_2$ es un idempotente principal; en otro caso, existe un idempotente distinto de cero $f_2 \in \mathfrak{L}_{e_2} \cap \mathfrak{R}_{e_2}$ de donde podemos obtener un nuevo idempotente distinto de cero $e_3 = e_2 + f_2$. Una iteración de este método de argumentación produce una sucesión de subalgebras $\mathfrak{L}_{e_j} \cap \mathfrak{R}_{e_j}$ para el cual

$$\left(\mathfrak{L}_{e_1} \cap \mathfrak{R}_{e_1}\right) \supseteq \cdots \supseteq \left(\mathfrak{L}_{e_j} \cap \mathfrak{R}_{e_j}\right) \supseteq \left(\mathfrak{L}_{e_{j+1}} \cap \mathfrak{R}_{e_{j+1}}\right) \supseteq \cdots \supseteq \{0\}$$

y una sucesión de idempotentes distintos de cero $e_{j+1} = e_j + f_j$ para algún idempotente distinto de cero $f_j \in \mathfrak{L}_{e_j} \cap \mathfrak{R}_{e_j}$. Se deberá probar ahora que cada iteración anterior se mantiene y es adecuada.

Si $z \in \mathfrak{L}_{e_{j+1}} \cap \mathfrak{R}_{e_{j+1}}$, entonces

$0 = ze_{j+1} = e_{j+1}z$; que es, $0 = ze_j + zf_j = e_j z + f_j z$.

Así,

$$\begin{aligned} 0 = e_{j+1}0 = e_{j+1}(e_j z) + e_{j+1}(f_j z) &= (e_j + f_j)e_j z + 0 \\ &= (e_j^2)z + (f_j e_j)z \\ &= e_j z + 0 \qquad \text{(Porque } f_j \in \mathfrak{L}_{e_j} \cap \mathfrak{R}_{e_j}\text{)} \\ &= e_j z. \end{aligned}$$

De una manera similar, la multiplicación de $0 = ze_j + zf_i$ en el lado derecho por e_{j+1} conduce a $ze_j = 0$. Por lo tanto, $z \in \mathfrak{L}_{e_j} \cap \mathfrak{R}_{e_j}$, como se había afirmado.

La inclusión $\left(\mathfrak{L}_{e_j} \cap \mathfrak{R}_{e_j}\right) \supseteq \left(\mathfrak{L}_{e_{j+1}} \cap \mathfrak{R}_{e_{j+1}}\right)$ es correcta porque $f_j \in \mathfrak{L}_{e_j} \cap \mathfrak{R}_{e_j}$, pero $f_j \notin \mathfrak{L}_{e_{j+1}} \cap \mathfrak{R}_{e_{j+1}}$.

Así, la sucesión de subalgebras $\mathfrak{L}_{e_j} \cap \mathfrak{R}_{e_j}$ es una sucesión correcta decreciente. Como A tiene dimensión finita, esta sucesión eventualmente tiende a $\{0\}$ o a una algebra nilpotente distinta de cero de la forma $\mathfrak{L}_{e_k} \cap \mathfrak{R}_{e_k}$. En cualquiera de los dos eventos, la iteración del procedimiento anterior se detiene y el último idempotente e_k producida por la iteración es un idempotente principal.

Asumamos ahora que $e \in A$ es un idempotente principal, y considere los siguientes cuatro subespecies lineales de A:

$$V_1 = eAe\,, \qquad V_2 = e\mathfrak{L}_e, \qquad V_3 = \mathfrak{R}_e e, \qquad V_4 = \mathfrak{L}_e \cap \mathfrak{R}_e$$

Dado cualquier $a \in A$, podemos escribir $a = a_1 + a_2 + a_3 + a_4$ tal que $a_j \in V_j$ para cada j: tomemos

$$a_1 = eae,\ \ a_2 = e(a - ae),\ \ a_3 = (a - ea)e,\ \ a_4 = a - ea - ae + eae. \quad (1)$$

De hecho, este es el único camino tal para representar $a \in A$ como una suma de $a_j \in V_j$, como ahora se demostrará. Supóngase que $a = a_1 + a_2 + a_3 + a_4$ para algún (todavía indeterminado) $a_j \in V_j$. Entonces la multiplicación de esta ecuación en el lado izquierdo por e y en el derecho por e produce:

$$ea = e(a_1 + a_2 + a_3 + a_4) = ea_1 + ea_2 + ea_3 + ea_4$$

$$= e(eae) + e[e(a - ae)] + e(a - ea)e + e(a - ea - ae + eae)$$

$$= e^2ae + e^2a - e^2ae + eae - e^2ae + ea - e^2a - eae + e^2ae$$

$$= e^2ae - e^2ae + ea = eae - eae + ea$$

$$= eae + [e(a - ae)]$$

$$= a_1 + a_2.$$

Análogamente se obtiene $ae = a_1e + a_3e = a_1 + a_3$.

Multiplicando la primera ecuación por la derecha por e se obtiene $eae = a_1e + 0 = a_1$, obteniendo así el valor de a_1. De las dos ecuaciones anteriores y el ultimo resultado obtenido se tiene que:

$$ea = a_1 + a_2, \quad \text{o} \quad a_2 = ea - eae; \text{ y}$$

$$ae = a_1 + a_3, \quad \text{o} \quad a_3 = ae - eae.$$

Teniendo ahora determinados los valores de a_1, a_2, a_3, el valor de a_4 es $a_4 = a - a_1 - a_2 - a_3 = a - ea - ae + eae$. Así, A es la suma directa de cuatro subespacios V_1, V_2, V_3, V_4.

Hasta este punto se ha utilizado solamente que A no es una algebra nilpotente; ahora se explotará el hecho que $Rad\, A = \{0\}$. Para empezar, como $\mathfrak{L}_e \cap \mathfrak{R}_e$ es una algebra nilpotente y como

$$\mathfrak{L}_e\mathfrak{R}_e = \left\{\sum_i y_i x_i \ : \ ey_i = x_i e = 0\right\}.$$

Hay un cierto número entero positivo k para el cual $(\mathfrak{L}_e\mathfrak{R}_e)^k = \{0\}$. Así, $\{0\} = \mathfrak{L}_e(\mathfrak{L}_e\mathfrak{R}_e)^k\mathfrak{R}_e = (\mathfrak{L}_e\mathfrak{R}_e)^{k+1}$, lo cual implica que el ideal $\mathfrak{L}_e\mathfrak{R}_e$ es nilpotente y, por lo tanto, $\mathfrak{L}_e\mathfrak{R}_e \subseteq Rad\ A = \{0\}$; en otras palabras $\mathfrak{L}_e\mathfrak{R}_e = \{0\}$.

Ahora sea $b \in e\mathfrak{L}_e$ arbitrario. Entonces hay un $x \in \mathfrak{L}_e$ tal que $b = ex$. Por lo tanto, para cualquier $a \in A$, expresado en la ecuación (1), tenemos

$$ba = ex(eae) + ex\big(e(a - ae)\big) + ex(a - ea)e + ex(a - ea - ae + eae). \quad (2)$$

Los primeros dos sumandos son cero porque $xe = 0$; el tercer y cuarto sumandos son cero porque $x(a - ea)$ y $x(a - ea - ae + eae)$ son elementos de $\mathfrak{L}_e\mathfrak{R}_e = \{0\}$. Esto prueba que para todo $a \in A, ba = 0$ (nilpotente). Por tanto, $b \in Rad\ A$ y así $b = 0$. Similarmente, si $c \in \mathfrak{R}_e e$, entonces hay un $y \in \mathfrak{R}_e$ tal que $c = ye$. Entonces, para cualquier $a \in A$,

$$ac = (eae)ye + e(a - ae)ye + \big((a - ea)e\big)ye + (a - ea - ae + eae)ye. \quad (3)$$

Como con la ecuación (2), la ecuación (3) prueba que $ac = 0$, lo que implica que $c \in Rad\ A$ y $c = 0$. Luego, V_3 y V_4 son cero. Finalmente, si $z \in V_4 = \mathfrak{L}_e \cap \mathfrak{R}_e$, entonces para cada $a \in A$,

$$za = z(eae) + z\big(e(a - ae)\big) + z(a - ea)e + z(a - ea - ae + eae). \quad (4)$$

Los primeros dos sumandos son cero porque $ze = 0$; el tercer y cuarto sumando son cero porque tanto $z(a - ea)$ como $z(a - ea - ae + eae)$ pertenecen a $\mathfrak{L}_e\mathfrak{R}_e = \{0\}$. Por lo tanto, como antes, z es nilpotente propio y así $z = 0$. Esto prueba que V_4 es cero.

Habiendo probado que V_2, V_3, V_4 son subespacios cero, la única descomposición de todo $a \in A$ en términos de $a_j \in V_j$ indica que $a_2 = a_3 = a_4 = 0$, lo cual implica que $a = a_1 = eae, ea = eae = a$, y $ae = eae = a$. Por lo tanto, el idempotente principal e es una identidad multiplicativa.

■

COROLARIO 2.9.12

Toda algebra simple finito-dimensional es unital.

Demostración:

El ideal $Rad\ A$ es cualquiera de los dos $\{0\}$ o A, como la algebra A es simple. Si $Rad\ A = \{0\}$, entonces A es una algebra unital, por el teorema 2.3.11. Así, solamente necesitamos probar que A no es nilpotente. Por definición, $A^2 \neq \{0\}$; pero como A^2 es un ideal de A, debe ser que $A^k = A$ para todo $k \in Z^+$, donde probamos que A no es nilpotente.

■

2.10 ESTRUCTURA DE ÁLGEBRAS SEMISIMPLES

DEFINICIÓN (ÁLGEBRA SEMISIMPLE) 2.10.1

Una algebra A finito-dimensional distinta de cero es llamada *algebra semisimple* si $Rad\ A = \{0\}$.

La demostración del corolario 2.9.12 indica que toda algebra simple es semisimple. La justificación para el término "semisimple" para algebras con radicales triviales es proporcionada por la siguiente proposición.

PROPOSICIÓN 2.10.2

Cualquier producto Cartesiano de un numero finito de algebras simples finito-dimensional es una algebra semisimple.

Para la demostración revisar el libro *Algebras of linear transformation* de Douglas R. Farenick.

No todas las algebras semisimples aparecen representadas como un producto Cartesiano.

PROPOSICIÓN 2. 10.3

$Rad\ (A/Rad\ A) = \{0\}$ para toda algebra A finito-dimensional. En particular, si $A \neq Rad\ A$, entonces la algebra cociente $A/Rad\ A$ es semisimple.

Demostración:

Sea $q: A \to A/Rad\ A$ un homomorfismo cociente canónico. Supóngase que $a \in A$ es tal que $q(a)$ es nilpotente. Nuestro objetivo es probar que a por si mismo es un nilpotente, que haría la implicación que $a \in Rad\ A$ y $q(a) = 0$. Sea $z \in A$ arbitrario; como $q(a)$ es nilpotente, $[q(a)q(z)]^k = 0 \in A/Rad\ A$ para algún entero positivo k. Esto es equivalente a $q([az]^k) = 0$ y $[az]^k \in Rad\ A$. Dado que todo elemento del radical es nilpotente, el elemento az por sí mismo debe ser nilpotente. En otras palabras, a es nilpotente.

■

TEOREMA 2. 10.4

Supóngase que G es un grupo finito, y sea F un campo de característica $Car\ F$. La algebra grupo FG es semisimple si y solo si $Car\ F = 0$ o $Car\ F$ no divide al orden de G.

Para la demostración revisar el libro *Algebras of linear transformation* de Douglas R. Farenick.

■

CAPÍTULO III:

INTRODUCCIÓN A LAS ÁLGEBRAS DE LIE

SECCIÓN 1: DEFINICIÓN DE ÁLGEBRAS DE LIE Y EJEMPLOS

3.1 DEFINICIÓN DE ÁLGEBRAS DE LIE

DEFINICIÓN (ÁLGEBRA DE LIE) 3.1.1

Sea F un campo. Una *álgebra de Lie* sobre F es un F espacio vectorial L junto con una función bilineal llamada *forma de Lie:*

$$L \times L \to L, \qquad (x, y) \mapsto [x, y].$$

Que satisface las siguientes propiedades:

$[x, x] = 0 \quad \forall x \in L.$ (L1)

$\big[x, [y, z]\big] + \big[y, [z, x]\big] + \big[z, [x, y]\big] = 0 \ \ \forall x, y, z \in L.$ (L2)

Una álgebra de Lie es *abeliana* si $\forall x, y \in L$ se cumple que $[x, y] = 0$.

Todas las álgebras que trabajaremos son reales o complejas, y se asumirá que todas son reales a menos que se haga otra especificación.

La forma de Lie $[x, y]$ es a menudo llamada el conmutador de x y y. La condición (L2) es conocida como *identidad Jacobiana*. Como la forma de Lie $[-,-]$ es bilineal, se tiene:

$$0 = [x + y, x + y] = [x, x] + [x, y] + [y, x] + [y, y] = [x, y] + [y, x].$$

Por lo tanto la condición (L1) implica:

$$[x, y] = -[y, x] \ \forall x, y \in L \qquad \text{(L1')}$$

escribiendo $x = y$ en (L1') mostramos que (L1') implica (L1).

A menos que sea especificado de otra manera, todas las algebras de Lie serán tomadas como finito-dimensionales.

Para ser más específicos, es posible enumerar todas las propiedades que demanda la definición de álgebra de Lie que cumplan sus elementos x, y, z , ... :

1. El conmutador de dos elementos es un elemento de la algebra

   $[x, y] \in L$ para todo $x, y \in L$.
2. Una combinación lineal $\alpha x + \beta y$ de elementos $x , y \in L$ con los números reales o complejos $\alpha \ y \ \beta$, es también un elemento del álgebra de Lie, es decir

   $\alpha x + \beta y \in L$ si $x, y \in L$.

   Asimismo el elemento 0 (cero) pertenece a el álgebra.
3. Las siguientes igualdades son válidas porque el conmutador es bilineal

   $[\alpha x + \beta y, z] = \alpha[x, z] + \beta[y, z]$ para todo $x, y, z \in L$.

$[x, \beta y + \gamma z] = \beta[x, y] + \gamma[x, z]$ para todo $x, y, z \in L$.

4. Intercambiando ambos elementos del conmutador resulta en la relación

   $[x, y] = -[y, x]$.

   Como se demostró en la página anterior.

5. Y finalmente, como es obvio la identidad de Jacobi

   $\big[x, [z, y]\big] + \big[y, [z, x]\big] + \big[z, [x, y]\big] = 0 \ \ \forall x, y, z \in L$.

Nótese que no demanda que el conmutador sea asociativo, es decir, la relación $\big[x, [y, z]\big] = \big[[x, y], z\big]$ no es verdadera en general. Algunos autores pueden cambiar la secuencia lógica de las propiedades que cumplen los elementos de una álgebra de Lie, sin embargo son las mismas.

PROPOSICIÓN 3.1.2

Sea L una álgebra de Lie, entonces $\big[x, [y, z]\big] = \big[x, -[z, y]\big]$ $\forall x, y, z \in L$.

Demostración:

$$-\big[x, [y, z]\big] + \big[x, [y, z]\big] = 0$$

$$\Longrightarrow -\big[x, -[z, y]\big] + \big[x, [y, z]\big] = 0$$

$$\Longrightarrow \big[x, [y, z]\big] = \big[x, -[z, y]\big].$$

■

De forma análoga se puede probar que $[x,[y,z]] = -[x,[z,y]]$. Se omitirá la prueba.

Para este estudio, demandaremos que la álgebra de Lie tenga dimensión finita, es decir, contiene un conjunto de n elementos linealmente independientes $e_1, e_2, e_3, \dots, e_n$, (que en realidad es una base de *L*) por lo cual todo elemento x de una álgebra de Lie puede ser representada por:

$$x = \sum_{j=1}^{n} \xi_j e_j \qquad \xi \in F.$$

En otras palabras, la álgebra constituye un espacio vectorial n-dimensional. En ocasiones la dimensión es llamada *orden*. Si los coeficientes ξ_j son reales, la álgebra es llamada real, en una álgebra compleja los coeficientes con complejos.

Los elementos e_j de la base satisfacen la identidad de Jacobi, y utilizaremos este argumento para demostrar lo siguiente: *Para probar que un espacio vectorial es una álgebra de Lie basta verificar que los elementos de la base satisfacen las condiciones de Lie.*

En este caso consideremos los elementos arbitrarios

$$x = \sum_{j=1}^{n} \xi_j e_j \ , \qquad y = \sum_{i=1}^{n} \eta_i e_i \ , \qquad z = \sum_{k=1}^{n} \zeta_k e_k.$$

Antes de probar que satisfacen la identidad de Jacobi, vamos a introducir la notación

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

Y con los elementos de la base, deberá cumplirse

$$\{e_j, e_i, e_k\} = \Big[e_j, [e_i, e_k]\Big] + \Big[e_i, \big[e_k, e_j\big]\Big] + \Big[e_k, \big[e_j, e_i\big]\Big].$$

Para la demostración, remplazaremos los valores de x, y, z

$$[x, [y, z]] = \left[\sum_{j=1}^{n} \xi_j e_j \, , \left[\sum_{i=1}^{n} \eta_i e_i \, , \sum_{k=1}^{n} \zeta_k e_k\right]\right].$$

Se analizará por separado cada conmutador

$$\left[\sum_{i=1}^{n} \eta_i e_i \, , \sum_{k=1}^{n} \zeta_k e_k\right] = \left[\eta_1 e_1 \, , \sum_{k=1}^{n} \zeta_k e_k\right] + \left[\eta_2 e_2 \, , \sum_{k=1}^{n} \zeta_k e_k\right] + \cdots + \left[\eta_n e_n \, , \sum_{k=1}^{n} \zeta_k e_k\right].$$

$$\left[\eta_1 e_1 \, , \sum_{k=1}^{n} \zeta_k e_k\right] = [\eta_1 e_1 \, , \zeta_1 e_1] + [\eta_1 e_1 \, , \zeta_2 e_2] + \cdots + [\eta_1 e_1 \, , \zeta_n e_n].$$

$$\left[\eta_2 e_2 \, , \sum_{k=1}^{n} \zeta_k e_k\right] = [\eta_2 e_2 \, , \zeta_1 e_1] + [\eta_2 e_2 \, , \zeta_2 e_2] + \cdots + [\eta_2 e_2 \, , \zeta_n e_n].$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$\left[\eta_n e_n \, , \sum_{k=1}^{n} \zeta_k e_k\right] = [\eta_n e_n \, , \zeta_1 e_1] + [\eta_n e_n \, , \zeta_2 e_2] + \cdots + [\eta_n e_n \, , \zeta_n e_n].$$

Luego se observa que

$$\left[\sum_{i=1}^{n}\eta_i e_i\ ,\sum_{k=1}^{n}\zeta_k e_k\right]=\sum_{i=1}^{n}\sum_{k=1}^{n}[\eta_i e_i\ ,\zeta_k e_k].$$

Luego bajo la misma idea se obtiene

$$\left[\sum_{j=1}^{n}\xi_j e_j\ ,\left[\sum_{i=1}^{n}\eta_i e_i\ ,\sum_{k=1}^{n}\zeta_k e_k\right]\right]=\sum_{j=1}^{n}\sum_{i=1}^{n}\sum_{k=1}^{n}\left[\xi_j e_j,[\eta_i e_i,\zeta_k e_k]\right].$$

De forma análoga podemos escribir cada conmutador de la identidad de Jacobi, y finalmente escribirla:

$$\{x,y,z\}=\left[x,[y,z]\right]+\left[y,[z,x]\right]+\left[z,[x,y]\right]$$

$$=\left[\sum_{j=1}^{n}\xi_j e_j\ ,\left[\sum_{i=1}^{n}\eta_i e_i\ ,\sum_{k=1}^{n}\zeta_k e_k\right]\right]+\left[\sum_{i=1}^{n}\eta_i e_i\ ,\left[\sum_{k=1}^{n}\zeta_k e_k\ ,\sum_{j=1}^{n}\xi_j e_j\right]\right]$$

$$+\left[\sum_{k=1}^{n}\zeta_k e_k\ ,\left[\sum_{j=1}^{n}\xi_j e_j\ ,\sum_{i=1}^{n}\eta_i e_i\right]\right]$$

$$=\sum_{j=1}^{n}\sum_{i=1}^{n}\sum_{k=1}^{n}\left[\xi_j e_j,[\eta_i e_i,\zeta_k e_k]\right]+\sum_{j=1}^{n}\sum_{i=1}^{n}\sum_{k=1}^{n}\left[\eta_i e_i,\left[\zeta_k e_k,\xi_j e_j\right]\right]$$

$$+\sum_{j=1}^{n}\sum_{i=1}^{n}\sum_{k=1}^{n}\left[\zeta_k e_k,\left[\xi_j e_j,\eta_i e_i\right]\right]$$

$$=\sum_{j=1}^{n}\sum_{i=1}^{n}\sum_{k=1}^{n}(\left[\xi_j e_j,[\eta_i e_i,\zeta_k e_k]\right]+\left[\eta_i e_i,\left[\zeta_k e_k,\xi_j e_j\right]\right]+\left[\zeta_k e_k,\left[\xi_j e_j,\eta_i e_i\right]\right])$$

(Como los ξ_j, η_i, ζ_k son arbitrarios, escribiremos la ultima expresión como sigue)

$$= \sum_{j=1}^{n}\sum_{i=1}^{n}\sum_{k=1}^{n} \xi_j \eta_i \, \zeta_k (\big[e_j, [e_i, e_k]\big] + \big[e_i, \big[e_k, e_j\big]\big] + \big[e_k, \big[e_j, e_i\big]\big])$$

$$= \sum_{j=1}^{n}\sum_{i=1}^{n}\sum_{k=1}^{n} \xi_j \eta_i \, \zeta_k \{e_j, e_i, e_k\}$$

$$= \sum_{jik}^{n} \xi_j \eta_i \, \zeta_k \{e_j, e_i, e_k\} = 0.$$

Como cada forma de Jacobi en el lado derecho de nuestra igualdad es una elección distinta, permite que se utilicen todas las combinaciones distintas de los elementos de la base, con este argumento, para probar la identidad de Jacobi para una álgebra de Lie es suficiente probar que la condición es válida para los elementos de la base.

Claramente los elementos $e_1, e_2, \dots, e_n$ de la base pueden dar origen a la construcción de una nueva base.

Con una matriz no singular $\underline{r}$, que contiene los números reales o complejos r_{kl}, una nueva base $e_1^*, e_2^*, \dots, e_n^*$ pueden construirse así:

$$e_k^* = \sum_{l=1}^{n} r_{kl} e_l \qquad r_{kl} \in F.$$

Los nuevos elementos satisfacen la identidad de Jacobi como fue probado previamente. Como bien sabemos, los elementos e_k^* son linealmente independientes si $e_1, e_2, \dots, e_n$ lo

son, y si $\underline{r}$ es no singular. Por supuesto un cambio de base de una álgebra de Lie compleja (o real) es compleja (o real), dependiendo de sus coeficientes.

3.2 LA ESTRUCTURA CONSTANTE

El conmutador de dos elementos de la base pertenece a la álgebra y, siguiendo el análisis podemos escribirlo como:

$$[e_i, e_k] = \sum_{l=1}^{n} C_{ikl} e_l$$

DEFINICIÓN (ESTRUCTURA CONSTANTE) 3.2.1

Los coeficientes de la relación $[e_i, e_k] = \sum_{l=1}^{n} C_{ikl} e_l$ son llamados *estructura constante* relativa a la base $\{e_i\}_{i=1}^{n}$.

Dado el conjunto de los elementos de la base, la estructura constante especifica el tipo de álgebra de Lie, es decir, una álgebra de Lie con estructura constante compleja es compleja, y si la estructura constante es real, la álgeabra de Lie es real.

1.3 ALGUNOS EJEMPLOS DE ÁLGEBRAS DE LIE

EJEMPLO 3.3.1

Sea $F = \mathbb{R}$. El producto de vectores $(x, y) \mapsto x \wedge y$ define la estructura de un álgebra de Lie sobre $\mathbb{R}^3$. Denotamos esta álgebra de Lie por $\mathbb{R}^3_\wedge$. Explícitamente si $x = (x_1, x_2, x_3)$ y $y = (y_1, y_2, y_3)$, entonces:

$$x \wedge y = (x_2 y_3 - x_3 y_2, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1).$$

Para verificar que en realidad es una álgebra de Lie, hay que demostrar que el producto de vectores es bilineal, y que además satisface las condiciones de Lie.

Para verificar que es bilineal. Sea $x_1 = (x_{11}, x_{12}, x_{13})$, $x_2 = (x_{21}, x_{22}, x_{23})$, $y = (y_1, y_2, y_3)$, $w_1 = (w_{11}, w_{12}, w_{13})$, $w_2 = (w_{21}, w_{22}, w_{23})$, y para todo $\lambda_i, \mu_i \in F$ hay que probar que se cumple:

i. $(\lambda_1 x_1 + \lambda_2 x_2, y) = \lambda_1 (x_1 + y) + \lambda_2 (x_2 + y)$.

ii. $(y, \mu_1 w_1 + \mu_2 w_2) = \mu_1 (y, w_1) + \mu_2 (y, w_2)$.

Prueba de i.

$\lambda_1 x_1 + \lambda_2 x_2 = \lambda_1 (x_{11}, x_{12}, x_{13}) + \lambda_2 (x_{21}, x_{22}, x_{23})$

$= (\lambda_1 x_{11} + \lambda_2 x_{21}, \lambda_1 x_{12} + \lambda_2 x_{22}, \lambda_1 x_{13} + \lambda_2 x_{23})$.

Luego

$$[\lambda_1 x_1 + \lambda_2 x_2, y] = (\lambda_1 x_1 + \lambda_2 x_2) \wedge y$$

$$= \{(\lambda_1 x_{12} + \lambda_2 x_{22}) y_3 - (\lambda_1 x_{13} + \lambda_2 x_{23}) y_2, (\lambda_1 x_{13} + \lambda_2 x_{23}) y_1$$
$$- (\lambda_1 x_{11} + \lambda_2 x_{21}) y_3, (\lambda_1 x_{11} + \lambda_2 x_{21}) y_2 - (\lambda_1 x_{12} + \lambda_2 x_{22}) y_1\}$$

$$= (\lambda_1 x_{12} y_3 + \lambda_2 x_{22} y_3 - \lambda_1 x_{13} y_2 - \lambda_2 x_{23} y_2, \lambda_1 x_{13} y_1 + \lambda_2 x_{23} y_1 - \lambda_1 x_{11} y_3$$
$$- \lambda_2 x_{21} y_3, \lambda_1 x_{11} y_2 + \lambda_2 x_{21} y_2 - \lambda_1 x_{12} y_1 - \lambda_2 x_{22} y_1)$$

$$= (\lambda_1 x_{12} y_3 - \lambda_1 x_{13} y_2, \lambda_1 x_{13} y_1 - \lambda_1 x_{11} y_3, \lambda_1 x_{11} y_2 - \lambda_1 x_{12} y_1) + (\lambda_2 x_{22} y_3$$
$$- \lambda_2 x_{23} y_2, \lambda_2 x_{23} y_1 - \lambda_2 x_{21} y_3, \lambda_2 x_{21} y_2 - \lambda_2 x_{22} y_1)$$

$$= \lambda_1 (x_{12} y_3 - x_{13} y_2, x_{13} y_1 - x_{11} y_3, x_{11} y_2 - x_{12} y_1) + \lambda_2 (x_{22} y_3 - x_{23} y_2, x_{23} y_1$$
$$- x_{21} y_3, x_{21} y_2 - x_{22} y_1)$$

$$= \lambda_1 (x_1 \wedge y) + \lambda_2 (x_2 \wedge y).$$

Para probar ii.

$$\mu_1 w_1 + \mu_2 w_2 = \mu_1 (w_{11}, w_{12}, w_{13}) + \mu_2 (w_{21}, w_{22}, w_{23})$$

$$= (\mu_1 w_{11} + \mu_2 w_{21}, \mu_1 w_{12} + \mu_2 w_{22}, \mu_1 w_{13} + \mu_2 w_{23}).$$

Luego

$$[y, \mu_1 w_1 + \mu_2 w_2] = y \wedge (\mu_1 w_1 + \mu_2 w_2)$$

$$= \{y_2(\mu_1 w_{13} + \mu_2 w_{23}) - y_3(\mu_1 w_{12} + \mu_2 w_{22}), y_3(\mu_1 w_{11} + \mu_2 w_{21}) - y_1(\mu_1 w_{13} + \mu_2 w_{23}), y_1(\mu_1 w_{12} + \mu_2 w_{22}) - y_2(\mu_1 w_{11} + \mu_2 w_{21})\}$$

$$= (y_2\mu_1 w_{13} + y_2\mu_2 w_{23} - y_3\mu_1 w_{12} - y_3\mu_2 w_{22}, y_3\mu_1 w_{11} + y_3\mu_2 w_{21} - y_1\mu_1 w_{13} - y_1\mu_2 w_{23}, \mu_1 y_1 w_{12} + y_1\mu_2 w_{22} - y_2\mu_1 w_{11} - y_2\mu_2 w_{21})$$

$$= (y_2\mu_1 w_{13} - y_3\mu_1 w_{12}, y_3\mu_1 w_{11} - y_1\mu_1 w_{13}, \mu_1 y_1 w_{12} - y_2\mu_1 w_{11}) + (y_2\mu_2 w_{23} - y_3\mu_2 w_{22}, y_3\mu_2 w_{21} - y_1\mu_2 w_{23}, y_1\mu_2 w_{22} - y_2\mu_2 w_{21})$$

$$= \mu_1(y_2 w_{13} - y_3 w_{12}, y_3 w_{11} - y_1 w_{13}, y_1 w_{12} - y_2 w_{11}) + \mu_2(y_2 w_{23} - y_3 w_{22}, y_3 w_{21} - y_1 w_{23}, y_1 w_{22} - y_2 w_{21})$$

$$= \mu_1(y \wedge w_1) + \mu_2(y \wedge w_2)$$

$$= \mu_1(y, w_1) + \mu_2(y, w_2).$$

Esto prueba que el producto vectorial es bilineal.

Falta verificar que cumple con las condiciones de Lie, es decir que

(a) $[x, x] = 0 \quad \forall x \in L.$

(b) $\big[x, [y, z]\big] + \big[y, [z, x]\big] + \big[z, [x, y]\big] = 0 \ \ \forall x, y, z \in L.$

Prueba de (a)

$$[x,x] = x \wedge x = (x_2x_3 - x_3x_2, x_3x_1 - x_1x_3, x_1x_2 - x_2x_1) = (0,0,0) = 0.$$

La demostración de (b) es un poco más extensa

$$[y,z] = y \wedge z = (y_2z_3 - y_3z_2, y_3z_1 - y_1z_3, y_1z_2 - y_2z_1).$$

$$[z,x] = z \wedge x = (z_2x_3 - z_3x, z_3x_1 - z_1x_3, z_1x_2 - z_2x_1).$$

$$[x,y] = x \wedge y = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1).$$

$$\big[x,[y,z]\big] = x \wedge (y \wedge z)$$

$$= \langle x_2(y_1z_2 - y_2z_1) - x_3(y_3z_1 - y_1z_3), x_3(y_2z_3 - y_3z_2)$$
$$- x_1(y_1z_2 - y_2z_1), x_1(y_3z_1 - y_1z_3) - x_2(y_2z_3 - y_3z_2)\rangle$$

$$= (x_2y_1z_2 - x_2y_2z_1 - x_3y_3z_1 + x_3y_1z_3, x_3y_2z_3 - x_3y_3z_2 - x_1y_1z_2 + x_1y_2z_1, x_1y_3z_1$$
$$- x_1y_1z_3 - x_2y_2z_3 + x_2y_3z_2). \ (*)$$

$$\big[y,[z,x]\big] = y \wedge (z \wedge x)$$

$$= \langle y_2(z_1x_2 - z_2x_1) - y_3(z_3x_1 - z_1x_3), y_3(z_2x_3 - z_3x)$$
$$- y_1(z_1x_2 - z_2x_1), y_1(z_3x_1 - z_1x_3) - y_2(z_2x_3 - z_3x)\rangle$$

$$= (y_2z_1x_2 - y_2z_2x_1 - y_3z_3x_1 + y_3z_1x_3, y_3z_2x_3 - y_3z_3x_2 - y_1z_1x_2 + y_1z_2x_1, y_1z_3x_1$$
$$- y_1z_1x_3 - y_2z_2x_3 + y_2z_3x_2). \ (**)$$

$$\big[z,[x,y]\big] = z \wedge (x \wedge y)$$

$$= \langle z_2(x_1y_2 - x_2y_1) - z_3(x_3y_1 - x_1y_3), z_3(x_2y_3 - x_3y_2)$$
$$- z_1(x_1y_2 - x_2y_1), z_1(x_3y_1 - x_1y_3) - z_2(x_2y_3 - x_3y_2)\rangle$$

$$= (z_2x_1y_2 - z_2x_2y_1 - z_3x_3y_1 + z_3x_1y_3, z_3x_2y_3 - z_3x_3y_2 - z_1x_1y_2 + z_1x_2y_1, z_1x_3y_1$$
$$- z_1x_1y_3 - z_2x_2y_3 + z_2x_3y_2) \ (***).$$

Sumando las primeras componentes de (*), (**) y (***) se obtiene

$$x_2y_1z_2 - x_2y_2z_1 - x_3y_3z_1 + x_3y_1z_3 + y_2z_1x_2 - y_2z_2x_1 - y_3z_3x_1 + y_3z_1x_3 + z_2x_1y_2$$
$$- z_2x_2y_1 - z_3x_3y_1 + z_3x_1y_3 = 0$$

Sumando las segundas componentes de (*), (**) y (***) se obtiene

$$x_3y_2z_3 - x_3y_3z_2 - x_1y_1z_2 + x_1y_2z_1 + y_3z_2x_3 - y_3z_3x_2 - y_1z_1x_2 + y_1z_2x_1 + z_3x_2y_3$$
$$- z_3x_3y_2 - z_1x_1y_2 + z_1x_2y_1 = 0.$$

Sumando las terceras componentes de (*), (**) y (***) se obtiene

$$x_1y_3z_1 - x_1y_1z_3 - x_2y_2z_3 + x_2y_3z_2 + y_1z_3x_1 - y_1z_1x_3 - y_2z_2x_3 + y_2z_3x_2 + z_1x_3y_1$$
$$- z_1x_1y_3 - z_2x_2y_3 + z_2x_3y_2 = 0.$$

Así se deduce que

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

Y por lo tanto es una álgebra de Lie.

EJEMPLO 3.3.2

Cualquier espacio de vectores V tiene una forma de Lie definida por $[x, y] = 0 \ \forall x, y \in V$. Esta es una álgebra de Lie *abeliana* sobre V. En particular el campo F puede considerarse como un álgebra de Lie 1-dimensional.

EJEMPLO 3.3.3

Supongamos que V es un espacio de vectores sobre F con dimensión finita. Denotamos por gl(V) el conjunto de todas las funciones lineales de V a V. Este es de nuevo un espacio de vectores sobre F, y puede definirse un conmutador sobre gl(V) de modo que sea una álgebra de Lie. Teniendo conocimientos sobre *álgebra lineal general*, podemos definir la forma de Lie $[-,-]$, como: $[x, y] = xoy - yox$, para $x, y \in$ gl(V), donde o denota la composición de funciones.

Asumiremos de una vez que el conmutador definido es bilineal, la prueba no presenta dificultad y se omitirá. Se probará únicamente que cumple las condiciones de Lie.

(a) $[x, x] = 0 \quad \forall x \in$ gl(V).

(b) $\big[x, [y, z]\big] + \big[y, [z, x]\big] + \big[z, [x, y]\big] = 0 \ \forall x, y, z \in$ gl(V).

La parte (a) es trivial

$[x, x] = xox - xox = 0.$

Luego, para verificar (b)

$[y,z] = yoz - zoy \qquad ,[z,x] = zox - xoz \qquad ,[x,y] = xoy - yox.$

$$[x,[y,z]] = xo(yoz - zoy) - (yoz - zoy)ox$$
$$= xo(yoz) - xo(zoy) - (yoz)ox + (zoy)ox.$$

$$[y,[z,x]] = yo(zox - xoz) - (zox - xoz)oy$$
$$= yo(zox) - yo(xoz) - (zox)oy + (xoz)oy.$$

$$[z,[x,y]] = zo(xoy - yox) - (xoy - yox)oz$$
$$= zo(xoy) - zo(yox) - (xoy)oz + (yox)oz.$$

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]]$$
$$= xo(yoz) - xo(zoy) - (yoz)ox + (zoy)ox + yo(zox) - yo(xoz)$$
$$- (zox)oy + (xoz)oy + zo(xoy) - zo(yox) - (xoy)oz + (yox)oz$$
$$= 0.$$

Por lo tanto es una álgebra de Lie.

EJEMPLO 3.3.4

Podemos hacer del ejemplo anterior una analogía con matrices. Denotemos por gl(n, F) el espacio de vectores de todas las matrices $n \times n$ sobre F, con la forma de Lie definida por:

$$[x,y] = xy - yx;$$

donde xy es el producto usual de matrices x entre y.

Para ilustrar considere las matrices $x = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, z = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. La prueba de L1 es trivial, se verificará solo la identidad de Jacobi.

$$[x, y] = xy - yx = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

$$[z, x] = zx - xz = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

$$[y, z] = yz - zy = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

$$\big[x, [y, z]\big] = x[y, z] - [y, z]x = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

$$\big[y, [z, x]\big] = y[z, x] - [z, x]y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

$$\big[z, [x, y]\big] = z[x, y] - [x, y]z = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Luego$\big[x, [y, z]\big] + \big[y, [z, x]\big] + \big[z, [x, y]\big] = 0$.

Así como un espacio de vectores gl(n, F) tiene una base que consiste en *matrices unidad* e_{ij} para todos $1 \leq i, j \leq n$. Aquí e_{ij} es la matriz $n \times n$ la cual tiene un 1 en la ij-ésima posición y en todas las demás posiciones 0. Nosotros podemos tomar la forma de Lie como:

$$\big[e_{ij}, e_{kl}\big] = \delta_{jk} e_{il} - \delta_{il} e_{kj}.$$

donde δ es la delta de Kronecker, definida por $\delta_{ij} = 1$ si $i = j$ y $\delta_{ij} = 0$ en cualquier otro caso.

EJEMPLO 3.3.5

Recordemos que la traza de una matriz cuadrada es la suma de sus entradas de la diagonal principal. Ahora bien, sea sl(n, F) el subespacio de gl(n, F) de todas las matrices de traza cero. Para matrices cuadradas arbitrarias $x, y \in$ sl(n, F) , la matriz $xy - yx$ tiene trazo 0, así $[x, y] = xy - yx$, define una estructura de álgebra de Lie sobre sl(n, F). Ésta álgebra de Lie es conocida como *algebra lineal especial.* Como un espacio de vectores sl(n, F) tiene una base que consiste en las matrices unidad e_{ij}, para $i \neq j$ junto con $e_{ii} - e_{i+1,i+1}$ para $1 \leq i < n$.

Estos resultados son variaciones surgidas del análisis hecho al inicio del capítulo, donde se demostró que para comprobar que un espacio vectorial es una álgebra de Lie basta que los elementos de la base satisfagan las condiciones de Lie. Recuérdese que cualquier matriz puede formarse con elementos de la base e_{ij}. Este análisis se inició en el capítulo anterior.

EJEMPLO 3.3.6

Sea b(n, F) el conjunto de matrices triangulares superiores en gl(n, F). (Una matriz x es llamada triangular superior si cumple con $x_{ij} = 0$ siempre que $i > j$). Esta es un álgebra de Lie con la misma forma de Lie de gl(n, F).

Similarmente, sea n(n, F) el conjunto de matrices estrictamente triangulares superiores en gl(n, F). (Una matriz x es llamada estrictamente triangular superior si $x_{ij} = 0$ siempre que $i \geq j$). De nuevo ésta es una álgebra de Lie con la misma forma de Lie de gl(n, F).

SECCIÓN 2: ELEMENTOS DE LA TEORÍA DE ÁLGEBRAS DE LIE

3.4 SUBALGEBRAS E IDEALES DE UNA ÁLGEBRA DE LIE

En los últimos dos ejemplos sugerimos que teniendo un álgebra de Lie L, es posible definir una *subalgebra de Lie*.

DEFINICIÓN (SUBALGEBRA DE LIE) 3.4.1

Una *subalgebra de Lie* de L es un subespacio de vectores $K \subseteq L$ tal que:

$$[x, y] \in K \ \ \forall x, y \in K.$$

Las subalgebras de Lie son fáciles de observar en las propias álgebras de Lie. En los ejemplos (5) y (6) mostramos tres ejemplos de subalgebras de gl(n, F).

También definimos un *ideal* de una álgebra de Lie L.

DEFINICIÓN (IDEAL DE UNA ÁLGEBRA DE LIE) 3.4.2

Un *ideal* de una álgebra de Lie L es un subespacio I de L tal que:

$[x, y] \in I$ para todo $x \in L$, $y \in I$.

Por la condición (L1'), $[x, y] = -[y, x]$, así no necesitamos distinguir entre ideales izquierdos o derechos. Por ejemplo sl(n, F) es un ideal de gl(n, F) y n(n, F) es un ideal de b(n, F).

Un ideal siempre es una subalgebra. Pero, por otro lado, una subalgebra no necesariamente es un ideal. Por ejemplo b(n, F) es una subalgebra de gl(n, F), pero si $n > 2$, no es un ideal. Para ver esto note que $e_{11} \in$ b(n, F) y $e_{21} \in$ gl(n, F). Tenemos con el conmutador definido en el ejemplo 4 ($[x, y] = xy - yx$) que $[e_{21}, e_{11}] = e_{21} \notin$ b(n, F).

La álgebra de Lie L es por sí mismo un ideal de L, esto es válido porque $\forall x, y \in L$ se cumple que $[x, y] \in L$, la condición de ideal.Así como también $\{0\}$ es un ideal de L, a estos se les llama *ideales triviales* de L. Un ejemplo importante de un ideal que es no-trivial es el *centro* de L, el cual definimos por:

DEFINICIÓN (CENTRO DE UNA ÁLGEBRA DE LIE) 3.4.3

Se define el *centro* de una álgebra de Lie como:

$$Z(L) = \{x \in L : [x, y] = 0 \ \ \forall y \in L\}.$$

TEOREMA 3.4.4

Sea L una álgebra de Lie y $Z(L)$ su centro. Se cumple que $L = Z(L)$ si y sólo si L es abeliano.

Demostración:

" $\Longrightarrow$ "

Como $L = Z(L)$ entonces $[x, y] = 0 = [y, x] \quad \forall y, x \in L$, por lo tanto L es abeliano.

" $\Longleftarrow$ "

Como L es abeliano $\forall\, x \in L \;\; [x, y] = 0$, por lo tanto $L = Z(L)$.

■

3.5 HOMOMORFISMOS ENTRE ÁLGEBRAS DE LIE

DEFINICIÓN (HOMOMORFISMO ENTRE ÁLGEBRAS DE LIE) 3.5.1

Si L_1 y L_2 son álgebras de Lie sobre un campo F, entonces se dice que una función $\varphi: L_1 \to L_2$ es un *homomorfismo* si φ es una función lineal y:

$$\varphi([x, y]) = [\varphi(x), \varphi(y)] \; \forall x, y \in L_1.$$

Note que en esta ecuación la primera forma de Lie es tomada en L_1 y la segunda en L_2.

Decimos que φ es un *isomorfismo* si φ es biyectiva. Un importantísimo homomorfismo es el *homomorfismo adjunto*.

DEFINICIÓN (HOMOMORFISMO ADJUNTO) 3.5.2

Si L es un álgebra de Lie el *homomorfismo adjunto* es definido como:

$$ad: L \to \mathrm{gl}(L)$$

$$x \to adx \quad tal\ que$$

$$(adx)(y) = [x, y]\ para\ x, y \in L.$$

Obsérvese que la función $x \mapsto adx$ es por sí misma lineal. Luego para mostrar que ad es un homomorfismo todo lo que necesitamos verificar es que:

$$ad([x,y]) = adx\ o\ ady - ady\ o\ adx \qquad \forall x, y\ \in L.$$

Para llegar a este resultado recuérdese que *ad* es homomorfismo si

$ad[x,y] = [adx, ady]$.

Aplicaremos $ad([x,y])$ a un elemento $z \in L$.

$(ad[x,y])(z) = \big[[x,y],z\big]$

$= -\big[z,[x,y]\big]$

$= -\{-\big[x,[y,z]\big] - \big[y,[z,x]\big]\}$ Utilizando la identidad de Jacobi

$= \big[x,[y,z]\big] + \big[y,[z,x]\big]$

$= \big[x,[y,z]\big] - \big[y,[x,z]\big]$

$= (adx)[y,z] - (ady)[x,z]$

$= (adx)\{(ady)(z)\} - (ady)\{(adx)(z)\}$

$= (adxoady)(z) - (adyoadx)(z)$

$= (adxoady - adyoadx)(z).$

Al observar esta demostración el argumento principal es una sustitución generada } de la igualdad de Jacobi, por lo que el resultado puede tomarse como una equivalencia de dicha identidad.

A continuación se brinda una definición análoga de "álgebras" que ya estudiamos anteriormente, pero esta vez las estudiamos desde la perspectiva de las álgebras de Lie.

3.6 ÁLGEBRAS DESDE EL PUNTO DE VISTA DE LA TEORÍA DE LIE

En esta sección nos ocuparemos de hacer remembranza de la teoría de Álgebras en general, pero desde el punto de vista de la teoría de Lie, es decir, se definirá una álgebra como un espacio vectorial dotado de una función bilineal. De igual forma se definen conceptos necesarios de las álgebras en general.

DEFINICIÓN (ÁLGEBRA) 3.6.1

Una *álgebra* sobre un campo F, es un espacio de vectores A sobre F junto con una función bilineal

$$A \times A \to A, \quad (x, y) \mapsto xy.$$

Donde xy es el *producto* de x y y.

Usualmente en el estudio de álgebras el producto satisface algunas propiedades. En particular, las álgebras de Lie son álgebras que satisfacen las condiciones (L1) y (L2) y en este caso nosotros escribimos el producto de x y y como $[x, y]$.

DEFINICIÓN (ÁLGEBRA ASOCIATIVA) 3.6.2

La álgebra A es llamada *asociativa* si cumple:

$$(xy)z = x(yz) \ \ \forall x, y, z \ \in A.$$

DEFINICIÓN (UNIDAD DE UNA ÁLGEBRA) 3.6.3

Decimos que una álgebra A tiene *unidad* si tiene un elemento $1_A \in A$ tal que:

$$1_A x = x = x 1_A \ \ \forall x \in A.$$

Por ejemplo $\mathrm{gl}(V)$, recordando un poco el capítulo II, el espacio de vectores de transformaciones lineales del espacio vectorial V, tiene una estructura asociativa y tiene unidad, donde el producto es dado por la composición de funciones. La transformación identidad es el elemento unidad en esta álgebra. Así mismo $\mathrm{gl}(n, F)$, el conjunto de matrices $n \times n$ sobre F, es una álgebra asociativa y tiene unidad, con respecto a la multiplicación de matrices.

Aparte de las álgebras de Lie, muchas álgebras son asociativas y tienen unidad. Es importante no generar confusión entre los distintos tipos de álgebras, por ello, para hacer una distinción, adoptamos escribir el producto en las álgebras de Lie con corchetes, es decir de la forma $[x, y]$.

DEFINICIÓN (DERIVACIÓN) 3.6.4

Sea *A* una álgebra definida sobre un campo *F*. Una *derivación* de *A* es una función lineal $D: A \to A$ tal que

$$D(ab) = aD(b) + D(a)b \qquad \forall\, a, b \in A.$$

Denotemos por Der *A* al conjunto de todas las derivaciones de *A*.

TEOREMA 3.6.5

Der *A* es un subespacio vectorial de gl(*A*). Además, Der *A* es una subalgebra de Lie de gl(*A*).

Demostración:

Para verificar que es un subespacio vectorial hay que probar que Der *A* como conjunto es cerrado bajo la adición y bajo la multiplicación por un escalar y además contiene la función cero.

Sean $D_1\ y\ D_2$ dos derivaciones en Der *A*, y $a, b, c \in A$

$D_1(ab) + D_2(ab) = (aD_1(b) + D_1(a)b) + (aD_2(b) + D_2(a)b)$

$$= a\big(D_1(b) + D_2(b)\big) + \big(D_1(a) + D_2(a)\big)b \in \text{Der } A.$$

Similarmente se prueba que Der A es cerrada bajo la multiplicación por escalar.

Para mostrar que Der *A* es una subalgebra de Lie de gl(*A*) basta observar que un conmutador definido por una derivación en *A* sigue perteneciendo a *A*.

■

EJEMPLO:

Sea $A = C^{\infty}\mathbb{R}$ el espacio de vectores formado por todas las funciones infinitamente diferenciables de $\mathbb{R} \to \mathbb{R}$. Para $f, g \in A$, se define el producto fg por $(fg)(x) = f(x)g(x)$. Con esta definición, A es una álgebra asociativa. La derivada usual $Df = f'$, es una derivación de *A* ya que por la regla del producto tenemos

$$D(fg) = (fg)' = f'g + fg' = (Df)g + f(Dg).$$

EJEMPLO:

Sea L una álgebra de Lie y sea $x \in L$. La función $adx: L \to L$ es una derivación de L, ya que, por la identidad de Jacobi tenemos

$$(adx)[y,z] = \big[x,[y,z]\big] = \big[[x,y],z\big] + \big[y,[x,z]\big]$$

$$= [(adx)y,z] + [y,(adx)z] \qquad \forall\, y,z \in L.$$

TEOREMA 3.6.6

Sea L_1 y L_2 dos álgebras abelianas. L_1 y L_2 son isomorfas si y solo si tienen la misma dimensión.

Demostración:

" $\Rightarrow$ "

Un isomorfismo de L_1 y L_2 es necesariamente un isomorfismo de sus espacios vectoriales asociados, por lo que si L_1 y L_2 son isomorfos, entonces tienen la misma dimensión.

El lector puede revisar la segunda parte de la demostración [1].

■

TEOREMA 3.6.7

Sea A una algebra, y sea $\delta: A \to A$ una derivación, entonces δ satisface la regla de *Leibniz*

$$\delta^n(xy) = \sum_{r=0}^{n} \binom{n}{r} \delta^r(x)\delta^{n-r}(y) \qquad \forall x, y \in A.$$

[1] **ERDMANN, Karin y Mark J. Wildon,** *Introduction to Lie Algebras*, 1ª edición, Springer-Verlag Londres, Estados Unidos de América, 2006. Pág 231.

Demostración:

Se procede por inducción.

Probemos que se cumple para $n = 1$

$$\delta^1(xy) = \binom{1}{0}\delta^0(x)\delta^1(y) + \binom{1}{1}\delta^1(x)\delta^0(y)$$

$$= x\delta(y) + \delta(x)y.$$

Supongamos que se cumple para $n = k$

$$\delta^k(xy) = \sum_{r=0}^{k}\binom{k}{r}\delta^r(x)\delta^{k-r}(y) \qquad \forall x, y \in A.$$

Probemos que se cumple para $n = k + 1$

$\delta^{k+1}(xy) = \delta(\delta^k(xy))$

$$= \delta(\sum_{r=0}^{k}\binom{k}{r}\delta^r(x)\delta^{k-r}(y))$$

$$= \delta\left\{\begin{matrix}\binom{k}{0}x\delta^k(y) + \binom{k}{1}\delta(x)\delta^{k-1}(y) + \binom{k}{2}\delta^2(x)\delta^{k-2}(y) \\ + \cdots + \binom{k}{k}\delta^k(x)y\end{matrix}\right\}$$

$$= \delta\left\{\binom{k}{0} x\delta^k(y)\right\} + \delta\left\{\binom{k}{1}\delta(x)\delta^{k-1}(y)\right\} + \delta\left\{\binom{k}{2}\delta^2(x)\delta^{k-2}(y)\right\} + \cdots$$

$$+ \delta\left\{\binom{k}{k}\delta^k(x)y\right\}$$

$$= \left\{\binom{k}{0}\delta(x)\delta^k(y) + \binom{k}{0}x\delta^{k+1}(y)\right\} + \left\{\binom{k}{1}\delta^2(x)\delta^{k-1}(y) + \binom{k}{1}\delta(x)\delta^k(y)\right\}$$

$$+ \left\{\binom{k}{2}\delta^3(x)\delta^{k-2}(y) + \binom{k}{2}\delta^2(x)\delta^{k-1}(y)\right\} + \cdots$$

$$+ \left\{\binom{k}{k}\delta^{k+1}(x)y + \binom{k}{k}\delta^k(x)\delta(y)\right\}$$

$$= \binom{k}{0}\delta(x)\delta^k(y) + \binom{k}{0}x\delta^{k+1}(y) + \binom{k}{1}\delta^2(x)\delta^{k-1}(y) + \binom{k}{1}\delta(x)\delta^k(y)$$

$$+ \binom{k}{2}\delta^3(x)\delta^{k-2}(y) + \binom{k}{2}\delta^2(x)\delta^{k-1}(y) + \cdots + \binom{k}{k}\delta^{k+1}(x)y$$

$$+ \binom{k}{k}\delta^k(x)\delta(y)$$

(Asociamos los términos alternadamente)

$$= \left\{\binom{k}{0}\delta(x)\delta^{k}(y) + \binom{k}{1}\delta^{2}(x)\delta^{k-1}(y)\binom{k}{2}\delta^{3}(x)\delta^{k-2}(y) + \cdots + \binom{k}{k}\delta^{k+1}(x)y\right\}$$

$$+ \left\{\binom{k}{0}x\delta^{k+1}(y) + \binom{k}{1}\delta(x)\delta^{k}(y) + \binom{k}{2}\delta^{2}(x)\delta^{k-1}(y) + \cdots\right.$$

$$\left. + \binom{k}{k}\delta^{k}(x)\delta(y)\right\}.$$

Obsérvese que en podemos remplazar de manera conveniente

$$\binom{k}{0} = \binom{k+1}{0} \qquad y \qquad \binom{k}{k} = \binom{k+1}{k+1},$$

(Continuando con la igualdad)

$$= \left\{\binom{k}{0}\delta(x)\delta^k(y) + \binom{k}{1}\delta^2(x)\delta^{k-1}(y)\binom{k}{2}\delta^3(x)\delta^{k-2}(y) + \cdots \right.$$
$$\left. + \binom{k}{k-1}\delta^k(x)\delta(y)\right\} + \binom{k+1}{k+1}\delta^{k+1}(x)y + \binom{k+1}{0}x\delta^{k+1}(y)$$
$$+ \left\{\binom{k}{1}\delta(x)\delta^k(y) + \binom{k}{2}\delta^2(x)\delta^{k-1}(y) + \cdots \right.$$
$$\left. + \binom{k}{k}\delta^k(x)\delta(y)\right\}$$
$$= \sum_{r=0}^{k-1}\left\{\binom{k}{r}\delta^{r+1}(x)\delta^{k-r}(y)\right\} + \binom{k+1}{k+1}\delta^{k+1}(x)y + \binom{k+1}{0}x\delta^{k+1}(y)$$
$$+ \sum_{r=1}^{k}\left\{\binom{k}{r}\delta^r(x)\delta^{k-r+1}(y)\right\}$$
$$= \sum_{r=1}^{k}\left\{\binom{k}{r-1}\delta^r(x)\delta^{(k+1)-r}(y)\right\} + \binom{k+1}{k+1}\delta^{k+1}(x)y$$
$$+ \binom{k+1}{0}x\delta^{k+1}(y) + \sum_{r=1}^{k}\left\{\binom{k}{r}\delta^r(x)\delta^{(k+1)-r}(y)\right\}$$

$$= \binom{k+1}{0}x\delta^{k+1}(y) + \sum_{r=1}^{k}\left\{\binom{k}{r}\delta^r(x)\delta^{(k+1)-r}(y) + \binom{k}{r}\delta^r(x)\delta^{(k+1)-r}(y)\right\}$$
$$+ \binom{k+1}{k+1}\delta^{k+1}(x)\delta^0(y)$$

$$= \binom{k+1}{0}\delta^0(x)\delta^{k+1}(y) + \sum_{r=1}^{k}\left\{\left(\binom{k}{r-1} + \binom{k}{r}\right)\delta^r(x)\delta^{(k+1)-r}(y)\right\}$$
$$+ \binom{k+1}{k+1}\delta^{k+1}(x)\delta^0(y).$$

Luego se utiliza la identidad

$$\binom{k}{r-1} + \binom{k}{r} = \binom{k+1}{r}.$$

Continuando la igualdad

$$= \binom{k+1}{0} \delta^0(x)\delta^{k+1}(y) + \sum_{r=1}^{k} \left\{ \binom{k+1}{r} \delta^r(x)\delta^{(k+1)-r}(y) \right\}$$

$$+ \binom{k+1}{k+1} \delta^{k+1}(x)\delta^0(y)$$

$$= \sum_{r=0}^{k+1} \binom{k+1}{r} \delta^r(x)\delta^{(k+1)-r}(y).$$

Con lo cual se completa la prueba.

■

3.7 CONSTRUCCION DE IDEALES

Supongamos que I y J son ideales de una álgebra de Lie L. Podemos construir nuevos ideales a partir de I y J. Primero se muestra que $I \cap J$ es un ideal de L. Sabemos que $I \cap J$ es un subespacio de L. Así, todo lo que debemos verificar es que si $x \in L$ y $y \in I \cap J$, entonces $[x, y] \in I \cap J$, esto es consecuencia de que I y J son ideales.

Ahora bien, si denotamos por $[I, J]$ el subconjunto de L generado por el conmutador de Lie $[x, y]$, con $x \in I$ y $y \in J$. En primer lugar, por definición $[I, J]$ es un subespacio de L y también una subalgebra de L. En segundo lugar si $x \in I, y \in J, u \in L$, entonces la identidad de Jacobi está dada por:

$$\big[u, [x, y]\big] + \big[x, [y, u]\big] + \big[y, [u, x]\big] = 0$$

$$\Longrightarrow \big[u, [x, y]\big] = -\big[x, [y, u]\big] - \big[y, [u, x]\big]$$

$$\Longrightarrow \big[u, [x, y]\big] = \big[x, [u, y]\big] + \big[[u, x], y\big].$$

Aquí $[u, y] \in J$, ya que J es un ideal, así $\big[x, [u, y]\big] \in [I, J]$. De argumento similar se deduce que $\big[[u, x], y\big] \in [I, J]$. Por lo tanto la suma pertenece a $[I, J]$.

Un elemento general t de $[I, J]$ es una combinación lineal de la forma $t = \sum c_i [x_i, y_i]$ donde los c_i son escalares, $x_i \in I$ y $y_i \in J$. Entonces para cualquier $u \in L$ tenemos:

$$[u,t] = \left[u, \sum c_i[x_i, y_i]\right] = \sum c_i\left[u, [x_i, y_i]\right].$$

Donde $\left[u, [x_i, y_i]\right] \in [I,J]$ como se mostró anteriormente. Por lo tanto $[u,t] \in [I,J]$ y así $[I,J]$ es un ideal de L. ■

Un ejemplo importante de la construcción antes mencionada ocurre cuando tomamos $I = J = L$.

DEFINICIÓN (ÁLGEBRA DERIVADA) 3.7.1

La subalgebra $[L,L]$ de L, es llamada *álgebra derivada* de L y se denota usualmente por L'.

Es decir:

$$L' = \left\{t = \sum c_i[x_i, y_i]\,;\, x_i, y_i \in L, c_i \in F\right\}.$$

EJEMPLO:

Supongamos que L es un álgebra de Lie dada por matrices de la siguiente forma:

$$L = \left\{\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}; a \in \mathbb{C}\right\}.$$

Observemos que:

Si $x = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, entonces

$$[x,y] = xy - yx = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = 0.$$

Por lo tanto toda combinación lineal de la forma $c_1[x_1, y_1] + c_2[x_2, y_2] + \cdots = 0$, ya que los conmutadores $[x, y]$ son iguales a cero para todos $x, y \in L$.

Es claro que toda combinación lineal de esta forma será igual a cero, por lo tanto, en este caso en particular $L' = \{0\}$.

.

En general, si V es un espacio vectorial, al cual lo dotamos de una función bilineal que cumple con $[x, y] = 0$ para todos $x, y \in V$, inmediatamente verificamos que V tiene una estructura de una álgebra de Lie. También llamaremos a esta álgebra de Lie *álgebra Abeliana*, ya que si $[x, y] = 0$ resulta trivial que $[x, y] = [y, x]$. Esto muestra que cualquier espacio vectorial se puede convertir en álgebra de Lie.

Del ejemplo anterior se tiene que una álgebra de Lie L es abeliana si y sólo si $L' = \{0\}$. Esto se evidencia en el hecho de que si $[x, y] = 0 \; \forall \; x, y \in L$ entonces toda combinación lineal $\sum_i^n C_i[x_i, y_i]$; $x_i, y_i \in L$ será igual a cero, por lo tanto $L' = \{0\}$.

Si I es un ideal de una algebra de Lie L, entonces I es en particular un subespacio de L, así el espacio cociente L/I se puede dotar de una estructura de álgebra de Lie de manera natural definiendo:

$$[w + I, z + I] = [w, z] + I \quad para\, w, z \in L.$$

Aquí la forma del lado derecho es la misma que la forma de Lie en L.

DEFINICIÓN (ÁLGEBRA COCIENTE) 3.7.2

Si I es un ideal de una algebra de Lie L, entonces se puede definir la *álgebra cociente de L por I* como:

$$L/I=\{[w+I,z+I]=[w,z]+I; \quad w,z\in L\}.$$

Para estar seguros que la forma de Lie en L/I está bien definida, verificamos que $[w,z]+I$ depende solo de las clases que contienen a w y z, y no de las clases particulares w y z.

Supongamos que $w+I=w'+I$ y $z+I=z'+I$ entonces $w-w'\in I$ y $z-z'\in I$. Necesitamos verificar que $[w'+I,z'+I]=[w',z']+I$.

Ya que la forma de Lie es bilineal, podemos usar los criterios de las formas bilineales descritos en el capitulo anterior, así tenemos:

$[w',z']=[w'+(w-w'),z'+(z-z')]$ donde $w-w'\in I\ y\ z-z'\in I$

$$=[w,z]+[w-w',z']+[w',z-z']+[w-w',z-z'].$$

Donde los tres últimos sumandos pertenecen a I.

Por lo tanto $[w' + I, z' + I] = [w, z] + I$ lo cual es lo que necesitábamos. Por lo tanto L/I es un ideal y de esta forma L/I es un algebra de Lie.

Una vez teniendo definidos los conceptos más relevantes para el estudio de las álgebras de Lie, nos introducimos al estudio de su clasificación, lo cual, se desarrolla en la siguiente sección.

SECCIÓN 3: CLASIFICACIÓN DE LAS ÁLGEBRAS DE LIE

Dependiendo de sus propiedades las algebras de Lie se pueden clasificar como resolubles, nilpotentes y semisimples. En esta sección nos dedicaremos al estudio de estas álgebras de Lie resolubles y algunas de sus propiedades.

Vale la pena aclarar que existen otros tipos de clasificaciones de álgebras de Lie, pero nos limitaremos al estudio de las mencionadas anteriormente.

3.8 ÁLGEBRAS DE LIE RESOLUBLES

Para comenzar, tomamos un ideal I de un álgebra de Lie L y nos preguntamos ¿Cuándo el álgebra L/I es abeliana? El siguiente lema nos proporciona una respuesta.

LEMA 3.8.1

Supongamos que I es un ideal de L. Entonces L/I es abeliana si y sólo si I contiene el álgebra derivada L'.

Demostración:

El álgebra *L/I* es abeliana si y sólo si para todos $x, y \in L$ tenemos

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

Por lo tanto, para todos $x, y \in L$ tenemos que $[x, y] \in I$. De lo cual se concluye que $L' \subseteq I$. Esto se debe a que L' está formado por las combinaciones lineales de los conmutadores $[x, y]$ para todos $x, y \in L$.

■

Observamos que la esencia del de lema anterior es mostrar que existe un ideal I de L que contiene el álgebra derivada L, es decir I contiene a L', con lo cual se deduce que $L' \subseteq I \subseteq L$. De esta forma también la álgebra derivada L', puede tener en sí misma un ideal, que a su vez contiene una álgebra derivada, es decir la derivada de la derivada de L, la cual se denota por $L^{(2)}$, así $L^{(2)} \subseteq L' \subseteq L$. Con lo cual, la intuición nos indica que se puede formar una cadena con las álgebras derivadas, todas ellas contenidas en L, este resultado se define formalmente a continuación.

DEFINICIÓN (SERIE DE DERIVADAS) 3.8.2

Se define la *serie de derivadas* de L por la serie con los términos

$$L^{(1)} = L' \text{ y } L^{(k)} = \left[L^{(k-1)}, L^{(k-1)}\right] \quad k \geq 2.$$

donde tenemos que $L \supseteq L^{(1)} \supseteq L^{(2)} \supseteq \cdots$

DEFINICIÓN (ÁLGEBRA RESOLUBLE) 3.8.3

La álgebra de Lie L es llamada *resoluble* si para algún $m \geq 1$, donde $m \in \mathbb{N}$, tenemos que $L^{(m)} = 0$.

EJEMPLO (EL ÁLGEBRA DE HEISENBERG):

El álgebra de Heisenberg $\mathcal{H}_n$, es el álgebra de Lie real de dimensión $2n + 1$ que tiene como base los elementos:

$$\{P_1, P_2, \ldots, P_n, \ \ Q_1, Q_2, \ldots, Q_n, \ \ C\}.$$

Y la forma de Lie definida por:

$$\left[P_i, P_j\right] = \left[Q_i, Q_j\right] = [P_i, C] = [Q_i, C] = [C, C] = 0 \qquad \left[P_i, Q_j\right] = C.$$

Donde C es un elemento de la base.

Tomando un caso particular cuando $n = 1$, tendremos como base $\{P, Q, C\}$ tal que:

$$p = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ Q = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},\ C = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Así, una combinación lineal podría ser $pP + qQ + cC$, entonces una forma de definir la forma matricial de los elementos del álgebra es:

$$pP + qQ + cC = \begin{pmatrix} 0 & p & c \\ 0 & 0 & q \\ 0 & 0 & 0 \end{pmatrix}.$$

De esta forma, tomando los elementos P, Q y C de la base, y tomando la forma de Lie como $[P, Q] = PQ - QP$, resulta obvio que

$$[P, Q] = C.$$

De forma análoga tenemos que

$$[Q, C] = [P, C] = 0.$$

Ahora bien, si tomamos

$$L = H_1 = \left\{ \begin{pmatrix} 0 & p & c \\ 0 & 0 & q \\ 0 & 0 & 0 \end{pmatrix};\ p, q, c \in \mathbb{C} \right\}.$$

Se puede observar que

$$\left[\begin{pmatrix} 0 & p & c \\ 0 & 0 & q \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & p & c \\ 0 & 0 & q \\ 0 & 0 & 0 \end{pmatrix} \right] = 0$$

$$\left[\begin{pmatrix} 0 & p & c \\ 0 & 0 & q \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & p' & c' \\ 0 & 0 & q' \\ 0 & 0 & 0 \end{pmatrix}\right] = \begin{pmatrix} 0 & 0 & pq' - p'q \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Entonces toda combinación lineal de los elementos de L será de la forma

$$\begin{pmatrix} 0 & 0 & \alpha \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix};\ \alpha \in \mathbb{C}.$$

Así tenemos que

$$L' = H_1' = \left\{\begin{pmatrix} 0 & 0 & \alpha \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix};\ \alpha \in \mathbb{C}\right\}.$$

Por lo cual es obvio que

$$\left[\begin{pmatrix} 0 & 0 & \alpha \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \beta \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right] = 0.$$

Por lo tanto toda combinación lineal de los elementos de L' será igual a cero, de esta forma $L^{(2)} = 0$, por lo cual, el álgebra de Heisenberg es resoluble.

Similarmente el álgebra de matrices triangulares superiores es resoluble.

Por otro lado, si $L = \mathrm{sl}(2, \mathbb{C})$, tenemos que $L = L'$ y por lo tanto $L^{(m)} = L$ para todo $m \geq 1$, así $\mathrm{sl}(2, \mathbb{C})$ no es resoluble.

Si L es resoluble, entonces la serie de derivadas de L nos proporciona una "aproximación" de L, dada por una serie finita de ideales con cocientes abelianos. Esto también puede ser cierto en sentido contrario, veamos el siguiente lema.

LEMA 3.8.4

Si L es un álgebra de Lie con ideales de la siguiente forma

$$L = I_0 \supseteq I_1 \supseteq \cdots \supseteq I_{m-1} \supseteq I_m = 0.$$

tal que I_{k-1}/I_k es abeliano para $1 \leq k \leq m$, entonces L es resoluble.

Demostración:

Basta mostrar que $L^{(k)}$ está contenido en I_k para $1 \leq k \leq m$, ya que si hacemos $k = m$, entonces se cumple que $L^{(m)} = 0$.

Puesto que L/I_1 es abeliano, tenemos debido al lema 1 que $L' \subseteq I_1$. Utilizando los pasos inductivos, supongamos que $L^{(k-1)} \subseteq I_{k-1}$, donde $k \geq 2$. El álgebra de Lie I_{k-1}/I_k es abeliana. Por otra parte, aplicando el lema 3.8.1 al álgebra de Lie I_{k-1}, tenemos que $[I_{k-1}, I_{k-1}] \subseteq I_k$. Pero $L^{(k-1)}$ está contenido en I_{k-1} por nuestra hipótesis inductiva, así se deduce que

$$L^{(k)} = \left[L^{(k-1)}, L^{(k-1)}\right] \subseteq [I_{k-1}, I_{k-1}].$$

y por lo tanto $L^{(k)} \subseteq I_k$.

■

Ésta prueba muestra que si $L^{(k)}$ es diferente de cero, entonces I_k también es diferente de cero. Puesto que la serie de derivadas puede ser considerada como la serie descendente más cercana cuyos cocientes sucesivos son abelianos.

Así como los ideales, sabemos existen otros "objetos" algebraicos muy importantes que desempeñan un rol fundamental en el desarrollo de las álgebras. Uno de esos objetos son los homomorfismos.

Los homomorfismos en las álgebras de Lie son funciones lineales que preservan la condición de Lie, así, es lógico pensar que también preserven las series de derivadas.

LEMA 3.8.5

Supongamos que $\varphi: L_1 \to L_2$ es un homomorfismo sobreyectivo de álgebras de Lie. Entonces se cumple que:

$$\varphi\left(L_1^{(k)}\right) = (L_2)^{(k)}.$$

Demostración:

Se realizará la prueba mediante inducción sobre k.

En primer lugar verifiquemos que se cumple para $k = 1$:

Si $\varphi: L_1 \to L_2$ es un homomorfismo sobreyectivo entonces se cumple que

$$\varphi\left(L_1^{(1)}\right) = \varphi(L_1') = \varphi([L_1, L_1])$$

$$= [\varphi(L_1), \varphi(L_1)]$$

$$= [L_2, L_2]$$

$$= (L_2)^{(1)}.$$

así se cumple para $k = 1$.

Ahora supongamos que se cumple para $k = n$ y luego probamos que se cumple para $k = n + 1$.

Tenemos que $\varphi\left(L_1^{(n+1)}\right) = \varphi\left(\left[L_1^{((n+1)-1)}, L_1^{((n+1)-1)}\right]\right)$, esto por definición de series derivadas.

Entonces tenemos que:

$$\varphi\left(L_1^{(n+1)}\right) = \varphi\left(\left[L_1^{(n)}, L_1^{(n)}\right]\right).$$

Por lo tanto $\varphi\left(L_1^{(n+1)}\right) = \left[\varphi\left(L_1^{(n)}\right), \varphi\left(L_1^{(n)}\right)\right]$, por definición de homomorfismos sobre álgebras de Lie.

Esto último no es más que:

$\varphi\left(L_1^{(n+1)}\right) = \left[\varphi\left(L_1^{(n)}\right), \varphi\left(L_1^{(n)}\right)\right] = \left[L_2^{(n)}, L_2^{(n)}\right] = (L_2)^{(n+1)}$, ya que aplicamos el homomorfismo φ que va de L_1 a L_2, el cual es sobreyectivo.

Por lo tanto tenemos que se cumple para $k = n + 1$

Por lo tanto $\varphi(L_1^{(k)}) = (L_2)^{(k)}$, con lo cual se completa la prueba.

■

Este lema sugiere que en realidad, la propiedad de un álgebra de ser resoluble, debe ser heredada por varias construcciones.

LEMA 3.8.6

Sea *L* un álgebra de Lie

a) Si *L* es resoluble y $\varphi: L \to L$es un homomorfismo, entonces toda subalgebra y toda imagen homomórfica de φ son resolubles.
b) Suponga que *L* tiene un ideal *I* tal que *I* y *L*/*I* son resolubles. Entonces *L* es resoluble.
c) Si *I* y *J* son ideales resolubles de *L*, entonces $I + J$ es un ideal resoluble de *L*.

Demostración:

a) En primer lugar se debe demostrar que si *L* es resoluble, toda subalgebra de *L* es resoluble. Si L_1 es una subalgebra de *L*, entonces para cada *k* es evidente que $L_1^{(k)} \subseteq L^{(k)}$, así tenemos que si $L^{(m)} = 0$, entonces $L_1^{(m)} = 0$, para algún $m \geq 1$ por lo tanto L_1 es resoluble. Para la segunda parte de éste inciso, se debe probar que toda imagen homomórfica de *L* es resoluble, para ello se aplica el lema 3.8.5 de la siguiente forma:

Supongamos que L_1 es una subalgebra de L y sea $\varphi: L \to L_1$, pero utilizando el lema 3.8.5 se tiene que $\varphi\left(L^{(m)}\right) = L_1^{(m)}$ para algún $m \geq 1$, pero tenemos que $L_1^{(m)} = 0$ por ser L_1 subalgebra de L, de ésta forma $\varphi\left(L^{(m)}\right) = 0$, así $\varphi\left(L^{(m)}\right)$ es resoluble.

b) Se observa que $(L/I)^{(k)} = \left(L^{(k)} + I\right)/I$. (Esto se obtiene aplicando el lema 3.8.5 sobre el homomorfismo canónico $L \to L/I$ o haciendo la prueba mediante inducción sobre k, por ejemplo observe que $(L/I)' = \left(\{[w+I, z+I] = [w,z] + I;\ w,z \in L\}\right)' = \{(\sum c_i[x_i, y_i] + c_i I) + I\,; x_i, y_i \in L, c_i \in F\} = (L' + I)/I$ lo cual se puede generalizar para $(L/I)^{(k)}$). Ahora bien, si L/I es resoluble, entonces para algún $m \geq 1$ tenemos que $(L/I)^{(m)} = 0$, esto es $L^{(m)} + I = I$, por lo tanto $L^{(m)} \subseteq I$. Si I es resoluble, entonces $I^{(k)} = 0$ para algún $k \geq 1$ y por lo tanto $\left(L^{(m)}\right)^{(k)} \subseteq I^{(k)} = 0$. Ahora bien, por conveniencia definimos

$$\left(L^{(m)}\right)^{(k)} = L^{(m+k)}.$$

De ésta forma tenemos que $L^{(n)} = 0$, donde $n = m + k$, por lo tanto L es soluble.

c) Por el segundo teorema de isomorfismos tenemos que $(I + J)/I \cong J/I \cap J$, los ideales J y $I \cap J$ son resolubles, por tanto, por la parte (b) de este teorema $\frac{J}{I} \cap J$ es resoluble, así $(I + J)/I$ es resoluble por el literal (a) de este lema, puesto que

I es resoluble, la parte (b) de este lema implica que $I + J$ es soluble.

■

COROLARIO 3.8.7

Sea L una álgebra de Lie finito-dimensional, entonces existe un único ideal resoluble de L que contiene todos los ideales resolubles de L.

Demostración:

Sea R un ideal resoluble que tiene la dimensión más grande posible. Supongamos que I es cualquier ideal resoluble. Por el lema 3.8.6 (c) tenemos que $R + I$ es un ideal resoluble. Ahora bien, $R \subseteq R + I$ y por lo tanto $\dim R \leq \dim(R + I)$. Se definió a R como el ideal con máxima dimensión posible, de esta forma tenemos que $\dim R = \dim(R + I)$ y por lo tanto $R = R + I$, así I está contenido en R con lo cual se completa la prueba. Obviamente no puede existir otro ideal con las propiedades de R ya que ello implicaría la existencia de un ideal con dimensión mayor que la de R, lo cual no es posible. Por lo tanto R debe ser único.

■

El ideal descrito anteriormente va llegar a ser una herramienta esencial para ayudar a describir álgebras de Lie de dimensión finita, lo cual se evidencia en el estudio de las álgebras semisimples que se definen a continuación:

3.9 ALGEBRAS DE LIE SEMISIMPLES

DEFINICIÓN (RADICAL) 3.9.1

El ideal resoluble "más grande" (es decir el ideal resoluble maximal), de una álgebra de Lie L, es llamado el *radical de L* y es denotado por $rad\ L$.

DEFINICIÓN (ÁLGEBRA SEMISIMPLE) 3.9.2

Una álgebra de Lie L diferente de cero es llamada *semisimple* si no tiene ideales resolubles diferentes de cero o equivalentemente, un álgebra de Lie L es semisimple si $rad\ L = 0$.

EJEMPLO:

La álgebra $\mathrm{sl}(2, \mathbb{C})$, que consiste en todas las matrices de 2×2 con traza cero es semisimple, ya que:

$$[\mathrm{sl}(2,\mathbb{C}),\mathrm{sl}(2,\mathbb{C})] = \mathrm{sl}(2,\mathbb{C}).$$

Lo cual se evidencia de la siguiente manera:

$$\left[\begin{pmatrix} -a & y \\ x & a \end{pmatrix},\begin{pmatrix} b & n \\ m & -b \end{pmatrix}\right] = \begin{pmatrix} -a & y \\ x & a \end{pmatrix}\begin{pmatrix} b & n \\ m & -b \end{pmatrix} - \begin{pmatrix} b & n \\ m & -b \end{pmatrix}\begin{pmatrix} -a & y \\ x & a \end{pmatrix}$$

$$= \begin{pmatrix} -ab+my & -an-by \\ bx+am & nx-ab \end{pmatrix} - \begin{pmatrix} -ab+nx & by+an \\ -am-bx & my-ab \end{pmatrix}$$

$$= \begin{pmatrix} my-nx & -2an-2by \\ 2bx+2am & nx-my \end{pmatrix}.$$

Observe que $(my-nx)+(nx-my)$ es la traza de la matriz resultante al aplicarle la condición de Lie a las matrices, pero $(my-nx)+(nx-my)=0$, por lo tanto la matriz resultante al aplicarle la forma de Lie es de traza cero. Así, toda combinación lineal de matrices de esta forma también de dará como resultado una matriz de traza cero. Si se continúa aplicando sucesivamente la definición de álgebras derivadas para obtener la serie de derivadas, en realidad siempre dará como resultado una expresión matricial, la cual siempre tendrá traza cero.

Por ello se deduce que si tomamos $L = \mathrm{sl}(2,\mathbb{C})$ entonces $L = L' = L^{(k)}$.

Por lo tanto se deduce que la álgebra $\mathrm{sl}(2,\mathbb{C})$ no tiene ideales resolubles distintos de cero, y debido a eso, la álgebra es semisimple.

LEMA 3.9.3

Si L es una álgebra de Lie, entonces la álgebra $L/rad\ L$ es semisimple.

Demostración:

Sea $\bar{J}$ un ideal resoluble de $L/rad\ L$. Supongamos que existe un ideale J de L y que - J contiene a $rad\ L$, tal que $\bar{J} = J/rad\ L$. Por definición, $rad\ L$ es resoluble, y $J/rad\ L = \bar{J}$ es soluble por hipótesis. Por lo tanto, por el lema 3.8.6 implica que J es soluble. Pero entonces, J está contenido en $rad\ L$, esto es $\bar{J} = 0$.

■

3.10 ALGEBRAS DE LIE NILPOTENTES

DEFINICIÓN (SERIE CENTRAL INFERIOR) 3.10.1

Se define la *serie central inferior* de un álgebra de Lie L como la serie con los términos:

$$L^1 = L' \text{ y } L^k = [L, L^{k-1}], k \geq 2.$$

Donde $L \supseteq L^1 \supseteq L^2 \supseteq \cdots$ como el producto de ideales es un ideal, L^k es incluso un ideal de L (y no necesariamente un ideal de L^{k-1}). La razón por la que se le nombra "serie central" proviene del hecho que L^k/L^{k+1} está contenido en el centro de L/L^{k+1}.

DEFINICIÓN (ÁLGEBRA NILPOTENTE) 3.10.2

Una álgebra de Lie L es llamada *nilpotente* si para algún $m \geq 1$, donde $m \in \mathbb{N}$, tenemos que $L^m = 0$.

EJEMPLO:

La álgebra de Heisenberg es nilpotente.

EJEMPLO:

Sea L una álgebra de Lie de la forma:

$$L = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}, b \in \mathbb{C} \right\}.$$

Es inmediato que $L^1 = [L, L] = 0$, luego L es una álgebra de Lie nilpotente.

EJEMPLO:

Sea L una álgebra de Lie de la forma:

$$L = \left\{ \begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix}, a \in \mathbb{C} \right\}.$$

En este caso, L es una álgebra de Lie nilpotente, ya que también se cumple que $L^1 = [L, L] = 0$. Tanto en este ejemplo como en el anterior, el álgebra es además abeliana, pero no todas las álgebras nilpotentes son abelianas, aunque todas las abelianas son nilpotentes, como se deduce de forma inmediata de la definición.

LEMA 3.10.3

Toda álgebra de Lie nilpotente es resoluble.

Demostración:

Basta con demostrar que $L^{(k)} \subseteq L^k$, ya que si $L^k = 0$ entonces $L^{(k)} = 0$.

Se usará inducción sobre k. Para $k = 1$ tenemos:

$$L^{(1)} = L = L^1$$

$$\Longrightarrow L^{(1)} = L^1$$

$$\Longrightarrow L^{(1)} \subseteq L^1.$$

Supongamos que se cumple para $k = n$, es decir que $L^{(n)} \subseteq L^n$. Es decir, esta será nuestra hipótesis inductiva.

Ahora se prueba para $k = n + 1$. Para $k = n + 1$ tenemos que:

$$L^{(n+1)} = \left[L^{(n)},\ L^{(n)}\right] \quad \text{y}$$

$$L^{n+1} = [L, L^n].$$

Ahora bien, por definición de series de derivadas tenemos que $L^{(n)} \subseteq L$ y por nuestra hipótesis inductiva tenemos que $L^{(n)} \subseteq L^n$, por lo tanto, si los componentes en la forma de Lie en $L^{(n+1)}$ es subconjunto de los componentes de la forma de Lie en L^{n+1}, forzadamente tendremos que $L^{(n+1)} \subseteq L^{n+1}$. Con lo cual se completa la prueba.

■

El reciproco de este lema no necesariamente es cierto, ya que existen álgebras de Lie resolubles que no son nilpotenes, el ejemplo estándar es la álgebra de Lie b(n, F) de todas las matrices triangulares superiores sobre un campo *F*, para $n \geq 2$.

LEMA 3.10.4

Sea *L* una álgebra de Lie

(a) Si *L* es nilpotente, entonces cualquier subalgebra de Lie de *L* es nilpotente

(b) Si $L/Z(L)$ es nilpotente, entonces *L* es nilpotente.

Demostración:

Para la parte (a) supongamos que L_1 es subalgebra de L, entonces para cada k es claro que $L_1^k \subseteq L^k$, por lo tanto, si $L^m = 0$ entonces $L_1^m = 0$, para algún $m \geq 2$. Por lo tanto L_1 es nilpotente.

Para la parte (b) se puede usar inducción o una analogía del lema 3 para mostrar que $(L/Z(L))^k = (L^k + Z(L))/Z(L)$. Por lo que si $(L/Z(L))^m = 0$, entonces L^m está contenido en $Z(L)$ y por lo tanto $L^{m+1} = 0$.

■

Nota: el análogo del lema 4 b) no se sostiene o no necesariamente es cierto, es decir, si *I* es cualquier ideal de un álgebra de Lie *L*, entonces es posible que tanto *L/I* como *I* sean nilpotentes, pero *L* no lo es.

3.4 APLICACIONES DE LAS ÁLGEBRAS DE LIE A LA ECONOMÍA Y LAS FINANZAS

En la literatura actual (nos referimos mayoritariamente a artículos de principios del siglo XXI) existe la tendencia a estudiar la relación entre la teoría de Lie y diversos problemas económicos y financieros. Dicha tendencia está proporcionando unas herramientas de estudio interesantes que están basadas en las álgebras de Lie y los grupos de Lie. Teniendo este hecho en cuenta, nos interesaría hacer un breve recorrido histórico previo por algunos de los problemas y tópicos más significativos empleando la Teoría de Lie. Posteriormente se analizará con más detalle uno de estos trabajos.

En primer lugar, queremos enfatizar el trabajo de Lo y Hui (2001, 2002), quienes estudiaron la valoración de derivados financieros y, más concretamente, de derivados multiactivos introduciendo diversas técnicas basadas en las álgebras de Lie. Previamente, Lo y Hui ya emplearon la Teoría de Lie para estudiar ecuaciones en derivadas parciales con coeficientes dependientes del tiempo, modelos CEV (siglas en inglés de *elasticidad constante de varianza*) y opciones con barrera.

Independientemente, y empleando igualmente las álgebras de Lie, Björk y Landén (2002) hicieron un estudio para diversos modelos de tasa de interés, modelos introducidos previamente por el propio Björk (2001). Posteriormente, Polidoro (2003) realizó un estudio sobre un problema financiero correspondiente a la toma de decisiones bajo riesgo por parte de los agentes en el marco de la teoría de las funciones de utilidad. Para su estudio, empleó un tipo especial de grupos de Lie: los denominados *nilpotentes*.

Otra interesantísima aplicación de la Teoría de Lie a la Economía es la introducida por Basov (2004). Este describió algunos métodos basados en las propiedades de los grupos de Lie, para resolver el problema de *screening* multidimensional. También queremos resaltar el estudio realizado por Gaspar (2006), quien obtuvo un modelo general para la estructura de los precios a plazos basándose en la metodología dada por Björk y aplicando las álgebras de Lie. De hecho, Björk (2001, 2004) estudió cómo las álgebras de Lie podían emplearse en el tratamiento de problemas referentes a volatilidades constantes y otros conceptos derivados de estas.

ALGUNAS NOCIONES ECONÓMICAS Y FINANCIERAS

En la presente sección, recordaremos y explicaremos los términos económicos y financieros que aparecen a lo largo del presente texto, para facilitar el seguimiento del mismo al lector poco habituado a ellos.

Se denomina *derivado financiero* a cualquier producto financiero cuyo valor está basado en el precio que posee un determinado activo. Consisten en operaciones hipotéticas cuya liquidación se realiza mediante la diferencia existente entre el precio de mercado del activo y el precio pactado en la operación hipotética. En vista de su definición, el posible catálogo de derivados financieros no está delimitado, ya que cualquier operación financiera podría dar lugar a un derivado financiero.

En su origen, los derivados financieros tenían como función eliminar o reducir las consecuencias adversas producidas por cambios desfavorables en el activo sobre el que se define el derivado (es decir, eliminar el riesgo en las operaciones financieras). Hoy en día no solo tienen ese uso, sino que también se emplean como un producto financiero basado en la especulación con los precios del activo.

Existen también los denominados *derivados financieros multiactivos*, consistentes en productos financieros cuyo valor se basa en el precio que poseen varios activos (y no solamente uno como ocurría en el caso anterior).

En el presente artículo trataremos concretamente con uno de los más conocidos derivados financieros: las denominadas *opciones*. Se denomina *opción* al derecho a comprar o vender un activo en el futuro a un precio pactado. Debe tenerse en cuenta que, al comprar una opción, el comprador paga una prima por disfrutar del derecho adquirido, mientras que el vendedor cobra dicha prima. Por tanto, se realiza una transacción en el instante de la contratación de la opción. Debe tenerse en cuenta que también pueden considerarse opciones multiactivos, en las que el derecho de compra o venta no se limita a un único activo, sino a varios.

Existen dos tipos de opciones estándar: las opciones de *estilo americano* y las de *estilo europeo*. Las primeras son aquellas en las que es posible ejercer derecho de compra-venta en cualquier momento anterior a la fecha de vencimiento del contrato; mientras

que en las segundas solo puedes ejercer dicho derecho en la fecha de vencimiento. Cualquier otro tipo de opción se denomina *exótica*. Un caso particular de opciones exóticas son las opciones con barreras. Se denomina *opción con barrera* a toda opción cuya cancelación o activación depende del valor alcanzado durante un período de tiempo determinado por el precio del activo subyacente. Este valor será independiente del valor del activo en la fecha de vencimiento de la opción. Es decir, la activación o cancelación de la opción depende de que el precio del activo alcance unos determinados valores umbrales (de ahí la denominación de opciones con barrera).

Son varios los tipos de opciones con barreras existentes, dependiendo de los umbrales que le pongamos al valor del activo. Seguidamente indicamos los principales tipos y subtipos de opciones con barrera:

1. Opciones con barrera *de entrada* (*knock-in*): la opción pasa a activarse y a ser estándar si el precio del activo subyacente alcanza el valor fijado en la barrera durante el período acordado.
    a. Opciones *abajo y de entrada* (*down-in*): la barrera se fija por debajo del precio inicial del activo, activándose la opción cuando el precio llega a ser inferior a la barrera.
    b. Opciones *arriba y de entrada* (*up-in*): la barrera se fija por encima del precio inicial del activo, activándose la opción cuando el precio es superior a la barrera.
2. Opciones con barrera *de salida* (*knock-out*): la opción deja de existir o expira sin valor cuando se alcanza el valor fijado en la barrera para el precio del activo.

a. Opciones *abajo y de salida* (*down-out*): la barrera se fija por debajo del precio inicial del activo, expirando la opción cuando el precio llega a ser inferior a la barrera.
b. Opciones *arriba y de salida* (*up-out*): la barrera se fija por encima del precio inicial del activo, expirando la opción cuando el precio llega a ser superior a la barrera.

Teniendo en cuenta lo anterior, las opciones con barrera pueden contratarse de tal modo que la barrera sea doble (es decir, que sea arriba y abajo a la vez) e incluso puede establecerse una barrera móvil, que vaya ajustándose durante toda la vida de la opción hasta alcanzar la fecha de vencimiento.

Cualquier producto financiero (incluidas las opciones) presenta la problemática de la fijación de precios. En la fijación de precios, la empresa debe considerar tanto las necesidades del mercado hacia el producto ofertado como el proceso productivo (con sus costes y objetivos de rentabilidad). Es decir, cuando se fijan los precios, la empresa busca obtener el máximo beneficio posible, para lo que debe buscar el equilibrio entre elegir un precio "competitivo" (más fácil de vender) y un precio que permita unos márgenes más amplios. Frecuentemente se busca realizar el mayor número de ventas posibles (para que los ingresos sean apropiados), pero es obvio que no deben establecerse los precios de los productos sin tener en cuenta el coste, ya que este es un dato objetivo e importante del que suele disponer el empresario, mientras que los datos correspondientes a la demanda no son siempre tan fáciles de conocer o determinar y, además, esta facilidad depende del producto, concretamente de su elasticidad. No

obstante, los productos financieros no siguen exactamente el mismo proceso que los productos (o servicios) de empresas no financieras y presentan características particulares. Así, por ejemplo, en los productos de renta fija el precio se marca por subasta pública, mientras que en los productos de renta variable el precio lo marca el mercado.

A la hora de determinar los precios de un producto financiero (en nuestro caso, de las opciones), suele considerarse el modelo CEV. Este modelo, introducido por Cox (1975), extiende el de Black-Scholes para la fijación de precios e introduce la posibilidad de considerar una volatilidad estocástica. En el modelo CEV, se supone que el precio *S*(*t*) del activo sigue el siguiente proceso de difusión en función del tiempo *t* :

$$dS(t) = \mu(t)S(t)dt + \sigma(t)S(t)^{\beta/2}dZ(t).$$

Donde $\mu(t)$ es el parámetro que indica la tasa de crecimiento, $\sigma(t)$ es el parámetro de volatilidad, β es el parámetro que determina la elasticidad de la función de volatilidad local y, $Z(t)$ es un proceso de Wiener. (Un *proceso de Wiener* es un proceso estocástico dependiendo continuamente del tiempo. El ejemplo más conocido de proceso de Wiener es el movimiento Browniano. Para una explicación de los procesos de Wiener y su funcionamiento, recomendamos a Karatsas y Shreve (1997)).

Debe tenerse en cuenta que el parámetro β suele elegirse en el intervalo [0,2), porque es en tales casos en los que se puede asegurar alguna significación económica. Más

concretamente, en dicho escenario, la volatilidad aumentará a medida que el precio del activo decrezca. En el caso $\beta = 2$ estaríamos en otros modelos particulares.

Al exponer el modelo CEV, hemos nombrado el término *volatilidad*. Este es un término perteneciente al ámbito de los procesos estocásticos, siendo usado en Finanzas para medir el riesgo de un derivado financiero en un determinado período de tiempo. Más concretamente, la volatilidad mide la desviación estándar que presentan los cambios de valor de un determinado derivado financiero en un horizonte temporal específico. La volatilidad suele medirse tomando como periodo temporal un año completo; en caso de considerar un período de tiempo distinto a un año, estamos ante una volatilidad generalizada.

Lo usual es considerar un modelo con volatilidad constante durante toda la vida del derivado considerado. En consecuencia, no influiría ninguno de los cambios existentes en el precio del activo. Es por este motivo que se consideran procesos en los que la volatilidad no es constante, sino que ella misma es un proceso estocástico. Esta opción permite modelizar más correcta y rentablemente los derivados financieros.

DEFINICIÓN

Una función de producción $Y = f(K, L)$ se dice *neoclásica* si es homogénea de grado 1 (rendimiento a escala constante) y disminuye suavemente respecto de los factores individuales. $Y = f(K, L)$ se dice que *disminuye suavemente respecto a un factor*

individual si al aumentar uno de los factores de la producción, permaneciendo los demás constantes, las ganancias globales decrecen relativamente a partir de un cierto punto.

DEFINICIÓN

Sean $f: R^{n+m} \to R^m$ una función continuamente diferenciable definida como

$$(x, y) \to f(x, y).$$

Y un punto $(a, b) \in R^{n+m}$, tal que $f(a, b) = 0$. Si la matriz

$$\left(\frac{\partial f_i}{\partial y_j}(a, b)\right)_{i,j}.$$

tiene determinante no nulo, entonces existe un entorno *U* de a, otro *V* de b y una única función $g: U \to V$ tal que $y = g(x)$.

A continuación, pasamos a tratar las nociones de efecto a escala y de cambio técnico en una economía dada. Consideramos una economía en la que *K* y *L* representan el capital y la mano de obra, respectivamente. Dicha economía se representa mediante una función de producción neoclásica $Y = f(K, L)$, que sea continuamente diferenciable. La función de producción anterior no siempre se mantiene constante, sino que sufre modificaciones a lo largo del tiempo. Dichas modificaciones pueden deberse bien a variaciones en el capital bien a mejoras en la investigación. Los conceptos empleados en economía para representar estos cambios son el de *cambio técnico* y el más restrictivo de *progreso técnico.*

Por *cambio técnico* entendemos cualquier cambio en la función de producción que altera la relación entre consumos y producciones. El cambio técnico se denomina *progreso técnico* si la producción aumenta para cualquier consumo, con respecto al obtenido antes del cambio. Al introducirse un cambio técnico en una economía, la función de producción f se supone que no varía, pero sí lo hacen los niveles de producción. Por tanto, la función de producción tras el cambio técnico pasaría a expresarse como $\bar{Y} = \bar{f}(K, L, t)$, donde t es el parámetro de progreso térmico e $\bar{Y}$ es la producción para el capital K y la mano de obra L tras el proceso técnico.

Para denotar un progreso técnico con parámetro *t* , suele emplearse la notación:

$$T_t: \quad R^3 \to R^3$$

$$(K, L, t) \to \bar{Y} = \bar{f}(K, L, t)$$

En caso de que no haya lugar a confusión con respecto al parámetro, el progreso técnico puede denotarse exclusivamente por *T*.

El progreso técnico puede definirse también como la variación de la economía en las necesidades del capital y de la mano de obra tras dicho progreso. Para ello, se emplea el concepto de *funciones ϕ y ψ de un proceso técnico de K y L*, que combinan los dos factores mediante el parámetro de progreso técnico t:

$$T_t: \bar{K} = \phi(K, L, t), \qquad \bar{L} = \psi(K, L, t).$$

Las variables $\bar{K}$ y $\bar{L}$ se denominan *capital efectivo* y *mano de obra efectiva*, respectivamente. Las funciones. Las funciones ϕ y ψ deben suponerse analíticas y reales respecto a las tres variables (i.e. *K*, *L* y *t*). Además, las funciones ϕ *y* ψ son

independientes respecto de las variables K y L; es decir, se verifica la siguiente condición:

$$\begin{vmatrix} \frac{\partial \phi}{\partial K} & \frac{\partial \phi}{\partial L} \\ \frac{\partial \psi}{\partial K} & \frac{\partial \psi}{\partial K} \end{vmatrix} \neq 0.$$

Al satisfacerse la condición anterior, puede aplicarse el Teorema de la función implícita a la función vectorial $T(\phi, \psi)$, formada por las dos funciones de progreso técnico, menos la función vectorial constante consistente en $(\overline{K}, \overline{L})$. De este modo podemos despejar las variables K y L en función de las variables $\overline{K}$ y $\overline{L}$ (pudiendo conocer las necesidades de capital y mano de obra tras el progreso técnico).

DEFINICIÓN (APLICADA A ESTE CASO)

Sea la función de producción f y el progreso técnico T definido por (ϕ, ψ). Se dice que f es una función *holotética* bajo el progreso técnico T si el efecto total del progreso técnico T sobre f puede ser representado por una función F estrictamente monótona. Esta condición puede expresarse como:

$$\bar{Y} = \bar{f}(K, L, t) = f(\overline{K}, \overline{L}) = f\big(\phi(K, L, t), \psi(K, L, t)\big) = g(f(K, L), t) = F_t(Y)$$

TEORÍA DE LIE Y FIJACIÓN DE PRECIOS PARA OPCIONES CON BARRERA MÓVIL Y CON PARÁMETROS TEMPORALES

A principios del presente siglo, Lo y Hui (2001, 2002) presentaron una metodología basada en las álgebras de Lie, que permitía fijar el precio de diferente derivados

financieros con parámetros dependientes del tiempo. La presente sección muestra el siguiente paso en la investigación de dichos autores, aplicando la metodología al problema de la fijación de precios de las opciones con barrera móvil (Lo y Hui, 2006). La metodología anteriormente indicada aplicaba como fundamentación teórica el Teorema de Wei-Norman (Wei y Norman, 1963) y que nunca se había aplicado al campo de las Finanzas. Lo y Hui ajustan y aplican este modelo basado en las álgebras de Lie al problema de la evaluación de las opciones con barrera móvil y con parámetros dependientes del tiempo. Para realizar dicha evaluación, supusieron que el valor del activo subyacente sigue el siguiente proceso de difusión CEV

$$dS(t) = \mu(t)S(t)dt + \sigma(t)S(t)^{\beta/2}dZ(t) \qquad 0 \leq \beta < 2. \qquad (1)$$

Donde $\mu(t)$ es la media del precio de las acciones en el instante t, $\sigma(t)S(t)^{\beta/2}$ es la varianza instantánea de dicho precio, $dZ(t)$ es un proceso de Wiener y β es el factor de elasticidad.

Partiendo de la ecuación (1), la varianza instantánea del cambio porcentual en el precio se define como $\sigma(t)^2/S(t)^{2-\beta}$, siendo además una función inversa directa del precio de las acciones.

Centrándonos en las expresiones y cálculos matemáticos, Lo y Hui (2006) partieron de la ecuación diferencial de operador lineal de primer orden:

$$\frac{dU(t)}{dt} = H(t)U(dt) \quad ; \quad U(0) = 1. \qquad (2)$$

Donde *H* y *U* eran operadores lineales dependientes del tiempo en un espacio de Banach o uno de dimensión finita. El Teorema de Wei-Norman determina la expresión que tienen las soluciones de la ecuación (2) en un entorno del instante inicial $t = 0$. Dicho Teorema solo exigía como hipótesis que el operador *H* pudiese escribirse como combinación lineal de los elementos de una base de un álgebra de Lie de dimensión finita; es decir, que pudiese escribirse como sigue:

$$H(t) = \sum_{n=1}^{N} a_n(t) L_n . \qquad (3)$$

Siendo a_n funciones escalares dependientes del tiempo y L_n los elementos en una base de un álgebra de Lie resoluble *N*-dimensional o generadores del álgebra de Lie simple real desplegada de dimensión 3. Bajo esta hipótesis, el Teorema de Wei-Norman afirma que el operador *U* de la expresión (3) es expresable en un entorno de $t = 0$ de la siguiente forma:

$$U(t) = \prod_{n=1}^{N} \exp(g_n(t) L_n). \qquad (3)$$

Siendo $g_n$funciones escalares dependientes de la variable *t* y a determinar *a posteriori*. Lo y Hui dan un ejemplo en el que calculan dichas funciones g_n, lo cual hacen sustituyendo la ecuación (3) en la (2) y comparando dicho resultado con la expresión (1), término a término. De este modo, se obtiene el siguiente conjunto de ecuaciones diferenciales:

$$\frac{\partial P(S,r)}{\partial r} = \frac{1}{2}\sigma(t)^2 S(t)^{\beta} \frac{\partial^2 P(S,r)}{\partial S} + [r(t) - d(r)] S \frac{\partial P(S,r)}{\partial S} - r(t) P(S,r) . \qquad (4)$$

Para $0 \leq \beta < 2$. En esta ecuación, *P* es el valor de la opción, *S* es el precio del activo subyacente, *t* es el tiempo al vencimiento, σ es la volatilidad, *r* es la tasa de interés libre de riesgo y *d* son los dividendos generados. La ecuación (4) puede rescribirse como sigue, mediante el cambio de variable $x = \sqrt{S^{(2-\beta)}}$:

$$\frac{\partial u(x,t)}{\partial r} = \frac{1}{8}\tilde{\sigma}(r)^2 \frac{\partial^2 u(x,t)}{\partial x^2} + \frac{1}{2}\left[\tilde{\mu}(t)x - \frac{(4-\beta)\tilde{\sigma}(r)^2}{4(2-\beta)x}\right]\frac{\partial u(x,t)}{\partial x}$$

$$+ \left[\frac{(4-\beta)\tilde{\sigma}(r)^2}{8(2-\beta)x} - r(t)\right]u(x,t) = H(r)u(x,r). \qquad (5)$$

Siendo $\tilde{\sigma}(r) = (2-\beta)\sigma(t)$, $\tilde{\mu}(r) = (2-\beta)[r(t) - d(t)]$ y $u(x,r) = xP(S,t)$. Esta nueva forma de expresar la ecuación (4), les permitió a Lo y Hui dar otra fórmula para el operador $H(t)$ mediante los generadores de un álgebra de Lie. La expresión a la que hacemos referencia para *H* es la siguiente:

$$H(t) = a_1 K_+ + a_2 K_0 + a_3 K_- + b(r). \qquad (6)$$

Donde

$$K_- = \frac{1}{2}\left[\frac{\partial^2}{\partial x^2} - \frac{4-\beta}{(2-\beta)x}\frac{\partial}{\partial x} + \frac{4-\beta}{(2-\beta)x^2}\right]$$

$$K_0 = \frac{1}{2}\left(x\frac{\partial}{\partial x} - \frac{1}{2-\beta}\right)$$

$$K_+ = \frac{1}{2}x^2$$

$$a_1(r) = 0$$

$$a_2(r) = \tilde{\mu}(t)$$

$$a_3 = \frac{1}{4}\tilde{\sigma}(r)^2$$

$$b(t) = -\frac{1-\beta}{2(2-\beta)}\tilde{\mu}(t) - r(t).$$

Como se indicó antes, la expresión (6) buscaba escribir el operador *H* como una combinación de los generadores de una algebra de Lie. Pues bien, dichos generadores son los operadores K_-, K_0 y K_+ que aparecen en las últimas expresiones. De hecho, los tres operadores generan una álgebra de Lie, cuya definición particular viene dada por los siguientes conmutadores:

$$\begin{cases} [K_-, K_-] = 0 \\ [K_0, K_0] = 0 \\ [K_+, K_+] = 0 \\ [K_+, K_-] = -2K_0 \\ [K_0, K_-] = -K_- \\ [K_0, K_+] = K_+ \end{cases}.$$

Para probar que se genera una algebra de Lie, basta probar las condiciones de Lie para los generadores. Obsérvese que por la definición de los conmutadores basta probar que se cumple la identidad de Jacobi:

$$\big[K_-, [K_0, K_+]\big] + \big[K_0, [K_+, K_-]\big] + \big[K_+, [K_-, K_0]\big] = [K_-, K_+] + [K_0, -2K_0] + [K_+, K_-]$$

$$= [K_-, K_+] - 2[K_0, K_0] - [K_-, K_+] = 0.$$

El ejemplo anterior solo sirve como una referencia para tener una idea sobre una aplicación de las álgebras de Lie, sin duda alguna, en muchas ciencias modernas podemos encontrar muchas más aplicaciones. En general, las álgebras de Lie se han venido a posicionar como una de las áreas de mayor interés dentro del álgebra moderna. Por lo tanto, se exhorta al lector y a los estudiantes que continúen con los estudios sobre la teoría de Lie, (recordemos que este trabajo es introductorio en dicha teoría) ya que su

trabajo es muy extenso, por ejemplo en el área de las álgebras se podría incluso trabajar una tesis completa con las aplicaciones de las álgebras de Lie, o siendo visionarios se puede continuar con el estudio de la clasificación de estas álgebras, estudiando las álgebras de Lie simples, las filiformes y otras clasificaciones. También se puede seguir una línea de investigación para demostrar el famoso teorema de Lie, cuya prueba está basada en el trabajo de grandes matemáticos como Killing, Engel y Cartan.

BIBLIOGRAFÍA

Bibliográficos

ERDMANN, Karin y Mark J. Wildon, *Introduction to Lie Algebras*, 1ª edición, Springer-Verlag Londres, Estados Unidos de América, 2006.

FARENICK, Douglas R., *Algebras of linear transformations*, 1ª edición, Springer-Verlag New York, New York, 2001.

HERSTEIN, I. N., *Álgebra moderna*, traducido por VELASCO COBA, Federico, 1ª edición en español, 5ª reimpresión, editorial Trillas S.A., México, 1980.

IACHELLO, Francesco, *Lie Algebras and aplications*, S Ed, Springer-Verlag Berlin Heidelberg, New York, 2006.

PFEIFER, Walter, *The Lie Algebras su(N) an introduction*, S Ed, Suecia, 2003 revisada 2008, disponible en www.walterpfeifer.ch, revisado el 10 de abril de 2013.

RODRÍGUEZ, Miguel A., *Álgebras de Lie*, 4ª edición, M.A.R., Madrid, 2007.

Otras fuentes:

HERNÁNDEZ FERNÁNDEZ, Isabel y otros, *Algunas aplicaciones de las Álgebras de Lie a la Economía y las Finanzas*, Revista de métodos cuantitativos para la economía y la empresa (6). Vol. XV, Nos 1 y 2 (2008)74-94, Sevilla, disponible en www.upo.es/RevMetCuant/art24.pdf , revisado el 15 de abril de 2013.

MARTÍN, Verónica, **Juán NÚNEZ y Ángel F. Tenorio,** *Sophus Lie: un matemático visionario*, Boletín de la Asociación de Matemática Venezolana, Vol. XIV, Nos. 1 y 2 (2007)41, Sevilla.

Se agradece al lector que haga las correcciones y observaciones que encuentre, con el fin de enriquecer este texto.