UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CIENCIAS

INTRODUCCIÓN A ÁLGEBRAS DE DIMENSIÓN FINITA

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

PRESENTA:

ISAAC BARRÓN JIMÉNEZ

TUTORA

DRA. EDITH CORINA SÁENZ VALADEZ

CIUDAD UNIVERSITARIA, CD. MX., 2022

A mis abuelos Casimiro † y Juan †
A mis abuelas Camerina † y Yolanda
A mis padres Casimiro y María
A mis hermanas Diana y Lizeth

Índice general

Índice general **ii**

Introducción **iii**

1. Preliminares **1**

1.1. Anillos 1

1.2. K–álgebras 4

1.3. El radical de un álgebra 11

2. Módulos sobre álgebras **16**

2.1. Módulos 16

2.2. Homomorfismos de módulos y anillos de endomorfismos 20

2.3. Suma directa interna y suma directa externa de módulos 25

3. Módulos simples y semisimples **30**

3.1. Módulos simples y semisimples 30

3.2. El soclo, el radical y el tope de un módulo 33

3.3. El Teorema de Jordan-Hölder 38

4. Módulos proyectivos y álgebras básicas **41**

4.1. Suma directa e idempotentes 41

4.2. Módulos proyectivos 51

4.3. Álgebras básicas 57

Bibliografía **60**

Introducción

La teoría de representaciones de álgebras encuentra su origen en la descripción que da Hamilton de los números complejos como parejas ordenadas de números reales. Sin embargo, sería en 1930 que la matemática alemana Emmy Noether interpretaría a las representaciones de álgebras como módulos. Con esto, se introduce a la teoría de representaciones toda la teoría existente sobre álgebras semisimples junto con las herramientas que proporcionan el Álgebra Homológica y la Teoría de Categorías.

En la actualidad, el estudio de la teoría de representaciones de álgebras (las cuales en esta tesis son de dimensión finita sobre un campo algebraicamente cerrado, asociativas y con elemento unitario) ha cobrado mucho interés, lo cual ha resultado en un rápido crecimiento en el volumen de la literatura original producida en el área. Debido a esto, resulta complicado para los estudiantes que desean iniciarse en el estudio de esta área introducirse a ella.

Es por esto que el propósito de esta tesis es proveer de un material introductorio a aquellos estudiantes que deseen iniciarse en la teoría de representaciones de álgebras.

En el primer capítulo se presentará un resumen rápido del material de teoría de anillos que se requiere para poder introducir a las álgebras asociativas de dimensión finita. Así mismo se presentará el concepto de radical de un álgebra y se mostrarán sus principales resultados. En el capítulo 2 se da la definición de módulo sobre K–álgebras y de sus homomorfismos además de tratar de manera breve las sumas directas internas y externas de módulos. En el tercer capítulo se profundizará más en el estudio de módulos sobre K–álgebras para presentar los conceptos de módulos simples y semisimples, así como de soclo, tope y radical de un módulo. Esto permitirá, entre otras cosas, enunciar en este capítulo el Teorema de Jordan-Hölder. Por último, el cuarto capítulo reunirá varios resultados acerca de la teoría de módulos sobre K–álgebras y los elementos idempotentes de álgebras. Esto con el propósito de poder presentar las descomposiciones inescindibles en suma directa del módulo regular de un álgebra, así como de introducir el concepto de módulo proyectivo. Este capítulo concluye con un estudio breve sobre álgebras básicas.

Con el material presentado en la tesis se sientan las bases para que los estudiantes puedan estudiar, si así lo desean, a las álgebras de carcaj (centrales en la teoría de representaciones) y/o continuar con el estudio más avanzado de la teoría de representaciones. Se presume que el lector está familiarizado con la teoría de anillos y la teoría de módulos sobre anillos.

Capítulo 1

Preliminares

El objetivo de este capítulo es introducir el material preliminar requerido para el desarrollo del presente trabajo. El capítulo está divido en tres secciones que se describen a continuación. En la primera sección se enuncian las definiciones de la teoría de anillos que serán utilizadas en las secciones y capítulos siguientes. Posteriormente, en la segunda sección se introducen las K–álgebras, las cuales serán anillos unitarios con estructura de K–espacio vectorial y el principal objeto de interés en este texto. Finalmente, en la última sección se da la definición de radical de un álgebra y se establecen algunos resultados relacionados a radicales que probarán ser de utilidad y relevancia en capítulos posteriores.

1.1. Anillos

Dado que los principales objetos de estudio en este trabajo son las K–álgebras y éstas resultan ser anillos con estructura de K–espacio vectorial, la primera sección de este capítulo introductorio se encargará de recordar las principales definiciones relacionadas a la teoría de anillos. De esta manera, primero se darán las definiciones de anillo, anillo conmutativo, anillo unitario y anillo con división para, posteriormente, llegar a las definiciones de campo y campo algebraicamente cerrado. Por último, se dan las definiciones de homomorfismo de anillos y de homomorfismo de anillos unitario.

1.1.1 Definición.
*Un **anillo** es una terna $(R,+,\cdot)$ que consiste de un conjunto no vacío R junto con dos operaciones binarias*

$$+\colon R\times R\to R$$

$$\cdot\colon R\times R\to R$$

llamadas suma (o adición) y producto respectivamente, tales que

a) $(R,+)$ *es un grupo abeliano cuyo elemento neutro se denota por* 0_R *o simplemente* 0 *si no existe ambigüedad.*

b) $(R,\cdot)$ *es un semigrupo.*

c) El producto se distribuye sobre la suma por ambos lados. Es decir, para cualesquiera $a,b,c\in R$

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

*Si además se cumple que la operación producto es conmutativa, se dice que el anillo $(R,+,\cdot)$ es un **anillo conmutativo**.*

Con el propósito de aligerar la notación, se denotará al anillo $(R,+,\cdot)$ simplemente por R. Además, se escribirá el producto $a\cdot b$ como ab.

1.1.2 Definición.
*Sea R un anillo. Se dice que R es un **anillo unitario** o un **anillo con uno** si existe un elemento $1 \in R$ tal que*

$$1a = a1 = a$$

para todo $a \in R$.

*A este elemento se le llamará el **uno** de R y será denotado por 1_R o simplemente 1 cuando no exista ambigüedad.*

1.1.3 Definición.
*Sea R un anillo unitario. Se dice que R es un **anillo con división** si para toda $a \in R\backslash\{0\}$ existe un elemento $b \in R$ tal que*

$$ab = ba = 1_R$$

Como en general los anillos serán siempre unitarios, se referirá a ellos simplemente como anillos.

Otra de las estructuras que surge naturalmente de la teoría de anillos y que también será necesaria para desarrollar la teoría de K–álgebras es la de campo. Por ello es que a continuación se presenta su definición junto con algunos ejemplos.

1.1.4 Definición.
*Se dice que un anillo unitario K es un **campo** si K es un anillo conmutativo con división.*

A continuación se dan algunos ejemplos de las definiciones anteriores.

1.1.5 Ejemplos.

a) *$\mathbb{Z}$ es un anillo conmutativo con uno con las operaciones suma y producto definidas de la manera usual.*

b) *$\mathbb{Z}_n$ con las operaciones de suma y producto usuales es un anillo conmutativo con uno. Más aún, si p es primo, entonces $\mathbb{Z}_p$ es un campo.*

c) *Si A y B son anillos conmutativos con uno, entonces el producto $A \times B$ con las operaciones*

$$\begin{aligned} +\colon (A\times B)\times(A\times B) &\to A\times B \\ ((a,b),(c,d)) &\mapsto (a +_A c, b +_B d) \end{aligned}$$

y

$$\begin{aligned} \cdot\colon (A\times B)\times(A\times B) &\to A\times B \\ ((a,b),(c,d)) &\mapsto (a \cdot_A c, b \cdot_B d) \end{aligned}$$

es un anillo unitario conmutativo donde $0_{A\times B} = (0_A, 0_B)$ y $1_{A\times B} = (1_A, 1_B)$.
En particular, $\mathbb{Z}\times\mathbb{Z}$ es un anillo con las operaciones definidas de esta manera.

d) *El conjunto $\mathbb{R}^{[a,b]}$ de las funciones de variable real con dominio un intervalo $[a,b] \subseteq \mathbb{R}$ es un anillo conmutativo con las operaciones usuales de suma y multiplicación. Es decir,*

$$\begin{aligned} +\colon \mathbb{R}^{[a,b]}\times\mathbb{R}^{[a,b]} &\to \mathbb{R}^{[a,b]} \\ (f,g) &\mapsto f+g \end{aligned}$$

con $f+g$ definida de la siguiente manera

$$(f+g)(x) = f(x) + g(x)$$

$$\begin{aligned} \cdot\colon \mathbb{R}^{[a,b]}\times\mathbb{R}^{[a,b]} &\to \mathbb{R}^{[a,b]} \\ (f,g) &\mapsto fg \end{aligned}$$

con fg definida de la siguiente manera

$$(fg)(x) = f(x)g(x)$$

e) *Sea G un grupo abeliano. Se dice que $f\colon G\to G$ es un* ***endomorfismo*** *de G si f es un homomorfismo de grupos. El conjunto de endomorfismos de G dotado con la operación usual de suma de funciones resulta ser un grupo abeliano. Por otro lado, dados dos endomorfismos f y g de G, se tiene que su composición se puede ver de dos formas distintas dependiendo de si las funciones se componen a la izquierda o a la derecha. Esto es:*

   a) *Cuando la composición se hace de derecha a izquierda. Es decir, $fg(a)=f(g(a))$ para toda $a\in G$.*
   b) *Cuando la composición se hace de izquierda a derecha. Es decir, $(a)fg=((a)f)g$ para toda $a\in G$.*

   De esta manera, usando la composición de funciones como la operación producto, se tiene que por cada grupo abeliano G se obtienen dos anillos unitarios. El de los ***endomorfismos a la izquierda*** *de G denotado por $\mathrm{End}^{\mathrm{I}}(G)$ (es decir, $(\mathrm{End}^{\mathrm{I}}(G),+,\circ)$) y el de los* ***endomorfismos a la derecha*** *de G denotado por $\mathrm{End}^{\mathrm{D}}(G)$.*

f) *El conjunto de matrices cuadradas de orden n con coeficientes en $\mathbb{R}$, denotado por $\mathbb{M}_n(\mathbb{R})$, con las operaciones de suma y producto de matrices usuales es un anillo unitario no conmutativo.*

g) *Dado un anillo $(A,+,\cdot)$, la terna $(A,+,*)$ con*

$$\begin{aligned} *\colon A\times A &\to A\\ (a,b)&\mapsto b\cdot a\end{aligned}$$

   es un anillo. A la terna $(A,+,*)$ se le llama el ***anillo opuesto*** *de A y es denotado por A^{op}.*

h) *Dado un conjunto X, la terna $(\mathscr{P}(X),\triangle,\cap)$ con*

$$\triangle=(A\backslash B)\cup(B\backslash A)$$

   la diferencia simétrica, es un anillo conmutativo con uno donde la diferencia simétrica y la intersección son la suma y el producto del anillo respectivamente.

i) *$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son todos campos con las operaciones de suma y producto usuales.*

j) *Dado un campo K, el conjunto $K[x]$ de polinomios con coeficientes en K e indeterminada x es un anillo conmutativo con uno con la suma y producto usual de polinomios.*

k) *Dado $(G,\cdot)$ un grupo finito con neutro e y A un anillo unitario se define el* ***anillo de grupo*** *de G denotado por AG, como el conjunto de las sumas formales $\sum_{g\in G}\alpha_g g$ con $\alpha_g\in A$ con las operaciones*

$$\begin{aligned} +\colon A[G]\times A[G]&\to A[G]\\ \left(\sum_{g\in G}\alpha_g g,\sum_{h\in G}\beta_g g\right)&\mapsto \sum_{g\in G}(\alpha_g+\beta_g)g\end{aligned}$$

   y

$$\begin{aligned} \cdot\colon A[G]\times A[G]&\to A[G]\\ \left(\sum_{g\in G}\alpha_g g,\sum_{h\in G}\beta_h h\right)&\mapsto \sum_{f=gh\in G}(\alpha_g\beta_h)f\end{aligned}$$

   como suma y producto respectivamente. Más aún, este anillo resulta ser un anillo unitario con

$$1_A e$$

   como su uno.

Dado que en general se considerará que todos los campos son algebraicamente cerrados, se da la siguiente definición.

1.1.6 Definición.
Sea K un campo. Se dice que K es un ***campo algebraicamente cerrado*** *si todo polinomio no constante $p\in K[x]$ se factoriza linealmente en K (equivalentemente si p tiene todas sus raíces en K).*

1.1.7 Ejemplos.

a) *$\mathbb{R}$ no es un campo algebraicamente cerrado pues el polinomio $1+x^2 \in \mathbb{R}[x]$ no tiene sus raíces en $\mathbb{R}$.*

b) *Por otro lado, del Teorema Fundamental del Álgebra se sigue que $\mathbb{C}$ sí es un campo algebraicamente cerrado.*

Para concluir la sección, se enuncian las definiciones de homomorfismo de anillos y homomorfismo de anillos unitario que serán de utilidad para definir a los homomorfismos de álgebras en la siguiente sección.

1.1.8 Definición.
Sean A y B anillos (no necesariamente unitarios). Se dice que una función

$$f\colon A \to B$$

*es un **homomorfismo de anillos** si para cualesquiera $a,b \in A$*

$$f(a +_A b) = f(a) +_B f(b)$$
$$f(a \cdot_A b) = f(a) \cdot_B f(b)$$

*Si además A y B son anillos unitarios, se dirá que un homomorfismo de anillos f es un **homomorfismo de anillos unitario** si*

$$f(1_A) = 1_B$$

1.1.9 Ejemplos.

a) *Si se considera al anillo $\mathbb{Z}$ con las operaciones usuales y a $\mathbb{Z}\times\mathbb{Z}$ con las operaciones definidas en 1.1.5 c), la función*

$$\begin{aligned} i\colon \mathbb{Z} &\to \mathbb{Z}\times\mathbb{Z} \\ a &\mapsto (a,0) \end{aligned}$$

es un homomorfismo de anillos no unitario.

b) *Dado A un anillo unitario se tiene que existe un único homomorfismo de anillos unitario de $\mathbb{Z}$ a A, el cual está dado por:*

$$\begin{aligned} f\colon \mathbb{Z} &\to A \\ n &\mapsto n1_A \end{aligned}$$

1.2. K–álgebras

Una vez que se ha expuesto lo necesario sobre la teoría de anillos, es posible dar la definición de K–álgebras. Así, en esta sección se comenzará definiendo estos objetos para posteriormente hablar de sus subálgebras, sus ideales y sus ideales generados. Enseguida, se dará la definición de objetos idempotentes y nilpotentes así como de subconjuntos nil y nilpotentes de un anillo. Después, se enunciará la definición de homomorfismos de álgebras así como del kernel y la imagen de un homomorfismo de álgebras. Finalmente, se concluirá la sección con la definición de ideal maximal de un álgebra.

1.2.1 Definición.
*Dado un campo K (no necesariamente algebraicamente cerrado), una **K–álgebra** es un anillo unitario A tal que $(A,+)$ tiene una estructura de K–espacio vectorial con la suma del anillo como la suma de vectores y para cualesquiera $\alpha \in K$ y $a,b \in A$ se satisface que*

$$\alpha(ab) = (\alpha a)b = a(\alpha b)$$

*Además, se dice que A es una K–álgebra de **dimensión finita** si $\dim({}_K A) < \infty$.*

1.2.2 Definición.
*Sea A una K–álgebra. Una K–**subálgebra** de A es un K–subespacio vectorial B de A tal que*

a) $1_A \in B$.

b) $\forall\, a,b \in B\,(ab \in B)$.

Algunas veces se referirá a una K–álgebra simplemente como álgebra, y a una K–subálgebra como subálgebra.

A continuación se muestran algunos ejemplos de álgebras y subálgebras.

1.2.3 Ejemplos.

a) Todo campo K es una K–álgebra.

b) El conjunto $\mathbb{R}^{[a,b]}$ *de las funciones de variable real con dominio en el intervalo* $[a,b] \subset \mathbb{R}$ *es una* $\mathbb{R}$*–álgebra.*

c) El conjunto $\mathbb{M}_n(K)$ *de las matrices cuadradas de orden n con coeficientes en el campo K es una K–álgebra.*
Más aún, dado un conjunto finito $I = \{a_1, \ldots, a_n\}$ *con* $\preccurlyeq$ *un orden parcial en I, el conjunto*

$$KI := \{[\lambda_{ij}] \in \mathbb{M}_n(K) \mid \lambda_{ij} = 0 \text{ si } a_i \not\preccurlyeq a_j\}$$

es una subálgebra de $\mathbb{M}_n(K)$.
*A esta subálgebra se le llama el **álgebra de incidencia** de I con coeficientes en K.*
En general, tanto el conjunto de matrices triangulares superiores $\overline{\mathbb{T}}_n(K)$ *como el de matrices triangulares inferiores* $\underline{\mathbb{T}}_n(K)$ *resultan ser subálgebras de* $\mathbb{M}_n(K)$.

d) Dado un campo K, el conjunto $K[x]$ *de polinomios con coeficientes en K e indeterminada x es una K–álgebra.*

*e) Dada una K–álgebra A, se define el **álgebra opuesta** de A como el anillo opuesto* A^{op} *visto con estructura de K–álgebra.*

f) Dadas dos K–álgebras A y B, el producto $A \times B$ *vuelve a ser una K–álgebra.*

g) Dado $(G,\cdot)$ *un grupo finito con neutro e y A una K–álgebra, se tiene que el anillo de grupo AG es una K–álgebra.*
*A esta álgebra se le llama el **álgebra de grupo** de G. Más aún, se tiene que* $\dim({}_KA[G]) = o(G)\cdot\dim({}_KA)$.
Además, si $A = K$ *entonces los elementos de G forman una base para* ${}_KAG$.

De manera análoga a como sucede con la teoría de anillos, los ideales de un álgebra serán relevantes para su estudio, es por eso que a continuación se presenta su definición.

1.2.4 Definición.
Sea A una K–álgebra e I un subespacio vectorial de A. Se dice que

*a) I es un **ideal izquierdo** de A si para cualesquiera* $a \in A$ *e* $i \in I$, $ai \in I$.

*b) Similarmente se dice que I es un **ideal derecho** de A si para cualesquiera* $a \in A$ *e* $i \in I$, $ia \in I$.

*c) Se dice que I es un **ideal bilateral** de A o simplemente un **ideal** de A si I es tanto un ideal izquierdo como derecho de A.*

Es importante observar que así como el ideal de un álgebra siempre es ideal de su anillo subyacente, el recíproco también se cumple.

1.2.5 Observación.
Sea A una K–álgebra.

a) *Si I es un ideal del anillo A, entonces I es un ideal del álgebra A.*
Para verificar esto es necesario ver que I es también un subespacio vectorial de A. Como, por definición de ideal de un anillo, I es ya un subgrupo de A, entonces basta con ver que es cerrado bajo el producto por escalares. Sean entonces $\alpha \in K$ e $i \in I$. Dado que A es una K–álgebra se sigue que $\alpha(1_A) \in A$. De donde, $(\alpha 1_A)i \in I$ y, por definición de K–álgebra, se tiene que $\alpha(1_A \cdot i) = \alpha i \in I$. Con lo que se prueba que I es un subespacio vectorial de A y por tanto un ideal del álgebra.

b) *Por otro lado, un subanillo B de la K–álgebra no necesariamente es una subálgebra de B.*
Para esto basta considerar a $\mathbb{R}$ con estructura de $\mathbb{R}$–álgebra y a $\mathbb{Z}$ como subanillo de $\mathbb{R}$. Como $\mathbb{Z}$ no es subespacio vectorial de $\mathbb{R}$, entonces no se cumple que sea una subálgebra de $\mathbb{R}$.

Una de las propiedades que interesa mostrar sobre los ideales de álgebras es que su intersección también es un ideal. Esto será particularmente relevante cuando se presente la definición del radical de un álgebra en la siguiente sección.

1.2.6 Ejemplo.

a) *De manera análoga a como pasa en la teoría de anillos, dada una K–álgebra A e I un ideal de A, el cociente A/I resulta ser una K–álgebra. En efecto, dado que I es un ideal del anillo A, por la teoría de anillos se tiene que el cociente A/I tiene estructura de anillo unitario con las operaciones*

$$\begin{aligned} +\colon A/I \times A/I &\to A/I \\ (a+I, b+I) &\mapsto (a+b)+I \end{aligned}$$

$$\begin{aligned} \cdot\colon A/I \times A/I &\to A/I \\ (a+I, b+I) &\mapsto (ab)+I \end{aligned}$$

Por otro lado, como el grupo $(A/I,+)$ es un K–espacio vectorial con la operación

$$\begin{aligned} *\colon K \times A/I &\to A/I \\ (\alpha, a+I) &\mapsto (\alpha a)+I \end{aligned}$$

como producto por escalares (con αa dado por el producto por escalares de $_KA$), se concluye que A/I es también una K–álgebra.

1.2.7 Proposición.
Sea A una K–álgebra e $\{I_l\}_{l\in\Omega}$ una familia de ideales bilaterales (respectivamente izquierdos o derechos) de A, entonces $\cap_{l\in\Omega} I_l$ es un ideal bilateral (respectivamente izquierdo o derecho) de A.

Demostración. Como por definición I_l es un subespacio vectorial de A para toda $l \in \Omega$, se sigue de la teoría de espacios vectoriales que $\cap_{l\in\Omega} I_l$ vuelve a ser un subespacio vectorial de A. Por otro lado, como además I_l es un ideal bilateral (respectivamente izquierdo o derecho) del anillo A para cada $l \in \Omega$, se sigue de la teoría de anillos que $\cap_{l\in\Omega} I_l$ es un ideal bilateral (respectivamente izquierdo o derecho) de A.
De lo anterior se concluye que $\cap_{l\in\Omega} I_l$ es un ideal bilateral (respectivamente izquierdo o derecho) de la K–álgebra A.

□

Otra de las consecuencias que se tienen de la proposición anterior es el concepto de ideal generado por un conjunto. En la definición que se enuncia a continuación se hace énfasis en un caso especial cuando el conjunto a partir del cual se genera el ideal es ya un conjunto de productos de elementos de algún otro ideal.

1.2.8 Definición.
Sea A una K–álgebra y X un subconjunto no vacío de A. Se define al ***ideal*** *(respectivamente izquierdo o derecho)* ***generado por*** *X , denotado por* $\langle X \rangle$ *(respectivamente* ${}_I\langle X \rangle$ *o* $\langle X \rangle_D$*), como la intersección de todos los ideales (respectivamente izquierdos o derechos) de A que contienen a X. Es decir,*

$$\langle X \rangle := \bigcap \{ I \subseteq A \mid I \text{ es ideal de } A \text{ y } X \subseteq I \}$$

Si en particular $X = \{\prod_{i=1}^{m} a_i \mid a_i \in I \ \forall\, i \in \{1,\ldots,m\}\} \subseteq I$ *con I un ideal de A, se denota a* $\langle X \rangle$ *como* I^m.

En este trabajo el principal interés se encuentra en el estudio de las K–álgebras. Dado que éstas son en particular anillos, se darán las siguientes definiciones de algunos elementos y conjuntos destacados en anillos.

1.2.9 Definición.
Sea A un anillo unitario.

a) *Se dice que un elemento* $a \in A$ *es* ***idempotente*** *si* $a^2 = a$.

b) *Se dice que un elemento* $a \in A$ *es* ***nilpotente*** *si existe algún* $m \in \mathbb{Z}^+$ *tal que* $a^m = 0$. *Se define el* ***índice de nilpotencia*** *de a como n, donde n es el mínimo entero positivo tal que* $a^n = 0$.

c) *Se dice que un subconjunto B de A es* ***nil*** *si todos sus elementos son nilpotentes.*

d) *Se dice que un subconjunto B de A es un* ***conjunto nilpotente*** *si existe algún* $m \in \mathbb{Z}^+$ *tal que*

$$x_1 x_2 \cdots x_m = 0$$

para cualesquiera $x_1, x_2, \ldots, x_m \in B$. *Se define el* ***índice de nilpotencia*** *de B como n, donde n es el mínimo entero positivo tal que* $x_1 x_2 \cdots x_n = 0$ *para cualesquiera* $x_1, x_2, \ldots, x_n \in B$.

Como consecuencia de la definición anterior, se tiene que dado un subconjunto nilpotente de un anillo A, éste resulta ser nil. Sin embargo, el recíproco no siempre es cierto. Este hecho queda reflejado en la siguiente proposición y en el ejemplo que la sucede.

1.2.10 Proposición.
Todo subconjunto nilpotente de un anillo unitario A es nil.

Demostración. Sea B un subconjunto nilpotente del anillo unitario A con índice de nilpotencia m. Así,

$$x_1 x_2 \cdots x_m = 0$$

para cualesquiera $x_1, x_2, \ldots, x_m \in B$. En particular, para cualquier $x \in B$ se tiene que

$$x^m = \underbrace{x \cdots x}_{m\text{–veces}} = 0$$

de donde se tiene que x es un elemento nilpotente y dado que x fue un elemento arbitrario, se concluye que todo elemento en B es nilpotente y por lo tanto B es nil.

□

1.2.11 Ejemplos.

a) *Considérese el anillo unitario* $\mathbb{M}_2(\mathbb{Z})$ *y sean*

$$[a]^* = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$$

$$[b]_* = \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}$$

para cualesquiera $a,b \in \mathbb{Z}$.
Sea entonces el conjunto

$$X = \{[a]^* \mid a \in \mathbb{Z}\backslash\{0\}\} \cup \{[b]_* \mid b \in \mathbb{Z}\backslash\{0\}\} \subseteq \mathbb{M}_2(\mathbb{Z})$$

Se afirma que X es un conjunto nil que no es nilpotente.
En efecto, dado que para cualesquiera $a,b \in \mathbb{Z}\backslash\{0\}$ se tiene que

$$([a]^*)^2 = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

y

$$([b]_*)^2 = \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

se concluye que X es nil. Por otro lado, nótese que como $\mathbb{Z}$ no tiene divisores de cero, entonces para cualesquiera $a,b,c \in \mathbb{Z}\backslash\{0\}$ se tiene que

$$[a]^*\,[b]_* = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \neq 0_{\mathbb{M}_2(\mathbb{Z})}$$

y

$$[a]^*\,[b]_*\,[c]^* = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}[c]^* = [abc]^* \neq 0_{\mathbb{M}_2(\mathbb{Z})}$$

Luego, supóngase que para cualesquiera $a_1,\ldots,a_n \in \mathbb{Z}\backslash\{0\}$ con la función

$$\begin{aligned} \varphi\colon \{a_1,\ldots,a_n\} &\to X \\ a_i &\mapsto \begin{cases} [a_i]^* & : i = 2k+1 \text{ para algún } k \in \mathbb{Z}_{\geq 0} \\ [a_i]_* & : i = 2k \text{ para algún } k \in \mathbb{Z}_{\geq 0} \end{cases} \end{aligned}$$

se cumple que

$$\prod_{i=1}^{n} \varphi(a_i) \neq 0_{\mathbb{M}_2(\mathbb{Z})}$$

Finalmente, sean $a_1,\ldots,a_{n+1} \in \mathbb{Z}\backslash\{0\}$ y considérese la función

$$\begin{aligned} \varphi\colon \{a_1,\ldots,a_{n+1}\} &\to X \\ a_i &\mapsto \begin{cases} [a_i]^* & : i = 2k+1 \text{ para algún } k \in \mathbb{Z}_{\geq 0} \\ [a_i]_* & : i = 2k \text{ para algún } k \in \mathbb{Z}_{\geq 0} \end{cases} \end{aligned}$$

Nótese que de la hipótesis de inducción se sigue que para

$$\varphi_n \coloneqq \varphi|_{\{a_1,\ldots,a_n\}} : \{a_1,\ldots,a_n\} \to X$$

se cumple que

$$\prod_{i=1}^{n} \varphi_n(a_i) \neq 0_{\mathbb{M}_2(\mathbb{Z})}$$

Ahora, considérense los siguientes casos.

Caso 1. *n es par. Así, de la hipótesis de inducción*

$$\begin{aligned} \prod_{i=1}^{n+1} \varphi(a_i) &= \left(\prod_{i=1}^{n} \varphi(a_i)\right)\varphi(a_{n+1}) \\ &= \left(\prod_{i=1}^{n} \varphi_n(a_i)\right)\varphi(a_{n+1}) = \begin{pmatrix} \prod_{i=1}^{n} a_i & 0 \\ 0 & 0 \end{pmatrix}[a_{n+1}]^* \\ &= \left[\prod_{i=1}^{n+1} a_i\right]^* \neq 0_{\mathbb{M}_2(\mathbb{Z})} \end{aligned}$$

Caso 2. *n es impar. Análogamente al caso anterior,*

$$\begin{aligned}\prod_{i=1}^{n+1}\varphi(a_i) &= \left(\prod_{i=1}^{n}\varphi(a_i)\right)\varphi(a_{n+1})\\ &= \left(\prod_{i=1}^{n}\varphi_n(a_i)\right)\varphi(a_{n+1}) = \left[\prod_{i=1}^{n}a_i\right]^*[a_{n+1}]_*\\ &= \begin{pmatrix}\prod_{i=1}^{n+1}a_i & 0\\ 0 & 0\end{pmatrix} \neq 0_{\mathbb{M}_2(\mathbb{Z})}\end{aligned}$$

Como además $0_{\mathbb{M}_2(\mathbb{Z})} \notin X$, se concluye que para cualquier $n \in \mathbb{Z}^+$ existen $x_1,\ldots,x_n \in X$ tales que $x_1\cdots x_n \neq 0_{\mathbb{M}_2(\mathbb{Z})}$ y por lo tanto X no es nilpotente.

Adicionalmente al ejemplo anterior, se hace la observación de que si se considera la $\mathbb{R}$–álgebra $\mathbb{M}_2(\mathbb{R})$, entonces el conjunto $X = \{[a]^* \mid a \in \mathbb{R}\backslash\{0\}\} \cup \{[b]_* \mid b \in \mathbb{R}\backslash\{0\}\} \subseteq \mathbb{M}_2(\mathbb{R})$ es un ejemplo de un subconjunto de una R–álgebra que es nil, pero no nilpotente.

A continuación se enuncia una proposición que establece que todo elemento nilpotente a de un anillo, induce un elemento invertible. A saber, $1-a$.

1.2.12 Proposición.
Sea A un anillo unitario. Si $a \in A$ es nilpotente, entonces $(1-a)$ es invertible.

Demostración. Sea $a \in A$ un elemento nilpotente con índice de nilpotencia m. Así, se sigue que

$$(1+a+\cdots+a^{m-1})(1-a) = 1$$
$$(1-a)(1+a+\cdots+a^{m-1}) = 1$$

Con lo que se prueba que $(1-a)$ tiene tanto inverso izquierdo como derecho y por lo tanto es invertible.

□

Así, se sigue que si I es un ideal de una K–álgebra A tal que también es un subconjunto nilpotente con índice de nilpotencia m, entonces $I^m = \{0_A\}$. En tal caso, se dirá que I es un **ideal nilpotente** de A.

Por otro lado, se sigue de la teoría de anillos que si $X = \{a_1, a_2, \ldots, a_n\}$ es un subconjunto finito de A y A es una K–álgebra, se puede expresar a $\langle X\rangle$ como sigue

$$\langle X\rangle = \left\{\sum_{\text{finita}} r_i a_i s_i \,\middle|\, r_i, s_i \in A \text{ y } a_i \in X\right\}$$

Para el caso particular en el que $X = \left\{\prod_{j=1}^{m} a_j \mid a_j \in I\ \forall\, j \in \{1,\ldots,m\}\right\}$ con I un ideal de A, entonces

$$\langle X\rangle = \left\{\sum_{\text{finita}} r_i \left(\prod_{j=1}^{m} a_j\right)_i s_i \,\middle|\, r_i, s_i \in A \text{ y } \left(\prod_{j=1}^{m} a_j\right)_i \in X\right\} = \left\{\sum_{\text{finita}} \left(\prod_{j=1}^{m} a_j\right)_i \,\middle|\, \left(\prod_{j=1}^{m} a_j\right)_i \in X\right\}$$

Una vez que se expusieron las definiciones y resultados principales sobre K–álgebras, con la siguiente definición se introducen sus homomorfismos, los cuales serán homomorfismos de anillos unitarios que además sean transformaciones K–lineales.

1.2.13 Definición.
*Sean A, B dos K–álgebras. Un **homomorfismo de K–álgebras** es una función*

$$f\colon A \to B$$

tal que f es una transformación K–lineal y además un homomorfismo de anillos unitario.

De manera similar, la siguiente definición provee los conceptos usuales asociados a los homomorfismos de K–álgebras.

1.2.14 Definición.
Sea $f\colon A \to B$ un homomorfismo de K–álgebras. Se dice que

a) *f es un* ***monomorfismo*** *si f es inyectiva.*

b) *f es un* ***isomorfismo*** *si f es biyectiva. En este caso se dice que A y B son* ***isomorfas*** *y se denota por $A \cong B$.*

Así mismo, se define el ***kernel*** *de f denotado por $\mathrm{Ker}(f)$ como*

$$\mathrm{Ker}(f) = \{a \in a \mid f(a) = 0\}$$

y la ***imagen*** *de f denotada por $\mathrm{Im}(f)$ como*

$$\mathrm{Im}(f) = \{f(a) \mid a \in A.\}$$

Más aún, se tendrá que el kernel de un homomorfismos de álgebras será siempre un ideal de su dominio, mientras que su imagen será una subálgebra del codominio.

1.2.15 Proposición.
Sean A y B dos K–álgebras, y $f\colon A \to B$ un homomorfismo de álgebras. Entonces

a) $\mathrm{Ker}(f)$ *es un ideal de A.*

b) $\mathrm{Im}(f)$ *es una subálgebra de B.*

Demostración.

a) Se sigue de la observación 1.2.5 y de la teoría general de anillos.

b) De la teoría de espacios vectoriales y de anillos se sabe que $\mathrm{Im}(f)$ es tanto un subespacio vectorial como un subanillo unitario de B. Por lo tanto, $\mathrm{Im}(f)$ resulta ser una subálgebra de B.

□

Enseguida se muestra un ejemplo importante de cómo se relaciona el campo K con una K–álgebra A a través de homomorfismos de K–álgebras.

1.2.16 Ejemplos.
Dada una K–álgebra A se tiene la existencia del monomorfismo de K–álgebras:

$$\begin{aligned} i\colon K &\to A \\ \alpha &\mapsto \alpha\, 1_A \end{aligned}$$

De donde, $K \cong \mathrm{Im}(i) \subseteq A$. Así, por la proposición 1.2.15 se tiene que K es isomorfo a una subálgebra de A. Es decir, el monomorfismo canónico permite ver al campo K como una subálgebra de A.

Más aún, dado un ideal I del álgebra A, se tiene la existencia de un homomorfismo de álgebras suprayectivo entre el álgebra A y el álgebra cociente A/I dado de la siguiente manera:

$$\begin{aligned} \pi\colon A &\to A/I \\ a &\mapsto a + I \end{aligned}$$

A este homomorfismo se le conoce como la ***proyección canónica****.*

Para concluir esta sección, se enuncia la definición de ideal maximal que será esencial en la sección que sigue.

1.2.17 Definición.
Sea A una K–álgebra e $I \subsetneq A$ un ideal bilateral (respectivamente izquierdo o derecho) de A. Se dice que I es un ***ideal bilateral maximal*** *(respectivamente izquierdo o derecho) de A si para todo ideal bilateral (respectivamente izquierdo o derecho) J de A tal que $I \subseteq J$, se cumple que $J = I$ o $J = A$.*

1.3. El radical de un álgebra

Para concluir este capítulo de preliminares en esta sección se dará la definición de radical de Jacobson de una K–álgebra junto con varios resultados en relación a este objeto. Así, después de mostrar algunas equivalencias sobre su definición, se probará que el radical es de hecho el ideal bilateral que contiene a todos los ideales nilpotentes del álgebra. Finalmente, para concluir el capítulo se enuncia el Teorema de Wedderburn-Malcev con el cual se obtiene que el espacio vectorial subyacente de un álgebra admite una descomposición en suma directa donde uno de los sumandos es el radical del álgebra.

Un resultado bastante útil que se sigue de la teoría de anillos (ver [8, Sección 7.4, Proposición 11]) y de la observación 1.2.5 es que dado cualquier ideal bilateral (respectivamente izquierdo o derecho) propio de una K–álgebra A, existe un ideal bilateral (respectivamente izquierdo o derecho) maximal de A que lo contiene. En particular, se tiene la existencia de ideales maximales de K–álgebras. De esta manera, se tiene la siguiente definición.

1.3.1 Definición.
*Sea A una K–álgebra. Se define el **radical** (de Jacobson) de A denotado por* $\operatorname{rad}(A)$ *como*

$$\operatorname{rad}(A) := \bigcap\{I \subseteq A \mid I \text{ es un ideal izquierdo maximal de } A\}$$

En principio, por la manera en la que se dio la definición del radical de una K–álgebra, podría parecer necesario dar una definición análoga en la que, en vez de intersecar ideales izquierdos maximales, se intersequen ideales derechos maximales. De esta manera, al radical definido en 1.3.1 se le llamaría el radical izquierdo de Jacobson de A y a su análogo con ideales derechos se le llamaría el radical derecho de Jacobson de A. Sin embargo, resulta que esta distinción es innecesaria, ya que ambos radicales coinciden. Para poder probar este resultado, es necesario probar primero el siguiente lema.

1.3.2 Lema.
Sea A una K–álgebra y $a \in A$. Entonces, las siguientes condiciones son equivalentes:

a) $a \in \operatorname{rad}(A)$.

b) $\forall b \in A$ *el elemento* $(1-ba)$ *tiene inverso izquierdo.*

c) $\forall b \in A$ *el elemento* $(1-ba)$ *es invertible.*

d) $\forall b \in A$ *el elemento* $(1-ab)$ *es invertible.*

e) $\forall b \in A$ *el elemento* $(1-ab)$ *tiene inverso derecho.*

f) $a \in \bigcap\{I \subseteq A \mid I \text{ es ideal derecho maximal de } A\}$.

Demostración.

$(a \Rightarrow b)$ Sea $b \in A$ y supóngase que $(1-ba)$ no tiene inverso izquierdo. Entonces, el ideal $A(1-ba)$ es un ideal izquierdo propio de A. Por lo tanto, existe un ideal izquierdo maximal M de A tal que $A(1-ba) \subseteq M$.

Por otro lado, como $\operatorname{rad}(A)$ es un ideal izquierdo de A y por hipótesis $a \in \operatorname{rad}(A)$, se sigue que $ba \in \operatorname{rad}(A)$ de donde $ba \in M$. Finalmente, como M es también un subespacio vectorial de ${}_KA$, se tiene que $(1-ba)+ba = 1+(-ba+ba) = 1 \in M$. Por lo que $M = A$ lo cual es una contradicción al hecho de que M sea ideal izquierdo maximal de A.

Por lo tanto, se concluye que $(1-ba)$ tiene inverso izquierdo.

$(b \Rightarrow a)$ Sea $b \in A$ y considérese el elemento $(1-ba)$ el cual, por hipótesis, tiene inverso izquierdo. Luego, supóngase que $a \notin \operatorname{rad}(A)$. Así, existe algún ideal izquierdo maximal I para el que $a \notin I$. Entonces, se afirma que $A = I + Aa$. En efecto, nótese primero que para cualquier elemento $i \in I$, se tiene que $i = i + 0a \in I + Aa$, de manera que $I \subseteq I + Aa$. Sin embargo, dado que $a = 0 + 1a \notin I$, se tiene entonces que $I \subsetneq I + Aa$. Así, dado que I es un ideal izquierdo maximal de A, entonces $A = I + Aa$. De donde, en particular, existen $i \in I$ y $b \in A$ tales que $1 = i + ba$, de donde se sigue que $1 - ba = i \in I$ por lo que $(1-ba)$ no tiene inverso izquierdo, lo cual es una contradicción a la hipótesis. Por lo tanto, se concluye que $a \in \operatorname{rad}(A)$.

($b \Rightarrow c$) Sea $b \in A$. Como por hipótesis $(1-ba)$ tiene inverso izquierdo, existe $x \in A$ tal que $x(1-ba) = 1$, de donde $x - x(ba) = 1$ y $x = 1 + x(ba) = 1 - ((-xb)a)$. Por otro lado, dado que $(-xb) \in A$, se sigue por hipótesis que $x = 1 - ((-xb)a)$ tiene inverso izquierdo, es decir, existe $y \in A$ tal que $1 = yx = y - y((-xb)a) = y + yxba = y + ba$. De donde $y = (1-ba)$, y como $1 = yx = (1-ba)x$, se concluye que $(1-ba)$ tiene inverso derecho y por lo tanto es invertible.

($c \Rightarrow b$) Sea $b \in A$. Como por hipótesis $(1-ba)$ es invertible, entonces existe $x \in A$ tal que $x(1-ba) = 1$ y $(1-ba)x = 1$, de donde se sigue que $(1-ba)$ tiene inverso izquierdo.

($c \Rightarrow d$) Sea $b \in A$. Como por hipótesis $(1-ba)$ es invertible, existe un elemento $x \in A$ tal que $x(1-ba) = 1$ y $(1-ba)x = 1$.

De que $x(1-ba) = 1$ se tiene la siguiente serie de implicaciones.

$$
\begin{aligned}
& x(1-ba) = 1 \\
\Longrightarrow\; & x - xba = 1 \\
\Longrightarrow\; & -xba = 1 - x \\
\Longrightarrow\; & -xbab = b - xb \\
\Longrightarrow\; & xb - xbab = b \\
\Longrightarrow\; & axb - axbab = ab \\
\Longrightarrow\; & 1 + axb - axbab = 1 + ab \\
\Longrightarrow\; & 1 - ab + axb - axbab = 1 \\
\Longrightarrow\; & 1 - ab + axb(1-ab) = 1 \\
\Longrightarrow\; & (1+axb)(1-ab) = 1
\end{aligned}
$$

Con lo que se concluye que $(1-ab)$ tiene inverso izquierdo.

Análogamente, de que $(1-ba)x = 1$ se tiene la siguiente serie de implicaciones.

$$
\begin{aligned}
& (1-ba)x = 1 \\
\Longrightarrow\; & x - bax = 1 \\
\Longrightarrow\; & -bax = 1 - x \\
\Longrightarrow\; & -baxb = b - xb \\
\Longrightarrow\; & xb - baxb = b \\
\Longrightarrow\; & axb - abaxb = ab \\
\Longrightarrow\; & 1 + axb - abaxb = 1 + ab \\
\Longrightarrow\; & 1 + axb - ab - abaxb = 1 \\
\Longrightarrow\; & 1 + axb - ab(1+axb) = 1 \\
\Longrightarrow\; & (1-ab)(1+axb) = 1
\end{aligned}
$$

Con lo que se concluye que $(1-ab)$ tiene inverso derecho.

Como $(1-ab)$ tiene tanto inverso inverso izquierdo como derecho, se sigue que $(1-ab)$ es invertible.

($d \Rightarrow c$) Análogo a ($c \Rightarrow d$).

($d \Rightarrow e$) Análogo a ($c \Rightarrow b$).

($e \Rightarrow d$) Análogo a ($b \Rightarrow c$).

($e \Rightarrow f$) Análogo a ($b \Rightarrow a$).

($f \Rightarrow e$) Análogo a ($a \Rightarrow b$).

De esta manera se prueba la equivalencia de las condiciones anteriores.

$\square$

Del lema anterior se tiene el siguiente corolario con el cual se establece que el radical de un álgebra A coincide con la intersección de todos los ideales derechos maximales de A y por tanto es un ideal bilateral. Más aún, se sigue que el radical del álgebra cociente $A/\operatorname{rad}(A)$ es 0.

1.3.3 Corolario.
Sea A una K–álgebra y $\operatorname{rad}(A)$ el radical de A. Entonces,

a) $\operatorname{rad}(A)$ *es la intersección de todos los ideales derechos maximales de A.*

b) $\operatorname{rad}(A)$ *es un ideal bilateral de A y además* $\operatorname{rad}(A/\operatorname{rad}(A)) = 0$.

Demostración.

a) Del Lema 1.3.2 se sigue que $a \in rad(A)$ si y sólo si $a \in \bigcap\{I \subseteq A \mid I$ es ideal derecho maximal de $A\}$. De donde, $\operatorname{rad}(A) = \bigcap\{I \subseteq A \mid I$ es ideal derecho maximal de $A\}$.

b) Del inciso anterior y de la definición de radical de A se sigue que $\operatorname{rad}(A)$ es un ideal izquierdo y un ideal derecho de A, por lo que, de la definición 1.2.4 se tiene que $\operatorname{rad}(A)$ es un ideal bilateral de A.

   Por otro lado, para $a+\operatorname{rad}(A) \in \operatorname{rad}(A/\operatorname{rad}(A))$ se cumple por definición que está en todos los ideales izquierdos maximales de $A/\operatorname{rad}(A)$. Más aún, dado que por el Teorema de la Correspondencia se sigue que dichos ideales son de la forma $I/\operatorname{rad}(A)$ con I un ideal izquierdo maximal de A, se sigue que $a \in I$ para todo ideal izquierdo maximal de A y por lo tanto, $a \in \operatorname{rad}(A)$. Así, $a+\operatorname{rad}(A) = \operatorname{rad}(A) = 0_{A/\operatorname{rad}(A)}$, con lo que se concluye que $\operatorname{rad}(A/\operatorname{rad}(A)) = 0$.

$\square$

Un resultado más que se obtiene del lema 1.3.2 es el que asegura que todos los ideales nilpotentes de una K–álgebra A están contenidos en su radical. Sin embargo, para poder probar dicho resultado es necesario primero probar el siguiente lema.

1.3.4 Lema. *Sean A y B dos K–álgebras. Entonces,*

a) *I es un ideal bilateral (respectivamente izquierdo o derecho) de la K–álgebra $A \times B$ si y sólo si $I = I_A \times I_B$ con I_A e I_B ideales bilaterales (respectivamente izquierdos o derechos) de A y B respectivamente.*

b) *I es un ideal bilateral (respectivamente izquierdo o derecho) maximal de $A \times B$ si y sólo si $I = I_A \times I_B$ donde $I_A = A$ e I_B es un ideal bilateral (respectivamente izquierdo o derecho) maximal de B, o bien I_A es un ideal bilateral (respectivamente izquierdo o derecho) maximal de A e $I_B = B$.*

c) $\operatorname{rad}(A \times B) = \operatorname{rad}(A) \times \operatorname{rad}(B)$.

d) *Si $f\colon A \to B$ es un isomorfismo de K–álgebras, entonces también lo es $f^{-1}\colon B \to A$.*

e) *Supóngase que $A \cong_f B$. Entonces, I es un ideal de A si y sólo si $f[I]$ es un ideal de B.*

f) *Supóngase que $A \cong_f B$. Entonces, I es un ideal maximal de A si y sólo si $f[I]$ es un ideal maximal de B.*

g) *Si $f\colon A \to B$ es un homomorfismo de K–álgebras y $a \in A$ es un elemento invertible, entonces $f(a)$ también es invertible.*

Demostración.

a) Sea I un ideal de $A \times B$. Así, para cualesquiera $(a,b) \in A \times B$ y $(i,j) \in I$, se sigue que $(a,b)\cdot(i,j) = (ai,bj) \in I$ y $(i,j)\cdot(a,b) = (ia,jb) \in I$, de donde $\operatorname{Dom}(I)$ e $\operatorname{Im}(I)$ son ideales de A y B respectivamente.

   Luego, dado $(x,y) \in \operatorname{Dom}(I) \times \operatorname{Im}(I)$ se tiene que $x \in \operatorname{Dom}(I)$ y $y \in \operatorname{Im}(I)$, de donde existen $x' \in \operatorname{Im}(I)$ y $y' \in \operatorname{Dom}(I)$ tales que $(x,x'),(y',y) \in I$. De esta manera, como I es un ideal, se tiene que $(1,0)\cdot(x,x') = (x,0) \in I$ y $(0,1)\cdot(y',y) = (0,y) \in I$. Finalmente, dado que I es un K–subespacio vectorial (y en particular un subgrupo) de $A \times B$, se cumple que $(x,y) = (x,0) + (0,y) \in I$. Como trivialmente $I \subseteq \mathrm{Dom}(I) \times \mathrm{Im}(I)$, de lo anterior se concluye que $I = \mathrm{Dom}(I) \times \mathrm{Im}(I)$.

Por otro lado, sea $I = I_A \times I_B$ con I_A y I_B ideales de A y B respectivamente. Así, dados $(a,b) \in A \times B$ y $(i,j) \in I$ se tiene que, como $ai, ia \in I_A$ y $bj, jb \in I_B$, entonces $(ai,bj),(ia,jb) \in I$, de donde I es un ideal de $A \times B$.

b) Sea I un ideal maximal de $A \times B$ y sean I_A e I_B los ideales de A y B, respectivamente, tales que $I = I_A \times I_B$. Supóngase primero que $I_A \neq A$. Así se tiene entonces que I_A debe ser un ideal maximal de A e $I_B = B$ pues de no ser así se tendrían los siguientes casos: Por un lado, si I_A no es un ideal maximal, entonces existiría $J_A \subsetneq A$ ideal de A tal que $I_A \subsetneq J_A$ de manera que $I = I_A \times I_B \subsetneq J_A \times B \subsetneq A \times B$, lo cual es una contradicción a la maximalidad de I. Por otro lado, si $I_B \neq B$, entonces $I = I_A \times I_B \subsetneq I_A \times B \subsetneq A \times B$, lo cual contradice la minimalidad de I.

Luego, nótese que si $I_A = A$, entonces I_B debe ser un ideal maximal de B pues de otra forma existiría $J_B \subsetneq B$ ideal maximal de B tal que $I_B \subsetneq J_B$ de manera que $I = A \times I_B \subsetneq A \times J_B \subsetneq A \times B$, contradiciendo nuevamente la maximalidad de I.

De lo anterior se concluye que si $I = I_A \times I_B$ es un ideal maximal de $A \times B$, entonces $I_A = A$ e I_B es un ideal maximal de B o bien $I_B = B$ e I_A es un ideal maximal de A.

Para la implicación inversa considérese primero el caso $I = I_A \times I_B$ con $I_A = A$ e I_B un ideal maximal de B. Luego, tómese J un ideal de $A \times B$ con $J = J_A \times J_B$ tal que $I \subseteq J$. Es decir, $I_A \subseteq J_A$ y $I_B \subseteq J_B$. Así, se sigue que $J_A = A$ y, dado que I_B es un ideal maximal de B, se concluye que $J_B = I_B$. Esto es, $I = J$. Finalmente, es claro que como $I_B \subsetneq B$, entonces $I \subsetneq A \times B$, de manera que I es un ideal maximal de $A \times B$. El caso en el que $I = I_A \times I_B$ con I_A un ideal maximal de A e $I_B = B$ es análogo.

c) Sea $x = (a,b) \in \mathrm{rad}(A \times B)$. Así, $x \in I$ para todo ideal izquierdo maximal de $A \times B$. Como de los dos incisos anteriores se tiene que cada ideal izquierdo maximal de $A \times B$ es de la forma $A \times I_B$, con I_B un ideal izquierdo maximal de B, o bien de la forma $I_A \times B$ con I_A un ideal izquierdo maximal de A, se tiene que $a \in I_A$ para todo ideal izquierdo maximal I_A de A y $b \in I_B$ para todo ideal izquierdo maximal I_B de B. De donde se sigue que $a \in \mathrm{rad}(A)$ y $b \in \mathrm{rad}(B)$ de manera que $x = (a,b) \in \mathrm{rad}(A) \times \mathrm{rad}(B)$.

Inversamente, si $x = (a,b) \in \mathrm{rad}(A) \times \mathrm{rad}(B)$, se tiene que $a \in \mathrm{rad}(A)$ y $b \in \mathrm{rad}(B)$, de manera que $a \in I_A$ para todo ideal maximal I_A de A y $b \in I_B$ para todo ideal maximal I_B de B. Así, se cumple que x está en todos los ideales de $A \times B$ de la forma $A \times I_B$, con I_B un ideal izquierdo maximal de B y $I_A \times B$ con I_A un ideal izquierdo maximal de A. Es decir, $x = (a,b) \in I$ para todo ideal maximal I de $A \times B$. De donde se concluye que $x \in \mathrm{rad}(A \times B)$.

d) Por propiedades de funciones se tiene que f^{-1} es biyectiva. Además, de la teoría de espacios vectoriales se tiene que f^{-1} es una transformación K–lineal. Finalmente, de la teoría de anillos, f^{-1} es un homomorfismo de anillos unitarios. Por lo tanto f^{-1} es un isomorfismo de K–álgebras.

e) Se deja como ejercicio al lector.

f) Se deja como ejercicio al lector.

g) Se deja como ejercicio al lector.

□

Con el siguiente corolario se demuestra que el radical de una K–álgebra A contiene a todos los ideales nilpotentes de A. Más aún, a pesar de que $\mathrm{rad}(A)$ no necesariamente es un ideal nilpotente de A, en el siguiente capítulo se probará que bajo la condición de que A sea de dimensión finita, $\mathrm{rad}(A)$ sí es un ideal nilpotente de A.

1.3.5 Corolario. *Si A una K–álgebra e I es un ideal nilpotente de A, entonces $I \subseteq \mathrm{rad}(A)$. Más aún, si $A/I \cong K \times \cdots \times K$, entonces $I = \mathrm{rad}(A)$.*

Demostración. Sea I un ideal nilpotente de A con índice de nilpotencia m. Entonces, para cualesquiera $i \in I$ y $a \in A$, $ai \in I$, de donde, por la proposición 1.2.10, ai es un elemento nilpotente de A y así, por la proposición 1.2.12 $(1-ai)$ es un elemento invertible. De lo anterior y usando el lema 1.3.2, se tiene que $i \in \mathrm{rad}(A)$, concluyendo que $I \subseteq \mathrm{rad}(A)$.

Finalmente, supóngase que $A/I \cong K \times K \times \cdots \times K$. Así, dado que $\mathrm{rad}(K \times K \times \cdots \times K) = \mathrm{rad}(K) \times \mathrm{rad}(K) \times \cdots \times \mathrm{rad}(K)$ y $\mathrm{rad}(K) = 0$ pues K es un campo, se sigue que $\mathrm{rad}(A/I) = 0$. Luego, dados $a \in \mathrm{rad}(A)$ y $b \in A$ se sigue del lema 1.3.2 que $1-ab$ es invertible, de manera que su imagen bajo el epimorfismo canónico $\pi_I \colon A \to A/I$ dada por $\pi_I(1-ba) = (1+I) - (\pi_I(a)\pi_I(b))$ también lo es. De esta manera se sigue por lema 1.3.2 que $\pi_I(a) \in \mathrm{rad}(A/I) = 0$. De donde $\mathrm{rad}(A) \subseteq \mathrm{Ker}(\pi_I) = I \subseteq \mathrm{rad}(A)$ y por lo tanto $I = \mathrm{rad}(A)$.

□

1.3.6 Ejemplo.

a) *Sea I un conjunto finito parcialmente ordenado y KI el álgebra de incidencia de I con coeficientes en K definida como en 1.2.3 y vista como subálgebra de $\mathbb{M}_n(K)$. Se afirma entonces que $U = \{[\lambda_{ij}] \in KI \mid \lambda_{ii} = 0$ para toda $i \in \{1, \ldots, |I|\}\}$ es el radical de KI. En efecto, se sigue de la definición de producto de matrices que U es un ideal bilateral de KI. Más aún, se puede probar que $U^n = 0$ y que $A/U \cong \prod_{i=1}^{n} K$, de donde, por el corolario 1.3.5, $U = \mathrm{rad}(A)$.*

Para finalizar esta sección se enuncia el Teorema de Weddernburn-Malcev el cual establece que dada una K–álgebra A, existe una subálgebra B tal que el K–espacio vectorial ${}_KA$ se puede descomponer como la suma directa ${}_KA = B \oplus \mathrm{rad}(A)$. Este resultado muestra la importancia que tiene el radical de un álgebra. Se omite la demostración del teorema dado que para ésta se requiere material que no se ha abarcado en el presente trabajo.

1.3.7 Teorema.
Sea A una K–álgebra de dimensión finita tal que K es un campo algebraicamente cerrado y $\pi_{\mathrm{rad}(A)} \colon A \to A/\mathrm{rad}(A)$ la proyección canónica. Entonces, existe B una K–subálgebra de A tal que el espacio vectorial ${}_KA$ se puede descomponer como ${}_KA = B \oplus \mathrm{rad}(A)$ y $\pi_{\mathrm{rad}(A)}\big|_B$ es un isomorfismo de álgebras.

Demostración. Ver [7, Sección VI.2] y [12, Sección 11.6].

Capítulo 2

Módulos sobre álgebras

De manera similar a como sucede en el caso de la teoría de anillos, el estudio de módulos sobre K–álgebras será de provecho para explorar conceptos relevantes para la teoría de álgebras asociativas. Con ese propósito en este capítulo se expondrá lo fundamental del estudio de módulos sobre K–álgebras. Dado que una mayor parte de la teoría se obtiene naturalmente del estudio de módulos sobre anillos, se hará hincapié en resultados a los que concierne la estructura del álgebra subyacente al módulo. Posteriormente, se tratará el estudio de los homomorfismos de módulos para hacer particular énfasis en los conjuntos de homomorfismos y endomorfismos de módulos así como de las estructuras que éstos pueden adoptar. Finalmente, se da una breve discusión sobre la suma directa interna y la suma directa externa de módulos así como de algunos ejemplos en los que se observa una característica importante de los módulos sobre álgebras con la cual es posible ver cada módulo como una colección de espacios vectoriales relacionados entre sí a través de transformaciones lineales.

2.1. Módulos

En esta primera sección se darán las definiciones de módulos izquierdos, derechos y bilaterales sobre álgebras. Así mismo, tras enunciar las definiciones de módulos finitamente generados y módulos de dimensión finita, se presenta un resultado que enlaza estos dos conceptos para módulos sobre álgebras de dimensión finita. Para terminar, se enuncia el Lema de Nakayama junto con uno de sus corolarios con el cual se obtiene que el radical de un álgebra de dimensión finita es nilpotente.

2.1.1 Definición.
*Sea A una K–álgebra. Un A**–módulo izquierdo** es un K–espacio vectorial M junto con una operación producto por elementos de A*

$$\cdot : A \times M \to M$$

tal que para cualesquiera $a, b \in A$, $x, y \in M$ y $\lambda \in K$,

1. $(a+b)x = ax + bx$
2. $a(x+y) = ax + ay$
3. $a(bx) = (ab)x$
4. $1_A x = x$
5. $a(\lambda x) = (\lambda a)x = \lambda(ax)$

Al A–módulo izquierdo M se le denota por ${}_AM$.

*De manera análoga se puede definir un A**–módulo derecho** como un K–espacio vectorial M junto con una operación producto por elementos de A*

$$\cdot : M \times A \to M$$

tal que para cualesquiera $a,b \in A$, $x,y \in M$ y $\lambda \in K$,

1. $x(a+b) = xa + xb$
2. $(x+y)a = xa + ya$
3. $(xa)b = x(ab)$
4. $x1_A = x$
5. $(\lambda x)a = x(\lambda a) = \lambda(xa)$

Al A–módulo derecho M se le denota por M_A.

*De esta manera, dadas A y B dos K–álgebras, un $A-B$–**bimódulo** es un K–espacio vectorial M tal que es un A–módulo izquierdo y un B–módulo derecho, y que satisface que para cualesquiera $a \in A$, $b \in B$ y $x \in M$*

$$a(xb) = (ax)b$$

Al A–B–bimódulo M se le denota por ${}_AM_B$.

Dado que en el presente trabajo se tratará principalmente con módulos izquierdos sobre K–álgebras, se referirá a esta estructura únicamente como módulo y se mencionará explícitamente cuando sea de otra manera.

2.1.2 Definición.
*Sea M un A–módulo y M' un subespacio vectorial de ${}_KM$. Se dice que M' es un A–**submódulo** (izquierdo) de M si para cualesquiera $a \in A$ y $m \in M'$ se tiene que*

$$am \in M'$$

Esto se denota por $M' \leq M$. Al conjunto de todos los submódulos de un A–módulo M se le denota por $\mathscr{L}(M)$.

A continuación se presentan algunos ejemplos de módulos y submódulos.

2.1.3 Ejemplos.

a) *Toda K–álgebra A resulta ser un A–módulo izquierdo donde el producto de elementos por A es el producto del álgebra. A este módulo se le conoce como el módulo regular izquierdo y se le denota por ${}_AA$. Más aún, si I es un ideal del álgebra A, entonces I es un A–submódulo de A.*

b) *El conjunto $\mathbb{M}_n(\mathbb{C})$ de las matrices cuadradas de orden n con entradas en el campo $\mathbb{C}$ es un $\mathbb{R}$–módulo. Más aún, ${}_\mathbb{R}\mathbb{M}_n(\mathbb{C})$ es un módulo de dimensión finita.*

   Por otro lado, el conjunto de matrices triangulares superiores $\overline{\mathbb{T}}_n(\mathbb{C})$ resulta ser un $\mathbb{R}$–submódulo de $\mathbb{M}_n(\mathbb{C})$.

c) *Dado M un A–módulo e I un ideal izquierdo del anillo A, se tiene que el conjunto de las combinaciones lineales IM resulta ser un submódulo de M.*

d) *Sea M un A–módulo y $M_1,\ldots,M_s$ submódulos de ${}_AM$. La suma de los submódulos $M_1,\ldots,M_s$ denotada por*

$$M_1 + \cdots + M_s = \{m_1 + \cdots + m_s \mid m_i \in M_i \text{ para toda } i \in \{1,\ldots,s\}\}$$

   es un submódulo de M. Más aún, se cumple que $M_1 + \cdots + M_1 = A\left(\bigcup_{i=1}^{s} M_i\right)$.

e) *Dado un submódulo M' de un A–módulo M, el cociente M/M' resulta tener una estructura de A–módulo con la operación*

$$\begin{aligned} \cdot : A \times M/M' &\to M/M' \\ (a, m+M') &\mapsto am + M' \end{aligned}$$

   como producto por elementos de A.

f) Dado un campo K, todo K–espacio vectorial es un K–módulo.

g) Sea M un A–módulo y $M_1, \ldots, M_n$ submódulos de M. Así, el producto $M_1 \times \cdots \times M_n$ es un módulo con la operación

$$\begin{aligned} \cdot : A \times (M_1 \times \cdots \times M_n) &\to M_1 \times \cdots \times M_n \\ (a, (m_1, \cdots, m_n)) &\mapsto (am_1, \cdots, am_n) \end{aligned}$$

como producto por elementos de A.

El ejemplo 2.1.3 c) motiva la definición de módulo generado por un conjunto y de módulo finitamente generado. Este último concepto probará ser de relevancia en los siguientes capítulos.

2.1.4 Definición.
*Sea M un A–módulo y $\emptyset \neq X \subseteq M$. Se dice que M es **generado** por X si $M = AX$. Esto es, todo elemento $m \in M$ es de la forma*

$$\sum_{i=1}^{s} a_i m_i$$

con $a_i \in A$ y $m_i \in X$ para toda $i \in \{1, \ldots, s\}$ y alguna $s \in \mathbb{N}$.

*En el caso de que X sea un conjunto finito, se dice que M es un módulo **finitamente generado**. Si en particular X es un conjunto unitario, se dice que M es un módulo **cíclico**.*

El siguiente resultado, el cual se obtiene de la teoría de módulos sobre anillos, asegura que todo submódulo propio de un módulo finitamente generado está contenido en un submódulo maximal. En particular, si se tiene un módulo finitamente generado, siempre se tendrá la existencia de un submódulo maximal de dicho módulo. Antes de enunciarlo, se recordará la definición de submódulo maximal.

2.1.5 Definición. *Sea A una K–álgebra y M un A–módulo. Se dice que $N \leq M$ es un **submódulo maximal** de M si $N \neq M$ y no existe otro A–submódulo de M que contenga a N.*

2.1.6 Proposición.
Sea M un A–módulo no-cero finitamente generado. Entonces, si N es un submódulo propio de M, existe N' submódulo maximal de M tal que $N \leq N'$.

Demostración. Ver [1, Página 32].

□

Tomando en cuenta que todo módulo sobre una K–álgebra A es también un K–espacio vectorial, se obtiene de forma natural la siguiente definición de módulo de dimensión finita.

2.1.7 Definición.
*Se dice que el A–módulo M es de **dimensión finita** si ${}_KM$ es dimensión finita.*

A pesar de que en general las nociones de módulo finitamente generado y de módulo de dimensión finita no coinciden, la siguiente proposición revelerá una relación existente entre ellas. A saber, se tendrá que un módulo de dimensión finita es finitamente generado y viceversa, siempre y cuando el álgebra sea de dimensión finita.

2.1.8 Proposición.
Sea A una K–álgebra de dimensión finita y M un módulo sobre A. Entonces ${}_AM$ es finitamente generado si y sólo si es dimensión finita.

Demostración. Supóngase que ${}_AM$ es finitamente generado. Así, existen $m_1, \ldots, m_s \in M$ tales que

$$A\{m_1, \ldots, m_s\} = Am_1 + \cdots + Am_s = M$$

De esta manera para $m \in M$ arbitrario, existen $a_1, \ldots, a_s \in A$ tales que

$$m = \sum_{i=1}^{s} a_i m_i$$

Luego, dado que $_KA$ es de dimensión finita, se tiene la existencia de $\mathscr{B} = \{\alpha_1, \ldots, \alpha_t\} \subseteq A$ una base para $_KA$ de manera que para cada $i \in \{1, \ldots, s\}$ existen $\lambda_1^i, \ldots, \lambda_t^i$ en K tales que

$$a_i = \sum_{j=1}^{t} \lambda_j^i \alpha_j$$

Así, de todo lo anterior, se tiene que

$$m = \sum_{i=1}^{s} \left(\sum_{j=1}^{t} \lambda_j^i \alpha_j \right) m_i = \sum_{i=1}^{s} \left(\sum_{j=1}^{t} (\lambda_j^i \alpha_j) m_i \right) = \sum_{i=1}^{s} \left(\sum_{j=1}^{t} \lambda_j^i (\alpha_j m_i) \right)$$

De donde se sigue que $\mathscr{B}' = \{ \alpha_j m_i \mid i \in \{1, \ldots, s\},\ j \in \{1, \ldots, t\}\}$ es un conjunto generador para $_KM$, de manera que por la teoría de espacios vectoriales existe un subconjunto de $\mathscr{B}'$ que es base para $_KM$. Así, dado que $\mathscr{B}'$ es un conjunto finito, entonces dicha base también debe serlo, de donde se concluye que $_AM$ es de dimensión finita.

Por otro lado, supóngase que $_AM$ es de K–dimensión finita. Así, existe $\mathscr{B} = \{m_1, \ldots, m_s\}$ una base para $_KM$, de manera que para cada $m \in M$ existen únicos $\lambda_1, \ldots, \lambda_s \in K$ tales que

$$m = \sum_{i=1}^{s} \lambda_i m_i$$

Luego, de las propiedades de A–módulo tenemos:

$$m = \sum_{i=1}^{s} \lambda_i m_i = \sum_{i=1}^{s} \lambda_i (1_A m_i) = \sum_{i=1}^{s} (\lambda_i 1_A) m_i$$

Dado que $(\lambda_i 1_A) \in A$ para cada $i \in \{1, \ldots, s\}$, se concluye que $\mathscr{B}$ es un generador para $_AM$ y por lo tanto, $_AM$ es finitamente generado.

□

Con lo anterior es posible enunciar dos resultados que serán utilizados de manera frecuente. El primero de ellos, conocido como el Lema de Nakayama, expone que si I es un ideal de A contenido en $\mathrm{rad}(A)$ tal que $IM = M$, entonces M es el módulo trivial.

2.1.9 Lema.
Sea A una K–álgebra, M un A–módulo finitamente generado e $I \subseteq \mathrm{rad}(A)$ un ideal bilateral de A. Si $IM = M$, entonces $M = 0$.

Demostración. Supóngase que $IM = M$ y que M es generado por $m_1, m_2, \ldots, m_s \in M$. Es decir,

$$M = Am_1 + Am_2 + \cdots + Am_s$$

Luego, procediendo por inducción sobre s se tiene lo siguiente.
Si $s = 1$, entonces $Am_1 = IM = IAm_1 = Im_1$. De donde $m_1 = x_1 m_1$ con $x_1 \in I$ y por lo tanto $(1_A - x_1)m_1 = 0$. Dado que $I \subseteq \mathrm{rad}(A)$, entonces se sigue del lema 1.3.2 que $(1_A - x_1)$ es invertible y por lo tanto $m_1 = 0$, de donde $M = 0$.

Luego, supóngase que $s \geq 2$. Como $M = IM$ y $M = Am_1 + Am_2 + \cdots + Am_s$, se tiene que

$$M = IM = Im_1 + Im_2 + \cdots + Im_s$$

de donde $m_1 = x_1 m_1 + x_2 m_2 + \cdots + x_s m_s$ con $x_1, x_2, \ldots, x_s \in I$. Por tanto, $(1_A - x_1)m_1 = x_2 m_2 + x_3 m_3 + \cdots + x_s m_s$ y como $(1_A - x_1)$ es invertible, se sigue que $m_1 \in Am_2 + \cdots + Am_s$ de forma que $Am_1 \subseteq Am_2 + \cdots + Am_s$. Así, como $M = Am_1 + Am_2 + \cdots + Am_s$ se tiene que $M = Am_2 + \cdots + Am_s$. Es decir, M está generado por $s - 1$ elementos, de manera que por la hipótesis de inducción se concluye que $M = 0$.

□

El siguiente resultado es un corolario del Lema de Nakayama en el cual se prueba, como se mencionó al final del capítulo anterior, que bajo la condición de que la K–álgebra sea de dimensión finita, se cumple que su radical es un ideal nilpotente.

2.1.10 Corolario.
Si A es una K–álgebra de dimensión finita, entonces $\mathrm{rad}(A)$ *es nilpotente.*

Demostración. Nótese primero que como

$$X_n = \left\{ \prod_{i=1}^{n} a_i \mid a_i \in \mathrm{rad}(A) \, \forall \, i \in \{1,\dots,n\} \right\} \supseteq \left\{ \prod_{i=1}^{n+1} a_i \mid a_i \in \mathrm{rad}(A) \, \forall \, i \in \{1,\dots,n+1\} \right\} = X_{n+1}$$

para todo $n \in \mathbb{N}$, se sigue que

$$(\mathrm{rad}(A))^n = \langle X_n \rangle \supseteq \langle X_{n+1} \rangle = (\mathrm{rad}(A))^{n+1}$$

para todo $n \in \mathbb{N}$. Así, se tiene que

$$A \supseteq \mathrm{rad}(A) \supseteq \cdots \supseteq (\mathrm{rad}(A))^n \supseteq (\mathrm{rad}(A))^{n+1} \supseteq \dots$$

Luego, dado que cada elemento de la sucesión es un subespacio vectorial de ${}_KA$ y ${}_KA$ es de dimensión finita, entonces también lo es cada elemento de la sucesión. Así, esta sucesión debe ser eventualmente constante. De esta manera, existe un $m \in \mathbb{N}$ tal que $\mathrm{rad}(A)(\mathrm{rad}(A))^m = (\mathrm{rad}(A))^m$. De donde, por el lema 2.1.9, $(\mathrm{rad}(A))^m = 0$, con lo que se prueba que $\mathrm{rad}(A)$ es nilpotente.

□

2.2. Homomorfismos de módulos y anillos de endomorfismos

Habiendo explorado las ideas fundamentales de los módulos sobre álgebras, surge naturalmente el interés en estudiar funciones que preserven esta estructura, es decir, homomorfismos de módulos sobre álgebras. Asimismo, se revisarán resultados importantes relacionados con los conjuntos de estos homomorfismos. De esta manera, esta sección iniciará dando las definiciones básicas sobre homomorfismos de módulos sobre álgebras hasta enunciar a modo de recordatorio los Teoremas de Isomorfismo. Posteriormente, se iniciará una discusión sobre cómo para un módulo ${}_AM$ se obtienen dos anillos de endomorfismos considerando dos formas de componer estos objetos. Esto llevará a ver que todo A–módulo izquierdo (respectivamente derecho) se puede ver al mismo tiempo como un $\mathrm{End}({}_AM)$–módulo derecho (respectivamente $\mathrm{End}(M_A)$–módulo izquierdo) y se probará una equivalencia para bimódulos en términos de isomorfismos de anillos. Finalmente, se darán las definiciones de kernel, imagen, cokernel y coimagen de un homomorfismo de módulos sobre K–álgebras y se enunciará la equivalencia de que un homomorfismo es un monomorfismo si y sólo si su kernel es 0.

2.2.1 Definición.
Sean M,N dos A–módulos y A una K–álgebra. Un ***A–homomorfismo de módulos*** *es una transformación K–lineal*

$$f\colon M \to N$$

tal que para cualesquiera $a \in A$ y $m \in M$

$$f(am) = af(m)$$

Al conjunto de los A–homomorfismos de módulos entre ${}_AM$ y ${}_AN$ se le denota por $\mathrm{Hom}({}_AM, {}_AN)$.

En general se referirá a los A–homomorfismos de módulos simplemente como homomorfismos a menos que sea necesario hacer énfasis en el álgebra que se está considerando.

Como ya es costumbre, se presenta la siguiente definición de monomorfismo, epimorfismos e isomorfismos de A–módulos.

2.2.2 Definición.
Sean M,N dos A–módulos y $f\colon M \to N$ un homomorfismo de A–módulos. Se dice que

*a) f es un **monomorfismo** si f es inyectiva.*

*b) f es un **epimorfismo** si f es suprayectiva.*

*c) f es un **isomorfismo** si f es biyectiva.*

En particular, si existe un isomorfismo $f\colon M \to N$, se dice que M y N son isomorfos. Este hecho se denota por $M \cong N$.

Los Teoremas de isomorfismo están íntimamente relacionados con el concepto de isomorfismo de módulos. Por comodidad del lector se enuncian a continuación.

2.2.3 Teorema.
Sea A una K–álgebra y sean M, N dos A–módulos.

1. *Si $f\colon M \to N$ es un epimorfismo, entonces existe un único epimorfismo $\hat{f}\colon M/\operatorname{Ker}(f) \to N$ tal que $\hat{f}(m+\operatorname{Ker}(f)) = f(m)$ para todo $m \in M$.*
2. *Si $K \leq L \leq M$, entonces $M/L \cong (M/K)/(L/K)$.*
3. *Si $H \leq M$ y $K \leq M$, entonces $(H+K)/K \cong H/(H\cap K)$.*

Demostración. Ver [1, Página 46]. □

Continuando con los conceptos relacionados a los homomorfismos de módulos, se presenta la siguiente definición para homomorfismos cuyo dominio y contradominio coinciden.

2.2.4 Definición.
*Sea M un A–módulo izquierdo. Un A–homomorfismo $f\colon M \to M$ se llama **A–endomorfismo** de ${}_AM$. El conjunto de todos los endomorfismos de ${}_AM$ se denota por $\operatorname{End}({}_AM)$. Esto es:*

$$\operatorname{End}({}_AM) = \operatorname{Hom}({}_AM, {}_AM)$$

Análogamente a como ocurre cuando se considera la composición de endomorfismos de un grupo, se encontrará que hay dos formas de componer endomorfismos de módulos. Así, para un A–módulo izquierdo ${}_AM$, dos endomorfismos $f,g \in \operatorname{End}({}_AM)$ y $m \in M$, se tienen las composiciones

a) De derecha a izquierda, es decir, $fg(m) = f(g(m))$.

b) De izquierda a derecha, es decir, $(m)fg = ((m)f)g$.

Por lo anterior, y dado que el conjunto de endomorfismos del módulo ${}_AM$ tiene estructura de anillo con la suma y la composición usual de funciones –como suma y producto respectivamente–, se obtienen dos anillos unitarios para el conjunto $\operatorname{End}({}_AM)$. El primero de ellos será el de los endomorfismos a la izquierda, con la composición de derecha a izquierda, denotado por $\operatorname{End}^{\mathrm{I}}({}_AM)$; mientras que el segundo será el de los endomorfismos a la derecha, con la composición de izquierda a derecha, denotado por $\operatorname{End}^{\mathrm{D}}({}_AM)$.

Una convención que suele adoptarse es la de escribir los endomorfismos de módulos del lado contrario del que actúa el álgebra. Esto es, para un A–módulo izquierdo ${}_AM$, un A–endomorfismo $f\colon M \to M$ se escribirá por la derecha y la composición se hará de izquierda a derecha, es decir,

$$(ax+y)fg = a((x)f)g + ((y)f)g$$

para cualesquiera $x,y \in M$, $a \in A$ y f,g endomorfismos de ${}_AM$. De esta manera se tiene que el anillo de endomorfismos de un A–módulo izquierdo ${}_AM$ será el anillo de endomorfismos a la derecha, es decir,

$$\operatorname{End}({}_AM) = \operatorname{End}^{\mathrm{D}}({}_AM)$$

mientras que para un A–módulo derecho M_A el anillo de endomorfismos será el anillo de endomorfismos a la izquierda, es decir,

$$\mathrm{End}(M_A) = \mathrm{End}^{\mathrm{I}}(M_A)$$

Por otro lado, dados dos A–módulos izquierdos M y N, se cumple que $\mathrm{Hom}({}_AM, {}_AN)$ tiene estructura de K–espacio vectorial a través del producto por escalares $K \times \mathrm{Hom}({}_AM, {}_AN) \to \mathrm{Hom}({}_AM, {}_AN)$ dado por $(\lambda, f) \mapsto \lambda f$ con $\lambda f(x) = f(\lambda x)$. Así, si L, M y N son tres A–módulos izquierdos, se tiene que la composición

$$\circ\colon \ \mathrm{Hom}_A(M,N) \times \mathrm{Hom}_A(L,M) \to \mathrm{Hom}_A(L,N)$$

es una transformación K–bilineal. En particular, para un A–módulo izquierdo ${}_AM$, el anillo $\mathrm{End}({}_AM)$ es una K–álgebra.

De esta manera, por definición de A–homomorfismo y la discusión anterior, se cumple lo siguiente

1. $(x+y)f = (x)f + (y)f$ para todo $x, y \in M$ y $f \in \mathrm{End}({}_AM)$.
2. $(x)f + g = (x)f + (x)g$ para todo $x \in M$ y $f, g \in \mathrm{End}({}_AM)$.
3. $(x)fg = ((x)f)g$ para todo $x \in M$ y $f, g \in \mathrm{End}({}_AM)$.
4. $(x)\,\mathrm{Id}_{{}_AM} = x$ para todo $x \in M$.
5. $(x)\lambda f = (\lambda x)f = \lambda((x)f)$ para todo $x \in M$, $f \in \mathrm{End}({}_AM)$ y $\lambda \in K$.
6. $(ax)f = a((x)f)$ para todo $x \in M$, $f \in \mathrm{End}({}_AM)$ y $a \in A$.

Esto es, se puede considerar una acción derecha de $\mathrm{End}({}_AM)$ en M dada por $(m, f) \mapsto (m)f$ tal que cumple las condiciones de la definición de módulo derecho. Por lo tanto, se tiene que todo módulo izquierdo ${}_AM$ puede considerarse también un $\mathrm{End}({}_AM)$–módulo derecho. Como además, del último inciso se deduce que el producto por elementos de A es compatible con el de elementos de $\mathrm{End}({}_AM)$, se concluye que todo módulo izquierdo ${}_AM$ puede ser visto como un A–$\mathrm{End}({}_AM)$–bimódulo. Análogamente, todo A–módulo derecho puede ser visto como un $\mathrm{End}(M_A)$–A–bimódulo.

Finalmente, considérense dos K–álgebras A y B, y M un K–espacio vectorial tal que

a) M es un A–módulo izquierdo. Equivalentemente, existe un homomorfismo de anillos

$$\lambda : A \to \mathrm{End}^{\mathrm{I}}(M)$$

b) M es un B–módulo derecho. Equivalentemente, existe un homomorfismo de anillos

$$\rho : B \to \mathrm{End}^{\mathrm{D}}(M)$$

Como se sabe que

$$\mathrm{End}({}_AM) := \mathrm{End}^{\mathrm{D}}({}_AM) \subseteq \mathrm{End}^{\mathrm{D}}({}_{\mathbb{Z}}M) = \mathrm{End}^{\mathrm{D}}(M)$$
$$\mathrm{End}(M_B) := \mathrm{End}^{\mathrm{I}}(M_B) \subseteq \mathrm{End}^{\mathrm{I}}(M_{\mathbb{Z}}) = \mathrm{End}^{\mathrm{I}}(M)$$

entonces tiene sentido preguntarse, para $b \in B$, cuándo sucede que $\rho(b) = \rho_b \in \mathrm{End}({}_AM)$. La respuesta es que para que esto suceda debe cumplirse que para toda $a \in A$ y para toda $m \in M$,

$$(am)\rho_b = a(m\rho_b)$$

o bien,

$$(am)b = a(mb)$$

Esto es, M debe ser un A–B–bimódulo. De lo anterior, se tiene el siguiente resultado que caracteriza a los bimódulos.

2.2.5 Teorema.
Sean A y B dos K–álgebras, y M un K–espacio vectorial tal que

a) M es un A–módulo izquierdo. Equivalentemente, existe un homomorfismo de anillos

$$\lambda : A \to \mathrm{End}^{\mathrm{I}}(M)$$

b) M es un B–módulo derecho. Equivalentemente, existe un homomorfismo de anillos

$$\rho : B \to \mathrm{End}^{\mathrm{D}}(M)$$

Entonces, los siguientes enunciados son equivalentes.

i) M es un A–B–bimódulo.

ii) $\lambda : A \to \mathrm{End}(M_B)$ *es un homomorfismo de K–álgebras.*

iii) $\rho : B \to \mathrm{End}({}_AM)$ *es un homomorfismo de K–álgebras.*

□

De esta manera, se tiene que para un bimódulo ${}_AM_B$ se puede hablar del producto a la izquierda $\lambda : A \to \mathrm{End}(M_B)$ y del producto a la derecha $\rho : B \to \mathrm{End}({}_AM)$.

Adicionalmente, recuérdese que dados dos K–espacios vectoriales M y N, junto con tres K–álgebras A, B y C, se tiene que

a) los bimódulos ${}_AM_B$ y ${}_AN_C$ inducen una estructura de B–C–bimódulo sobre $\mathrm{Hom}({}_AM, {}_AN)$ a través de los productos

$$(bf)(x) = f(xb)$$
$$(fc)(x) = f(x)c$$

donde $b \in B$, $c \in C$, $f \in \mathrm{Hom}({}_AM, {}_AN)$ y $x \in M$.

b) los bimódulos ${}_BM_A$ y ${}_CN_A$ inducen una estructura de C–B–bimódulo sobre $\mathrm{Hom}({}_AM, {}_AN)$ a través de los productos

$$(cf)(x) = cf(x)$$
$$(fb)(x) = f(bx)$$

donde $b \in B$, $c \in C$, $f \in \mathrm{Hom}({}_AM, {}_AN)$ y $x \in M$.

De donde, para un A–módulo izquierdo M, se tiene que $\mathrm{Hom}({}_AA, {}_AM)$ obtiene naturalmente una estructura de A–módulo izquierdo a través del producto

$$(af)(x) = f(xa)$$

Más aún, haciendo uso de la proposición que se enuncia a continuación se obtiene otro resultado con el que se asegura que los productos λ y ρ del bimódulo regular de una K–álgebra serán en realidad isomorfismos de módulos.

2.2.6 Proposición.
Sea A una K–álgebra y M un A–módulo. Entonces, la transformación K–lineal

$$f : M \to \mathrm{Hom}({}_AA, {}_AM)$$
$$m \mapsto f_m$$

donde $f_m(a) = am$ *para toda* $a \in A$*, es un isomorfismo de A–módulos.*

Demostración. Ver [1, Página 57] □

Como se mencionó anteriormente, se sigue de la discusión anterior y de la proposición 2.2.6 que los productos λ y ρ del bimódulo ${}_AA_A$ son isomorfismos de módulos.

2.2.7 Corolario.
Dada una K–álgebra A, los homomorfismos de álgebras

$$\begin{aligned} \lambda : A &\to \mathrm{End}(A_A) \\ a &\mapsto \lambda_a \end{aligned}$$

$$\begin{aligned} \rho : A &\to \mathrm{End}({}_AA) \\ a &\mapsto \rho_a \end{aligned}$$

con $\lambda_a(a') = a'a$ *y* $(a')\rho_a = aa'$ *son también isomorfismos de módulos.* □

Enseguida se presentan algunos ejemplos de homomorfismos de K–módulos entre los cuales se encuentran algunos que serán relevantes más adelante.

2.2.8 Ejemplos.

a) Sea M un A–módulo y M' un submódulo de M. Entonces la función ***inclusión canónica*** *dada por*

$$\begin{aligned} i\colon M' &\to M \\ m &\mapsto m \end{aligned}$$

es un monomorfismo de módulos.

b) Sea M un A–módulo y $M_1, \dots, M_n$ submódulos de M. Entonces, la función

$$\begin{aligned} j\colon M_1 \times \cdots \times M_n &\to M \\ (m_1, \dots, m_n) &\mapsto \sum_{i=1}^{m} m_i \end{aligned}$$

es un homomorfismo de módulos.

c) Sea M un A–módulo y considérese el módulo cociente M/M' con $M' \leq M$. Entonces, la función ***proyección canónica***

$$\begin{aligned} \pi_{M'}\colon M &\to M/M' \\ m &\mapsto m + M' \end{aligned}$$

es un epimorfismo de módulos.

Para concluir esta sección se presentan las definiciones de kernel, imagen, cokernel y coimagen de un homomorfismos de módulos para, posteriormente, enunciar el resultado que relaciona la inyectividad de un homomorfismo con su kernel.

2.2.9 Definición. *Sean M, N dos A–módulos y $f\colon M \to N$ un homomorfismo de módulos. Se define*

a) el ***kernel*** *de f, denotado por* $\mathrm{Ker}(f)$*, como el conjunto*

$$\mathrm{Ker}(f) = \{m \in M \mid f(m) = 0\}$$

b) la ***imagen*** *de f, denotada por* $\mathrm{Im}(f)$*, como el conjunto*

$$\mathrm{Im}(f) = \{f(m) \mid m \in M\}$$

c) el ***cokernel*** *de f, denotado por* $\mathrm{Coker}(f)$*, como el cociente*

$$\mathrm{Coker}(f) = N/\mathrm{Im}(f)$$

d) la ***coimagen*** *de f, denotada por* $\mathrm{Coim}(f)$*, como el cociente*

$$\mathrm{Coim}(f) = M/\mathrm{Ker}(f)$$

Así, de la definición de homomorfismo de A–módulos y de la teoría de espacios vectoriales se sigue que dado $f : M \to N$ un homomorfismo de A–módulos, $\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ son submódulos de M y N respectivamente. Más aún, se sigue del ejemplo 2.1.3 e) que el cokernel y la coimagen de f, tienen estructura de A–módulos.

Asimismo, cualquier homomorfismo de módulos $f \in \mathrm{Hom}({}_AM, {}_AN)$ induce de manera natural un isomorfismo

$$\begin{aligned} \mathrm{Coim}(f) &\to \mathrm{Im}(f) \\ m + \mathrm{Ker}(f) &\mapsto f(m) \end{aligned}$$

Por último, se tiene la siguiente proposición que relaciona la inyectividad de un homomorfismo de módulos con su kernel.

2.2.10 Proposición.
Sea M y N dos A–módulos y $f \in \mathrm{Hom}({}_AM, {}_AN)$. Entonces, f es monomorfismo si y sólo si $\mathrm{Ker}(f) = \{0\}$.

Demostración. Se deja como ejercicio al lector.

□

2.3. Suma directa interna y suma directa externa de módulos

Para concluir el capítulo, en esta sección se presentan las definiciones de suma directa interna y de suma directa externa de módulos sobre K–álgebras. Así mismo, se hará la observación de que ambas sumas son de hecho isomorfas y se dará la definición de módulo inescindible. Además, se establecerá la notación que se usará para hablar de isomorfismos entre sumas directas internas y externas de módulos. Finalmente, se mostrarán algunos ejemplos con el propósito de exhibir una cualidad importante de los módulos sobre K–álgebras en los que cada módulo se puede ver como una colección de K–espacios vectoriales.

2.3.1 Definición.
Sean $M_1, M_2, \ldots, M_n$ A–módulos. Se define la ***suma directa externa*** *de $M_1, M_2, \ldots, M_n$ como la suma directa (externa) de K–espacios vectoriales*

$$M_1 \times M_2 \times \cdots \times M_n$$

junto con la operación producto por elementos de A dada por

$$\begin{aligned} \cdot : A \times \bigtimes_{i=1}^{n} M_i &\to \bigtimes_{i=1}^{n} M_i \\ (a, (m_1, m_2, \ldots, m_n)) &\mapsto (am_1, am_2, \ldots, am_n) \end{aligned}$$

Si en particular $M_i = M$ para toda $i \in \{1, \ldots, n\}$, se denota por M^n a $\bigtimes_{i=1}^{n} M_i$. Se acostumbra denotar a la suma directa externa de $M_1, M_2, \ldots, M_n$ por $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

Es consecuencia del ejemplo 2.1.3 *g)* que la suma directa de módulos vuelve a ser un módulo.

2.3.2 Definición.
Sea M un A–módulo y $N_1, N_2, \ldots, N_n$ A–submódulos de M. Se dice que M es la ***suma directa interna*** *de $N_1, N_2, \ldots, N_n$ si*

a) $M = N_1 + N_2 + \cdots + N_n$

b) $N_i \cap (\sum_{j \neq i} N_j) = \{0\}$

En dicho caso esto se denota por $M = N_1 \oplus N_2 \oplus \cdots \oplus N_n$.

*Se dice que $N \leq M$ es un **sumando directo** de M si existe otro submódulo L de M tal que $M = L \oplus N$.*

A pesar de que se usa la misma notación para ambas sumas, el contexto establecerá a cuál se está haciendo referencia. Más aún, resulta importante observar que si bien en principio la suma directa externa y la suma directa interna de una familia de módulos $M_1, M_2, \cdots, M_n$ son objetos distintos, existe un isomorfismo entre ellos dado por

$$\begin{aligned} \bigoplus_{i=1}^{n} M_i &\to \bigoplus_{i=1}^{n} M_i \\ (m_1, m_2, \ldots, m_n) &\mapsto \sum_{i=1}^{n} m_i \end{aligned}$$

Dado que no se puede asegurar que todo módulo se pueda ver como suma directa no trivial de sus submódulos, la siguiente definición introduce terminología para referirnos a los módulos que no admiten una descomposición en suma directa no trivial interna de submódulos.

2.3.3 Definición.
*Se dice que un A–módulo no–cero M es **inescindible** si no existen A–módulos no–cero N, L tales que*

$$M \cong N \oplus L$$

A continuación se establece notación que se utilizará a lo largo del texto para homomorfismo entre sumas directas de módulos.

Sean $(L_j)_{j=1}^{n}$ y $(N_k)_{k=1}^{m}$ dos familias de A–módulos y M un A–módulo. Dadas $(f_j)_{j=1}^{n}$ y $(g_k)_{k=1}^{m}$ familias de homomorfismos de A–módulos tales que

$$\begin{aligned} f_j &\colon L_j \to M \\ g_k &\colon M \to N_k \end{aligned}$$

para toda $j \in \{1, \ldots, n\}$ y $k \in \{1, \ldots, m\}$, se definen

$$f := (f_1, \ldots, f_m) \colon \bigoplus_{j=1}^{n} L_j \to Y$$

$$g := \begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix} \colon M \to \bigoplus_{k=1}^{m} N_k$$

dadas por

$$\begin{aligned} f(l_1, \ldots, l_n) &= f_1(l_1) + \cdots + f_n(l_n) \\ g(m) &= (g_1(m), \ldots, g_m(m)) \end{aligned}$$

para cualesquiera $(l_1, \ldots, l_n) \in \bigoplus_{j=1}^{n} L_j$ y $m \in M$.

Más aún, f y g cumplen ser los únicos homomorfismos tales que

$$\begin{aligned} f i_j &= f_j \\ \pi_k g &= g_k \end{aligned}$$

para toda $j \in \{1, \ldots, n\}$ y $k \in \{1, \ldots, m\}$, con

$$\begin{aligned} i_j \colon L_j &\to \bigoplus_{r=1}^{n} L_r \\ x_j &\mapsto (0, \ldots, 0, x_j, 0, \ldots, 0) \end{aligned}$$

y

$$\pi_k\colon \bigoplus_{r=1}^{m} N_r \to N_k$$
$$(z_1,\dots,z_k,\dots,z_m) \mapsto z_k$$

De esta manera, dado un homomorfismo de A–módulos

$$h\colon \bigoplus_{j=1}^{n} L_j \to \bigoplus_{k=1}^{m} N_k$$

éste se puede expresar a través de la matriz de $m\times n$

$$\begin{pmatrix} h_{11} & h_{12} & \dots & h_{1n}\\ h_{21} & h_{22} & \dots & h_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ h_{m1} & h_{m2} & \dots & h_{mn}\end{pmatrix}$$

donde $h_{kj} = \pi_k h i_j$.

Finalmente, dada una K–álgebra A, a lo largo del presente trabajo se denotará por A–Mod a la categoría cuyos objetos son A–módulos izquierdos y sus morfismos son los homomorfismos de A–módulos junto con la composición usual de funciones. Asimismo, se denotará por A–mod a la subcategoría plena de A–Mod cuyos objetos son todos los módulos izquierdos finitamente generados.

Un aspecto importante a la teoría de módulos sobre K–álgebras es la posibilidad de ver un módulo como una colección de K–espacios vectoriales relacionados entre sí a través de funciones K–lineales. Para ver esto se exponen los siguiente ejemplos.

2.3.4 Ejemplos.
Sea K un campo y considérese $A = \mathbb{T}_2(K)$ la K–álgebra de las matrices triangulares inferiores de orden 2 con coeficientes en el campo K.

Nótese que A es un álgebra de dimensión finita pues el conjunto

$$\left\{ e_1 = \begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix}, e_{21} = \begin{pmatrix} 0 & 0\\ 1 & 0\end{pmatrix}, e_2 = \begin{pmatrix} 0 & 0\\ 0 & 1\end{pmatrix} \right\}$$

forma una base para $_KA$. De esta manera, se sigue de la proposición 2.1.8 que todo módulo en A–mod es de dimensión finita.

Luego, sea M en A–mod, y defínanse

$$M_1 := e_1 M; \qquad M_2 := e_2 M$$

los cuales son subespacios vectoriales de $_KM$. De esta manera, como $e_1 + e_2 = 1_A$, se tiene que M tiene una descomposición como K–espacio vectorial en suma directa interna de sus K-subespacios vectoriales M_1 y M_2:

$$M_1 \oplus M_2$$

Así, dados $m = \begin{pmatrix} m_1\\ m_2\end{pmatrix} \in M$ con $m_1 \in M_1$ y $m_2 \in M_2$, y $a \in A$ se tiene que

$$am = \begin{pmatrix} a_{11} & 0\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix} m_1\\ m_2\end{pmatrix} = \begin{pmatrix} a_{11}m_1\\ a_{21}m_1 + a_{22}m_2\end{pmatrix} = \begin{pmatrix} a_{11}m_1\\ a_{21}f_M(m_1) + a_{22}m_2\end{pmatrix}$$

donde $f_M\colon M_1 \to M_2$ es una transformación K–lineal dada por $m_1 \mapsto e_{21}m_1$. De esta manera, el A–módulo M se puede identificar a través de la terna (M_1, M_2, f_M).

Más aún, si N es otro A–módulo identificado a través de la terna $(N_1, N_2, f_N : N_1 \to N_2)$ *y* $h : M \to N$ *es un homomorfismo de módulos, éste se puede identificar a través de la pareja* (h_1, h_2) *con*

$$h_1 : M_1 \to N_1$$
$$h_2 : M_2 \to N_2$$

las restricciones de h *a* M_1 *y* M_2 *respectivamente vistas como transformaciones K–lineales tales que el siguiente diagrama conmuta.*

$$\begin{tikzcd} M_1 \arrow[r, "f_M"] \arrow[d, "h_1"'] & M_2 \arrow[d, "h_2"] \\ N_1 \arrow[r, "f_N"'] & N_2 \end{tikzcd}$$

Inversamente, dada una terna $(M_1, M_2, f : M_1 \to M_2)$ *donde* M_1 *y* M_2 *son K–espacios vectoriales, y* f *es una transformación K–lineal, el K–espacio vectorial*

$$M := M_1 \oplus M_2$$

junto con la operación

$$\begin{aligned} \cdot : A \times M &\to M \\ (a, m) &\mapsto (a_{11}m_1, a_{21}f(m_1) + a_{22}m_2) \end{aligned}$$

donde $m_1 \in M_1$ *y* $m_2 \in M_2$ *es un A–módulo.*

2.3.5 Ejemplos.
Considérese el campo $\mathbb{R}$ *y la* $\mathbb{R}$*–álgebra* $\mathbb{T}_2(\mathbb{R})$ *de matrices triangulares inferiores con entradas en* $\mathbb{R}$*. Luego, tómese los espacios vectoriales* ${}_{\mathbb{R}}\mathbb{R}$ *y* ${}_{\mathbb{R}}\mathbb{R}^2$ *junto con la transformación lineal*

$$\begin{aligned} h : \mathbb{R}^2 &\to \mathbb{R} \\ (a, b) &\mapsto a + b \end{aligned}$$

Así, $M = \mathbb{R}^2 \oplus \mathbb{R}$ *junto con la operación*

$$\begin{aligned} \cdot : A \times M &\to M \\ (a, m) &\mapsto (a_{11}m_1, a_{21}h(m_1) + a_{22}m_2) \end{aligned}$$

donde $m = (m_1, m_2)$*, resulta ser un A–módulo.*

2.3.6 Ejemplos.
Sea K un campo y $K[t]$ *la K–álgebra de polinomios con coeficientes en K e indeterminada* t*.*

Luego, sea M un $K[t]$*–módulo. Así,* ${}_{K[t]}M$ *puede identificarse a través de la pareja* $({}_KM, h_M : M \to M)$ *con* ${}_KM$ *el K–espacio vectorial subyacente del álgebra* ${}_{K[t]}M$ *y* h_M *una transformación K–lineal dada por* $m \xmapsto{h_M} tv$*.*

De esta manera, dado otro $K[t]$*–módulo N, con identificación* $({}_KN, h_N)$*, un homomorfismo de álgebras* $f : M \to N$ *se puede identificar a través de sí mismo visto como transformación K–lineal*

$$f : {}_KM \to K_N$$

de tal manera que el siguiente diagrama conmuta.

$$\begin{tikzcd} M \arrow[r, "h_M"] \arrow[d, "f"'] & M \arrow[d, "f"] \\ N \arrow[r, "h_N"'] & N \end{tikzcd}$$

Inversamente, por cada par $({}_KM,h)$ con ${}_KM$ un K–espacio vectorial y $h\colon M\to M$ una transformación lineal, el espacio vectorial M dotado con la operación producto por elementos de $K[t]$

$$\cdot\colon K[t]\times M\to M$$

dada por

$$(\lambda_0+\lambda_1 t+\cdots+\lambda_n t^n, m)\mapsto \lambda_0 m+\lambda_1 h(m)+\cdots+\lambda_n h^n(m)$$

es un $K[t]$–módulo.

2.3.7 Ejemplos. *Considérese el campo $\mathbb{R}$, la $\mathbb{R}$–álgebra $\mathbb{R}[t]$ de los polinomios con indeterminada t y coeficientes en $\mathbb{R}$, y el espacio vectoria ${}_{\mathbb{R}}\mathbb{R}^2$ junto con la transformación*

$$\begin{aligned} f\colon \mathbb{R}^2 &\to \mathbb{R}^2\\ (x,y)&\mapsto(-y,x)\end{aligned}$$

Así, $\mathbb{R}^2$ resulta ser un $\mathbb{R}[t]$–módulo con

$$\begin{aligned} \cdot\colon \mathbb{R}[t]\times\mathbb{R}^2 &\to \mathbb{R}^2\\ \left(\sum_{i=1}^{n} r_i t^i,(x,y)\right)&\mapsto \sum_{i=1}^{n} r_i f^i(x,y)\end{aligned}$$

como producto por elementos de $\mathbb{R}[t]$.

2.3.8 Ejemplos.
Sean A,B dos K–álgebras y considérese la K–álgebra producto $A\times B$. Así, se tiene que $1_{A\times B}=(1_A,1_B)=e_1+e_2$, donde $e_1=(1_A,0), e_2=(0,1_B)\in A\times B$. Luego, dado un $A\times B$–módulo M, se tiene que e_1M es un A–módulo y e_2M es un B–módulo con las operaciones producto por elementos de A dadas por

$$\begin{aligned}(a,e_1m)&\mapsto(a,0)x \text{ para toda } a\in A \text{ y } m\in M\\ (b,e_2m)&\mapsto(0,b)x \text{ para toda } b\in B \text{ y } m\in M\end{aligned}$$

respectivamente. Más aún, dado que se tienen las proyecciones

$$\begin{aligned}p_A\colon A\times B&\to A \text{ dada por } (a,b)\mapsto a\\ p_B\colon A\times B&\to B \text{ dada por } (a,b)\mapsto b\end{aligned}$$

es posible dar a e_1M y e_2M estructuras de $A\times B$–módulos (ver [1, Pág. 34]) con las operaciones

$$\begin{aligned}((a,b),e_1m)&\mapsto p_A(a,b)(e_1m)=a(e_1m)=(a,0)m \text{ para todo } (a,b)\in A\times B \text{ y } m\in M\\ ((a,b),e_2m)&\mapsto p_B(a,b)(e_2m)=b(e_2m)=(0,b)m \text{ para todo } (a,b)\in A\times B \text{ y } m\in M\end{aligned}$$

De esta manera se tiene que el módulo ${}_{A\times B}M$ se puede descomponer a través de la suma directa de módulos ${}_{A\times B}M={}_{A\times B}e_1M\oplus{}_{A\times B}e_2M$.

De lo anterior, y siguiendo un razonamiento análogo al utilizado en los ejemplos 2.3.4 y 2.3.6, se tiene que esta correspondencia define una equivalencia de categorías

$$(A\times B)-\mathrm{Mod}\cong A-Mod\times B-\mathrm{Mod}$$

Capítulo 3

Módulos simples y semisimples

En este capítulo se presentarán resultados relacionados con el estudio de módulos simples y semisimples sobre K–álgebras. Así mismo, se definirán los conceptos de soclo, radical y tope de un módulo y se enunciarán sus principales propiedades. Posteriormente, se enuncia el teorema de Jordan-Hölder el cual establece que la longitud de las series de composición de un módulo finitamente generado sobre una K–álgebra es invariante y, para concluir, se presenta un corolario de dicho teorema que muestra la similitud que el concepto de longitud de un módulo tiene con el de dimensión para espacios vectoriales.

A lo largo del capítulo se supondrá que todos los campos son algebraicamente cerrados y que todas las álgebras son de dimensión finita. Se denotará a una K–álgebra por A.

3.1. Módulos simples y semisimples

Esta primera sección comienza con las definiciones de módulo simple y de módulo semisimple. Posteriormente, se enuncia el Lema de Schur con el cual se muestra que es posible decir si un morfismo entre A–módulos es un monomorfismo, un epimorfismo o un isomorfismo verificando si el dominio y/o el contradominio del morfismo es un módulo simple. Inmediatamente después se utiliza este lema para exhibir un isomorfismo entre el anillo de endomorfismos de un A–módulo simple y el campo K sobre el que se define la K–álgebra. Finalmente, se da una caracterización para módulos simples en términos de sus sumandos directos junto con un corolario que involucra al módulo cociente.

3.1.1 Definición.
*Sea S un A–módulo no-cero. Se dice que S es **simple** si sus únicos submódulos son* 0 *y S.*

3.1.2 Definición.
*Sea S un A–módulo. Se dice que S es **semisimple** si existe una descomposición de S como suma directa de submódulos simples de S.*

3.1.3 Proposición.
Todo A–módulo simple es cíclico.

Demostración. Sea M un A–módulo simple. Así, para cualquier elemento $m \in M$ con $m \neq 0$ se tiene que $0 \neq Am \leq M$. Como M es simple, se concluye que $Am = M$ y por lo tanto M es cíclico.

$\square$

El siguiente lema que se obtiene de la definición de módulo simple, conocido como el Lema de Schur, establece que para dos A–módulos S y S' se puede asegurar que un homomorfismo no–cero $f \in \mathrm{Hom}({}_AS, {}_AS')$ es un monomorfismo, un epimorfismo o un isomorfismo en función de si alguno de los dos módulos es simple. La demostración de este enunciado se obtiene fácilmente al considerar los casos que existen para el kernel y la imagen del homomorfismo de módulos. Se demostrará el primero de los incisos y el resto se dejarán al lector.

3.1.4 Lema. *Sean S y S' dos A–módulos y $f\colon S \to S'$ un A–homomorfismo no cero. Se cumple que,*

a) Si S es simple, entonces f es un monomorfismo.

b) Si S' es simple, entonces f es un epimorfismo.

c) Si S y S' son simples, entonces f es un isomorfismo.

Demostración.

a) Dado que S es simple se tiene que los únicos submódulos de S son 0 y S. Así, para f no-cero, se sigue que $S \neq \operatorname{Ker}(f) \leq S$, de donde se concluye que $\operatorname{Ker}(f) = 0$ y por lo tanto f es un monomorfismo.

b) Se deja como ejercicio al lector.

c) Se deja como ejercicio al lector.

□

Como corolario del resultado anterior se tendrá que dado un A–módulo simple M, hay un isomorfismo de K–álgebras entre $\operatorname{End}({}_AM)$ y el campo K. A pesar de que el isomorfismo dado por el corolario se obtendrá directamente del Lema de Schur, dicho enunciado se utiliza para hacer la observación de que todo elemento no cero en $\operatorname{End}({}_AM)$ debe ser un isomorfismo y por lo tanto el anillo de endomorfismos será en particular un anillo con división, a partir de lo cual se obtendrá el resultado deseado.

3.1.5 Corolario.
Si M es un A–módulo simple, entonces existe un isomorfismo de K–álgebras

$$f\colon \operatorname{End}({}_AM) \to K$$

Demostración. Sea M un A–módulo simple. Dado que todo elemento en $\operatorname{End}({}_AM)$ es un homomorfismo de A–módulos de M y M es un módulo simple, se sigue del Lema de Schur que todo elemento no-cero en $\operatorname{End}({}_AM)$ es un isomorfismo y por lo tanto es invertible. Así, se tiene que $\operatorname{End}({}_AM)$ es un anillo con división. Por otro lado, dado que M es simple se sigue que es cíclico y como A es de dimensión finita, entonces M es también de dimensión finita. Así mismo, de la teoría de espacios vectoriales (ver [9, Página 104]) se sigue que $\operatorname{End}({}_AM)$ también es de dimensión finita. Por lo tanto, para un elemento no-cero $\phi \in \operatorname{End}({}_AM)$ con $\phi \neq \operatorname{Id}_M$ se tiene que los elementos

$$\operatorname{Id}_M, \phi, \phi^2, \ldots, \phi^m, \ldots$$

son distintos y además linealmente dependientes. Esto es, existe una K–combinación lineal

$$\sum_{i=1}^{l} \lambda_i \phi^i = 0_{\operatorname{End}({}_AM)}$$

tal que $\lambda_j \neq 0$ para algún $j \in \{0, \ldots, l\}$. De esta manera, se tiene que ϕ es raíz del polinomio

$$g(t) = \sum_{i=1}^{l} \lambda_i t^i$$

de manera que existe un polinomio mónico irreducible no-cero $f(t) \in K[t]$ tal que $f(\phi) = 0$. Más aún, dado que K es algebraicamente cerrado, se tiene que $\operatorname{gr}(f(t)) = 1$ y por lo tanto $f(t) = \lambda_\phi + t$ para algún $\lambda_\phi \in K$. De lo anterior se sigue que

$$f(\phi) = \lambda_\phi \operatorname{Id}_M + \phi = 0$$

Esto es,

$$\phi = -\lambda_\phi \operatorname{Id}_M$$

Así, se define entonces la función

$$T: \operatorname{End}({}_AM) \to K$$
$$\phi \mapsto \begin{cases} 0_K & : \phi = 0_{\operatorname{End}({}_AM)} \\ 1_K & : \phi = \operatorname{Id}_M \\ -\lambda_\phi & : \phi \neq 0_{\operatorname{End}({}_AM)}, \operatorname{Id}_M \end{cases}$$

la cual resulta ser el isomorfismo de K–álgebras buscado.

□

Continuando con el estudio de los módulos simples y semisimples, más allá del Lema de Schur, el siguiente lema proporciona una caracterización para módulos semisimples en términos de sus sumandos directos. Además, este resultado mostrará que los submódulos de un módulo semisimple de dimensión finita, también serán semisimples.

3.1.6 Lema.

a) *Un módulo ${}_AM$ de dimensión finita es semisimple si y sólo si para cada submódulo de N de M existe un submódulo L de M tal que $M = L \oplus N$.*

b) *Todo submódulo de un módulo semisimple de dimensión finita también es semisimple.*

Demostración.

a) Supóngase primero que M es semisimple y sea N un submódulo de M. Dado que M es semisimple existen $S_1, S_2, \ldots, S_n$ submódulos de M tales que
$$M = \bigoplus_{i=1}^{n} S_i$$
Luego, tómese $\{S_{j_1}, S_{j_2}, \ldots, S_{j_t}\}$ una familia de elementos de $\{S_1, S_2, \ldots, S_n\}$ máxima respecto a la propiedad de que la intersección de N con $L = \bigoplus_{i=1}^{n} S_{j_1}$ es cero. De esta manera se tiene que $N \cap (L + S_t) \neq 0$ para todo $t \notin \{j_1, j_2, \ldots, j_n\}$ y por lo tanto existe $n \in N \cap (L + S_t)$ tal que $n \neq 0$ y $n = l + s$ para algún $l \in L$ y algún $s \in S_t$. Más aún, nótese que $s \neq 0$ pues en caso contrario $0 \neq n = l \in N \cap L$ lo cual es una contradicción. De lo anterior se sigue que $0 \neq s = n - l \in (N + L) \cap S_t$, de manera que $(N + L) \cap S_t \neq 0$ para todo $t \notin \{j_1, j_2, \ldots, j_n\}$. Así, se tiene que $S_t \leq N + L$ para todo $t \notin \{j_1, j_2, \ldots, j_n\}$ y como S_t es simple para todo $t \notin \{j_1, j_2, \ldots, j_n\}$ se concluye que $N + L = M$ y por lo tanto $M = N \oplus L$.

Para probar el enunciado recíproco se procederá por inducción sobre la dimensión de ${}_KM$.

Considérese primero un A–módulo M tal que todo submódulo $N \leq M$ es un sumando directo de M y supóngase que $\dim({}_KM) = 1$. Así, trivialmente se tiene que ${}_AM$ es simple y por lo tanto es semisimple.

Luego, supóngase que todo módulo ${}_AM$ con dimensión menor o igual a n y con la propiedad de que todo submódulo de M es un sumando directo es semisimple.

Finalmente, sea M un A–módulo tal que todo submódulo de M es un sumando de directo y supóngase además que $\dim({}_KM) = n + 1$. Así, dado N un submódulo propio de M existe un submódulo L de M tal que

$$M = L \oplus N$$

Más aún, nótese que para N' un submódulo de N se tiene que existe $L' \leq M$ tal que

$$M = L' \oplus N'$$

De donde
$$N = M \cap N = (N' \oplus L') \cap N = N \oplus (L' \cap N)$$
Esto es, para $N' \leq N$ se encontró un submódulo de N $L_{N'} := L' \cap N$ tal que $N = N' \oplus L'$, es decir, se probó que todo submódulo de N es un sumando directo de N. Así, dado que $\dim({}_KM) \leq n$, se sigue que N es semisimple. Análogamente, se obtiene que L es también semisimple y por lo tanto, $M = L \oplus N$ es semisimple.

b) Sea M un A–módulo semisimple de dimensión finita y tómese $N \leq M$. Análogamente al inciso anterior se tiene que para $N' \leq N \leq M$ existe un submódulo $L_{N'} \leq N$ tal que

$$N = N' \oplus L_{N'}$$

como $\dim({}_K N) \leq \dim({}_K M) < \infty$, del inciso anterior se concluye que N es semisimple.

□

Finalmente, recuérdese que dado un submódulo H de un A–módulo M se definen las retículas de submódulos

$$\mathscr{L}(M)/H := \{N \leq M : H \leq N\} \text{ y } \mathscr{L}(M/H) := \{N/H \leq M : H \leq N \leq M\}$$

De esta forma, dado que para cada $N \in \mathscr{L}(M)/H$ el cociente N/H es un submódulo de M/H y además para un submódulo $T \leq M/H$ el conjunto $\{x : x+H \in T\}$ resulta ser un submódulo de M que contiene a H, se obtienen las funciones

$$\begin{aligned} n_H : \mathscr{L}(M)/H &\to \mathscr{L}(M/H) \\ N &\mapsto N/H \end{aligned}$$

$$\begin{aligned} n_H^{\leftarrow} : \mathscr{L}(M/H) &\to \mathscr{L}(M)/H \\ T &\mapsto \{x : x+H \in T\} \end{aligned}$$

que resultarán ser funciones inversas, con lo cual se establece una correspondencia biunívoca entre las retículas $\mathscr{L}(M)/H$ y $\mathscr{L}(M/H)$. Como consecuencia de lo anterior se tiene el siguiente corolario que será de bastante utilidad a lo largo del capítulo pues establece condiciones necesarias y suficientes para que un módulo cociente sea simple.

3.1.7 Corolario.
Sea M un A–módulo y N un submódulo de M. Entonces, el módulo cociente M/N es simple si y sólo si N es maximal en M.

□

3.2. El soclo, el radical y el tope de un módulo

Una vez que se han estudiado algunas propiedades sobre módulos simples y semisimples, en esta sección se introducirán los conceptos de soclo, radical y tope de un módulo. Primero, el soclo de un módulo resultará ser una forma de obtener un submódulo semisimple de cualquier módulo no–cero. Más aún, se utilizará esta motivación para llegar a la definición de álgebra semisimple junto con un teorema que da condiciones necesarias y suficientes para determinar cuándo un álgebra de grupo es semisimple usando la característica de su campo. Posteriormente, se presentará el concepto de radical de un módulo, el cual guardará similitudes con su contraparte para álgebras. A través del radical se probarán propiedades importantes acerca del módulo cociente $M/\operatorname{rad}(M)$ para módulos finitamente generados. Así, se motiva la definición de tope de un módulo finitamente generado, el cual no será más que el módulo cociente $M/\operatorname{rad}(M)$.

3.2.1 Definición.
*Sea M un A–módulo no cero. Se define el **soclo** de M denotado por* $\operatorname{soc} M$ *como la suma de todos los submódulos propios simples de M. Es decir,*

$$\operatorname{soc}(M) := \sum_{\substack{N \leq M \\ N \text{ simple}}} N$$

Si M no tiene submódulos propios simples, se define $\operatorname{soc}(M) = 0$.

Así, se tendrá que un A–módulo M es semisimple si y solamente si $\operatorname{soc}(M) = M$. Resultará de particular interés cuando, dada una K–álgebra A sobre un campo algebraicamente cerrado K, todos sus módulos sean semisimples. En ese caso, se dirá que el álgebra es semisimple. Con esto en mente, el siguiente teorema conocido como el Teorema de Weddeburn-Artin establecerá varias equivalencias que permitirán en la práctica decidir cuándo un álgebra es semisimple o no. De hecho, será en términos de este resultado que posteriormente se dará la definición de álgebra semisimple.

3.2.2 Teorema.
Dado un campo algebraicamente cerrado K y A una K–álgebra de dimensión finita, los siguientes enunciados son equivalentes:

a) *Todo A–módulo izquierdo es semisimple.*

b) *El módulo regular izquierdo ${}_AA$ es semisimple.*

c) *Todo A–módulo derecho es semisimple.*

d) *El módulo regular derecho A_A es semisimple.*

e) $\operatorname{rad}(A) = 0$.

f) *Existen enteros positivos $m_1, m_2, \dots, m_n$ tales que*

$$A \cong \mathbb{M}_{m_1}(K) \times \mathbb{M}_{m_2}(K) \times \cdots \times \mathbb{M}_{m_n}(K)$$

Demostración. Ver [1], [6], [7], [12] y [15].

□

3.2.3 Definición.
Se dice que una K–álgebra A de dimensión finita sobre un campo algebraicamente cerrado es ***semisimple*** *si se satisface alguna de las equivalencias del Teorema de Wedderburn-Artin.*

3.2.4 Ejemplos.

a) *Sea $I = \{a_1, a_2, \dots, a_n\}$ un conjunto finito con un orden parcial $\preceq$ y supóngase que $a_i \not\preceq a_j$ si y sólo si $a_i \neq a_j$. De esta manera se sigue que el álgebra de incidencia de I es*

$$\begin{aligned} KI &= \{[\lambda_{ij}] \in \mathbb{M}_n(K) : \lambda_{ij} = 0 \text{ si } a_i \neq a_j\} \\ &= \{[\lambda_{ij}] \in \mathbb{M}_n(K) : \lambda_{ij} = 0 \text{ si } i \neq j\} \end{aligned}$$

Esto es, KI es el álgebra de matrices diagonales con coeficientes en K. Así, se tiene que todo ideal maximal no–cero del álgebra es de la forma

$$\{[\lambda_{ij}] \in \mathbb{M}_n(K) : \lambda_{ij} = 0 \text{ si } i \neq j \text{ o } i = l = j\}$$

con $1 \leq l \leq n$. Por lo tanto se obtiene que $\operatorname{rad}(KI) = 0$*, de donde se concluye que KI es semisimple.*

b) *Trivialmente se tiene del corolario 1.3.3 que para una K–álgebra A, el álgebra cociente $A/rad(A)$ es semisimple.*

Cuando en particular el álgebra en cuestión es un álgebra de grupo, se tiene otro resultado conocido como el Teorema de Maschke que establece una equivalencia para cuando el álgebra es semisimple en términos de la característica de su campo.

3.2.5 Teorema.
Sea G un grupo finito y K un campo. Entonces el álgebra de grupo KG es semisimple si y sólo si la característica de K no divide al orden de G.

Demostración. Ver [7], [12] y [15].

□

Por otro lado, nótese que si se considera al módulo regular ${}_AA$ de una K–álgebra A, se tendrá que todos los submódulos de este módulo corresponden a ideales del álgebra y viceversa. En particular, si I es un ideal maximal del álgebra A, entonces será también un submódulo maximal del módulo regular. Así, es natural pensar que si se considera el radical de A, entonces una definición equivalente podría ser tomar la intersección de los submódulos maximales del módulo regular ${}_AA$.

3.2.6 Definición.
*Sea M un A–módulo. Se define el **radical** (de Jacobson) de M, denotado por* $\mathrm{rad}(M)$*, como sigue*

$$\mathrm{rad}(M) := \bigcap\{N \leq M : N \textit{ es submódulo maximal de } M\}$$

Antes de poder probar propiedades relacionadas con el radical de un módulo sobre una K–álgebra, será necesario enunciar la siguiente proposición. Este resultado indica bajo qué condiciones se puede asegurar que un A–módulo M tiene estructura de A/I–módulo con I un ideal del álgebra.

3.2.7 Proposición.
Sea M un A–módulo e I un ideal de A. Entonces, si $IM = 0$, se sigue que M tiene estructura de A/I–módulo.

Demostración. Sea M un A–módulo y tómese $I \subseteq A$ un ideal de la K–álgebra A. Así, defínase la función

$$\begin{aligned} \cdot : A/I \times M &\to M \\ (a+I, m) &\mapsto am \end{aligned}$$

Se afirma entonces que esta función no depende de los representantes. En efecto, sean $a+I, b+I \in A/I$ tales que $a+I = b+I$. Así, se sigue de la definición de álgebra cociente que $a-b \in I$, de manera que

$$am - bm = (a-b)m = 0$$

y por lo tanto $am = bm$. Como $am = (a+I)m$ y $bm = (b+I)m$, se concluye que

$$(a+I)m = (b+I)m$$

Es decir, la función no depende de representantes. Más aún, nótese que para cualesquiera $a, b \in A$; $m, m' \in M$ y $\lambda \in K$ se cumple que

i) $[(a+I)+(b+I)]m = (a+b+I)m = (a+b)m = am+bm = (a+I)m+(b+I)m$.

ii) $(a+I)(m+m') = a(m+m') = am+am' = (a+I)m+(a+I)m'$.

iii) $(1+I) = 1m = m$.

iv) $(a+I)[(b+I)m] = (a+I)(bm) = a(bm) = (ab)m = (ab+I)m = [(a+I)(b+I)]m$.

v) $(a+I)(\lambda m) = a(\lambda m) = (\lambda a)m = (\lambda a+I)m = (\lambda a)m = \lambda(am) = \lambda[(a+I)m]$.

De donde se concluye que M es un A/I–módulo con la función $(a+I, m) \mapsto am$ como producto por elementos de A/I. □

Con el resultado anterior es posible probar la siguiente proposición que agrupa varias propiedades del radical de un módulo.

3.2.8 Proposición.
Sea A una K–álgebra de dimensión finita y M, L y N A–módulos finitamente generados. Entonces

a) $m \in \mathrm{rad}(M)$ *si y sólo si* $f(m) = 0$ *para cualquier* $f \in \mathrm{Hom}({}_AM, {}_AS)$ *con S un A–módulo simple.*

b) $\mathrm{rad}(M \oplus N) = \mathrm{rad}(M) \oplus \mathrm{rad}(N)$.

c) *Si $f\colon {}_AM \to_A N$ es un homomorfismo de módulos, entonces $f(\mathrm{rad}(M)) \subseteq \mathrm{rad}(N)$.*

d) $\mathrm{rad}(A)M = \mathrm{rad}(M)$.

e) *Sean N y L submódulos del módulo M. Si $L \subseteq \mathrm{rad}(M)$ y $L+N = M$, entonces $M = N$.*

Demostración.

a) Considérese primero un elemento $m \in \mathrm{rad}(M)$, un A–módulo simple S y $f \in \mathrm{Hom}({}_AM,{}_A S)$. Así, se tiene del Lema de Schur que f es suprayectiva, de modo que $\mathrm{Coim}(f) = M/\mathrm{Ker}(f) \cong S$, de donde al ser S simple, se sigue que $M/\mathrm{Ker}(f)$ es simple y por lo tanto $\mathrm{Ker}(f)$ es maximal en M. De lo anterior se tiene que $\mathrm{rad}(M) \subseteq \mathrm{Ker}(f)$ y por lo tanto $m \in \mathrm{Ker}(f)$, es decir, $f(m) = 0$.

   Por otro lado, sea $m \in M$ con la propiedad de que para cualquier módulo simple ${}_AS$ y $f \in \mathrm{Hom}({}_AM, {}_AS)$, $f(m) = 0$. Así, si M' es un submódulo maximal de M, se tiene que $\pi_{M'}(m) = 0$, de donde $m \in \mathrm{Ker}(\pi_{M'}) = M'$. Dado que esto se cumple para todo submódulo maximal de M, se concluye que $m \in \mathrm{rad}(M)$.

b) Sea $(m,n) \in \mathrm{rad}(M \oplus N)$. Considérese S un A–módulo simple y homomorfismos

$$f\colon M \to S \quad \text{y} \quad g\colon N \to S$$

   Considérense además los homomorfismos

$$\begin{aligned} f'\colon M \oplus N &\to S \\ (m,n) &\mapsto f(m) \end{aligned}$$

   y

$$\begin{aligned} g'\colon M \oplus N &\to S \\ (m,n) &\mapsto g(n) \end{aligned}$$

   Así, del inciso anterior se tiene que $f'(m,n) = 0$ y $g'(m,n) = 0$, de donde $m \in \mathrm{rad}(M)$ y $n \in \mathrm{rad}(N)$ con lo que se concluye que $\mathrm{rad}(M \oplus N) \subseteq \mathrm{rad}(M) \oplus \mathrm{rad}(N)$.

   La contención recíproca se obtiene de forma análoga.

c) Sea $f \in \mathrm{Hom}({}_AM, {}_AN)$ y $g\colon N \to S$ con S un A–módulo simple. Así, se tiene que para $m \in \mathrm{rad}(M)$ $g \circ f(m) = g(f(m)) = 0$, de donde se concluye que $f(m) \in \mathrm{rad}(N)$.

d) Considérese primero $m \in M$ y defínase el A–homomorfismo

$$\begin{aligned} f_m\colon {}_AA &\to_A M \\ a &\mapsto am \end{aligned}$$

   Así, por el inciso anterior se tiene que

$$\mathrm{rad}(A)m = f_m(\mathrm{rad}(A)) \subseteq \mathrm{rad}(M)$$

   para toda $m \in M$. De esta manera, se tiene que

$$\mathrm{rad}(A)M = \bigcup_{m \in M} \mathrm{rad}(A)m \subseteq \mathrm{rad}(M)$$

   Por otro lado, es claro que $\mathrm{rad}(A)(M/\mathrm{rad}(A)M) = 0$ de donde, por la proposición 3.2.7, $M/\mathrm{rad}(A)M$ es un $A/\mathrm{rad}(A)$–módulo. Más aún, dado que $A/\mathrm{rad}(A)$ es un anillo semisimple se sigue que $M/\mathrm{rad}(A)M$ es un $A/\mathrm{rad}(A)$–módulo semisimple. Así, del iniciso (b) se tiene que $\mathrm{rad}(M/\mathrm{rad}(A)M) = 0$ y por lo tanto al considerar

$$\pi\colon {}_AM \to {}_A(M/\mathrm{rad}(A)M)$$

   se tiene que

$$\pi(\mathrm{rad}(M)) \subseteq \mathrm{rad}(M/\mathrm{rad}(A)M) = 0$$

   y por lo tanto,

$$\mathrm{rad}(M) \subseteq \mathrm{Ker}(\pi) = \mathrm{rad}(A)M$$

e) Sean L y N submódulos de M tal que $L \subseteq \operatorname{rad}(M)$ y $L+N=M$. Supóngase, para llegar a una contradicción, que $M \neq N$. Así, N es un submódulo propio de M, de donde se tiene la existencia de un submódulo maximal $N' < M$ tal que $N \leq N'$. Como además se tiene que $L \subseteq \operatorname{rad}(M) \subseteq N'$, se concluye que

$$M = L+N \subseteq N'+N = N'$$

lo cual contradice que N' sea submódulo maximal de M.

$\square$

Entre las propiedades obtenidas en la proposición anterior, se destacan los incisos c) y d) que resultarán de utilidad para estudiar más de cerca al módulo cociente $M/\operatorname{rad}(M)$. Así, el siguiente corolario muestra que dado un módulo finitamente generado M, el módulo cociente $M/\operatorname{rad}(M)$ será semisimple y además tendrá estructura de $A/\operatorname{rad}(A)$–módulo. Más aún, se tiene que $\operatorname{rad}(M)$ es el submódulo de M más pequeño que hace semisimple al cociente.

3.2.9 Corolario.
Sea M un A–módulo finitamente generado. Entonces,

a) El A–módulo $M/\operatorname{rad}(M)$ es semisimple y es un módulo sobre la K–álgebra $A/\operatorname{rad}(A)$.

b) Si L es un submódulo de M tal que M/L es semisimple, entonces $\operatorname{rad}(M) \subseteq L$.

Demostración.

a) Se sabe del inciso (d) de la proposición anterior que $\operatorname{rad}(M) = \operatorname{rad}(A)M$, de donde, por la proposición 3.2.7, se obtiene el resultado buscado.

b) Sea $L \leq M$ tal que M/L es semisimple. Así, para el epimorfismo

$$\pi_L \colon M \to M/L$$

se tiene que $\pi_L(\operatorname{rad}(M)) \subseteq \operatorname{rad}(M/L) = 0$, de donde $\operatorname{rad}(M) \subseteq \operatorname{Ker}(\pi_L) = L$.

$\square$

Como se pudo observar anteriormente, el módulo cociente $M/\operatorname{rad}(M)$ es un objeto con propiedades de interés para la teoría. De hecho, se verá en el siguiente capítulo que este módulo será relevante en el estudio de los módulos proyectivos y las cubiertas proyectivas de módulos. Es por esto que, para un módulo M, este módulo suele recibir el nombre de tope de M, lo cual queda reflejado en la siguiente definición.

3.2.10 Definición.
*Sea M un A–módulo. Se define el **tope** de M denotado por $\operatorname{top}(M)$ como*

$$\operatorname{top}(M) := M/\operatorname{rad}(M)$$

Es consecuencia de los resultados anteriores que para un A–módulo izquierdo M, $\operatorname{top}(M)$ es un $A/\operatorname{rad}(A)$–módulo izquierdo. Más aún, dado que para cualquier homomorfismo

$$f \colon {}_AM \to_A N$$

se tiene que $f(\operatorname{rad}(M)) \subseteq \operatorname{rad}(N)$, f induce de manera natural el homomorfismo

$$\begin{aligned} \operatorname{top} f \colon\ \operatorname{top}(M) &\to \operatorname{top}(N) \\ m+\operatorname{rad}(M) &\mapsto f(m)+\operatorname{rad}(N) \end{aligned}$$

Al homomorfismo $\operatorname{top} f \colon\ \operatorname{top}(M) \to \operatorname{top}(N)$ se le llamada el **tope** de f.

Para concluir esta sección se enuncia el siguiente corolario con el cual se obtiene un resultado respecto al tope de un homomorfismo y dos que relacionan las condiciones de un módulo de ser simple o semisimple con su radical.

3.2.11 Corolario.

a) Sean M y N dos A–módulos finitamente generados. Un A–homomorfismo $f: M \to N$ es suprayectivo si y sólo si $\operatorname{top} f$ *es suprayectiva.*

b) Si S es un A–módulo simple, entonces $\operatorname{rad}(A)S = 0$ *y S es un* $A/\operatorname{rad}(A)$*–módulo simple.*

c) Un A–módulo M es semisimple si y sólo si $\operatorname{rad}(M) = 0$.

Demostración.

a) Supóngase primero que f es suprayectiva y sea $n + \operatorname{rad}(N) \in N/\operatorname{rad}(N)$. Dado que f es suprayectiva se tiene que existe $m_n \in M$ tal que $f(m_n) = n$. De esta manera se sigue, por definición de $\operatorname{top} f$, que

$$\operatorname{top} f(m_n + \operatorname{rad}(M)) = f(m_n) + \operatorname{rad}(N) = n + \operatorname{rad}(N)$$

de donde se concluye que $\operatorname{top} f$ es suprayectiva.

Por otro lado, supóngase que $\operatorname{top} f$ es suprayectiva. Así, para cada $n + \operatorname{rad}(N) \in N/\operatorname{rad}(N)$ existe $m_n + \operatorname{rad}(M) \in M/\operatorname{rad}(M)$ tal que $\operatorname{top} f(m_n + \operatorname{rad}(M)) = n + \operatorname{rad}(N)$, esto es,

$$f(m_n) + \operatorname{rad}(N) = n + \operatorname{rad}(N)$$

de donde $f(m_n) - n \in \operatorname{rad}(N)$. Así,

$$f(m_n) - (f(m_n) - n) = n \in \operatorname{Im}(f) + \operatorname{rad}(N)$$

con lo que se prueba que $N \subseteq \operatorname{Im}(f) + \operatorname{rad}(N)$ y por lo tanto $N = \operatorname{Im}(f) + \operatorname{rad}(N)$. De esta manera, del inciso (e) de la proposición anterior se tiene que $\operatorname{Im}(f) = N$ y por lo tanto f es suprayectiva.

b) Dado un A–módulo simple S, se tiene que S es cíclico. Así, por el lema de Nakayama,

$$S \neq \operatorname{rad}(A)S$$

y por lo tanto $\operatorname{rad}(A)S = 0$, de donde S es un $A/\operatorname{rad}(A)$ módulo. Más aún, si T es un $A/\operatorname{rad}(A)$–submódulo de S, T es también un A–submódulo de S de forma que $T = S$ o $T = 0$. De lo anterior se concluye que S es $A/\operatorname{rad}(A)$–simple.

c) Sea M un A–módulo semisimple. Así, de la proposición 3.2.8 se sigue que

$$\operatorname{rad}(M) = \bigoplus_{i=1}^{n} \operatorname{rad}(S_i)$$

Como $\operatorname{rad}(S_i) = 0$ para toda $i \in \{1, \ldots, n\}$, se concluye que $\operatorname{rad}(M) = 0$.

Inversamente, si $\operatorname{rad}(M) = 0$, entonces del corolario 3.2.9 se tiene que $M/\operatorname{rad}(M) = M/0 = M$ es simple.

□

3.3. El Teorema de Jordan-Hölder

Para concluir este capítulo se da una discusión acerca de las series de composición de un módulo no–cero finitamente generado M, las cuales son sucesiones finitas de submódulos de M tales que cada submódulo se encuentra propiamente contenido en los anteriores. Así, después de probar que todo módulo no–cero finitamente generado admite una serie de descomposición, se enunciará el teorema de Jordan-Hölder, con el cual se obtiene que dos series de descomposición distintas para un mismo módulo M tendrán la misma longitud y sus cocientes serán isomorfos. De esta manera, se podrá establecer una similitud entre el concepto de longitud de un módulo y la dimensión de un espacio vectorial.

Para comenzar, es importante recordar que a lo largo de este capítulo se consideran únicamente álgebras de dimensión finita. Así, dada una K–álgebra A y M un A–módulo no–cero finitamente generado se tiene de la proposición 2.1.6 que todo submódulo propio de M está contenido en un submódulo maximal, de manera que es posible asegurar la existencia de un submódulo maximal M_1 de M. Análogamente, si $M_1 \neq 0$ se sigue que al ser finitamente generado se puede asegurar la existencia de un submódulo maximal M_2 de M_1 tal que

$$M_2 < M_1 < M_0 = M$$

Procediendo de esta manera se tienen dos posibilidades. La primera es que exista una cadena infinita de submódulos de M tales que

$$\cdots < M_2 < M_1 < M_0 = M$$

y M_{j+i} sea un submódulo maximal de M_j para todo $j \in \mathbb{N}$. La segunda posibilidad es que exista una cadena finita de submódulos de M con

$$0 = M_n < \cdots < M_2 < M_1 < M_0 = M$$

para algún $n \in \mathbb{N}$ y tal que M_{j+1} sea submódulo maximal de M_j para todo $j \in \{0,\ldots,n-1\}$.

A una cadena finita de submódulos, como en la segunda posibilidad, de un A–módulo M se le llama **serie de composición** de M y a los submódulos simples M_j/M_{j+1} con $j \in \{0,\ldots,n-1\}$ se les llama **factores de composición** de M.

Con el siguiente lema se prueba que si M es un A–módulo de dimensión finita, entonces se puede asegurar la existencia de una serie de composición para dicho módulo.

3.3.1 Lema.
Sea A una K–álgebra de dimensión finita y $M \neq 0$ un A–módulo finitamente generado. Entonces, existe una serie de composición

$$0 = M_n < \cdots < M_2 < M_1 < M_0 = M$$

para M.

Demostración. Por inducción sobre $\dim({}_KM)$.

Para $\dim({}_KM) = 1$ se sigue que M es un módulo simple y por lo tanto se tiene la serie de composición trivial

$$0 = M_1 < M_0 = M$$

Luego, supóngase que para todo módulo M tal que $\dim({}_KM) \leq n$ se tiene una serie de composición para M.

Finalmente, sea M un A–módulo tal que $\dim_K(M) = n+1$. Nótese que si M es simple, se tiene nuevamente la serie trivial, de manera que se supondrá que M no es simple. Así, existe $N \leq M$ tal que $0 \neq N \neq M$. Dado que M es finitamente generado, existe un submódulo maximal M_1 de M. Más aún, dado que M_1 es un submódulo propio de M, se cumple que $\dim_K(M_1) \leq n$ y por lo tanto, de la hipótesis inductiva, existe una serie de composición de M_1

$$0 = M_{1_n} < \cdots < M_{1_2} < M_{1_1} < M_{1_0} = M_1$$

la cual se puede extender para formar la serie de composición de M

$$0 = M_{n+1} = M_{1_n} < \cdots < M_3 = M_{1_2} < M_2 = M_{1_1} < M_1 = M_{1_0} < M_0 = M$$

□

Como consecuencia del lema anterior se tiene que para una K–álgebra de dimensión finita A, todo módulo en A–mod tiene una serie de composición. Así, para un módulo M en A–mod con serie de composición

$$0 = M_n < \cdots < M_2 < M_1 < M_0 = M$$

se tiene que al número n se le llama la **longitud** de M y se denota por $l(M)$. Con el siguiente resultado, conocido como el Teorema de Jordan–Hölder, se establece que para una K–álgebra de dimensión finita A y un A–módulo M finitamente generado, la longitud de M es invariante.

3.3.2 Teorema.
Sea A una K–álgebra de dimensión finita y M un A–módulo finitamente generado. Si

$$0 = M_m < \cdots < M_2 < M_1 < M_0 = M$$

$$0 = N_n < \cdots < N_2 < N_1 < N_0 = M$$

son dos series de composición de M, entonces $n = m$ y existe una permutación σ de $\{1, \dots, m\}$ tal que

$$M_j/M_{j+1} \cong N_{\sigma(j)}/N_{\sigma(j+1)}$$

para cada $j \in \{0, \dots, m-1\}$.

Demostración. Ver [1, Página 135].

□

Del Teorema de Jordan-Hölder se sigue que la longitud de un módulo M dependerá únicamente de M. Para finalizar el capítulo se enuncia el siguiente corolario el cual muestra la importancia que el concepto de longitud de un módulo tiene en la teoría.

3.3.3 Corolario.
Sea A una K–álgebra de dimensión finita y M un módulo en A–mod.

a) Si $N \leq M$, entonces $l(M) = l(N) + l(M/N)$.

b) Si $L, N \leq M$, entonces $l(L+N) + l(L \cap N) = l(L) + l(N)$.

Demostración.

a) Considérese una serie de composición para el A–módulo M/N

$$0 = N/N = M_m/N < \cdots < M_2/N < M_1/N < M_0/N = M/N$$

y una serie de composición para el módulo N

$$0 = N_n < \cdots < N_2 < N_1 < N_0 = N$$

Así, del segundo teorema de isomorfismo y del teorema de correspondencia se sigue que

$$0 = N_n < \cdots < N_2 < N_1 < N_0 = N = M_m < M_{m-1} < \cdots < M_2 < M_1 < M_0 = M$$

es una serie de composición para M, de donde $l(M) = n + m = l(N) + l(M/N)$.

b) Ver [1, Página 137].

□

Capítulo 4

Módulos proyectivos y álgebras básicas

Este capítulo, que se encuentra dividido en tres secciones, se ocupará de agrupar los últimos resultados que se explorarán en este trabajo sobre la teoría de módulos sobre K–álgebras y los elementos idempotentes en dichas álgebras. En la primera sección se mostrará la relación que existe entre las descomposiciones como suma directa de inescindibles del módulo regular de un álgebra y sus idempotentes para, posteriormente, extender el alcance de estos resultados con el objetivo de poder considerar cualquier módulo finitamente generado sobre un álgebra de dimensión finita y llegar así al Teorema de Descomposición Única. En la segunda sección se estudiarán a los módulos proyectivos finitamente generados con la intención de probar que sus descomposiciones inescindibles son, de hecho, isomorfas a una suma directa de submódulos inescindibles del módulo regular. Se probará que a pesar de que no todo módulo finitamente generado es proyectivo, sí se les puede asociar una cubierta proyectiva y que, más aún, el tope del módulo será isomorfo al tope de su cubierta proyectiva. En la última sección se centrará la atención a una clase particular de álgebras llamadas álgebras básicas. Estas álgebras cumplirán que los submódulos inescindibles obtenidos a partir de un conjunto completo de idempotentes ortogonales primitivos no serán isomorfos entre sí. Finalmente, se expondrá una manera de asociar a cada álgebra un álgebra básica la cual será única salvo isomorfismo.

4.1. Suma directa e idempotentes

En esta sección se mostrarán los resultados que vinculan las descomposiciones en suma directa de ciertos módulos sobre K—álgebras con los elementos idempotentes de álgebras relacionadas a dichos módulos. De forma inicial se tratará únicamente con el módulo regular del álgebra exhibiendo que cada sumando directo tendrá asociado un idempotente del álgebra. Se hará énfasis en que dichos sumandos directos serán inescindibles siempre que el idempotente asociado sea primitivo. Posteriormente, se generalizarán estos resultados para alcanzar módulos finitamente generados sobre un álgebra de dimensión finita. Para este último caso, los idempotentes en cuestión no serán precisamente los del álgebra sobre el que se defina el módulo, sino del álgebra de endomorfismos del módulo. Para llegar a esto, será necesario explorar la noción de álgebra local. Finalmente, se enunciará el Teorema de Descomposición Única el cual muestra que todo módulo finitamente generado sobre un álgebra de dimensión finita admitirá una descomposición inescindible en suma directa y que además ésta será única salvo isomorfismo. Como corolario de este teorema se tendrá el caso particular en el que el módulo a considerar sea el módulo regular de un álgebra de dimensión finita, regresando así al caso con el que se inició la sección.

Para poder dar paso a los resultados antes mencionados, es necesario dar la siguiente definición.

4.1.1 Definición.
Sea A una K–álgebra y sean $e, e_1, e_2 \in A$ elementos idempotentes.

*a) Se dice que e es **central** si para todo $a \in A$ se cumple que $ae = ea$.*

*b) Se dice que e_1 y e_2 son **ortogonales** si $e_1e_2 = e_2e_1 = 0$.*

*c) Se dice que e es **primitivo** si no puede escribirse como suma de idempotentes ortogonales no-cero de A.*

A continuación se exhiben algunos ejemplos.

4.1.2 Ejemplos.

a) Dada una K–álgebra A, los elementos 0 *y* 1 *son idempotentes de A y se les conoce como los* ***idempotentes triviales*** *del álgebra A.*

b) Dado $e \in A$ un elemento idempotente, el elemento $1-e$ es también un idempotente.

$$(1-e)^2 = (1-e)(1-e) = 1(1-e) - e(1-e) = 1-e+e-e^2 = 1-e$$

c) Si $e \in A$ es un elemento idempotente no trivial, entonces se tiene que los elementos e y $1-e$ son idempotentes ortogonales no triviales.

$$e(1-e) = e-e^2 = e-e = 0$$
$$(1-e)e = e-e^2 = e-e = 0$$

De los ejemplos anteriores se sigue que dados dos idempotentes ortogonales no triviales e y $1-e$ de una K–álgebra A, existe una descomposición no trivial del módulo regular $_AA$ como suma directa dada por:

$$_AA = {_AAe} \oplus {_AA(1-e)}$$

En efecto, como $1_A = e + (1-e)$, se sigue que para cualquier $a \in A$,

$$a = a1_A = a(e+(1-e)) = ae + a(1-e)$$

Más aún, si $x \in Ae \cap A(1-e)$, entonces $x = ae$ y $x = b(1-e)$ para algunos $a, b \in A$. Así,

$$ae = ae^2 = (ae)e = xe = b(1-e)e = 0$$

de donde se concluye que $x = 0$ y por lo tanto $Ae \cap A(1-e) = 0$.

Recíprocamente, se tendrá que si $_AA = {_AM_1} \oplus {_AM_2}$ es una descomposición no trivial en suma directa del módulo regular $_AA$, entonces existirán idempotentes ortogonales no triviales $e_1 \in M_1$ y $e_2 \in M_2$ tales que $1 = e_1 + e_2$ y $M_i = Ae_i$ con $i \in \{1,2\}$.

Sin embargo, para poder probar este hecho será necesario recordar el siguiente resultado de la teoría de módulos.

4.1.3 Proposición.
Sea A una K–álgebra y M un A–módulo izquierdo con descomposición en suma directa dada por

$$_AM = {_AK} \oplus {_AK'}$$

Entonces, existe un único idempotente $e_K \in \mathrm{End}(_AM)$ tal que

$$K = \mathrm{Im}(e_K) \text{ y } K' = \mathrm{Im}(\mathrm{Id}_{_AM} - e_K)$$

Demostración. Ver [1, Página 71]

□

Ahora bien, si dada una K–álgebra A se tiene una descomposición no trivial del módulo regular

$$_AA = {_AM_1} \oplus {_AM_2}$$

entonces de la proposición 4.1.3 se tiene la existencia de un único idempotente $\overline{e_1} \in \mathrm{End}(_AA)$ tal que $M_1 = \mathrm{Im}(\overline{e_1})$ y $M_2 = \mathrm{Im}(\mathrm{Id}_{_AA} - \overline{e_1})$. Así, de la proposición 2.2.7 se sigue que existe un idempotente $e_1 \in A$ tal que $\rho(e_1) = \overline{e_1}$ con

$$\rho : A \to \mathrm{End}(_AA)$$
$$a \mapsto \rho_a$$

donde $\rho_a(a') = aa'$. Finalmente, dado que $\mathrm{Im}(\overline{e_1}) = M_1$, se cumple que

$$M_1 = \mathrm{Im}(\overline{e_1}) = \mathrm{Im}(\rho(e_1)) = \mathrm{Im}(\rho_{e_1}) = Ae_1$$

y, análogamente,

$$M_2 = \mathrm{Im}(\mathrm{Id}_{_AA} - \overline{e_1}) = \mathrm{Im}(\rho(1_A - e_1)) = \mathrm{Im}(\rho_{(1_A - e_1)}) = A(1 - e_1)$$

de donde se obtiene que los idempotentes buscados son e_1 y $1 - e_1$, respectivamente.

Como ya es costumbre, al tratar con la descomposición en suma directa de módulos será de particular interés el caso en el que dicha descomposición se pueda dar a través módulos inescindibles. Más aún, siguiendo con la idea de lograr caracterizar una descomposición a través de elementos idempotentes del álgebra, surge la necesidad de encontrar condiciones para los idempotentes bajo las cuales se pueda asegurar que el sumando directo asociado a ellos sea inescindible. En este contexto es que se presenta el siguiente resultado con el cual se obtiene que el sumando directo asociado a un idempotente será inescindible si y solamente si el idempotente en cuestión es primitivo.

4.1.4 Corolario.
Sea A una K–álgebra y $e \in A$ un elemento idempotente no-cero. Entonces las siguientes condiciones son equivalentes:

a) e es un idempotente primitivo.

b) Ae es un sumando directo inescindible de ${}_AA$.

c) eA es un sumando directo inescindible de A_A.

Demostración. Ver [1, Página 97]

□

Generalizando la discusión anterior se tiene que dada una K–álgebra A de dimensión finita, el módulo regular ${}_AA$ admite una descomposición en suma directa interna dada por

$${}_AA = {}_AP_1 \oplus {}_AP_2 \oplus \cdots \oplus {}_AP_n$$

donde P_i es un A–módulo izquierdo inescindible para todo $i \in \{1, \ldots, n\}$. Así, por lo anterior se tiene que $P_i = Ae_i$ para toda $i \in \{1, \ldots, n\}$ donde $e_1, e_2, \ldots, e_n$ son idempotentes ortogonales dos a dos, primitivos y tales que $1 = \sum_{i=1}^{n} e_i$.

Recíprocamente, se obtiene también que dados $e_1, e_2, \ldots, e_n$ elementos idempotentes ortogonales dos a dos, primitivos y tales que $1 = \sum_{i=1}^{n} e_i$ estos inducen una descomposición en suma directa interna del módulo regular ${}_AA$ dada por

$${}_AA = {}_AAe_1 \oplus {}_AAe_2 \oplus \cdots \oplus {}_AAe_n$$

Esto último motiva la siguiente definición.

4.1.5 Definición.
Sea A un K–álgebra de dimensión finita. A una descomposición del módulo regular

$${}_AA = {}_AP_1 \oplus {}_AP_2 \oplus \cdots \oplus {}_AP_n$$

tal que $P_i = Ae_i$ para toda $i \in \{1, \ldots, n\}$ y $e_1, e_2, \ldots, e_n$ son idempotentes ortogonales dos a dos, primitivos y tales que $1 = \sum_{i=1}^{n} e_i$ se le llama ***descomposición inescindible*** *de A. Además, se dice que el conjunto $\{e_1, e_2, \ldots, e_n\}$ es un* ***conjunto completo de idempotentes ortogonales primitivos*** *de A.*

Un caso de particular interés es en el que el idempotente e tal que

$${}_AA = {}_AAe \oplus {}_AA(1 - e)$$

es central, pues entonces el submódulo Ae resultará ser un ideal bilateral del álgebra A. Más aún, como se tiene que si e es un idempotente central, también lo es $1 - e$, se sigue que $A(1 - e)$ será también un ideal bilateral de A. De esta forma se observa que si e es un idempotente central no trivial, entonces Ae y $A(1 - e)$ son K–álgebras con elemento neutro e

y $1-e$, respectivamente. En este caso se dice que la descomposición ${}_AA = Ae \oplus A(1-e)$ es una **descomposición en producto directo interno** del álgebra A a través de las K–álgebras Ae y $A(1-e)$.

De manera similar a como ocurre con las descomposiciones en suma directa de A–módulos, se tendrá un concepto que refleje la imposibilidad de descomponer un álgebra en producto directo interno. Dicho concepto se presenta en la siguiente definición.

4.1.6 Definición.
Se dice que una K–álgebra A es ***inescindible (o conectada)*** *si no se puede descomponer como suma directa interna de dos ideales bilaterales del álgebra.*

A continuación se presenta un lema que da una equivalencia bastante útil que en la práctica servirá para verificar si un álgebra es inescindible. Posteriormente, se da un ejemplo de una descomposición inescindible de un álgebra.

4.1.7 Lema.
Un álgebra de dimensión finita es inescindible si y sólo si 0 *y* 1 *son sus únicos idempotentes centrales.*

Demostración. Supóngase primero, para llegar a una contradicción, que A es una K–álgebra inescindible y que existe un elemento idempotente central no trivial $e \in A$. Así, se tiene entonces que $Ae \oplus A(1-e)$ es una descomposición del álgebra como suma directa interna de los ideales bilaterales Ae y $A(1-e)$, con lo que se contradice la hipótesis de que A es inescindible.

Por el otro lado, supóngase también para llegar a una contradicción, que los únicos idempotentes centrales de un álgebra A son los idempotentes triviales, pero que A no es inescindible. Así, se tiene que existen dos ideales bilaterales A_1 y A_2 de A tales que

$$A = A_1 \oplus A_2$$

De esta manera, para $1_A \in A$, existen $e_1 \in A_1$ y $e_2 \in A_2$ tales que $1_A = e_1 + e_2$. Como además $1_A \notin A_1$ y $1_A \notin A_2$, se puede asegurar que $1_A \neq e_1 \neq 0_A$ y $1_A \neq e_2 \neq 0_A$. Por otro lado, se cumple también que para cualquier $a \in A$ $e_1ae_2 = 0_A = e_2ae_1$, pues de otra manera, al ser A_1 y A_2 ideales bilaterales, se tendría que $0_A \neq e_1ae_2 \in A_1 \cap A_2$, lo cual contradice que $A_1 \cap A_2 = \{0_A\}$. En particular, si $a = 1_A$ se cumple que $e_1e_2 = 0_A = e_2e_1$.

De lo anterior, se puede observar que

$$e_1 = e_1 1_A = e_1(e_1+e_2) = e_1e_1 + e_1e_2 = e_1e_1 = e_1^2$$

$$e_2 = e_2 1_A = e_2(e_1+e_2) = e_2e_1 + e_2e_2 = e_2e_2 = e_2^2$$

Y además, para $a \in A$,

$$\begin{aligned} ae_1 &= 1_A(ae_1) = (e_1+e_2)(ae_1) \\ &= e_1ae_1 + e_2ae_1 = e_1ae_1 + 0_A = e_1ae_1 = 0_A + e_1ae_1 = e_1ae_2 + e_1ae_1 \\ &= (e_1a)(e_2+e_1) = (e_1a)1_A = e_1a \end{aligned}$$

y análogamente, $ae_2 = e_2a$. Es decir, e_1 y e_2 son idempotentes centrales no triviales de A, lo cual es una contradicción a la hipótesis de que los únicos idempotentes centrales de A son 0 y 1.

□

4.1.8 Ejemplos.

a) Considérese la K–álgebra de dimensión finita

$$A = \begin{pmatrix} K & 0 & 0 \\ 0 & K & 0 \\ K & K & K \end{pmatrix}$$

Así, se tiene que A es inescindible y que el módulo regular ${}_AA$ tiene una descomposición inescindible dada por

$${}_AA = Ae_1 \oplus Ae_2 \oplus Ae_3$$

donde

$$e_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Adicionalmente, se puede notar que $\dim_K(Ae_1) = 2 = \dim_K(Ae_2)$ *y que* $\dim_K(Ae_3) = 1$*, de donde* Ae_3 *es un A–módulo simple. De esto mismo y del lema 3.3.1 se tiene que la longitud de los A–módulos* Ae_1 *y* Ae_2 *es* 2*. Es decir, existe una serie de descomposición de longitud* 2 *tanto para* Ae_1 *como para* Ae_2*, a saber*

$$0 < \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ K & 0 & 0 \end{pmatrix} < Ae_1$$

$$0 < \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & K & 0 \end{pmatrix} < Ae_2$$

Una vez se ha evidenciado la importancia que tienen los elementos idempotentes de un álgebra en el estudio de su módulo regular, surge la pregunta de si existirá alguna relación entre estos idempotentes y aquellos que se obtengan a partir del álgebra cociente. Para responder esta pregunta se presenta un resultado conocido como el Lema de Levantamiento de Idempotentes, el cual establece que todo idempotente del álgebra cociente $A/\operatorname{rad}(A)$ es la clase lateral de un idempotente del álgebra A. Para poder enunciarlo será necesario dar la siguiente definición.

4.1.9 Definición.
Sea A una K–álgebra y L un K–subespacio vectorial de A. Se dice que los idempotentes de A ***se levantan módulo*** *L si para todo* $a \in A$ *tal que* $a - a^2 \in L$*, existe un idempotente* $e \in A$ *tal que* $e - a \in L$*.*

En particular, cuando L es un ideal bilateral del álgebra A, la condición de que $a - a^2 \in L$ es equivalente a pedir que $a + L$ sea un elemento idempotente del álgebra cociente A/L. De esta manera, se tiene que dado un ideal L de A, se dice que los idempotentes de A **se levantan módulo** L si para cada idempotente x de A/L existe un idempotente $e \in A$ tal que $x = e + L$.

Con esto, es posible enunciar el Lema de Levantamiento de Idempotentes.

4.1.10 Lema.
Dada una K–álgebra de dimensión finita A, sus idempotentes se levantan módulo $\operatorname{rad}(A)$.

Demostración. Ver [2, página 19]

□

Habiendo establecido la relación entre los idempotentes de un álgebra A y los de su álgebra cociente $A/\operatorname{rad}(A)$, la siguiente proposición estudia la conexión que existe entre elementos idempotentes y la descomposición en suma directa de los módulos de un álgebra, centrándose en particular en el álgebra cociente $A/\operatorname{rad}(A)$. Este resultado indica primero que todo ideal del álgebra $A/\operatorname{rad}(A)$ se puede escribir como suma directa de ideales izquierdos simples de $A/\operatorname{rad}(A)$ que se obtienen a partir de idempotentes primitivos de esta misma álgebra para posteriormente obtener que todo $A/\operatorname{rad}(A)$–módulo finitamente generado es isomorfo a una suma directa de ideales izquierdos del álgebra cociente. Por último, se muestra que dado un idempotente primitivo de A, el $A/\operatorname{rad}(A)$–módulo $\operatorname{top}(Ae)$ será simple, de forma que por el Teorema de la Correspondencia para módulos $\operatorname{rad}(Ae)$ será el único submódulo maximal del A–módulo inescindible Ae.

4.1.11 Proposición.
Sea A una K–álgebra de dimensión finita y $B = A/\operatorname{rad}(A)$*. Entonces,*

a) *Todo ideal izquierdo I de B tiene una descomposición como suma directa de ideales izquierdos simples de B de la forma Be donde* $e \in B$ *es un idempotente primitivo. Más aún, se tiene que el módulo regular* ${}_BB$ *es semisimple.*

b) *Todo módulo M en B–mod es isomorfo a una suma directa de ideales izquierdos de B de la forma Be donde e es un idempotente primitivo de B.*

c) *Si e es un idempotente primitivo de A, entonces el B–módulo* $\operatorname{top}(Ae)$ *es simple y además se tiene que* $\operatorname{rad}(Ae) = \operatorname{rad}(A)e \subseteq Ae$ *es el único submódulo maximal de Ae*

Demostración. Ver [2, página 20]

□

Ya que se ha estudiado cómo los idempotentes de un álgebra tienen un papel importante a la hora de estudiar la descomposición en suma directa de su módulo regular, surge el interés por buscar resultados que ayuden a generalizar estas nociones para lograr abarcar no solo el módulo regular, sino cualquier otro módulo que pueda presentarse sobre un álgebra. Como se verá a continuación, esta inquietud será respondida de forma satisfactoria siempre que se consideren módulos finitamente generados sobre un álgebra de dimensión finita. A pesar de estas restricciones los resultados que se obtendrán durante las siguientes páginas, y que concluirán con el Teorema de Descomposición Única, serán de vital importancia pues en las secciones posteriores se tendrá particular interés en ciertos módulos finitamente generados con características especiales. Para poder llegar a estos resultados, primero será necesario dar la siguiente definición de álgebra local la cual será central en los resultados por venir.

4.1.12 Definición.
*Se dice que un álgebra A es **local** si tiene un único ideal izquierdo maximal.*

4.1.13 Ejemplos.

a) *El álgebra conmutativa*
$$A = K[x_1,\dots,x_n]/\langle x_1^{s_1},\dots,x_n^{s_n}\rangle$$
donde $s_1,s_2,\dots,s_n \in \mathbb{N}^+$ *es un álgebra local.*

b) *Dado un conjunto parcialmente ordenado I de cardinalidad al menos* 2 *se tiene que el álgebra de incidencia KI no es un álgebra local.*

El siguiente lema establecerá varias equivalencias a la noción de álgebra local. La más importante de ellas y la que resultará también más útil será la que da una caracterización de álgebra local de dimensión finita a través de sus idempotentes pues nos permitirá, como se verá en los corolarios de este lema, dirigir la noción de álgebra local de vuelta a la discusión de descomposiciones inescindibles de módulos.

4.1.14 Lema.
Sea A una K–álgebra de dimensión finita. Los siguientes enunciados son equivalentes:

a) *A es un álgebra local.*

b) *El conjunto de los elementos no invertibles de A es un ideal bilateral del álgebra.*

c) *Para cada* $a \in A$ *se cumple que a es invertible o bien* $1-a$ *es invertible.*

d) *Los únicos idempotentes de A son los idempotentes triviales.*

e) *Las K–álgebras* $A/\operatorname{rad}(A)$ *y K son isomorfas.*

Demostración.

$(a \Rightarrow b)$ Dado que A es local, se tiene que $\operatorname{rad}(A)$ es su único ideal izquierdo maximal. Más aún, se tiene que $\operatorname{rad}(A) = \{x \in A : x \text{ no tiene inverso izquierdo}\}$. En efecto, dado $x \in \operatorname{rad}(A)$ debe ser sin inverso izquierdo pues en caso contrario existiría $y \in A$ tal que $yx = 1$, de donde $1 \in \operatorname{rad}(A)$, lo cual es una contradicción. Por otro lado, dado $x \in A$ sin inverso izquierdo se tiene que entonces el ideal $\langle x\rangle \neq A$. Esto es, $\langle x\rangle$ es un ideal propio de A de manera que existe un ideal maximal izquierdo de A tal que $\langle x\rangle \leq I$. Usando nuevamente que A es local se sigue entonces que $I = \operatorname{rad}(A)$ de donde $\langle x\rangle \leq \operatorname{rad}(A)$ y por lo tanto $x \in \operatorname{rad}(A)$.

Por otro lado, nótese que dado $x \in A$ con inverso izquierdo y se sigue que $yx = 1$ de donde $y(1-xy) = 0$. Así, se obtiene que y tiene inversa izquierda y $1-xy = 0$ pues en caso contrario se tendría que $y \in \operatorname{rad}(A)$ de manera que $1-xy$ es invertible y por lo tanto $y = 0$, lo cual es una contradicción pues y es inversa izquierda de x. Así, como con lo anterior se muestra que todo elemento con inverso izquierdo en A es invertible, se tiene que $\operatorname{rad}(A) = \{x \in A : x \text{ no tiene inverso izquierdo}\} = \{x \in A : x \text{ no es invertible}\}$, de donde se concluye (b).

$(b \Rightarrow c)$ Dado $a \in A$ se tiene dos casos.

Caso 1. $a \in \operatorname{rad}(A) = \{x \in A : x \text{ no es invertible}\}$.
Así, del lema 1.3.2 se tiene que $1 - ba$ es invertible para toda $b \in A$ y en particular para $b = 1$. Esto es, $1 - a$ es invertible.

Caso 2. $a \notin \operatorname{rad}(A)$.
Así, como $\operatorname{rad}(A)$ es el conjunto de los elementos no invertibles de A, se concluye que a debe ser invertible.

$(c \Rightarrow d)$ Dado $e \in A$ un elemento idempotente se sigue de la hipótesis que o bien e es invertible o bien $1 - e$ es invertible. Así, dado que $e(1 - e) = 0$ se concluye que $e = 1$ o bien $e = 0$.

$(d \Rightarrow e)$ Del lema de levantamiento de idempotentes se tiene que los únicos idempotentes del álgebra $A/\operatorname{rad}(A)$ son $0_{A/\operatorname{rad}(A)}$ y $1_{A/\operatorname{rad}(A)}$. Adicionalmente, del primer inciso de la proposición 4.1.11 se sigue que $A/\operatorname{rad}(A)$ es simple y por lo tanto del corolario 3.1.5 se tiene un isomorfismo de K–álgebras entre $\operatorname{End}({}_{A/\operatorname{rad}(A)}A/\operatorname{rad}(A))$ y K de donde se concluye, por el lema 4.1.15, que $A/\operatorname{rad}(A) \cong \operatorname{End}({}_{A/\operatorname{rad}(A)}A/\operatorname{rad}(A)) \cong K$

$(e \Rightarrow a)$ Como $A/\operatorname{rad}(A) \cong K$ se sigue del corolario 1.3.5 que $\operatorname{rad}(A)$ es el único ideal izquierdo maximal de A.

□

Como observación del lema anterior se hace hincapié en la importancia de que el álgebra sea de dimensión finita pues, por ejemplo, el álgebra de polinomios $K[x]$ tiene como únicos idempotentes a 0 y 1, a pesar de que no es un álgebra local. Esto se obtiene del hecho de que al ser K un campo, $K[x]$ es un dominio de ideales principales y por lo tanto sus ideales maximales coincidirán con sus ideales primos, los cuales se generan a partir de sus elementos irreducibles. De esta manera, se tiene que $K[x]$ tiene más de un ideal izquierdo maximal.

Anteriormente se había observado que dado un idempotente central de una K–álgebra A, el K–subespacio vectorial Ae será también una K–álgebra. Es posible obtener un resultado similar aún excluyendo la condición de que el idempotente sea central si se considera al K–subespacio vectorial eAe. En efecto, dado un idempotente $e \in A$, se sigue que el K–espacio vectorial eAe será una K–álgebra con elemento neutro e. Más aún, se sigue que eAe será una subálgebra de A si y solamente si $e = 1$.

Asimismo, se tiene que para un A–módulo M, el K–subespacio vectorial eM es un eAe–módulo a través de la operación por elementos de eAe dada por

$$\begin{aligned} eAe \times eM &\to eM \\ (eae, em) &\mapsto eaem \end{aligned}$$

En particular se cumple que eA es un eAe–módulo izquierdo y además que Ae es un eAe–módulo derecho.

Por otro lado, resultará ser posible dotar al K–espacio vectorial $\operatorname{Hom}({}_A Ae, {}_A M)$ de estructura de eAe–módulo izquierdo a través del producto

$$\begin{aligned} eAe \times \operatorname{Hom}({}_A Ae, {}_A M) &\to \operatorname{Hom}({}_A Ae, {}_A M) \\ (eae, \varphi) &\mapsto eae \cdot \varphi \end{aligned}$$

donde $(eae \cdot \varphi)(x) = \varphi(xeae)$.

Antes de presentar el primero de los dos corolarios del lema 4.1.14, se enuncia el siguiente resultado que exhibe que los eAe–módulos eM y $\operatorname{Hom}({}_A Ae, {}_A M)$ son isomorfos. Más aún, cuando se considera el caso particular en el que el módulo M es el A–submódulo Ae, se tendrá un isomorfismo de K–álgebras entre $\operatorname{End}({}_A Ae)$ y eAe.

4.1.15 Lema.
Sea A una K–álgebra, $e \in A$ un elemento idempotente y M un A–módulo izquierdo. Entonces,

a) La transformación K–lineal

$$\begin{aligned} \theta_M \colon \operatorname{Hom}({}_A Ae, {}_A M) &\to eM \\ \varphi &\mapsto e(\varphi(e)) = \varphi(e) \end{aligned}$$

es un isomorfismo de eAe–módulos izquierdos.

b) El isomorfismo

$$\theta_{Ae}\colon \operatorname{End}({}_AAe) \xrightarrow{\cong} eAe$$

induce un isomorfismo de K–álgebras.

Demostración.

a) Para ver que θ_M es un eAe–homomorfismo de módulos basta ver que abre el producto por elementos de eAe. Así, para $eae \in eAe$ y $\varphi \in \operatorname{Hom}({}_AAe, {}_AM)$ se tiene que

$$\theta_M(eae\cdot\varphi) = (eae\cdot\varphi)(e) = \varphi(e(eae)) = eae\,\varphi(e) = eae\,\theta_M(\varphi)$$

Con lo que se prueba que θ_M es un homomorfismo de eAe–módulos.

Luego, para probar que es un isomorfismo se define la transformación K–lineal

$$\begin{aligned}\theta'_M\colon eM &\to \operatorname{Hom}({}_AAe, {}_AM)\\ em &\mapsto \varphi_{em}\end{aligned}$$

con $\varphi_{em}(ae) = aem$. Análogamente a como sucedió con θ_M, se cumple que θ'_M es un homomorfismo de eAe–módulos pues para $eae \in eAe$, $em \in eM$ y $be \in Ae$ se tiene que

$$\begin{aligned}\varphi_{(eae)em}(be) = \varphi_{eaem}(be) &= be(eaem)\\ &= beaem = (beae)em = \varphi_{em}(beae)\\ &= \varphi_{em}(be(eae)) = (eae\cdot\varphi_{em})(be)\end{aligned}$$

Así, se afirma entonces que θ'_M es el homomorfismo inverso de θ_M. En efecto, dada $\varphi \in \operatorname{Hom}({}_AAe, {}_AM)$, se sigue que

$$\theta'_M\theta_M(\varphi) = \theta'_M(\theta_M(\varphi)) = \theta'_M(\varphi(e)) = \overline{\varphi}_{\varphi(e)}$$

de manera que esta parte se reduce a probar que $\varphi = \overline{\varphi}_{\varphi(e)}$. Para esto, considérese $ae \in Ae$. Entonces,

$$\overline{\varphi}_{\varphi(e)}(ae) = ae\varphi(e) = \varphi((ae)e) = \varphi(ae)$$

Con lo que se prueba que $\varphi = \overline{\varphi}_{\varphi(e)}$ y por lo tanto $\theta'_M\theta_M = \operatorname{Id}_{\operatorname{Hom}({}_AAe, {}_AM)}$.

Similarmente, para $em \in eM$ se tiene que

$$\theta_M\theta'_M(em) = \theta_M(\theta'_M(em)) = \theta_M(\varphi_{em}) = \varphi_{em}(e) = e(em) = em$$

Con lo que se prueba que $\theta_M\theta'_M = \operatorname{Id}_{eM}$.

De lo anterior, se concluye que $\theta'_M = \theta_M^{-1}$ y por lo tanto, θ_M es un isomorfismo de eAe–módulos.

b) Del inciso anterior se tiene ya que

$$\theta_{Ae}\colon \operatorname{End}({}_AAe) \to eAe$$

es una transformación K–lineal biyectiva. Así, basta probar que es un homomorfismo de anillos unitario.

i) Para ello, recordemos que dado que Ae es un A–módulo izquierdo, entonces la composición en $\operatorname{End}({}_AAe)$ debe hacer de izquierda a derecha. Así, dados $\psi, \varphi \in \operatorname{End}({}_AAe)$ se sigue que, usando la notación vista después de la definición 2.2.4,

$$\theta_{Ae}(\psi\varphi) = (e)\psi\varphi = ((e)\psi)\varphi$$

Como $(e)\psi \in Ae$, entonces $(e)\psi = ae$ para algún $a \in A$, de forma que $((e)\psi)e = (ae)e = ae = (e)\psi$. Así, como φ es un endomorfismo de A–módulos y $(e)\psi \in Ae \subseteq A$,

$$((e)\psi)\varphi = (((e)\psi)e)\varphi = (e)\psi(e)\varphi = \theta_{Ae}(\psi)\theta_{Ae}(\varphi)$$

ii) Finalmente, nótese que

$$\theta_{Ae}(\operatorname{Id}_{Ae}) = (e)\operatorname{Id}_{Ae} = e = 1_{eAe}$$

De lo anterior, se concluye que θ_{Ae} es un isomorfismo de K–álgebras.

□

El primero de los corolarios del lema 4.1.14, que se presenta a continuación, muestra que el álgebra eAe será local siempre que el idempotente e sea primitivo. Este resultado guarda una profunda relación con el corolario 4.1.4 pues, al ser eAe isomorfa a $\mathrm{End}({}_AAe)$, se cumplirá que existe una correspondencia biunívoca entre los idempotentes de ambas álgebras. Así, si el idempotente $e \in A$ es primitivo, entonces ${}_AAe$ será inescindible de manera que a la luz de la proposición 4.1.3, $\mathrm{End}({}_AAe)$ no tendrá idempotentes distintos a los triviales y por lo tanto tampoco los tendrá eAe. Es decir, eAe será local.

4.1.16 Corolario.
Un idempotente $e \in A$ es primitivo si y sólo si el álgebra $eAe \cong \mathrm{End}(Ae)$ tiene como únicos idempotentes a 0 y e, es decir, eAe es un álgebra local.

□

Luego, como segundo corolario del lema 4.1.14, el siguiente resultado indica que siempre que el álgebra de endomorfismos de un A–módulo sea local, entonces el módulo en cuestión será inescindible. Sin embargo, el recíproco de este resultado será únicamente válido cuando el módulo que se considere sea también de dimensión finita. Así, en este corolario se encuentra la segunda de las restricciones que al principio se mencionaron para nuestros objetos. Más importante aún, éste será el último resultado antes de poder enunciar el Teorema de Descomposición Única.

4.1.17 Corolario.
Sea A una K–álgebra y M un A–módulo izquierdo.

a) Si el álgebra $\mathrm{End}({}_AM)$ es local, entonces M es inescindible.

b) Si M es de dimensión finita e inescindible, entonces el álgebra $\mathrm{End}({}_AM)$ es local y cualquier A-endomorfismo de M es nilpotente o un isomorfismo.

Demostración.

a) Supóngase que M se puede descomponer como suma directa de la forma $M = M_1 \oplus M_2$ con $M_1, M_2 \neq 0$. Así, es posible encontrar proyecciones

$$p_1 \colon M \to M_1$$
$$p_2 \colon M \to M_2$$

e inclusiones

$$i_1 \colon M_1 \to M$$
$$i_2 \colon M_2 \to M$$

tales que $p_2 i_2 + p_1 i_1 = \mathrm{Id}_M$.
Dado que $p_1 i_1$ y $p_2 i_2$ son idempotentes no cero en $\mathrm{End}({}_AM)$, se sigue que $\mathrm{End}({}_AM)$ no es local pues de otra forma Id_M sería elemento del único ideal maximal en $\mathrm{End}({}_AM)$.

b) Supóngase que M es un módulo inescindible de dimensión finita, pero que $\mathrm{End}({}_AM)$ no es local. Así, es posible encontrar idempotentes no triviales $e_1, e_2 \in \mathrm{End}({}_AM)$ tales que

$$M \cong \mathrm{Im}(e_1) \oplus \mathrm{Im}(e_2)$$

lo cual es una contradicción. Por lo tanto, se concluye que $\mathrm{End}({}_AM)$ debe ser local.

Finalmente, para $f \in \mathrm{End}({}_AM)$ no invertible, se sigue de lema 4.1.14 que $f \in \mathrm{rad}(\mathrm{End}({}_AM))$. Así, al ser $\mathrm{End}({}_AM)$ de dimensión finita, se concluye que f es nilpotente

□

En relación a la demostración del segundo inciso del corolario anterior se hace nuevamente la observación de que la hipótesis de que el módulo sea de dimensión finita es importante pues este resultado en general no se satisface para módulos inescindibles de dimensión infinita sobre álgebras de dimensión finita.

4.1.18 Ejemplos.

a) *Considérese el álgebra* $\mathbb{T}_3(K)$ *de las matrices triangulares inferiores de orden* 3 *con entradas en* K *y tómese* A *el subálgebra de* $\mathbb{T}_3(K)$ *cuyos elementos son matrices de la forma*

$$\begin{pmatrix} a & 0 & 0 \\ d & a & 0 \\ g & h & a \end{pmatrix}$$

Así, se tiene que A *es un álgebra local no conmutativa, además su radical consiste del conjunto de las matrices de la forma*

$$\begin{pmatrix} 0 & 0 & 0 \\ d & 0 & 0 \\ g & h & 0 \end{pmatrix}$$

de donde $A/\operatorname{rad}(A) \cong K$.

Una vez que se ha expuesto lo anterior, es posible enunciar el Teorema de Descomposición Única. Este teorema no solamente muestra que todo módulo finitamente generado sobre un álgebra de dimensión finita admite una descomposición inescindible en suma directa, sino que establece que la descomposición dada será única salvo isomorfismo.

4.1.19 Teorema.
Sea A *una* K*–álgebra de dimensión finita.*

a) *Cada módulo* M *en* A*–mod admite una descomposición*

$$M \cong M_1 \oplus \cdots \oplus M_n$$

donde M_i *es un módulo inescindible y* $\operatorname{End}({}_AM_i)$ *es local para* $i \in \{1, \ldots, n\}$.

b) *Si* $M \cong \bigoplus_{i=1}^{n} M_i \cong \bigoplus_{j=1}^{m} N_j$ *con* M_i *y* N_j *inescindibles para* $i \in \{1, \ldots, n\}$ *y* $j \in \{1, \ldots, m\}$. *Entonces,* $n = m$ *y existe una permutación* σ *de* $\{1, \ldots, n\}$ *tal que* $M_i \cong N_{\sigma(i)}$ *para todo* $i \in \{1, \ldots, n\}$.

Demostración. Ver [2, página 23]

□

Finalmente, se presenta un corolario del Teorema de Descomposición Única que exhibe el caso particular en el que el modulo finitamente generado es el módulo regular de un álgebra de dimensión finita.

4.1.20 Corolario.
Sea A *una* K*–álgebra de dimensión finita. Entonces existe una descomposición para el módulo regular*

$${}_AA = {}_AP_1 \oplus {}_AP_2 \oplus \cdots \oplus {}_AP_n$$

tal que ${}_AP_i$ *es inescindible para todo* $i \in \{1, \ldots, n\}$. *Más aún, si existe otra descomposición*

$${}_AA = {}_AQ_1 \oplus {}_AQ_2 \oplus \cdots \oplus {}_AQ_m$$

entonces $n = m$ *y existe una permutación* σ *de* $\{1, \ldots, n\}$ *tal que* $P_i \cong Q_{\sigma(i)}$ *para todo* $i \in \{1, \ldots, n\}$.

□

Adicionalmente, dado que se sabe que si ${}_AA$ admite una descomposición como suma directa

$${}_AA = {}_AP_1 \oplus {}_AP_2 \oplus \cdots \oplus {}_AP_n$$

entonces $P_i = Ae_i$ para todo $i \in \{1, \ldots, n\}$ donde $\{e_1, e_2, \ldots, e_n\}$ es un conjunto completo de idempotentes ortogonales y primitivos de A, en particular se concluye que cualquier conjunto completo de idempotentes ortogonales primitivos de A debe tener cardinalidad n.

4.2. Módulos proyectivos

En la sección anterior se vio el Teorema de Descomposición Única ofrece un resultado bastante robusto sobre la descomposición inescindible de módulos finitamente generados sobre álgebras de dimensión finita. Motivados por dicho resultado, en esta sección se irá más lejos y se estudiará a los módulos libres y a los módulos proyectivos. Posteriormente se probará que la clase de módulos libres se encuentra contenida en la de los módulos proyectivos. Finalmente, se verá que a pesar de que no todo módulo finitamente generado es proyectivo, sí se les podrá asociar una cubierta proyectiva y que además, el tope de la cubierta será isomorfo al tope del módulo original. Antes de comenzar con la definición de módulo libre se hace la nota de que todas las álgebras consideradas en esta sección serán de dimensión finita.

4.2.1 Definición.
Sea A una K–álgebra de dimensión finita.

a) Se dice que un A–módulo F es ***libre*** *si F es isomorfo a una suma directa de copias del módulo regular ${}_AA$.*

b) Se dice que un A–módulo F es ***libre finitamente generado*** *si F es isomorfo a una suma directa finita de copias del módulo regular ${}_AA$.*

Los siguiente resultados ofrecen una caracterización para módulos libres y libres finitamente generados, respectivamente, que a menudo resultan mucho más útiles en la práctica. Estas caracterizaciones indican que los módulos libres y libres finitamente generados son aquellos con un subconjunto generador y linealmente independiente, es decir, una base. Para los módulos libres finitamente generados se tendrá en particular que esta base es finita.

4.2.2 Proposición.
F es un A–módulo libre si y sólo si existe un subconjunto generador linealmente independiente de F.

Demostración. Supóngase primero que F es un A–módulo libre. Es decir, $F \cong \bigoplus_\Lambda {}_AA$, de donde existe un isomorfismo de A–módulos $f\colon \bigoplus_\Lambda {}_AA \to F$. Así, tómese $X = \{f(e_\lambda)\}_{\lambda\in\Lambda} \subseteq F$ donde $e_\lambda\colon \Lambda \to A$ está dado por

$$e_\lambda(\mu) = \begin{cases} 1_A & : \mu = \lambda \\ 0 & : \mu \neq \lambda \end{cases}$$

Se afirma entonces que X es un subconjunto generador linealmente independiente de F. En efecto, dado $\Lambda' \subseteq \Lambda$ finito se tiene que si $\sum_{\lambda\in\Lambda'} r_\lambda f(e_\lambda) = 0$, entonces

$$f^{-1}\left(\sum_{\lambda\in\Lambda'} r_\lambda f(e_\lambda)\right) = \sum_{\lambda\in\Lambda'} r_\lambda f^{-1}(f(e_\lambda)) = \sum_{\lambda\in\Lambda'} r_\lambda e_\lambda = 0$$

de donde se concluye que $r_\lambda = 0$ para todo $\lambda \in \Lambda'$. Más aún, dado $m \in F$, se tiene que existe $a \in \bigoplus_\Lambda {}_AA$ tal que $f(a) = m$. Luego, sea $\Lambda_a = \{\lambda \in \Lambda : a(\lambda) \neq 0\}$. Así, $a = \sum_{\lambda\in\Lambda_a} a(\lambda)e_\lambda$, de donde

$$m = f(a) = f\left(\sum_{\lambda\in\Lambda_a} a(\lambda)e_\lambda\right) = \sum_{\lambda\in\Lambda_a} a(\lambda)f(e_\lambda)$$

con lo que se concluye que X es un conjunto linealmente independiente que genera a F.

Por otro lado, supóngase que F es un A–módulo y que $X \subseteq F$ es un subconjunto generador linealmente independiente de F. Defínase para $x \in X$,

$$\begin{aligned} \rho_x\colon A &\to F \\ a &\mapsto ax \end{aligned}$$

Se afirma entonces que

$$\bigoplus_X \rho_x\colon \bigoplus_X {}_AA \to F$$

es un isomorfismo de A–módulos. Para ver esto, considérese el homomorfismo de módulos

$$\begin{aligned} f\colon F &\to \bigoplus_X {}_A A \\ m &\mapsto \sum_{x\in X} a_x e_x \end{aligned}$$

donde $m = \sum_{x\in X} a_x x$. Así, se cumple que para $a \in \bigoplus_X {}_A A$ y $m = \sum_{x\in X} a_x x \in F$, se tiene que

$$f\bigoplus_X \rho_x(a) = f\left(\bigoplus_X \rho_x(a)\right) = f\left(\sum_{x\in X} ax\right) = \sum_{x\in X} ae_x = a$$

$$\bigoplus_X \rho_x f(m) = \bigoplus_X \rho_x f\left(\sum_{x\in X} a_x x\right) = \bigoplus_X \rho_x\left(f\left(\sum_{x\in X} a_x x\right)\right) = \bigoplus_X \rho_x\left(\sum_{x\in X} a_x e_x\right) = \sum_{x\in X} a_x x = m$$

con lo que se concluye que $f = \left(\bigoplus_X \rho_x\right)^{-1}$ y por lo tanto $F \cong \bigoplus_X {}_A A$.

$\square$

4.2.3 Corolario. *F es un A–módulo libre finitamente generado si y sólo si existe un subconjunto finito generador linealmente independiente de F.*

$\square$

Los módulos proyectivos serán los principales actores de esta sección, por lo que a continuación se da su definición. Como observación adicional se menciona que se trabajará únicamente con módulos proyectivos finitamente generados. Con el resultado inmediato a esta definición se muestra que de hecho los módulos proyectivos son, de cierta forma, una generalización de los módulos libres. Por último, se da también la definición de módulos inyectivos la cual se obtiene por dualidad de la de módulos proyectivos.

4.2.4 Definición.

a) *Se dice que un A–módulo finitamente generado P es* **proyectivo** *si se cumple que para cualquier epimorfismo $h\colon N \to M$ la función inducida*

$$\begin{aligned} \operatorname{Hom}_A(h,P)\colon \operatorname{Hom}_A(P,N) &\to \operatorname{Hom}_A(P,M) \\ f &\mapsto hf \end{aligned}$$

es suprayectiva. Es decir, si para cualquier epimorfismo $h\colon N \to M$ y cada morfismo $g\colon P \to M$ existe un morfismo $g'\colon P \to N$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} & P \arrow[dl, dashed, "g'"'] \arrow[d, "g"] & \\ N \arrow[r, two heads, "h"] & M \arrow[r] & 0 \end{tikzcd}$$

b) *Dualmente, se dice que un A–módulo finitamente generado E es inyectivo si se cumple que para cualquier monomorfismo $u\colon M \to L$ la función inducida*

$$\begin{aligned} \operatorname{Hom}_A(E,u)\colon \operatorname{Hom}_A(L,E) &\to \operatorname{Hom}_A(M,E) \\ f &\mapsto fu \end{aligned}$$

es suprayectiva. Es decir, para cada monomorfismo $u\colon M \to L$ y cada morfismo $g\colon M \to E$ existe un morfismo $g'\colon L \to E$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, hook, "u"] \arrow[d, "g"'] & L \arrow[dl, dashed, "g'"] \\ & E & \end{tikzcd}$$

Es consecuencia directa de la definición anterior y del corolario 4.2.3 que todo módulo libre finitamente generado es también un módulo proyectivo. El recíproco, sin embargo, no se cumplirá necesariamente.

4.2.5 Proposición.
Sea F un A–módulo libre finitamente generado, entonces F es proyectivo.

Demostración. Sean F un A–módulo libre y M,N dos A–módulos junto con el homomorfismo $g\colon F \to M$ y el epimorfismo $h\colon N \to M$. Dado que F es libre, se tiene que existe un subconjunto generador y linealmente independiente X de F. Así, para cada $x \in X$ debe existir $m \in M$ tal que $g(x) = m$. Como además h es suprayectiva, existe $n_x \in N$ tal que $h(n_x) = g(x) = m$. Defínase entonces el homomorfismo $f\colon F \to N$ dado por $f(x) = n_x$. De esta forma, se cumple que para $y = \sum_{x\in X} a_x x \in F$ se tiene que

$$\begin{aligned} hf(y) = h(f(y)) = h\left(f\left(\sum_{x\in X} a_x x\right)\right) \\ = h\left(\sum_{x\in X} a_x f(x)\right) = h\left(\sum_{x\in X} a_x n_x\right) = \sum_{x\in X} a_x h(n_x) \\ = \sum_{x\in X} a_x g(x) = g\left(\sum_{x\in X} a_x x\right) = g(y) \end{aligned}$$

de manera que que $g = hf$, con lo que se concluye que F es proyectivo.

$\square$

El lema que se presenta a continuación será el que establezca que la descomposición en suma directa de un módulo proyectivo también se puede poner en relación de isomorfismo con una suma directa de submódulos inescindibles del módulo regular del álgebra. Para ver eso, el mismo lema dará antes una caracterización para módulos proyectivos en función de módulos libres.

4.2.6 Lema.
Sea A una K–álgebra de dimensión finita.

a) *Un A–módulo izquierdo finitamente generado P es proyectivo si y sólo si existe un A–módulo libre F y un A–módulo izquierdo P' tal que $P \oplus P' \cong F$.*

b) *Si se tiene una descomposición en suma directa de módulos inescindibles del módulo regular*

$${}_AA = Ae_1 \oplus Ae_2 \oplus \cdots \oplus Ae_n$$

y P es un A–módulo izquierdo finitamente generado proyectivo, entonces P admite una descomposición en suma directa

$$P = P_1 \oplus P_2 \oplus \cdots \oplus P_m$$

tal que cada sumando P_j es inescindible e isomorfo a algún Ae_i.

Demostración.

a) Supóngase primero que P es un A–módulo proyectivo finitamente generado. Sea $\{m_j\}_{j\in J}$ un conjunto generador de P. Así, considérese el módulo libre
$$F = \bigoplus_{j\in J} Ax_j$$
con $\{x_j\}_{j\in J} \subseteq A$ un conjunto de generadores libres. Luego, defínase el morfismo $f\colon F \to P$ tal que $f(x_j) = m_j$. Como claramente f es suprayectiva, se tiene que existe $g\colon P \to F$ tal que $fg = \mathrm{Id}_P$, de donde $F = \mathrm{Im}(g) \oplus \mathrm{Ker}(f) \cong P \oplus \mathrm{Ker}(f)$.

Por otro lado, nótese que si F es un módulo libre se sigue de la proposición 4.2.5 que F es proyectivo. Más aún, si P y P' son dos A–módulos izquierdos tales que $F \cong P \oplus P'$ con el isomorfismo $s\colon F \to P \oplus P'$, entonces se obtiene del siguiente diagrama conmutativo que P también es proyectivo

$$\begin{tikzcd}
& F \arrow[d, "\pi_P s"] \arrow[ddl, dashed, "g'"'] \\
& P \arrow[d, "g"] \arrow[dl, dashed, "g' i_P s^{-1}"] \\
N \arrow[r, two heads, "h"'] & M
\end{tikzcd}$$

donde $\pi_P\colon P \oplus P' \to P$ y $i_P\colon P \to P \oplus P'$ están dadas por $\pi_P(x) = p$ y $i_P(p) = p + 0$ dado $x = p + p' \in P \oplus P'$ con $p \in P$, $p' \in P'$.

b) Supóngase que P es un módulo proyectivo finitamente generado. Así, del inciso anterior se tiene que existen un A–módulo libre F y un A–módulo izquierdo P' tales que $F \cong P \oplus P'$. De esta forma, por la definición 4.2.1 se sigue que F es isomorfo a una suma directa finita del módulo regular ${}_AA$. Esto es,

$$F \cong \bigoplus_{j=1}^{m} {}_AA$$

Más aún, como por hipótesis se tiene que

$${}_AA \cong \bigoplus_{i=1}^{n} Ae_i$$

con Ae_i un módulo inescindible tal que $\operatorname{End}(Ae_i)$ es local para todo $i \in \{1, \dots, n\}$, se obtiene entonces que

$$F \cong \bigoplus_{j=1}^{m} \left(\bigoplus_{i=1}^{n} Ae_i \right) = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} Ae_i = \bigoplus_{i=1}^{n} (Ae_i)^m$$

Por otro lado, como F es libre finitamente generado, entonces se sigue que P' también lo es. Así, del primer inciso del Teorema de Descomposición Única 4.1.19 se sigue que $P \cong \bigoplus_{\alpha=1}^{l} P_\alpha$ y $P' \cong \bigoplus_{\beta=1}^{k} P'_\beta$ con P_α y P'_β módulos inescindibles para $\alpha \in \{1, \dots, l\}$ y $\beta \in \{1, \dots, k\}$. De lo anterior se obtiene entonces que

$$F \cong \bigoplus_{\alpha=1}^{l} P_\alpha \oplus \bigoplus_{\beta=1}^{k} P'_\beta \cong \bigoplus_{i=1}^{n} (Ae_i)^m$$

de manera que por el segundo inciso del Teorema de Descomposición Única 4.1.19 se tiene que $n = l + k$ y además cada P_α es isomorfo a un único $(Ae_i)^m$ con $i \in \{1, \dots, n\}$. Así si se toma a $J = \{i \in \{1, \dots, n\} : \exists \alpha \in \{1, \dots, l\} \, ((Ae_i)^m \cong P_\alpha)\} \subsetneq \{1, \dots, n\}$ se obtiene entonces que

$$P \cong \bigoplus_{s \in J} (Ae_s)^m$$

lo cual es lo que se quería demostrar.

$\square$

A pesar de que al tomar un módulo en A–mod éste no necesariamente es proyectivo, sí será posible asociarle un módulo proyectivo finitamente generado. Este módulo que se le asociará será lo que se conoce como una cubierta proyectiva. A continuación se da la definición de este concepto.

4.2.7 Definición.
Sea A una K–álgebra.

a) *Se dice que un submódulo L de un A–módulo M es* ***superfluo*** *si para cada submódulo X de M se cumple que si* $L + X = M$*, entonces* $X = M$.

b) *Sean M y N dos A–módulos finitamente generados. Se dice que un A–epimorfismo* $h\colon M \to N$ *es* ***minimal*** *si* $\mathrm{Ker}(h)$ *es superfluo en M.*

c) *Dados dos A–módulos P y M finitamente generados se dice que un A–epimorfismo* $p\colon P \to M$ *es una* ***cubierta proyectiva*** *de M si P es un módulo proyectivo y p es un epimorfismo minimal.*

El siguiente lema dará una caracterización para cubiertas proyectivas.

4.2.8 Lema.
Dada una K–álgebra A junto con dos A–módulos izquierdos finitamente generados P y M, se cumple que un epimorfismo $p\colon P \to M$ *es una cubierta proyectiva de M si y sólo si P es un módulo proyectivo y además para cada homomorfismo de A–módulos* $g\colon N \to P$ *se cumple que si pg es suprayectiva, entonces g es suprayectiva.*

Demostración. Supóngase primero que $p\colon P \to M$ es una cubierta proyectiva y sea $g\colon N \to P$ un homomorfismo tal que pg es suprayectiva. Así, se sigue que para $x \in P$, como $p(x) \in M$, debe existir $n \in N$ tal que $pg(n) = p(g(n)) = p(x)$. De esta manera se tiene que $g(n) - x \in \mathrm{Ker}(p)$ y dado que $-g(n) \in \mathrm{Im}(g)$, es claro que $x = -g(n) + (g(n) + x) \in \mathrm{Im}(g) + \mathrm{Ker}(p)$, con lo que se prueba que $\mathrm{Im}(g) + \mathrm{Ker}(p) = P$. Más aún, como por hipótesis $\mathrm{Ker}(p)$ es superfluo en P, se concluye que $\mathrm{Im}(g) = P$, de donde g es suprayectiva. El hecho de que P sea un módulo proyectivo, se sigue inmediatamente de la definición de cubierta proyectiva.

Por otro lado, supóngase que P es un módulo finitamente generado proyectivo y $p\colon P \to M$ es tal que para cada morfismo $g\colon N \to P$ se cumple que la suprayectividad de pg implica la suprayectividad de g. Así, tómese N un submódulo de P tal que $N + \mathrm{Ker}(p) = P$ y $g\colon N \hookrightarrow P$ la inclusión natural. De esta forma se tiene que $pg\colon N \to P$ es suprayectiva de donde g es suprayectiva, probando así que entonces $\mathrm{Ker}(p)$ es un submódulo superfluo en P, con lo que se concluye que p es una cubierta proyectiva.

□

Finalmente, el siguiente teorema mostrará el resultado que se mencionó al principio de la sección con el cual se indica que a todo módulo finitamente generado sobre un álgebra de dimensión finita se le puede asociar una cubierta proyectiva y, más importante aún, dicha cubierta proyectiva es única salvo isomorfismo. Asimismo, se prueba con este resultado que el tope del módulo finitamente generado será isomorfo al tope de su cubierta proyectiva. Es importante observar que la demostración de este teorema es constructiva, de forma que de hecho otorga implícitamente un algoritmo para obtener la cubierta proyectiva de un módulo finitamente generado.

4.2.9 Teorema.
Sea A una K–álgebra de dimensión finita y considérese una descomposición del módulo regular

$$_AA = Ae_1 \oplus Ae_2 \oplus \cdots \oplus Ae_n$$

con $\{e_1, e_2, \ldots, e_n\}$ *un conjunto completo de idempotentes ortogonales de A.*

a) *Para cada A–módulo izquierdo M finitamente generado existe una cubierta proyectiva*

$$P(M) \xrightarrow{p} M \to 0$$

donde $P(M) \cong (Ae_1)^{s_1} \oplus (Ae_2)^{s_2} \oplus \cdots \oplus (Ae_n)^{s_n}$ *con* $s_i \geq 0$ *para toda* $i \in \{1, \ldots, n\}$*. Más aún, el homomorfismo p induce un isomorfismo* $P(M)/\mathrm{rad}(P(M)) \cong M/\mathrm{rad}(M)$.

b) *La cubierta proyectiva $P(M)$ de un módulo M en A–mod es única en el sentido de que si $p'\colon P' \to M$ es otra cubierta proyectiva de M, entonces se obtiene un diagrama conmutativo:*

$$\begin{tikzcd}
& 0 & \\
P(M) \arrow[r, "p"] & M \arrow[u] \arrow[r] & 0 \\
& P' \arrow[u, "p'"'] \arrow[ul, "g"] &
\end{tikzcd}$$

donde g es un isomorfismo.

Demostración.

a) Sean $B = A/\operatorname{rad}(A)$ y $\overline{e}_j = e_j + \operatorname{rad}(A) \in B$ para cada $j \in \{1,\dots,n\}$. Considérese además, $\pi\colon A \to B$ el epimorfismo dado por $\pi(a) = a + \operatorname{rad}(A)$. Como $\{e_1, e_2, \dots, e_n\}$ es un conjunto completo de idempotente primitivos ortogonales de A, entonces $\{\overline{e}_1, \overline{e}_2, \dots, \overline{e}_n\}$ también lo será de B. Así,

$${}_BB = B\overline{e}_1 \oplus B\overline{e}_2 \oplus \cdots \oplus B\overline{e}_n$$

es una descomposición inescindible del módulo regular ${}_BB$. Más aún, como de la proposición 4.1.11 se sigue que $\operatorname{rad}(Ae_j) \subseteq Ae_j$ es el único submódulo maximal de Ae_j, entonces $\operatorname{top}(Ae_j) \cong B\overline{e}_j$ es un B–módulo simple y además el epimorfismo

$$\begin{aligned}
\pi_j\colon Ae_j &\to \operatorname{top}(Ae_j)\\
ae_j &\mapsto ae_j + \operatorname{rad}(Ae_j)
\end{aligned}$$

es una cubierta proyectiva de $\operatorname{top}(Ae_j)$.

Así, dado M en A–mod, se tiene que $\operatorname{top}(M)$ es un módulo en B–mod de manera que por el corolario 3.2.9 y por la proposición 4.1.11 se sigue que

$$\operatorname{top}(M) \cong \bigoplus_{i=1}^{n} (B\overline{e}_i)^{s_i} \cong \bigoplus_{i=1}^{n} (\operatorname{top}(Ae_i))^{s_i}$$

con $s_i \geq 0$ para todo $i \in \{1,\dots,n\}$. Se define entonces

$$P(M) := \bigoplus_{i=1}^{n} (Ae_i)^{s_i}$$

De esta manera, por la proyectividad de $P(M)$ se tiene la existencia de un homomorfismo $p\colon P(M) \to M$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd}
P(M) \arrow[r, "p"] \arrow[d, "\pi_{\operatorname{top}(\operatorname{rad}(M))}"'] & M \arrow[d, "\pi_{\operatorname{rad}(M)}"] \\
\operatorname{top}(P(M)) \arrow[r, "\operatorname{top}(p)"'] & \operatorname{top}(M)
\end{tikzcd}$$

Dado que $\operatorname{top}(p)$ es isomorfismo se sigue del corolario 3.2.11(a) que p es suprayectiva. Más aún, como del diagrama se obtiene que

$$\operatorname{Ker}(p) \subseteq \operatorname{Ker}(\pi_{\operatorname{rad}(P(M))}) = \bigoplus_{i=1}^{n} \operatorname{rad}(Ae_i)^{s_i} = \operatorname{rad}(P(M))$$

entonces de la proposición 3.2.8 se obtiene que al ser $\mathrm{rad}(P(M))$ superfluo en $P(M)$, también lo es $\mathrm{Ker}(p)$, con lo cual se concluye que p es una cubierta proyectiva de M.

b) Sea $p' \colon P' \to M$ una cubierta proyectiva de M. Dado que $p \colon P(M) \to M$ es suprayectiva, se sigue de la proyectividad de P' que existe $g \colon P' \to P(M)$ tal que $pg = p'$. Así, como p' es suprayectiva se tiene que para $x \in P(M)$, existe $y \in P'$ tal que $p'(y) = p(x)$ de manera que como $g(y) - x \in \mathrm{Ker}(p)$ y $-g(y) \in \mathrm{Im}(g)$, se llega a que $P(M) = \mathrm{Im}(g) + \mathrm{Ker}(p)$. De lo anterior se obtiene que, como $\mathrm{Ker}(p)$ es superfluo en $P(M)$, entonces g es suprayectiva. Más aún, se tiene que $l(P') \geq l(P(M))$. Así, si se repite el argumento invirtiendo los papeles de $P(M)$ y P' se llega también a que $l(P(M)) \geq l(P')$, con lo que se concluye que g es un isomorfismo.

□

Para concluir esta sección, el siguiente corolario del teorema anterior considera el caso particular en el que el módulo finitamente generado en cuestión es proyectivo.

4.2.10 Corolario.
Si P es un módulo proyectivo en A–mod. Entonces, el epimorfismo canónico

$$t \colon P \to \mathrm{top}(P)$$

es una cubierta proyectiva de $\mathrm{top}(P)$ *y además existe un A–isomorfismo $P \cong (Ae_1)^{s_1} \oplus (Ae_2)^{s_2} \oplus \cdots \oplus (Ae_n)^{s_n}$ con $s_i \geq 0$ para toda $i \in \{1, \ldots, n\}$.*

Demostración. Ver [2, página 30]

□

4.3. Álgebras básicas

Para concluir este capítulo se expondrá de forma breve una clase de álgebras conocidas como álgebras básicas. Éstas cumplirán la propiedad de que para todo conjunto completo de idempotentes ortogonales primitivos, los submódulos inescindibles que estos idempotentes inducen no serán isomorfos entre sí. Como primer resultado de la sección se enunciará una proposición que aporta una equivalencia a la noción de álgebra básica en términos de su álgebra cociente, además de dar un resultado sobre sus módulos simples. Luego, de forma similar a como ocurría con los módulos proyectivos, se tendrá que a pesar de tener un álgebra no básica, siempre es posible asociarle una a través un subconjunto de idempotentes. Finalmente, se probará que el álgebra básica asociada a un álgebra es única salvo isomorfismo.

4.3.1 Definición.
*Sea A una K–álgebra con un conjunto completo de idempotentes primitivos $\{e_1, e_2, \ldots, e_n\}$. Se dice que el álgebra es **básica** si $Ae_i \ncong Ae_j$ para toda $i \neq j$.*

Así, se obtiene inmediatamente de la definición anterior que toda álgebra local de dimensión finita es un álgebra básica.

Con la siguiente proposición se obtiene una caracterización para álgebras básicas de dimensión finita así como un resultado sobre sus módulos simples.

4.3.2 Proposición.

a) Una K–álgebra de dimensión finita A es básica si y sólo si el álgebra $A/$ $\mathrm{rad}(A)$ *es isomorfa a un producto finito de copias de K.*

b) Todo módulo simple sobre un álgebra básica es 1*–dimensional.*

Demostración.

a) Sean $B = A/\operatorname{rad}(A)$ y $\overline{e}_j = e_j + \operatorname{rad}(A) \in B$. Supóngase primero que A es un álgebra básica y sea ${}_AA = Ae_1 \oplus \cdots \oplus Ae_n$ una descomposición inescindible del módulo regular de modo que $\{e_1, e_2, \ldots, e_n\}$ es un conjunto completo de idempotentes ortogonales de A. Así, se sigue del lema 4.1.10 y del inciso (c) de la proposición 4.1.11, que $B\overline{e}_j = \operatorname{top}(Ae_j)$ es un B–módulo simple. De donde, ${}_BB = \bigoplus_{j=1}^{n} B\overline{e}_j$ es una descomposición inescindible del módulo ${}_BB$. De esta forma se tiene, por el corolario 4.2.10 que $Ae_j \cong P(B\overline{e}_j)$ y por lo tanto $Ae_j \cong Ae_i$ si y sólo si $B\overline{e}_j \cong B\overline{e}_i$

Dado que A es un álgebra básica, se sigue que B es también un álgebra básica. Más aún, del Lema de Schur (3.1.4) se obtiene que $\operatorname{Hom}_B(B\overline{e}_j, B\overline{e}_i) = 0$ cuando $j \neq i$ de forma que por el corolario 3.1.5 $\operatorname{End}(B\overline{e}_j) \cong K$ para todo $j \in \{1, \ldots, n\}$. Luego, dado un elemento $b \in B$ y $j \leq n$ la función $b_j \colon B\overline{e}_j \to {}_BB$ dada por $b_j(y) = yb\overline{e}_j$ para toda $y \in B$ induce el endomorfismo de B–módulos $b'_j \colon B\overline{e}_j \to B\overline{e}_j$ y el homomorfismo de K–álgebras $\sigma_j \colon B \to \operatorname{End}(B\overline{e}_j) \cong K$ dado por $\sigma_j(b) = b'_j$. De esta forma se obtiene el homomorfismo de K–álgebras

$$\begin{aligned} \sigma \colon B &\to \operatorname{End}(B\overline{e}_1) \times \cdots \times \operatorname{End}(B\overline{e}_n) \cong K \times \cdots \times K \\ b &\mapsto (\sigma_1(b), \ldots, \sigma_n(b)) \end{aligned}$$

Dado que claramente σ es inyectiva, se sigue de comparar las dimensiones de las álgebras que σ también es biyectiva, con lo que se concluye la primera implicación.

Por otro lado, si se tiene que $B \cong K \times \cdots \times K$, entonces B es conmutativa y además $\overline{e}_1, \ldots, \overline{e}_n$ son idempotentes ortogonales centrales primitivos dos a dos de B. Se sigue entonces que $B\overline{e}_i \ncong B\overline{e}_j$ para $i \neq j$, de donde por el teorema 4.2.9, $Ae_i \cong P(B\overline{e}_i) \ncong P(B\overline{e}_j) \cong Ae_j$, con lo que se concluye que A es un álgebra básica.

b) Dado que por el inciso (b) del corolario 3.2.11 todo A–módulo simple es un módulo sobre el álgebra cociente $A/\operatorname{rad}(A)$, se obtiene del inciso anterior que si A es básica, entonces $A/\operatorname{rad}(A)$ es isomorfa a un producto $K \times K \times \cdots \times K$, de donde $\dim_K(S) = 1$

□

Nótese que dada una K–álgebra A con un conjunto completo de idempotentes ortogonales $\{e_1, e_2, \ldots, e_n\}$ ésta no necesariamente cumplirá ser un álgebra básica. Sin embargo, es posible obtener un álgebra básica a partir de A de la siguiente forma. Tómese

$$A^b = e_A A e_A$$

donde $e_A = e_{j_1} + \cdots + e_{j_a}$ con $e_{j_1}, \ldots, e_{j_a}$ escogidos de forma tal que $Ae_{j_i} \ncong Ae_{j_t}$ para todo $i \neq j$ y además cada módulo Ae_s con $s \in \{1, \ldots, n\}$ es isomorfo a alguno de los módulos Ae_{j_i} con $i \in \{1, \ldots, a\}$. Así claramente el álgebra A^b es un álgebra básica y se le llama el **álgebra básica asociada** a A.

El siguiente ejemplo muestra que la $\mathbb{C}$–álgebra $M_2(\mathbb{C})$ no es básica y además exhibe a dos álgebras básicas asociadas a ella.

4.3.3 Ejemplos.

a) *Considérese la $\mathbb{C}$–álgebra $M_2(\mathbb{C})$. Así, se sigue que al considerar los idempotentes canónicos*

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

se tiene que

$$M_2(\mathbb{C})e_1 = \begin{pmatrix} \mathbb{C} & 0 \\ \mathbb{C} & 0 \end{pmatrix} \cong \begin{pmatrix} 0 & \mathbb{C} \\ 0 & \mathbb{C} \end{pmatrix} = M_2(\mathbb{C})e_2$$

a través del isomorfismo

$$\begin{aligned} f \colon M_2(\mathbb{C})e_1 &\to M_2(\mathbb{C})e_2 \\ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} &\mapsto \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \end{aligned}$$

De donde se tiene que $M_2(\mathbb{C})$ no es un álgebra básica.

Por otro lado, nótese que tanto el álgebra

$$M_2(\mathbb{C})^b = e_1 M_2(\mathbb{C}) e_1 = \begin{pmatrix} \mathbb{C} & 0 \\ 0 & 0 \end{pmatrix}$$

como el álgebra

$$e_2 M_2(\mathbb{C}) e_2 = \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{C} \end{pmatrix}$$

son álgebras básicas asociadas a $M_2(\mathbb{C})$*. Más aún, es posible verificar que* $e_1 M_2(\mathbb{C}) e_1 \cong e_2 M_2(\mathbb{C}) e_2$ *a través del isomorfismo*

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \overset{\phi}{\mapsto} \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$$

de donde se concluye que la $\mathbb{C}$*–álgebra básica asociada a* $M_{2\times 2}(\mathbb{C})$ *es única salvo isomorfismo.*

El siguiente lema mostrará que el isomorfismo entre álgebras básicas asociadas a un álgebra, como el que aparece en el ejemplo anterior, existirá en general para cualquier álgebra de dimensión finita. Es decir, el álgebra asociada no depende de la elección de idempotentes.

4.3.4 Lema.
Sea A *una* K*–álgebra de dimensión finita y considérese* A^b *el álgebra básica asociada a* A*.*

a) El idempotente $e_A \in A^b$ *es el elemento identidad de* A^b *y además existe un isomorfismo de* K*–álgebras* $A^b \cong \mathrm{End}(Ae_{j_1} \oplus \cdots \oplus Ae_{j_a})$.

b) El álgebra A^b *no depende de la elección de los conjuntos* $\{e_1, e_2, \ldots, e_n\}$, $\{e_{j_1}, e_{j_2}, \ldots, e_{j_a}\}$ *salvo isomorfismo.*

Demostración.

a) Es consecuencia del lema 4.1.15 que $\mathrm{End}({}_A Ae_A) \cong e_A A e_A$. Como además $Ae_A \cong \bigoplus_{k=1}^{\alpha} Ae_{j_k}$, se tiene entonces que

$$A^b = e_A A e_A \cong \mathrm{End}({}_A Ae_A) \cong \mathrm{End}\left(\bigoplus_{k=1}^{\alpha} {}_A Ae_{j_k}\right)$$

b) Si $\{f_1, \ldots, f_n\}$ es otro conjunto completo de idempotentes ortogonales primitivos, entonces del Teorema de Descomposición Única 4.1.19, existe una permutación σ de $\{1, \ldots, n\}$, tal que $Ae_j \cong Af_{\sigma(j)}$. Así, se tiene que $Ae_j \ncong Ae_i$ si sólo si $Af_{\sigma(j)} \ncong Af_{\sigma(i)}$. De lo anterior se cumple también que la restricción $\sigma' = \sigma\restriction_{\{j_1, \ldots, j_\alpha\}}$ es tal que $Ae_{j_k} \cong Af_{\sigma'(j_k)}$, de forma que por el inciso (a)

$$A^b \cong \mathrm{End}\left(\bigoplus_{k=1}^{\alpha} {}_A Ae_{j_k}\right) \cong \mathrm{End}\left(\bigoplus_{k=1}^{\alpha} {}_A Af_{\sigma'(j_k)}\right) \cong A^{b'} = e_{A'} A e_{A'}$$

donde $e_{A'} = \sum_{k=1}^{\alpha} f_{j_k}$.

□

Bibliografía

[1] Frank W. Anderson and Kent R. Fuller, *Rings and categories of modules*, 2 ed., Graduate Texts in Mathematics, vol. 13, Springer-Verlag New York, 1992.

[2] Ibrahim Assem, Andrzej Skowronski, and Daniel Simson, *Elements of the representation theory of associative algebras: Techniques of representation theory*, London Mathematical Society Student Texts, vol. 1, Cambridge University Press, 2006.

[3] Maurice Auslander and Emilio Lluis, *Representations of algebras: Workshop notes of the third international conference on representations of algebras, held in puebla, mexico, august 4-8, 1980*, Lecture Notes in Mathematics, Springer Berlin Heidelberg, 2006.

[4] Paul E. Bland, *Rings and their modules*, De Gruyter Textbook, De Gruyter, 2011.

[5] C. Cibilis, F. Larrión, and Salmerón L., *Métodos diagramáticos en teoría de representaciones*, Monografías del Instituto de Matemáticas 11, 1982.

[6] Paul M. Cohn, *Algebra*, vol. Vols 1, 2 and 3, Wiley, 1990.

[7] Yurj A. Drozd and Vladimir V. Kirichenko, *Finite dimensional algebras*, Springer-Verlag Berlin Heidelberg, 1994.

[8] David S. Dummit and Richard M. Foote, *Abstract algebra*, Joohn Wiley & Sons, Inc., 2004.

[9] Stephen H. Friedberg, Arnold J. Insel, and Lawrence E. Spence, *Linear algebra*, Pearson, 2003.

[10] Hernán Giraldo, *Una introducción a la teoría de representaciones de Álgebras*, Lecturas Matemáticas **36** (2015), no. 1, 33–67.

[11] W. Keith Nicholson, *Lifting idempotents and exchange rings*, Trans. Amer. Math. Soc. (1977), no. 229, 269–278.

[12] Richard S. Pierce, *Associative algebras*, Springer-Verlag New York, 1982.

[13] Joseph J. Rotman, *An introduction to homological algebra*, Universitext, Springer New York, 2008.

[14] ______, *Advanced modern algebra*, Graduate Studies in Mathematics: volume 165, 180, American Mathematical Society, 2015.

[15] Bo Stenström, *Rings of quotients*, Springer-Verlag Berlin Heidelberg, 1975.