

GRADUACIONES DE GRUPOS ABELIANOS SOBRE EL ANILLO DE MATRICES

ELIECER FERNANDO RAMÍREZ ESCOBAR

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2025

GRADUACIONES DE GRUPOS ABELIANOS SOBRE EL ANILLO DE MATRICES

ELIECER FERNANDO RAMÍREZ ESCOBAR

Trabajo de grado para optar al título de
Licenciado en Matemáticas

Director
Héctor Edonis Pinedo Tapia
Doctor en Ciencias

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2025

DEDICATORIA

Dedico este trabajo a mis padres y a mi hermana,
que con su apoyo incondicional fueron mi fuente de inspiración y motivación para el
desarrollo de este trabajo y, en general, de toda la carrera.

AGRADECIMIENTOS

A Dios Padre Todopoderoso, por darme la sabiduría, el entendimiento y la fuerza de voluntad que me permitieron no rendirme en los momentos de adversidad.

A mis padres, quienes constantemente con su apoyo fueron mi gran fuente de inspiración y fortaleza en todo el transcurso de la carrera.

A mi hermana, que siempre estuvo apoyándome y brindándome el acompañamiento necesario.

Al profesor Héctor Pinedo, director de esta tesis, por brindarme la guía y el acompañamiento necesario. Así mismo, por sus observaciones y orientaciones constructivas para el desarrollo del trabajo.

A mis evaluadores, los profesores Arnoldo Teherán y Wilson Olaya; por los comentarios, observaciones y sugerencias que fueron fundamentales para lograr el mejor camino en el desarrollo de este trabajo.

A la profesora Sandra Evely Parada, que en algún momento de dificultad, sus palabras de aliento y motivación fueron de suma importancia para reconfortarme y continuar en este largo camino.

A mis compañeros y amigos, en especial, a mis amigos Kevin Martínez, Carlos Julio Ortiz y Néstor Ramírez, que siempre estuvieron ahí para apoyarme y aconsejarme.

A toda mi familia en general, que siempre estuvieron pendientes y que por medio de sus oraciones, siempre me desaron tener éxito en la carrera.

A la Universidad Industrial de Santander, en especial, a la Escuela de Matemáticas, por todos los conocimientos brindados que me permitieron obtener un verdadero aprendizaje significativo. Así mismo, por ayudarme en mi formación profesional.

CONTENIDO

	pág.
Introducción	8
1. Preliminares	9
1.1. Grupos	9
1.2. Anillos	10
1.3. Módulos	15
2. El Teorema de Skolem-Noether	24
2.1. Anillos semisimples	24
2.2. Producto Tensorial	32
3. Anillos Graduados y Buenas graduaciones	44
3.1. Anillos Graduados	44
3.2. Graduaciones por grupos cíclicos	46
3.3. Graduaciones por grupos abelianos finitos	54
Bibliografía	59

RESUMEN

TÍTULO: GRADUACIONES DE GRUPOS ABELIANOS SOBRE EL ANILLO DE MATRICES *

AUTOR: ELIECER FERNANDO RAMIREZ ESCOBAR **

PALABRAS CLAVE: GRUPOS ABELIANOS, ANILLOS GRADUADOS, BUENAS GRADUACIONES, COMPATIBILIDAD, RAÍCES PRIMITIVAS DE UNIDAD.

DESCRIPCIÓN:

Este trabajo consiste en estudiar las graduaciones del anillo de matrices, en particular, graduaciones para grupos cíclicos y grupos abelianos finitos sobre el anillo de matrices cuadradas, considerando el producto finito de dos grupos $(G \times H)$ para encontrar $(G \times H)$ -graduaciones y a través de la compatibilidad de dos graduaciones asociadas a $M_n(k)$. Así mismo, se muestran algunos resultados referentes a buenas graduaciones sobre $M_n(k)$, en el estudio de encontrar \mathbb{Z}_n -graduaciones, donde $n \in \mathbb{Z}^+$, y en la caracterización de $(G \times H)$ -graduaciones que son isomorfas a una buena graduación.

En el primer capítulo se abordan algunas definiciones preliminares correspondientes a grupos, anillos y módulos. En el capítulo siguiente, se presentan algunos conceptos y resultados importantes relacionados con anillos simples y producto tensorial que, de una u otra manera, son imprescindibles para el resultado de un teorema fundamental, El Teorema de Skolem-Noether, esencial en el estudio de las graduaciones. En el último capítulo, se abordan las definiciones de raíces m -ésimas de unidad, raíces primitivas m -ésimas de unidad y compatibilidad entre graduaciones en el estudio de las graduaciones del producto finito entre dos grupos.

* Trabajo de grado

** Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Ciencias.

ABSTRACT

TITLE: ABELIAN GROUP GRADINGS ON MATRIX RINGS *

AUTHOR: ELIECER FERNANDO RAMIREZ ESCOBAR **

KEYWORDS: ABELIAN GROUPS, GRADED RINGS, GOOD GRADINGS, COMPATIBILITY, PRIMITIVE ROOTS OF UNITY.

DESCRIPTION:

This work consists of studying the gradings on the matrix ring, in particular, gradings for cyclic groups and finite abelian groups on the ring of square matrices, considering the finite product of two groups $(G \times H)$ to find $(G \times H)$ -gradings and through compatibility of two gradings associated with $M_n(k)$. Likewise, some results are shown regarding good gradings on $M_n(k)$, in the study of finding \mathbb{Z}_n -gradations, where $n \in \mathbb{Z}^+$, and in the characterization of $(G \times H)$ -gradings that are isomorphic to a good gradings.

The first chapter addresses some preliminary definitions corresponding to groups, rings and modules. In the next chapter, some important concepts and results related to with simple rings and tensor product that, in one way or another, are essential for the result of a fundamental theorem, The Skolem-Noether Theorem, essential in the study of gradings. In the last chapter, the definitions of m th roots of unity, m th primitive roots of unity and compatibility between gradings in the study of the gradings of the finite product between two groups.

* Bachelor Thesis

** Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Matemáticas.

Introducción

El estudio de las buenas graduaciones sobre anillos de matrices es un tema de gran interés, de este modo, surge uno que otro problema que han hecho de este un trabajo exhaustivo. Uno de estos problemas consiste en determinar las G -graduaciones sobre el anillo de matrices sobre un cuerpo k , donde G es un grupo. En 1999, Dăscălescu resolvió este problema para los casos particulares cuando G es un grupo cíclico, luego, considerando \mathbb{Z}_n -graduaciones, estudió el caso particular cuando $n = 2$ y k es algebraicamente cerrado (ver ¹). Por otro lado, en un trabajo conjunto en 2001, Boboc y Dăscălescu se encargaron de estudiar las G -graduaciones de $M_n(k)$ cuando G es un producto finito de grupos cíclicos finitos (ver ²) y, siguiendo el trabajo anterior, Boboc estudió las $(\mathbb{Z}_2 \times \mathbb{Z}_2)$ -graduaciones de $M_2(k)$. Así, de manera más general, en el trabajo de Chung y Lee en 2007, se encargaron de estudiar las $(\mathbb{Z}_l \times \mathbb{Z}_m)$ -graduaciones sobre el anillo $M_n(k)$ considerando raíces primitivas m -ésimas y l -ésimas de unidad, a través de la compatibilidad entre dos graduaciones asociadas a $M_n(k)$ (ver ³). De este modo y teniendo en cuenta lo anterior, este trabajo tiene como finalidad entender el estudio de las graduaciones para grupos abelianos y grupos finitos sobre el anillo $M_n(k)$.

En primera instancia, se abordan los conceptos preliminares asociados con estructuras algebraicas, tales como grupos, anillos, módulos y a partir de estas definiciones introducir el Teorema de Skolem-Noether, resultado fundamental para el estudio de las \mathbb{Z}_m -graduaciones en el anillo de matrices $M_n(k)$, luego, se definen los anillos graduados que son esenciales a la hora de definir las buenas graduaciones. Para esto, se sigue con algunas proposiciones sobre el grupo multiplicativo de elementos invertibles que permiten determinar cuando un anillo es fuertemente graduado. Finalmente, se definirá el concepto de buena graduación y se estudiarán algunos resultados y teoremas para las \mathbb{Z}_m -graduaciones de $M_n(k)$ y $(\mathbb{Z}_l \times \mathbb{Z}_m)$ -graduaciones sobre el anillo de matrices.

¹ Dăscălescu, S., Ion, B., Năstăcescu, C., Rios Montes, J. (1999). Group gradings on full matrix rings. *J. Algebra* 220(2):709-728.

² Boboc, C., Dăscălescu, S. (2001). Gradings of matrix algebras by cyclic groups. *Comm Algebra* 29(11):5013-5021.

³ Chun, J., Lee, J. (2007). Abelian Group Gradings on Full Matrix Rings. *Comm Algebra* 35(10):3095-3102.

1. Preliminares

En este capítulo se introducirá de manera breve los conceptos de grupos, anillos y módulos, para que posteriormente se de paso a un resultado importante, a saber, en el análisis de encontrar graduaciones y buenas graduaciones para el anillo de matrices, el Teorema de Skolem-Noether (véase 2.2.8).

1.1. Grupos

Para esta sección se introducirá la definición de grupo con algunos ejemplos y resultados.

Definición 1.1.1. Un **grupo** $\langle G, * \rangle$ es un conjunto G , con una operación binaria $*$, que se denota $a * b = ab$, tal que los siguientes axiomas se cumplen,

- Para todo $a, b, c \in G$, se tiene que,

$$(a * b) * c = a * (b * c) \text{ (propiedad asociativa para *)}.$$

- Existe un elemento $e \in G$ tal que para todo $x \in G$,

$$e * x = x * e = x \text{ (elemento identidad } e \text{ para *)}.$$

- Para cada $a \in G$ existe un elemento $a' \in G$ tal que

$$a * a' = a' * a = e \text{ (inverso } a' \text{ de } a).$$

Ejemplo 1.1.2. El conjunto $M_{m \times n}(\mathbb{R})$ de todas las matrices $m \times n$ bajo la suma de matrices es un grupo, la matriz $m \times n$ con todas las entradas 0 es la matriz identidad.

Definición 1.1.3. Un *grupo* G es abeliano si su operación binaria es conmutativa. Es decir,

$$ab = ba$$

Para cada $a, b \in G$.

Definición 1.1.4. Sea G un grupo y $S \neq \emptyset$ un subconjunto de G . Se dice que S es un **subgrupo** de G si S bajo la operación $*$ tiene estructura de grupo. En tal caso se escribe $S \leq G$.

Observación 1.1.5. Sea G un grupo y $a \in G$ el conjunto de todas las potencias de a en G , definida de la siguiente manera

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\},$$

entonces $\langle a \rangle \leq G$.

Si $\langle a \rangle = G$ para algún $a \in G$, se dice que G es **cíclico**.

Observación 1.1.6. Todo grupo cíclico es abeliano.

Definición 1.1.7. Sea $\langle G, * \rangle$ un grupo. El centro de G es el conjunto

$$Z(G) = \{x \in G \mid \forall y \in G \ x * y = y * x\}.$$

Note que $Z(G)$ es un subgrupo abeliano de G .

Definición 1.1.8. Sean G y H grupos. Entonces un **homomorfismo de grupos** de G en H es una función $\varphi : G \rightarrow H$, tal que

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$$

para cada $g_1, g_2 \in G$.

Ejemplo 1.1.9. Sea $GL(n, \mathbb{R})$ el grupo multiplicativo de todas las matrices invertibles $n \times n$, entonces para las matrices $A, B \in GL(n, \mathbb{R})$ se tiene

$$\det(AB) = \det(A)\det(B).$$

donde $\det(A)$ denota el determinante de la matriz cuadrada A de orden n . Es decir, \det es un homomorfismo en el grupo multiplicativo \mathbb{R}^* de números reales distintos de cero.

1.2. Anillos

En esta sección, se abordarán los conceptos de anillo e ideal. Así mismo, se mostrarán algunos resultados importantes y se enunciarán los tres teoremas de isomorfismo.

Definición 1.2.1. Un **anillo** R es un conjunto R con dos operaciones binarias $+$ y \cdot , el cual se conoce como suma y producto, tales que:

- R es un grupo abeliano.
- El producto es asociativo.

- Para todos $a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Ejemplo 1.2.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y \mathbb{C} son anillos con las operaciones usuales de suma y producto.

Definición 1.2.3. Un anillo R se dice que es un **anillo con identidad** si R tiene un elemento, denotado por 1_R , tal que $1_R a = a 1_R = a$ para todo $a \in R$. En este caso, 1_R es llamado la **identidad** de R .

Ejemplo 1.2.4. Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y \mathbb{C} son anillos con identidad.

Definición 1.2.5. Sea R un anillo y u un elemento de R , se dice que u es una **unidad** si existe un elemento v en R tal que $uv = vu = 1_R$.

Definición 1.2.6. Sea R un anillo. Un subanillo I de R se dice que es un **ideal** si $ir, ri \in I$ para todo $i \in I$ y $r \in R$.

Definición 1.2.7. Un **ideal a la izquierda** I de un anillo R es un subconjunto de R que cumple las siguientes condiciones.

- Si $a, b \in I$, entonces $a + b \in I$
- Para todo $r \in R$ e $i \in I$, entonces $ri \in I$.

Definición 1.2.8. Un **ideal a la derecha** I de un anillo R es un subconjunto R que satisfacen las siguientes condiciones

- Si $a, b \in I$, entonces $a + b \in I$.
- Para todo $r \in R$ e $i \in I$, entonces $ir \in I$.

Proposición 1.2.9. Sea R un anillo con identidad. Si un ideal I de R contiene una unidad, entonces $I = R$

Demostración. Sea $u \in I$ una unidad, entonces por la propiedad de absorción, $1 = uu^{-1} \in I$. Por otro lado, para cualquier $a \in R$, se tiene que $a = 1a \in I$. Por lo tanto, $I = R$. □

Observación 1.2.10. Sea R un anillo, $M_n(R)$ su anillo de matrices y

$$J := \{H = [h_{ij}] \mid h_{ij} = 0, \text{ para } j \neq 1\},$$

entonces J es un ideal a la izquierda de $M_n(R)$. Con $i \neq 1$ se construye en forma similar un ideal a la derecha.

En términos de ideales, si se considera R como anillo e $\{I_i\}_{i \in I}$ una familia de ideales a la derecha de R , la intersección $\bigcap_{i \in I} I_i$ es un ideal a la derecha de R , el cual se denomina **ideal intersección**. De manera análoga se define la intersección de ideales a la izquierda e ideales biláteros.

Definición 1.2.11. El producto de dos ideales a izquierda I y J es el conjunto formado por todas las sumas finitas de productos de los elementos de I y J , es decir:

$$I \cdot J = \left\{ \sum_k i_k j_k \mid i_k \in I, j_k \in J \right\}.$$

Observación 1.2.12. Si R es un anillo, $S \subseteq R$ y $S \neq \emptyset$. El ideal a la derecha más pequeño de R que contiene al subconjunto S es la intersección de todos los ideales a la derecha de R que contienen a S , y se denota por $\{S\}$, es decir,

$$\{S\} := \bigcap_{S \subseteq I} I.$$

Observación 1.2.13. Sea R un anillo, $S \subseteq R, S \neq \emptyset$, entonces el ideal a la derecha generado por S coincide con el conjunto de sumas finitas de productos de elementos de S con elementos de R , es decir

$$\{S\} = \left\{ \sum_{k=1}^n s_k a_k \mid s_k \in S, a_k \in A, n \geq 1 \right\}.$$

Para llevar a cabo la prueba de la igualdad, se considera B como el conjunto de sumas finitas de productos de elementos de S con elementos de R y se debe probar que $B = \{S\}$. En primer lugar, se prueba que $\{S\} \subseteq B$, concluyendo así que B es un ideal a la derecha de R . Finalmente, se prueba que

$$B \subseteq \bigcap_{S \subseteq I} I = \{S\}.$$

Definición 1.2.14. Sean R y S anillos, un homomorfismo de anillos de R en S es una

función $\phi : R \rightarrow S$ que satisfice:

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2),$$

$$\phi(r_1 r_2) = \phi(r_1) \phi(r_2),$$

para todo $r_1, r_2 \in R$.

Definición 1.2.15. Sea $\phi : R \rightarrow S$ un homomorfismo de anillos, el kernel de ϕ es

$$\ker(\phi) = \{r \in R \mid \phi(r) = 0\}.$$

Ejemplo 1.2.16. La función definida $\phi : \mathbb{C} \rightarrow \mathbb{C}$ vía

$$\phi(a + bi) = a - bi$$

para todo $a, b \in \mathbb{R}$, es un homomorfismo de anillos.

Definición 1.2.17. Sean R y S anillos, entonces un isomorfismo de anillos es un homomorfismo biyectivo de R en S .

Cuando tal isomorfismo existe, se dice que R y S son anillos isomorfos y se denota $R \cong S$.

Ahora, se enunciarán los tres teoremas que permitirán demostrar que ciertos anillos son isomorfos, siendo el primero de ellos el más importante.

Teorema 1.2.18. (Primer Teorema de Isomorfismo). Sea $\phi : R \rightarrow S$ un homomorfismo, entonces $R/\ker(\phi)$ es isomorfo a $\phi(R)$.

Demostración. Ver (Lee, 2018, pág. 165) □

Teorema 1.2.19. (Segundo Teorema de Isomorfismo). Sea R un anillo con ideales I y J , entonces $I/(I \cap J)$ es isomorfo a $(I + J)/J$.

Demostración. Ver (Lee, 2018, pág. 166-167) □

Teorema 1.2.20. (Tercer Teorema de Isomorfismo). Sea R un anillo, y sean I y J ideales de R con $I \subseteq J$, entonces $(R/J)/(I/J)$ es isomorfo a (R/I) .

Demostración. Ver (Lee, 2018, pág. 167-168) □

Ejemplo 1.2.21. Para $n \geq 2$, se define $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ por $\phi(z) = \bar{z}$, para todo $z \in \mathbb{Z}$, se tiene que $\mathbb{Z}/n\mathbb{Z}$ es isomorfo a \mathbb{Z}_n .

Definición 1.2.22. Sea R un anillo, un automorfismo de R es un isomorfismo de R en R .

Ejemplo 1.2.23. Consideremos el anillo de matrices cuadradas $M_n(\mathbb{R})$. Se define la siguiente función $\varphi : M_n(\mathbb{R}) \rightarrow M_n(\mathbb{R})$ dada por $\varphi(A) = PAP^{-1}$, para todo $A \in M_n(\mathbb{R})$ y donde P es una matriz invertible en $M_n(\mathbb{R})$, entonces φ es un automorfismo de anillos. En efecto,

- I. φ está bien definida, pues dado que P es invertible, para cualquier $A \in M_n(\mathbb{R})$, el producto $PAP^{-1} \in M_n(\mathbb{R})$. Por lo tanto, φ está bien definida.
- II. Sean $A, B \in M_n(\mathbb{R})$, entonces:

$$\begin{aligned}\varphi(A + B) &= P(A + B)P^{-1} \\ &= (PA + PB)P^{-1} \\ &= PAP^{-1} + PBP^{-1}.\end{aligned}$$

Luego, φ preserva la suma.

- III. Sean $A, B \in M_n(\mathbb{R})$, entonces:

$$\begin{aligned}\varphi(AB) &= PABP^{-1} \\ &= PAP^{-1}PBP^{-1} \\ &= (PAP^{-1})(PBP^{-1}) \\ &= \varphi(A)\varphi(B).\end{aligned}$$

Y así, φ preserva el producto.

- IV. $\varphi(I_n) = PI_nP^{-1} = PP^{-1} = I_n$. Luego, φ preserva el elemento neutro.

- V. Como P es invertible, P^{-1} también es invertible. Luego, se define la siguiente función inversa:

$$\psi(B) = P^{-1}BP.$$

Entonces,

a)

$$\begin{aligned}\psi(\varphi(A)) &= P^{-1}(PAP^{-1})P \\ &= P^{-1}PAP^{-1}P \\ &= A\end{aligned}$$

b)

$$\begin{aligned}\varphi(\psi(B)) &= P(P^{-1}BP)P^{-1} \\ &= PP^{-1}BPP^{-1} \\ &= B\end{aligned}$$

Así, φ es invertible y su inversa es ψ . En consecuencia, φ es biyectiva y, por lo tanto, se tiene que φ es un automorfismo.

1.3. Módulos

En esta sección se abordarán los conceptos de módulos, sumas directas externa e internas y algunos resultados de interés. Por último, se presentará la definición de homomorfismo entre módulos.

Definición 1.3.1. Sean $\langle M, + \rangle$ un grupo abeliano y R un anillo. Se dice que M es un *módulo a derecha sobre R* , si se ha definido un producto entre los elementos de M y de R , es decir, una función

$$M \times R \longrightarrow M$$

$$(m, r) \longmapsto m \cdot r$$

para la cual se cumplen las siguientes condiciones:

- $(m_1 + m_2) \cdot r = m_1 \cdot r + m_2 \cdot r$;
- $m \cdot (r_1 + r_2) = m \cdot r_1 + m \cdot r_2$;
- $m \cdot (r_1 r_2) = (m \cdot r_1) \cdot r_2$;
- $m \cdot 1_R = m$,

con $m, m_1, m_2 \in M, r, r_1, r_2 \in R$.

Definición 1.3.2. Sea A un anillo conmutativo. Se dice que el anillo R es una A -álgebra si R es un A -módulo y,

$$a \cdot (rs) = (a \cdot r)s = r(a \cdot s),$$

para cada $r, s \in R$ y $a \in A$.

Ejemplo 1.3.3. Sea R un anillo.

I. Si R es conmutativo, entonces $M_n(R)$ es una R -álgebra.

II. R es una \mathbb{Z} -álgebra.

Ejemplo 1.3.4. Los grupos abelianos son considerados como \mathbb{Z} -módulos, pues en un grupo abeliano, para cada $g \in G$ y $n \in \mathbb{Z}$, se define la acción de n sobre g de la siguiente manera:

- Si $n \geq 0$, se define $n \cdot g = g + g \cdots + g$ (suma de g repetida n veces).
- Si $n < 0$, se define $n \cdot g$ como el elemento inverso de $(-n) \cdot g$, es decir, $n \cdot g = -((-n) \cdot g)$.

Esta acción cumple con las propiedades de \mathbb{Z} -módulo y por tanto los grupos abelianos se consideran \mathbb{Z} -módulos.

Definición 1.3.5. Sea M un R -módulo y N un subconjunto no vacío de M . Se dice que N es un R -submódulo de M , o simplemente, un submódulo de M , si N es un subgrupo de $\langle M, + \rangle$, y además,

$$n \cdot r \in N,$$

para cada $n \in N$ y cada $r \in R$, en tal caso se escribe $N \leq M$.

De la definición anterior se sigue que $\{0\}$ y M son submódulos de M y son llamados los submódulos triviales de M .

Observación 1.3.6. Sea R un R -módulo a la derecha y sea I un ideal a derecha de R , entonces $ir \in I$ para todo $i \in I$ y $r \in R$. Luego, por la Definición 1.3.5. note que el producto de cada elemento de un subconjunto no vacío del anillo con un elemento del anillo pertenecen al subconjunto del anillo. Por lo tanto, los submódulos de R son precisamente sus ideales a la derecha.

Ejemplo 1.3.7. Sea k un cuerpo. Si V es un k -espacio vectorial, entonces V es un k -módulo y los submódulos de V son precisamente los subespacios de V .

Observación 1.3.8. Si M y N son R -módulos, entonces $M \times N$ es un R -módulo, definiendo las operaciones de la siguiente manera:

$$(m, n) + (m' + n') = (m + m', n + n')$$

$$(m, n) \cdot r = (m \cdot r, n \cdot r),$$

para todo $r \in R$.

De manera más general si $\{M_i\}_{i \in I}$ es una familia de R -módulos y $M = \prod_{i \in I} M_i$ es el producto cartesiano de los miembros de la familia (es decir, el conjunto de las familias de la forma $(m_i)_{i \in I}$, donde $m_i \in M_i$, para cada $i \in I$), se puede introducir una estructura de R -módulo con las siguientes operaciones:

$$(m_i)_{i \in I} + (m'_i)_{i \in I} = (m_i + m'_i)_{i \in I}$$

$$(m_i)_{i \in I} \cdot r = (m_i \cdot r)_{i \in I},$$

para todo $r \in R$.

Observación 1.3.9. El R -módulo construido anteriormente es llamado producto directo o producto cartesiano de la familia $\{M_i\}_{i \in I}$. Si $I = \{1, 2, \dots, n\}$, se denota

$$\prod_{i \in I} M_i = M_1 \times \dots \times M_n.$$

Observación 1.3.10. Sea $\{M_i\}_{i \in I}$ una familia de R -módulos y $M = \prod_{i \in I} M_i$. Una familia $(m_i)_{i \in I} \in M$ se dice casi nula si $m_i \neq 0$ solamente para un número finito de índices.

Proposición 1.3.11. La suma de familias casi nulas es casi nula.

Demostración. Sean $x = (x_i), y = (y_i)$ dos familias casi nulas. Es decir, existen conjunto finitos $I_x, I_y \subseteq I$ tales que:

I. $x_i = 0$ si $i \notin I_x$,

II. $y_i = 0$ si $i \notin I_y$.

Luego, para todo $i \notin I_x \cup I_y$, se tiene que $x_i + y_i = 0 + 0 = 0$, luego $x_i + y_i \in I_x \cup I_y$. Y así, $x + y$ es una familia casi nula. \square

Proposición 1.3.12. El producto de un elemento del anillo por una familia casi nula es una familia casi nula.

Demostración. Sea $r \in R$ y $x = (x_i) \in \bigoplus_{i \in I} M_i$ una familia casi nula con $I_x \subseteq I$, entonces, para $i \notin I_x, x_i = 0$, luego, $rx_i = r \cdot 0 = 0$ y así, $(rx_i) \in I_x$ y, así, es finito. Por lo tanto, $r \cdot x$ es una familia casi nula. \square

Observación 1.3.13. Sea $\{M_i\}_{i \in I}$ una familia de R -módulos. El conjunto de las familias casi nulas de $M = \prod_{i \in I} M_i$, con la estructura de R -módulo definida por la restricción de operaciones de M se llama **suma directa externa** de la familia y se denota,

$$\bigoplus_{i \in I}^{\bullet} M_i,$$

si el conjunto $I = \{1, \dots, n\}$,

$$\bigoplus_{i \in I}^{\bullet} M_i = M_1 \bigoplus^{\bullet} \dots \bigoplus^{\bullet} M_n.$$

Observación 1.3.14. De la definición se tiene que la suma directa externa de una familia de R -módulos es un submódulo del producto directo y que

$$\bigoplus_{i \in I}^{\bullet} M_i = \prod_{i \in I} M_i.$$

si y solo si, el conjunto de índices I es finito.

Observación 1.3.15. Si en la familia de R -módulos $\{M_i\}_{i \in I}$ se tiene que $M_i = M$, para cada $i \in I$ se denota la suma directa externa de dicha familia como sigue

$$\bigoplus_{i \in I}^{\bullet} M_i = \bigoplus_{i \in I}^{\bullet} M = \prod_{i \in I} M_i = M^n.$$

Definición 1.3.16. Sea S un subconjunto del R -módulo M , se denota por $\{S\}$ la intersección de todos los submódulos de M que contienen a S , es decir,

$$\{S\} = \bigcap_{S \subseteq N \subseteq M} N.$$

Note que $\{S\}$ es el menor submódulo que contiene a S .

En caso que $\{S\} = M$, S es llamado un sistema de generadores para M .

El siguiente resultado, puede obtenerse efectuando un paso similar al descrito en la Observación 1.2.13.

Proposición 1.3.17. Sea M un R -módulo y $\emptyset \neq S \subseteq M$, entonces,

$$\langle S \rangle = \left\{ \sum_{i=1}^n s_i \cdot r_i \mid s_i \in S, r_i \in R, n \geq 1 \right\}.$$

Demostración. Sea B el conjunto de las sumas finitas de productos de elementos de S con elementos de R ,

$$B = \left\{ \sum_{i=1}^n s_i \cdot r_i \mid s_i \in S, r_i \in R, n \geq 1 \right\},$$

probemos que $\langle S \rangle = B$.

En efecto, sean $b_1, b_2 \in B$ y $r_1, r_2 \in R$, entonces:

- I. $(b_1 + b_2) \cdot r_1 = b_1 \cdot r_1 + b_2 \cdot r_1$,
- II. $b_1 \cdot (r_1 + r_2) = b_1 \cdot r_1 + b_1 \cdot r_2$,
- III. $b_1 \cdot (r_1 r_2) = (b_1 \cdot r_1) \cdot r_2$,
- IV. $b_1 \cdot 1_R = b_1$

Por lo tanto, B es un submódulo a derecha de R . Además, note que $S \subseteq B$, de donde se deduce que $\langle S \rangle \subseteq B$.

Sea ahora N un submódulo a derecha de R que contiene a S , entonces N contiene cada suma de la forma

$$\sum_{i=1}^n s_i r_i$$

donde $s_i \in S, r_i \in R$ y $n \geq 1$, es decir, $B \subseteq N$. Como esto es válido para todo submódulo que contenga a S , entonces

$$B \subseteq \bigcap_{S \subseteq N} N = \langle S \rangle.$$

□

Definición 1.3.18. Sea $\{M_i\}_{i \in I}$ una familia no vacía de submódulos de M , se denomina suma de la familia dada, y se denota por $\sum_{i \in I} M_i$, al submódulo generado por $\bigcup_{i \in I} M_i$.

Note que $\sum_{i \in I} M_i$ es el submódulo más pequeño que contiene simultáneamente a cada $M_i, i \in I$.

Para una familia finita se tiene,

$$M_1 + \cdots + M_n = \left\{ \sum_{i=1}^n m_j \mid m_j \in M_j, 1 \leq j \leq n \right\}.$$

Definición 1.3.19. Sea M un R -módulo y $\{M_i\}_{i \in I}$ una familia de submódulos de M . Se dice que M es una **suma directa interna** de la familia si

- I. $M = \sum_{i \in I} M_i$.
- II. $(\sum_{i \neq j} M_i) \cap M_j = \{0\}$, para cada $j \in I$.

En tal caso se denota

$$M = \bigoplus_{i \in I} M_i.$$

Si $I = \{1, \dots, n\}$ se escribe $M = M_1 \oplus \cdots \oplus M_n$.

Proposición 1.3.20. Sea $\{M_i\}_{i \in I}$ una familia de submódulos del módulo M tal que $M = \sum_{i \in I} M_i$. Las siguientes condiciones son equivalentes:

- I. $M = \bigoplus_{i \in I} M_i$.
- II. Para cada subconjunto finito $\{i_1, \dots, i_n\}$ de índices diferentes en I se cumple que,

$$m_{i_1} + \cdots + m_{i_n} = 0 \Leftrightarrow m_{i_k} = 0,$$

con $m_{i_k} \in M_{i_k}, 1 \leq k \leq n$.

- III. Para cada subconjunto finito $\{i_1, \dots, i_n\}$ de índices diferentes en I se cumple que,

$$m_{i_1} + \cdots + m_{i_n} = m'_{i_1} + \cdots + m'_{i_n} \Leftrightarrow m_{i_k} = m'_{i_k},$$

con $m_{i_k}, m'_{i_k} \in M_{i_k}, 1 \leq k \leq n$.

Demostración. (I) \Rightarrow (II). Sea $\{i_1, i_2, \dots, i_n\}$ un subconjunto de índices diferentes en I tales que $m_{i_1} + \cdots + m_{i_n} = 0$, donde $m_{i_k} \in M_{i_k}$ para cada $1 \leq k \leq n$. Fijando el subíndice k se tiene,

$$\begin{aligned} m_{i_k} &= -m_{i_1} - m_{i_2} - \cdots - m_{i_{k-1}} - m_{i_{k+1}} - \cdots - m_{i_n}, \\ &= -(m_{i_1} + m_{i_2} + \cdots + m_{i_{k-1}} + m_{i_{k+1}} + \cdots + m_{i_n}), \end{aligned}$$

luego $m_{i_k} \in M_{i_k} \cap \sum_{j \neq i_k} M_j$, de donde, $m_{i_k} = 0$, para cada $i \leq k \leq n$.

Recíprocamente si se da esta última condición se cumple que $m_{i_1} + \cdots + m_{i_n} = 0$, luego, se tiene que,

$$\left(\sum_{i \neq j} M_i \right) \cap M_j = \{0\},$$

para cada $j \in I$ y así, $M = \bigoplus_{i \in I} M_i$.

(II) \Rightarrow (III). Sea $\{i_1, i_2, \dots, i_n\}$ un subconjunto de índice diferentes en I tales que se cumple que,

$$m_{i_1} + \cdots + m_{i_n} = m'_{i_1} + \cdots + m'_{i_n},$$

entonces, $(m_{i_1} - m'_{i_1}) + \cdots + (m_{i_n} - m'_{i_n}) = 0$, y por (II), se tiene que $m_{i_k} = m'_{i_k}$, para cada $1 \leq k \leq n$.

Para el recíproco, supongamos que

$$m_{i_1} + \cdots + m_{i_n} = m'_{i_1} + \cdots + m'_{i_n} \Leftrightarrow m_{i_k} = m'_{i_k}.$$

Como $m_{i_k} = m'_{i_k}$, entonces

$$m_{i_1} + \cdots + m_{i_n} = 0$$

y por tanto, $m_{i_k} = 0$.

(III) \Rightarrow (I). Sea $j \in I$ un índice fijo, y sea $m \in M_j \cap \sum_{j \neq i_k} M_j$, entonces existen índices diferentes $i_1, \dots, i_m \in I$, tales que $j \notin \{i_1, \dots, i_m\}$ y además,

$$m = m_{i_1} + \cdots + m_{i_m},$$

donde $m_{i_k} \in M_{i_k}$, para cada $1 \leq k \leq m$.

La igualdad anterior se puede escribir como,

$$m'_{i_1} + \cdots + m'_{i_m} + m = m_{i_1} + \cdots + m_{i_m} + m_j,$$

donde $m'_{i_k} = 0$, para cada $1 \leq k \leq m$ y $m_j = 0$. Por (III), $m = m_j$, por lo tanto $M_j \cap \sum_{i \neq j} M_i = 0$. \square

Definición 1.3.21. Sea M un R -módulo y N un submódulo de M . Se dice que M es un

sumando directo de M si existe un submódulo N' de M tal que $M = N \oplus N'$.

Ejemplo 1.3.22. Para cualquier R -módulo M , se tiene que $M = M \oplus \{0\}$. Los submódulos M y $\{0\}$ son llamados los sumandos directos triviales.

Ejemplo 1.3.23. Consideremos el \mathbb{Z} -módulo $\mathbb{Z}_6 = \{0, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, se tienen los submódulos $H_1 = \{0, \bar{2}, \bar{4}\}$ y $H_2 = \{0, \bar{3}\}$ son submódulos tales que $H_1 \cap H_2 = \{0\}$. Por otro lado, se verifica también que $\mathbb{Z}_6 = H_1 + H_2$, luego,

$$\mathbb{Z}_6 = H_1 \oplus H_2.$$

Por lo tanto, H_1 es un sumando directo de \mathbb{Z}_6 .

Definición 1.3.24. Sea N un submódulo de M , se dice que:

- I. N es maximal, si cada vez que exista $N \leq N' \leq M$, entonces $N' = M$.
- II. N es minimal, si cada vez que exista $N' \leq N \leq M$, entonces $N' = \{0\}$.

Ejemplo 1.3.25. Sea $\mathbb{Z}_{2n} := \{\bar{0}, \bar{1}, \dots, \overline{2n-1}\}$, entonces los submódulos $M = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ y $P = \{\bar{0}, \bar{1}\}$ son submódulos maximales y minimales respectivamente.

Definición 1.3.26. Sea M un A -módulo. Se dice que:

- I. M es noetheriano (artiniano) si cada colección no vacía de submódulos de M tiene elemento maximal (minimal).
- II. El anillo A es noetheriano (artiniano) si el A -módulo es noetheriano (artiniano).

Ejemplo 1.3.27. El anillo \mathbb{Z} , considerado como \mathbb{Z} -módulo no es un anillo artiniano porque contiene una secuencia infinita decreciente de ideales a la izquierda $\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \dots$.

Definición 1.3.28. Sean A_1, A_2 anillos. Se dice que el grupo abeliano M es un (A_1, A_2) -bimódulo, si M es A_1 -módulo a la izquierda, A_2 -módulo a la derecha, y además,

$$(a \cdot m) \cdot b = a \cdot (m \cdot b),$$

para cada $a \in A_1, b \in A_2$ y $m \in M$.

Ejemplo 1.3.29. $M_n(A)$ es un $(A, M_n(A))$ -bimódulo.

Definición 1.3.30. Sea M un R -módulo. Se dice que M es **simple** sobre R si no tiene submódulos propios no triviales.

Ejemplo 1.3.31. Un \mathbb{Z} -módulo simple es un grupo abeliano que no tiene ningún subgrupo propio no nulo.

Definición 1.3.32. Un módulo sobre un anillo (no necesariamente conmutativo) se dice **semisimple** cuando es una suma directa de submódulos simples.

Observación 1.3.33. *Cada submódulo de M es un sumando directo; es decir, para cada submódulo N de M , existe un submódulo P tal que $M = N \oplus P$.*

Definición 1.3.34. Sean M y N dos R -módulos. Una función $f : M \rightarrow N$ se dice que es un R -homomorfismo, o también un homomorfismo de módulos, si:

I. $f(m + m') = f(m) + f(m')$;

II. $f(m \cdot r) = f(m) \cdot r$.

Para cada $m, m' \in M$ y $r \in R$.

Observación 1.3.35. *Los conceptos de núcleo, imagen, homomorfismo inyectivo, homomorfismo sobreyectivo, isomorfismo y endomorfismo de módulos, se definen similarmente en el caso de anillos.*

Observación 1.3.36. *Note que, en particular, $\ker(f) := \{m \in M \mid f(m) = 0\}$ es un submódulo de M e $\text{Im}(f) := \{f(m) \mid m \in M\}$ es un submódulo de N . Además, si $f : M \rightarrow N$ es homomorfismo, entonces f es inyectiva si y sólo si $\ker(f) = \{0\}$ y f es sobreyectiva si y sólo si $\text{Im}(f) = N$.*

2. El Teorema de Skolem-Noether

En este capítulo se abordarán en principio algunas definiciones y resultados importantes para demostrar El Teorema de Skolem-Noether, un resultado importante en el estudio de las graduaciones y buenas graduaciones sobre el anillo de matrices. Por otro lado, se considera k un cuerpo.

2.1. Anillos semisimples

En esta sección, se abordarán algunas definiciones preliminares y resultados importantes referente a anillos simples y anillos semisimples.

Definición 2.1.1. Un anillo A se denomina simple cuando $A \neq 0$ y cuando A no posee ideales bilaterales propios.

Definición 2.1.2. Sea A una k -álgebra.

- I. Se dice que A es finita si $\dim_k(A) < \infty$. Se denota por $[A : k] = \dim_k(A)$.
- II. Se dice que A es **central** si su centro, denotado por $C(A)$ es exactamente el cuerpo k , es decir, $Z(A) = k$.

Ejemplo 2.1.3. El centro de $M_n(k)$ consiste únicamente en las matrices escalares, es decir, matrices de la forma λI_n , donde $\lambda \in k$ e I_n es la matriz identidad. En consecuencia, el centro es isomorfo a k , y por tanto, $M_n(k)$ es un álgebra central.

Por otro lado, mostraremos que $M_n(k)$ es un anillo simple. En efecto, supongamos que $I \subseteq M_n(k)$ es un ideal bilateral no nulo y sea $A \in I$. Como $A \neq 0$, existe al menos un elemento no nulo en alguna posición (i, j) , es decir, $A_{ij} \neq 0$.

Sea $E_{ab} \in M_n(k)$, donde la entrada (a, b) es 1 y el resto son 0. Luego, consideremos $B = E_{ri}AE_{js} = A_{ij}E_{rs}$, entonces, es una matriz cuyo único valor no nulo está en la posición (r, s) . Luego:

$$E_{ri}AE_{js} = A_{ij}E_{rs}$$

Como $A \in I$, entonces:

$$E_{ri}AE_{js} = A_{ij}E_{rs} \in I$$

Como $A_{ij} \in k$ y $A_{ij} \neq 0$, entonces $A_{ij}^{-1} \in k$, de ahí que

$$E_{rs} = A_{ij}^{-1}(A_{ij}E_{rs}) = A_{ij}^{-1}(E_{ri}AE_{js}) \in I.$$

Por otro lado, note que el conjunto de matrices elementales $\{E_{rs}\}$ forman una base para $M_n(k)$. Es decir, cualquier matriz $M \in M_n(k)$ puede escribirse como combinación lineal

$$M = \sum_{r=1}^n \sum_{s=1}^n m_{rs} E_{rs}$$

donde $m_{rs} \in k$ son las entradas de M . Luego, I contiene a toda combinación lineal. Por lo tanto, $I = M_n(k)$ y así, $M_n(k)$ es un anillo simple.

Definición 2.1.4. Dada una k -álgebra A , se denota A^{op} a la k -álgebra que se obtiene invirtiendo el orden de la multiplicación en A . Es decir,

$$r * a = ar$$

para cada $a, r \in A$.

Definición 2.1.5. Un anillo R es **semisimple** si es un módulo semisimple sobre sí mismo.

Teorema 2.1.6. Lema de Schur. Sean M y M' R -módulos a izquierda simples, donde R es un anillo, entonces cada función $f : M \rightarrow M'$ no nula es un isomorfismo.

Demostración. Como M es simple, entonces tiene exactamente dos submódulos: M y $\{0\}$. Luego, el submódulo $\ker(f) \neq M$, dado que f es distinto de 0, por tanto $\ker(f) = \{0\}$, luego f es inyectiva. Análogamente, el submódulo $\text{im}(f) \neq \{0\}$, y así $\text{im}(f) = M'$ y, por tanto, f es sobreyectiva. \square

Lema 2.1.7. Si L y L' son ideales minimales a izquierda en un anillo R , entonces los siguientes enunciados son equivalentes:

- I. $LL' \neq \{0\}$,
- II. $\text{Hom}_R(L, L') \neq \{0\}$, y existe $b' \in L'$ con $L' = Lb'$,
- III. $L \cong L'$ como R -módulos a izquierda.

Demostración. Sean L y L' ideales minimales a izquierda.

- (I) \Rightarrow (II). Si $LL' \neq \{0\}$, entonces existe $b \in L$ y $b' \in L'$ con $bb' \neq 0$. De ahí que la función $f : L \rightarrow L'$, definida por $x \mapsto xb'$ es distinta de 0 y así $\text{Hom}_R(L, L') \neq \{0\}$. Además, $Lb' = L'$ ya que es un submódulo distinto de 0 del ideal mínimo a izquierda.

- (II) \Rightarrow (III). Si $\text{Hom}_R(L, L') \neq \{0\}$, entonces existe un homomorfismo $f : L \rightarrow L'$ no nulo y, por el Lema de Schur, f es un isomorfismo. Por lo tanto, $L \cong L'$.
- Si se cumple (III) y $L^2 \neq \{0\} \Rightarrow$ (I). Si $L^2 \neq \{0\}$, entonces existe $x, y \in L$ con $xy \neq 0$. Si $g : L \rightarrow L'$ es un isomorfismo, entonces $0 \neq g(xy) = xg(y) \in LL'$, y así $LL' \neq \{0\}$.

□

Corolario 2.1.8. Si $L^2 \neq \{0\}$, entonces (III) implica (I), y así los tres enunciados son equivalentes.

Proposición 2.1.9. Si R es un anillo y M un R -módulo a la izquierda, entonces $\text{Hom}_R(R, M)$ es un R -módulo a la izquierda y es isomorfo a M .

Demostración. Se define la acción de R sobre $\text{Hom}_R(R, M)$ de la siguiente forma. Sea $f \in \text{Hom}_R(R, M)$ y $r \in R$, luego, se define el homomorfismo $(r \cdot f) : R \rightarrow M$ de la siguiente forma

$$(r \cdot f)(a) := f(ar),$$

para todos $a, r \in R$ y $f \in \text{Hom}_R(R, M)$.

Como f es un homomorfismo, $(r \cdot f)$ es un homomorfismo de R a M . Es decir, si $f \in \text{Hom}_R(R, M)$, entonces $(r \cdot f) \in \text{Hom}_R(R, M)$.

En efecto,

$$\begin{aligned} (r \cdot f)(a + b) &= f((a + b)r) \\ &= f(ar + br) \\ &= f(ar) + f(br) \\ &= (r \cdot f)(a) + (r \cdot f)(b). \end{aligned}$$

Para cada $a, b \in R$.

$$\begin{aligned} (r \cdot f)(sa) &= f((sa)r) \\ &= f(s(ar)) \\ &= s \cdot f(ar) \\ &= s \cdot (r \cdot f)(a) \end{aligned}$$

para $s \in R$ y así, se tiene que $(r \cdot f) \in \text{Hom}_R(R, M)$.

Sean $r, r' \in R$ y $f, g \in \text{Hom}_R(R, M)$, entonces

I.

$$\begin{aligned}(r \cdot (f + g))(a) &= (f + g)(ar) \\ &= f(ar) + g(ar) \\ &= (r \cdot f)(a) + (r \cdot g)(a)\end{aligned}$$

II.

$$\begin{aligned}((r + r') \cdot f)(a) &= f(a(r + r')) \\ &= f(ar + ar') \\ &= f(ar) + f(ar') \\ &= (r \cdot f)(a) + (r' \cdot f)(a)\end{aligned}$$

III.

$$\begin{aligned}((rr') \cdot f)(a) &= f(a(rr')) \\ &= (r' \cdot f)(ar) \\ &= (r \cdot (r' \cdot f))(a)\end{aligned}$$

IV.

$$\begin{aligned}(1_R \cdot f)(a) &= f(a \cdot 1_R) \\ &= f(a)\end{aligned}$$

Y así, se tiene que $(r \cdot f) \in \text{Hom}_R(R, M)$. Por lo tanto, $\text{Hom}_R(R, M)$ tiene estructura de R -módulo a la izquierda.

Por otro lado, veamos que $\text{Hom}_R(R, M) \cong M$.

En efecto, se define la siguiente función $\varphi : \text{Hom}_R(R, M) \rightarrow M$, vía $\varphi(f) = f(1_R)$, donde $1_R \in R$ es el elemento neutro del anillo R .

I. Sean $f, g \in \text{Hom}_R(R, M)$ y $r \in R$, entonces

$$\begin{aligned}\varphi(f + g) &= (f + g)(1_R) \\ &= f(1_R) + g(1_R) \\ &= \varphi(f) + \varphi(g)\end{aligned}$$

Además, para $r' \in R$,

$$\varphi(r' \cdot f) = \varphi(f) \cdot r'.$$

II. Supongamos que $\varphi(f) = 0$, es decir, $f(1_R) = 0$, de ahí que $f(r) = rf(1_R) = 0$ para todo $r \in R$, por tanto, f es el homomorfismo cero y así, $f = 0$, luego, φ es inyectiva.

III. Para cualquier $m \in M$, se define el homomorfismo $f_m \in \text{Hom}_R(R, M)$ por $f_m(r) = rm$, entonces

$$\begin{aligned}\varphi(f_m) &= f_m(1_R) \\ &= 1_R m \\ &= m\end{aligned}$$

y así φ es sobreyectiva. Por lo tanto, φ es un isomorfismo y así $\text{Hom}_R(R, M) \cong M$.

□

Proposición 2.1.10. Si $R = \sum_j L_j$ es un anillo semisimple a la izquierda, donde L_j son ideales minimales a la izquierda, entonces cada R -módulo simple S es isomorfo a algún L_j , donde S es un R -módulo a la izquierda.

Demostración. Note que $S \cong \text{Hom}_R(R, S) \neq \{0\}$ por la Proposición 2.1.9. Si $\text{Hom}_R(L_j, S) = \{0\}$ para todo j , entonces $\text{Hom}_R(R, S) = \{0\}$ (para $R = L_1 \oplus \cdots \oplus L_m$), por tanto, $\text{Hom}_R(L_j, S) \neq \{0\}$ para algún j . Como L_j y S son simples, por el Teorema 2.1.6. se tiene que $L_j \cong S$. □

Lema 2.1.11. Sea R un anillo semisimple a izquierda, y sea

$$R = L_1 \oplus \cdots \oplus L_n = B_1 \oplus \cdots \oplus B_m$$

donde los L_j son ideales minimales a izquierda y los B_i son los correspondientes componentes simples de R . Si L es cualquier ideal minimal a izquierda en R , no necesariamente en la descomposición dada de R , entonces $L \cong L_i$ para algún i y $L \subseteq B_i$.

Demostración. Por la Proposición 2.1.10, un ideal minimal a izquierda L es isomorfo a L_i para algún i . Ahora,

$$\begin{aligned} L &= RL \\ &= (B_1 \oplus \cdots \oplus B_m)L \\ &\subseteq B_1L + \cdots + B_mL. \end{aligned}$$

Si $j \neq i$, entonces, por el Lema 2.1.7. $B_jL = \{0\}$. Por lo tanto,

$$L \subseteq B_iL \subseteq B_i.$$

□

Proposición 2.1.12. *Todo anillo artiniiano a izquierda y simple es semisimple.*

Demostración. Primero, veamos que si L es cualquier ideal a izquierda distinto de 0 en R y $\Delta = \text{End}_R(L)$, entonces $R \cong \text{End}_R(L)$. Ahora, sea L un Δ -módulo a la izquierda (con el producto escalar $\Delta \times L \rightarrow L$, dada por $(f, a) \mapsto f(a)$ para todo $f \in \Delta$ y $a \in L$).

Sea $\varphi : R \rightarrow \text{End}_R(L)$ donde φ_r la multiplicación a izquierda de r , es decir,

$$\varphi_r(a) = ra,$$

para todo $r \in R$ y $a \in L$. Note que φ_r está bien definida.

Si $f \in \Delta = \text{End}_R(L)$, entonces

$$\begin{aligned} \varphi_r(f(a)) &= rf(a) \\ &= f(ra) \\ &= f\varphi_r(a). \end{aligned}$$

Veamos que φ es un anillo de homomorfismo,

$$\begin{aligned} \varphi_{r+s}(a) &= (r+s)a = ra + sa = \varphi_r(a) + \varphi_s(a) \\ (\varphi_r \circ \varphi_s)(a) &= \varphi_r(\varphi_s(a)) = \varphi_r(sa) = r(sa) = (rs)a = \varphi_{rs}(a) \\ \varphi_{1_R}(a) &= 1_R \cdot a = a \end{aligned}$$

y así, φ_r es un homomorfismo de anillos.

Como $\varphi \neq 0$, entonces $\ker\varphi \neq R$, y dado que R es un anillo simple y $\ker\varphi$ es un ideal bilateral de R , entonces $\ker\varphi = \{0\}$, y así, φ es inyectiva.

Note que $\text{im}(\varphi)$ es un subanillo de $\text{End}_R(L)$. Como φ es inyectiva, entonces hay una correspondencia uno a uno entre R y $\text{im}\varphi$, luego, se puede identificar la imagen con R . Como R es un anillo simple, y φ es inyectiva, entonces $\varphi(R)$ es un anillo simple, por lo tanto, $\varphi(R) = \text{im}\varphi = \text{End}_R(L)$.

Si $b \in L$, se define $\rho_b : L \rightarrow L$ como la multiplicación por derecha de b :

$$\rho_b : a \mapsto ab.$$

Ahora, $\rho_b : L \rightarrow L$ está bien definida. Si $r \in L$ y $a \in L$, entonces

$$\begin{aligned}\rho_b(ra) &= (ra)b \\ &= r(ab) \\ &= r\rho_b(a),\end{aligned}$$

por lo tanto, $\rho_b \in \text{End}_R(L) = \Delta$.

Ahora, veamos que $\varphi(L)$ es un ideal a la izquierda en $\text{End}_\Delta(L)$.

En efecto, sea $h \in \text{End}_\Delta(L)$ y $a, b \in L$, entonces

$$h(\rho_b(a)) = \rho_b h(a),$$

luego

$$\begin{aligned}h(\rho_b(a)) &= h(ab) \\ &= h(\varphi_a(b)),\end{aligned}$$

y

$$\begin{aligned}\rho_b(h(a)) &= h(a)b \\ &= \varphi_{h(a)}(b),\end{aligned}$$

por lo tanto,

$$h\varphi_a = \varphi_{h(a)} \in \varphi(L),$$

y así $\varphi(L)$ es un ideal a la izquierda en $End_{\Delta}(L)$.

Note que el conjunto de sumas finitas

$$LR = \left\{ \sum_i v_i r_i : v_i \in R, r_i \in R \right\},$$

es un ideal bilateral en R , y $LR \neq 0$, dado que R tiene unidad. Por simplicidad de R , $LR = R$. Por lo tanto,

$$\begin{aligned}\varphi(R) &= \varphi(LR) \\ &= \varphi(L)\varphi(R),\end{aligned}$$

es un ideal a la izquierda en $End_{\Delta}(L)$ (dado que $\varphi(L)$ es un ideal a la izquierda). Ahora, $\varphi(R)$ contiene a $\varphi(1) = 1$, y así $\varphi(R)$ contiene a 1. Luego $\varphi(R) = End_{\Delta}(L)$ y por lo tanto $R \cong End_{\Delta}(L)$.

Sea L es un ideal minimal a la izquierda. Por el Lema de Schur, $\Delta = End_R(L)$ es un anillo de división. Además, L es un espacio vectorial a la izquierda sobre Δ . Si L tiene dimensión finita, es decir, $dim_{\Delta}(L) = n$, entonces $R \cong End_{\Delta}(L) \cong M_n(\Delta^{op})$. Por otro lado, Si L es de dimensión infinita, entonces existe un conjunto linealmente independiente $v_1, v_2, \dots, v_n, \dots$ que está contenida en una base, defina

$$I_j = \{T \in End_{\Delta}(L) : T(v_1) = 0 = \dots = T(v_j)\},$$

donde $1 \leq j \leq n$. Entonces $I_1 \supsetneq I_2 \supsetneq \dots$ es una sucesión estrictamente decreciente de ideales a la izquierda, que contradice el hecho de que R es un anillo artiniiano a la izquierda. \square

Proposición 2.1.13. *Sea A un anillo artiniiano simple. Dos A -módulos a izquierda M y N son isomorfos si y solo si $\dim_A(M) = \dim_A(N)$.*

Demostración. Como A es un anillo semisimple, cada módulo a la izquierda M es isomorfo a una suma directa de ideales minimales a la izquierda. Por el Lema 2.1.11, todos los ideales minimales a la izquierda son isomorfos a L , donde L es un ideal a la izquierda en A , y así $\dim_A(M)$ es el número de sumandos en una descomposición. Si $M \cong N$ como A -módulo a la izquierda, entonces M y N tienen la misma descomposición en suma directa de módulos simples, luego, la dimensión como suma directa es la misma, por lo tanto, $\dim_A(M) = \dim_A(N)$.

Recíprocamente si $\dim_A(M) = d = \dim_A(N)$, entonces M y N son sumas directas de d copias de L , y por lo tanto $M \cong N$ como A -módulos a la izquierda. \square

2.2. Producto Tensorial

Para esta sección, se presentarán algunas definiciones preliminares correspondientes al producto tensorial. Así mismo, se abordarán resultados importantes referentes al producto tensorial y anillos simples. Finalmente, se mostrará el Teorema de Skolem-Noether.

Definición 2.2.1. Sean U, V y W tres espacios vectoriales. Una transformación $\varphi : U \times V \rightarrow W$ se llama bilineal si se satisface las siguientes condiciones:

$$\varphi(\lambda x_1 + x_2, y) = \lambda \varphi(x_1, y) + \varphi(x_2, y),$$

para cada $x_1, x_2 \in U, y \in V$ y $\lambda \in \mathbb{C}$.

$$\varphi(x, \lambda y_1 + y_2) = \lambda \varphi(x, y_1) + \varphi(x, y_2),$$

para cada $y_1, y_2 \in V, x \in U$ y $\lambda \in \mathbb{C}$.

Observación 2.2.2. Si $W = \mathbb{R}$ ó $W = \mathbb{C}$, φ se llama una función bilineal.

$\varphi(U \times V) := \{z \in W \mid z = \varphi(x, y); x \in U, y \in V\}$, entonces $\varphi(U \times V)$ no es necesariamente un subespacio de W . Por lo tanto, se denota:

$$\text{im}\varphi = \langle \varphi(U \times V) \rangle$$

Además se denota

$$B(U, V; W) := \{\varphi : U \times V \rightarrow W \mid \varphi \text{ es transformación bilineal}\}.$$

Definición 2.2.3. Sean U, V y W espacios vectoriales y sea $\varphi : U \times V \rightarrow W$ una transformación bilineal. El par (W, φ) se llama un **producto tensorial** para U y V si satisfacen las siguientes condiciones:

I. $\text{im}\varphi = W$

II. si $\psi : U \times V \rightarrow T$ es una transformación bilineal de $U \times V$ en cualquier espacio vectorial T , entonces existe una transformación lineal $f : W \rightarrow T$ tal que $\psi = f \circ \varphi$ y por consiguiente, se tiene la siguiente propiedad de factorización.

$$\begin{array}{ccc} U \times V & \xrightarrow{\varphi} & W \\ \psi \downarrow & \searrow f & \downarrow \\ T & \xleftarrow{f} & W \end{array}$$

Notación 2.2.4. Si el par (W, φ) es un producto tensorial para U y V , se escribe W como $U \otimes V$ y $\varphi(x, y)$ como $x \otimes y$, luego, las igualdades en la Definición 2.80 toman la forma:

$$(\lambda x_1 + x_2) \otimes y = \lambda x_1 \otimes y + x_2 \otimes y,$$

para cada $x_1, x_2 \in U, y \in V$ y $\lambda \in \mathbb{C}$.

$$x \otimes (\lambda y_1 + y_2) = \lambda x \otimes y_1 + x \otimes y_2,$$

para cada $x \in U; y_1, y_2 \in V$ y $\lambda \in \mathbb{C}$.

Ejemplo 2.2.5. Sea $\beta : \mathbb{R}^n \times \mathbb{R}^m \rightarrow M_{n \times m}(\mathbb{R})$ definida por

$$\beta((x_1, \dots, x_n), (y_1, \dots, y_m)) = \begin{bmatrix} x_1 y_1 & \cdots & x_1 y_m \\ \vdots & & \vdots \\ x_n y_1 & \cdots & x_n y_m \end{bmatrix}_{n \times m},$$

entonces $(M_{n \times m}(\mathbb{R}), \beta)$ es un producto tensorial para \mathbb{R}^n y \mathbb{R}^m .

En efecto, veamos que se cumplen las condiciones de la Definición 2.82.

I. Si $A \in M_{n \times m}(\mathbb{R})$ es tal que $A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2m} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{2n} & \cdots & \alpha_{nm} \end{bmatrix}$, entonces

$$\begin{aligned} & \beta((\alpha_{11}, \alpha_{21}, \dots, \alpha_{n1}) + (1, 0, \dots, 0)) + \cdots + \beta((\alpha_{1m}, \alpha_{2m}, \dots, \alpha_{nm}) + (0, 0, \dots, 1)) \\ = & \begin{bmatrix} \alpha_{11} & 0 & \cdots & 0 \\ \alpha_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & 0 & \cdots & 0 \end{bmatrix} + \begin{bmatrix} 0 & \alpha_{12} & 0 & \cdots \\ 0 & \alpha_{22} & 0 & \cdots \\ \vdots & \vdots & \vdots & \\ 0 & \alpha_{2n} & 0 & \cdots \end{bmatrix} + \cdots + \begin{bmatrix} 0 & \cdots & 0 & \alpha_{1m} \\ 0 & \cdots & 0 & \alpha_{2m} \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & \alpha_{nm} \end{bmatrix} \\ = & \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{bmatrix} \end{aligned}$$

Es decir, para $A \in M_{n \times m}$, existen $x_i \in \mathbb{R}^n$ y $y_i \in \mathbb{R}^m$ tales que

$$A = \sum \beta(x_i, y_i).$$

Y así, $A \in \langle \beta(\mathbb{R}^n \times \mathbb{R}^m) \rangle$.

II. Se define:

$$f \left(\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix} \right) = \psi((1, 0, \dots, 0) + (\alpha_{11}, \dots, \alpha_{1m})) + \cdots + \psi(0, 0, \dots, 1) + (\alpha_{n1}, \dots, \alpha_{nm}).$$

Veamos que f es lineal:

$$f \left(\lambda \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix} + \begin{pmatrix} \alpha'_{11} & \cdots & \alpha'_{1m} \\ \vdots & & \vdots \\ \alpha'_{n1} & \cdots & \alpha'_{nm} \end{pmatrix} \right) = \begin{pmatrix} \lambda\alpha_{11} + \alpha'_{11} & \cdots & \lambda\alpha_{1m} + \alpha'_{1m} \\ \vdots & & \vdots \\ \lambda\alpha_{n1} + \alpha'_{n1} & \cdots & \lambda\alpha_{nm} + \alpha'_{nm} \end{pmatrix}$$

$$\begin{aligned}
&= \psi((1, \dots, 0), (\lambda\alpha_{11} + \alpha'_{11} + \dots + \lambda\alpha_{1m} + \alpha'_{1m})) \\
&+ \dots + \psi((0, \dots, 1), (\lambda\alpha_{n1} + \alpha'_{n1} + \dots + \lambda\alpha_{nm} + \alpha'_{nm})) \\
&= \psi((1, \dots, 0), \lambda(\alpha_{11}, \dots, \alpha_{1m}) + (\alpha'_{11}, \dots, \alpha'_{1m})) \\
&+ \dots + \psi((0, \dots, 1), \lambda(\alpha_{n1}, \dots, \alpha_{nm}) + (\alpha'_{n1}, \dots, \alpha'_{nm})) \\
&= \lambda\psi((1, \dots, 0), (\alpha_{11}, \dots, \alpha_{1m})) + \psi((1, \dots, 0), (\alpha'_{11}, \dots, \alpha'_{1m})) \\
&+ \dots + \lambda\psi((0, \dots, 1), (\alpha_{n1}, \dots, \alpha_{nm})) + \psi((0, \dots, 1), (\alpha'_{n1}, \dots, \alpha'_{nm})) \\
&= \lambda[\psi((1, \dots, 0), (\alpha_{11}, \dots, \alpha_{1m})) + \dots + \psi((0, \dots, 1), (\alpha_{n1}, \dots, \alpha_{nm}))] \\
&+ [\psi((1, \dots, 0), (\alpha'_{11}, \dots, \alpha'_{1m})) + \dots + \psi((0, \dots, 1), (\alpha'_{n1}, \dots, \alpha'_{nm}))] \\
&= \lambda f \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix} + f \begin{pmatrix} \alpha'_{11} & \cdots & \alpha'_{1m} \\ \vdots & & \vdots \\ \alpha'_{n1} & \cdots & \alpha'_{nm} \end{pmatrix}.
\end{aligned}$$

Finalmente,

$$\begin{aligned}
(f \circ \beta)((x_1, \dots, x_n), (y_1, \dots, y_m)) &= f \begin{pmatrix} x_1 y_1 & \cdots & x_1 y_m \\ \vdots & & \vdots \\ x_n y_1 & \cdots & x_n y_m \end{pmatrix} \\
&= \psi((1, 0, \dots, 0), (x_1 y_1, \dots, x_1 y_m)) + \dots + \psi(0, 0, \dots, 1), (x_n y_1, x_n y_m) \\
&= \psi((1, 0, \dots, 0), (x_1 y_1, \dots, x_1 y_m)) + \dots + \psi(0, 0, \dots, 1), (x_n y_1, x_n y_m) \\
&= \psi((1, 0, \dots, 0), x_1(y_1, \dots, y_m)) + \dots + \psi(0, 0, \dots, 1), x_n(y_1, \dots, y_m) \\
&= x_1\psi((1, 0, \dots, 0), (y_1, \dots, y_m)) + \dots + x_n\psi((0, 0, \dots, 1), (y_1, \dots, y_m)) \\
&= \psi(x_1(1, 0, \dots, 0), (y_1, \dots, y_m)) + \dots + \psi(x_n(0, 0, \dots, 1), (y_1, \dots, y_m)) \\
&= \psi((x_1, 0, \dots, 0), (y_1, \dots, y_m)) + \dots + \psi((0, 0, \dots, x_n), (y_1, \dots, y_m)) \\
&= \psi((x_1, 0, \dots, 0) + \dots + (0, x_n), (y_1, \dots, y_m)) \\
&= \psi((x_1, \dots, x_n), (y_1, \dots, y_m)),
\end{aligned}$$

luego, $f \circ \beta = \psi$ y así, $(M_{n \times m}(\mathbb{R}), \beta)$ es un producto tensorial para \mathbb{R}^n y \mathbb{R}^m .

Teorema 2.2.6. *Sea A una k -álgebra central simple. Si B es una k -álgebra simple, entonces $A \otimes_k B$ es una $Z(B)$ -álgebra central simple, es decir, $Z(B) = k$.*

Demostración. Cada $x \in A \otimes_k B$ tiene una expresión de la forma.

$$x = a_1 \otimes b_1 + \dots + a_n \otimes b_n \tag{2.1}$$

donde $a_i \in A$ y $b_i \in B$. Para $x \neq 0$, se define la longitud de x como el menor n que cumple la condición anterior.

Si x tiene longitud n , es decir, si (2.1) es la expresión más corta, entonces b_1, \dots, b_n son linealmente independiente en B (vistos como espacio vectorial sobre k). De lo contrario, si se supone que b_1, \dots, b_n no son linealmente independientes, entonces existen coeficientes $u_i \in k, u_i \neq 0$, tales que

$$b_j = \sum_{i \neq j} u_i b_i$$

y sustituyendo en la expresión de x y reagrupando términos, se llega a una contradicción, en efecto,

$$\begin{aligned} x &= \sum_{i=1}^n a_i \otimes b_i \\ &= \left(\sum_{i \neq j} a_i \otimes b_i \right) + a_j \otimes b_j. \end{aligned}$$

Sustituyendo $b_j = \sum_{i \neq j} u_i b_i$, se tiene que,

$$\begin{aligned} x &= \sum_{i \neq j} a_i \otimes b_i + a_j \otimes \left(\sum_{i \neq j} u_i b_i \right) \\ &= \sum_{i \neq j} a_i \otimes b_i + \sum_{i \neq j} a_j u_i \otimes b_i, \end{aligned}$$

y agrupando los términos con el mismo b_i para $i \neq j$, se tiene que:

$$x = \sum_{i \neq j} (a_i + a_j u_i) \otimes b_i.$$

Y así, se tiene una nueva expresión para x con $n - 1$ términos, lo que contradice la minimalidad de la longitud de x .

Sea $I \neq \{0\}$ un ideal bilateral en $A \otimes_k B$. Sea $x \in I$ con $x \neq 0$ y supongamos que (1) es la expresión más corta para x . Note que $a_1 \neq 0$. Como Aa_1A es un ideal bilateral en A , por simplicidad se tiene que $A = Aa_1A$. Luego, existen elementos a'_p y a''_p en A con

$1 = \sum_p a'_p a_1 a''_p$. Como I es un ideal bilateral, entonces

$$\begin{aligned} x' &= x \sum_p a'_p a_i a''_p \\ &= \sum_p a'_p x a''_p \\ &= 1 \otimes b_1 + c_2 \otimes b_2 + \cdots + c_n \otimes b_n \end{aligned} \quad (2.2)$$

donde $x' \in I, i \geq 2$, y $c_i = \sum_p a'_p a_i a''_p$.

Para cada $a \in A$, se tiene que $(a \otimes 1)x' - x'(a \otimes 1) \in I$.

Ahora

$$(a \otimes 1)x' - x'(a \otimes 1) = \sum_{i \geq 2} (ac_i - c_i a) \otimes b_i. \quad (2.3)$$

Note que este elemento es 0, para que no sea un elemento en I de longitud menor que la longitud de x . Como b_1, \dots, b_n son linealmente independientes, entonces generan el subespacio

$$\langle b_1, \dots, b_n \rangle = \langle b_1 \rangle \oplus \cdots \oplus \langle b_n \rangle$$

y así,

$$A \otimes_k \langle b_1, \dots, b_n \rangle = A \otimes_k \langle b_1 \rangle \oplus \cdots \oplus A \otimes_k \langle b_n \rangle$$

De (3) cada término $(ac_i - c_i a) \otimes b_i = 0$. De ahí que, $ac_i = c_i a$ para todo $a \in A$, es decir, cada $c_i \in C(A) = k$. (2) se convierte en

$$\begin{aligned} x' &= 1 \otimes b_1 + c_2 \otimes b_2 + \cdots + c_n \otimes b_n \\ &= 1 \otimes b_1 + 1 \otimes c_2 b_2 + \cdots + 1 \otimes c_n b_n \\ &= 1 \otimes (b_1 + c_2 b_2 + \cdots + c_n b_n). \end{aligned}$$

Ahora, $b_1 + c_2 b_2 + \cdots + c_n b_n \neq 0$, dado que b_1, \dots, b_n son linealmente independientes, y así $x' \neq 0$, luego, I contiene un elemento distinto de 0 de la forma $1 \otimes b$. Por simplicidad de B , $BbB = B$, y así, existen $b'_q, b''_q \in B$ con $1 = \sum_p b'_q b b''_q$, luego,

$$\sum_q (1 \otimes b'_q)(1 \otimes b)(1 \otimes b''_q) = 1 \otimes 1 \in I,$$

es decir, I contiene una unidad en $A \otimes_k B$. Por lo tanto, $I = A \otimes_k B$ y $A \otimes_k B$ es simple. Para determinar el centro de $A \otimes_k B$. Primero se verifica que $Z(A) \otimes_k Z(B) = k \otimes_k Z(B) \subseteq$

$Z(A \otimes_k B)$.

Sea $a' \otimes b' \in C(A) \otimes_k C(B)$, con $a' \in C(A)$ y $b' \in C(B)$ y sea $a \otimes b \in A \otimes_k B$, entonces:

$$(a' \otimes b')(a \otimes b) = (a'a) \otimes (b'b)$$

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$$

Como $a' \in C(A)$, $a'a = aa'$ para todo $a \in A$ y como $b' \in C(B)$, $b'b = bb'$, para todo $b \in B$. Por lo tanto, $(a'a) \otimes (b'b) = (aa') \otimes (bb')$, luego, $a' \otimes b'$ conmuta con todos los elementos de la forma $a \otimes b$. Por tanto, $C(A) \otimes_k C(B) = k \otimes_k C(B) \subseteq C(A \otimes_k B)$.

Ahora, sea $z \in C(A \otimes_k B)$ con $z \neq 0$ y sea

$$z = a_1 \otimes b_1 + \cdots + a_n \otimes b_n,$$

la expresión más corta para z , donde b_1, \dots, b_n son linealmente independientes sobre k . Para cada $a \in A$, se tiene que,

$$\begin{aligned} 0 &= (a \otimes 1)z - z(a \otimes 1) \\ &= \sum_i (aa_i - a_i a) \otimes b_i, \end{aligned}$$

luego, $(aa_i - a_i a) \otimes b_i = 0$ para cada i . Por tanto, $aa_i - a_i a = 0$ y así, $aa_i = a_i a$ para todo $a \in A$ y cada $a_i \in C(A) = k$, y así $z = 1 \otimes x$, donde

$$x = a_1 b_1 + \cdots + a_n b_n \in B.$$

Como $b \in B$, entonces,

$$\begin{aligned} 0 &= z(1 \otimes b) - (1 \otimes b)z \\ &= (1 \otimes x)(1 \otimes b) - (1 \otimes b)(1 \otimes x) \\ &= 1 \otimes (xb - bx), \end{aligned}$$

luego, $xb - bx = 0$ y $x \in Z(B)$. Por lo tanto, $z \in k \otimes_k Z(B) = Z(A) \otimes_k Z(B)$. \square

Lema 2.2.7. Sea k un cuerpo, sea B una k -álgebra simple y sea A una k -álgebra central simple. Si existen homomorfismo de funciones $f, g : B \rightarrow A$, entonces A es un (B, A) -bimódulo, y también un $(B \otimes_k A^{op})$ -módulo a la izquierda, donde $(b \otimes a') = baa'$, para todo $a, \in A$, $a' \in A^{op}$ y $b \in B$.

Demostración. La función f convierte a A en un B -módulo a la izquierda si se define la acción de $b \in B$ sobre un elemento $a \in A$ como $f(b)a$. En efecto,

I.

$$\begin{aligned}(b_1 + b_2) \cdot a &= f(b_1 + b_2)a \\ &= (f(b_1) + f(b_2))a \\ &= f(b_1)a + f(b_2)a \\ &= b_1 \cdot a + b_2 \cdot a,\end{aligned}$$

para cada $b_1, b_2 \in B$ y $a \in A$.

II.

$$\begin{aligned}b \cdot (a_1 + a_2) &= f(b)(a_1 + a_2) \\ &= f(b)a_1 + f(b)a_2 \\ &= b \cdot a_1 + b \cdot a_2,\end{aligned}$$

para cada $a_1, a_2 \in A$ y $b \in B$.

III.

$$\begin{aligned}(b_1 b_2) \cdot a &= f(b_1 b_2)a \\ &= f(b_1)(f(b_2)a) \\ &= b_1 \cdot (b_2 \cdot a),\end{aligned}$$

para cada $b_1, b_2 \in B$ y $a \in A$.

IV.

$$\begin{aligned}(\lambda b) \cdot a &= f(\lambda b)a \\ &= \lambda f(b)a \\ &= \lambda(b \cdot a),\end{aligned}$$

para cada $b \in B, a \in A$ y $\lambda \in k$.

Por lo tanto, A es un B -módulo a la izquierda.

Ahora, consideremos la multiplicación usual a derecha de A sobre sí mismo,

$$x \cdot a := xa,$$

para todo $x, a \in A$.

Note que esta acción es asociativa y compatible con con la acción a izquierda de B , en efecto,

$$\begin{aligned} (b \cdot x) \cdot a &= f(b)xa \\ &= f(b)(xa) \\ &= b \cdot (x \cdot a), \end{aligned}$$

para todo $b \in B$ y $x, a \in A$, por tanto, A es un (B, A) -bimódulo. Luego, el (B, A) -bimódulo puede verse como un $(B \otimes_k A^{op})$ -módulo a la izquierda, donde la acción viene dada por,

$$\begin{aligned} (b \cdot a') \cdot x &:= b \cdot x \cdot a' \\ &= f(b)xa \end{aligned}$$

donde $a' \in A^{op}$.

Esta acción define una estructura de módulo a la izquierda sobre $(B \otimes_k A^{op})$.

Si $b_1, b_2 \in B, a'_1, a'_2 \in A^{op}$, y $x \in A$, entonces

$$\begin{aligned} ((b_1 \otimes a'_1)(b_2 \otimes a'_2)) \cdot x &= (b_1 b_2 \otimes a'_1 a'_2) \cdot x \\ &= f(b_1 b_2) x a_2 a_1. \end{aligned}$$

Asimismo,

$$(b_2 \otimes a'_2) \cdot x = f(b_2) x a_2,$$

y

$$\begin{aligned} (b_1 \otimes a'_1) \cdot (f(b_2) x a_2) &= f(b_1)(f(b_2) x a_2) a_1 \\ &= f(b_1 b_2) x a_2 a_1, \end{aligned}$$

por tanto,

$$((b_1 \otimes a'_1)(b_2 \otimes a'_2)) \cdot x = (b_1 \otimes a'_1) \cdot ((b_2 \otimes a'_2) \cdot x),$$

y así, la acción es compatible con el producto.

I.

$$\begin{aligned}((b_1 + b_2) \otimes a') \cdot x &= f(b_1 + b_2)xa \\ &= (f(b_1) + f(b_2))xa \\ &= f(b_1)xa + f(b_2)xa \\ &= (b_1 \otimes a') \cdot x + (b_2 \otimes a') \cdot x.\end{aligned}$$

II.

$$\begin{aligned}(b \otimes (a'_1 + a'_2)) \cdot x &= f(b)x(a_1 + a_2) \\ &= f(b)xa_1 + f(b)xa_2 \\ &= (b \otimes a'_1) \cdot x + (b \otimes a'_2) \cdot x.\end{aligned}$$

III. Sea $\lambda \in k$, luego

$$\begin{aligned}(\lambda(b \otimes a')) \cdot x &= (\lambda b \otimes a') \cdot x \\ &= f(\lambda b)xa \\ &= \lambda f(b)xa \\ &= \lambda((b \otimes a') \cdot x).\end{aligned}$$

IV. Sean $x_1, x_2 \in A, \lambda \in k$, entonces

a)

$$\begin{aligned}(b \otimes a') \cdot (x_1 + x_2) &= f(b)(x_1 + x_2)a \\ &= f(b)x_1a + f(b)x_2a \\ &= (b \otimes a') \cdot x_1 + (b \otimes a') \cdot x_2\end{aligned}$$

b)

$$\begin{aligned}(b \otimes a') \cdot (\lambda x) &= f(b)(\lambda x)a \\ &= \lambda((b \otimes a') \cdot x).\end{aligned}$$

Y así, se tiene que esta acción es bilineal y lineal en $x \in A$. Por consiguiente, A es un módulo a la izquierda sobre $B \otimes A^{op}$. \square

Siguiendo las definiciones y resultados descritos anteriormente, se introduce el siguiente teorema.

Teorema 2.2.8. El Teorema de Skolem-Noether. *Sea k un cuerpo, sea B una k -álgebra simple, y sea A una k -álgebra central simple. Si existen homomorfismos de funciones $f, g : B \rightarrow A$, entonces existe una unidad $u \in A$ con,*

$$g(b) = uf(b)u^{-1},$$

para todo $b \in B$.

Demostración. Por el Lema 2.2.7, se tiene que la función f convierte a A en un B -módulo a la izquierda si se define la acción de $b \in B$ sobre un elemento $a \in A$ como $f(b)a$. Luego, esta acción convierte a A en un (B, A) -bimódulo. El (B, A) -bimódulo es un $(B \otimes_k A^{op})$ -módulo a la izquierda, donde $(b \otimes a') = ba a'$, para todo $a \in A$ (ver Lema 2.2.7). A esto se le va a denotar como ${}_f A$. Análogamente, g convierte a A en un $(B \otimes_k A^{op})$ -módulo a la izquierda y se denota por ${}_g A$. Por el Teorema 2.2.6, $B \otimes_k A^{op}$ es una k -álgebra simple. Ahora

$$[{}_f A : k] = [A : k] = [{}_g A : k],$$

luego, ${}_f A \cong {}_g A$ como $(B \otimes_k A^{op})$ -módulos, gracias a la Proposición 2.1.13. Si $\varphi : {}_f A \rightarrow {}_g A$ es un $(B \otimes_k A^{op})$ -isomorfismo, entonces

$$\varphi(f(b)aa') = \varphi(f(b))\varphi(a)a'$$

$$\varphi(f(b)aa') = g(b)\varphi(a)a' \tag{2.4}$$

para todo $b \in B$ y $a, a' \in A$. Como φ es un automorfismo de A como módulo derecho sobre sí mismo, $\varphi(a) = \varphi(1a) = ua$, donde $u = \varphi(1) \in A$. Para probar que u es una unidad, note que $\varphi^{-1}(a) = u'a$ para todo $a \in A$. Luego, $a = \varphi(\varphi^{-1}(a)) = \varphi(u'a) = uu'a$ para todo $a \in A$; en particular, cuando $a = 1$, se tiene que $1 = uu'$. La ecuación $\varphi^{-1}\varphi = 1_A$ da $1 = u'u$. Sustituyendo en (2.4), se tiene que

$$\begin{aligned} uf(b)a &= \varphi(f(b)a) \\ &= g(b)\varphi(a) \\ &= g(b)ua \end{aligned}$$

para cada $a \in A$. En particular, si $a = 1$, entonces $uf(b) = g(b)u$ y $g(b) = uf(b)u^{-1}$. \square

Corolario 2.2.9. *Sea k un cuerpo. Si ψ es un automorfismo de $M_n(k)$, entonces existe una matriz invertible $P \in M_n(k)$ tal que*

$$\psi(T) = PTP^{-1}$$

Demostración. Sea $A = M_n(k)$. $M_n(k)$ es una k -álgebra central simple (ver Ejemplo 2.1.3). Como ψ es un automorfismo, entonces $B = M_n(k)$ y por el Teorema de Skolem-Noether $\psi(T) = PTP^{-1}$, de ahí que P es una matriz invertible. \square

3. Anillos Graduados y Buenas graduaciones

Para este capítulo se abordará la definición de anillos graduados. De esta manera, se definirán los anillos graduados y fuertemente graduados. En lo que sigue, se va a considerar k un cuerpo, G un grupo y se denotará por $e_{i,j}$ a las matrices con 1_k en la posición (i, j) y 0_K en las demás posiciones.

3.1. Anillos Graduados

En esta sección se presentarán la definición de un anillo G -graduado y algunos resultados correspondientes a los anillos G -graduados.

Definición 3.1.1. Sea G un grupo con identidad $e \in G$. Un anillo R se dice **G -graduado** si existe una familia $\{R_g \mid g \in G\}$ de, subgrupos aditivos R_g de R , lo que es lo mismo que \mathbb{Z} -submódulos tal que,

I. $R = \bigoplus_{g \in G} R_g$,

II. $R_g R_h \subseteq R_{gh}$ para todo $g, h \in G$, donde $R_g R_h$ denota el conjunto de todas las sumas finitas de elementos de la forma $x \cdot y$ con $x \in R_g$ y $y \in R_h$.

Si $R_g R_h = R_{gh}$, para todos $g, h \in G$, se dice que R es **fuertemente graduado** por G .

Notación 3.1.2. Sea R un anillo, el conjunto $h(R) = \bigcup_{g \in G} R_g$ denota el conjunto de elementos homogéneos de R y el conjunto $U^{gr}(R) = \bigcup_{g \in G} (U(R) \cap R_g)$ denota al conjunto de elementos invertibles homogéneos de R .

Definición 3.1.3. Un elemento no nulo $x \in R_g$ es llamado **elemento homogéneo** de grado g y se denota $grad(x) = g$. Además, un elemento $r \in R$ tiene descomposición única como $r = \sum_{g \in G} r_g$ con $r_g \in R_g$ para todo $g \in G$, donde dicha suma es finita, es decir, casi todos los r_g son cero.

Proposición 3.1.4. Sea $R = \bigoplus_{g \in G} R_g$ un anillo G -graduado. Entonces:

I. $1_R \in R_e$ y R_e es un subanillo de R .

II. Si $r \in U(R)$ es un elemento homogéneo, entonces r^{-1} es un elemento homogéneo.

III. R es un anillo fuertemente graduado, sí y solo sí, $1_R \in R_g R_{g^{-1}}$ para cualquier $g \in G$.

Demostración. (I): Sea $a, b \in R_e$, dado que R_e es un subgrupo aditivo de R se tiene que $a - b \in R_e$ y $a \cdot b \in R_e R_e \subseteq R_e$ pues R es un anillo graduado, por tanto, R_e es un subanillo de R . Sea $1_R = \sum_{g \in G} r_g$ la descomposición de 1_R con $r_g \in R_g$ entonces, para cualquier $s_h \in R_h$, con $h \in G$, se tiene que $s_h = s_h \cdot 1_R = \sum_{g \in G} s_h \cdot r_g$, con $s_h, r_g \in R_{gh}$, desde que la descomposición de s_h como suma finita es única, entonces $s_h \cdot r_g = 0$ para cualquier $g \neq e$, es decir,

$$\begin{aligned} r_e &= 1_R \cdot r_e \\ &= \sum_{g \in G} r_g \cdot r_e \\ &= \sum_{g \in G} r_g \\ &= 1_R. \end{aligned}$$

Por lo tanto, $1_R = r_e \in R_e$.

(II). Sea $r \in U(R) \cap R_h$. Si $r^{-1} = \sum_{g \in G} (r^{-1})_g \in R_g$, entonces $1_R = r \cdot r^{-1} = \sum_{g \in G} r \cdot (r^{-1})_g$. Puesto que $1_R \in R_e$ y $r \cdot (r^{-1})_g \in R_{hg}$, se sigue que $r \cdot (r^{-1})_g = 0$ para cualquier $g \neq h^{-1}$ y dado que $r \in U(R)$, se tiene que $(r^{-1})_g \neq 0$ para $g = h^{-1}$, por lo anterior $r^{-1} = (r^{-1})_{h^{-1}}$.

(III). Si R es un anillo fuertemente graduado, entonces $R_g R_{g^{-1}} = R_e$ para todo $g \in G$ y por el item anterior $1 \in R_e = R_g R_{g^{-1}}$.

Recíprocamente, puesto que R es un anillo G -graduado, se tiene que $R_e R_{gh}$, por otra parte, si $x \in R_e$, por hipótesis, se tiene que $x = x \cdot 1 \in R_e R_g R_{g^{-1}} \subseteq R_g R_{g^{-1}}$, de ahí que, se concluye la igualdad. Por las pruebas anteriores, se tiene que

$$\begin{aligned} R_{gh} &= R_e R_{gh} \\ &= (R_g R_{g^{-1}}) R_{gh} \\ &= R_g (R_{g^{-1}} R_{gh}), \end{aligned}$$

por lo tanto, R es fuertemente graduado. □

El siguiente resultado prueba que el grado de los elementos idempotentes de un anillo conicida con el elemento neutro del grupo.

Proposición 3.1.5. *Sea R un anillo G -graduado y $0 \neq r \in R$ un elemento homogéneo idempotente, entonces $\text{grad}(r) = e$.*

Demostración. En efecto, puesto que r es un elemento homogéneo existe $g \in G$ tal que $r \in R_g$, además, por ser r idempotente

$$r = r \cdot r \in R_g R_g \subseteq R_{g^2}$$

y por ser R una suma directa se tiene que $R_g = R_{g^2}$, esto implica que $g = g^2$, es decir, g es un elemento idempotente del grupo, pero el único elemento idempotente de un grupo es el elemento neutro, así $g = e$. \square

Ejemplo 3.1.6. Un anillo R puede ser un anillo G -graduado si se considera la graduación trivial dada por $R_e = R$ y $R_g = 0$, para todo $g \in G$ con $g \neq e$.

Ejemplo 3.1.7. Si A es un anillo, entonces el anillo de polinomios $R = A[x]$ es un anillo \mathbb{Z} -graduado con la graduación estándar $R_n = AX^n$ para $n \geq 0$ y $R_n = 0$ para $n < 0$. Además, R no es un anillo fuertemente graduado, pues $R_{18} \not\subseteq R_{-3}R_{-6} = 0$.

Ejemplo 3.1.8. Sea A un anillo y $R = M_3(A)$ su anillo de matrices de orden 3 y con entradas en A , donde el componente A dentro de la matriz indica que cada elemento de la matriz proviene del conjunto de elementos del anillo, entonces

$$R_0 = \begin{bmatrix} A & A & 0 \\ A & A & 0 \\ 0 & 0 & A \end{bmatrix} \text{ y } R_1 = \begin{bmatrix} 0 & 0 & A \\ 0 & 0 & A \\ A & A & 0 \end{bmatrix}$$

es una \mathbb{Z}_2 -graduación en R . Además,

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Note que $1_R \in R_1 R_1$ y por definición de R_0 se tiene que $1_R \in R_0 R_0$, es decir, $1_R \in R_g R_{g^{-1}}$ para todo $g \in \mathbb{Z}_2$, luego, de la Proposición 3.1.4, concluimos que R es fuertemente graduado.

3.2. Graduaciones por grupos cíclicos

En esta sección, se van a considerar \mathbb{Z}_m -graduaciones del anillo de matrices $M_n(k)$ para cualesquiera m, n enteros positivos. Así mismo, se abordarán las definiciones de raíz m -ésima de unidad, raíz primitiva m -ésima de unidad y la definición de buena graduación.

Definición 3.2.1. Sea $m \in \mathbb{Z}^+$. Se dice que un elemento $\xi \in k$ es una raíz m -ésima de unidad si se cumple que:

$$\xi^m = 1.$$

El conjunto de todas la raíces m -ésimas de unidad en k se denota:

$$\mu_m(k) := \{\xi \in k \mid \xi^m = 1\}.$$

Definición 3.2.2. Una raíz m -ésima de la unidad ξ se dice que es **primitiva** si su orden multiplicativo es exactamente m , es decir:

$$\xi^m = 1 \text{ y } \xi^l \neq 1 \text{ para todo } 1 \leq l < m.$$

Proposición 3.2.3. Sea $\xi \in k$ un raíz primitiva m -ésima de la unidad y $s \neq 0 \in \mathbb{Z}_m$, entonces,

$$1 + \xi^s + \xi^{2s} + \dots + \xi^{(m-1)s} = 0.$$

Demostración. Sea $S = \sum_{k=0}^{m-1} \xi^{ks}$ y $q = \xi^s$. Para $q \neq 1$ se tiene que,

$$\begin{aligned} S &= \frac{1 - q^m}{1 - q} \\ &= \frac{1 - (\xi^s)^m}{1 - \xi^s} \\ &= \frac{1 - \xi^{sm}}{1 - \xi^s}. \end{aligned}$$

Como $\xi^m = 1$, entonces

$$\begin{aligned} \xi^{sm} &= (\xi^m)^s \\ &= 1^s \\ &= 1, \end{aligned}$$

y por lo tanto,

$$\begin{aligned} S &= \frac{1 - 1}{1 - \xi^s} \\ &= \frac{0}{1 - \xi^s} \\ &= 0, \end{aligned}$$

y así, $1 + \xi^s + \xi^{2s} + \dots + \xi^{(m-1)s} = 0$. □

Teorema 3.2.4. Sea $R = M_n(k)$, donde k es cuerpo que contiene una raíz primitiva m -ésima de unidad ξ , entonces una \mathbb{Z}_m -graduación de R es de la forma

$$R_i = \{A + \xi^{-i} X A X^{-1} + \dots + \xi^{-(m-1)i} X^{m-1} A X^{-m+1} \mid A \in M_n(K)\},$$

donde $X \in GL_n(k)$ con $X^m \in kI_n$.

Demostración. Sea $R = \bigoplus_{i \in \mathbb{Z}_m} R_i$ una \mathbb{Z}_m -graduación de $M_n(k)$. Se define la siguiente función $\varphi : R \rightarrow R$ por $\varphi(A) = \sum_{i \in \mathbb{Z}_m} \xi^i A_i$, donde $A = \bigoplus_{i \in \mathbb{Z}_m} A_i$ para cualquier $A \in R$. Se mostrará que φ es un automorfismo. En efecto,

I. φ está bien definida pues cada $A_i \in M_n(k)$, de ahí que $\sum_{i \in \mathbb{Z}_m} \xi^i A_i \in M_n(k)$. Por otro lado, cada matriz tiene una descomposición única en términos de los A_i , y así, φ está bien definida.

II. Sean $A, B \in M_n(k)$ y $\lambda \in k$, entonces:

$$\begin{aligned} \varphi(A + B) &= \sum_{i \in \mathbb{Z}_m} \xi^i (A_i + B_i) \\ &= \sum_{i \in \mathbb{Z}_m} \xi^i A_i + \sum_{i \in \mathbb{Z}_m} \xi^i B_i \\ &= \varphi(A) + \varphi(B), \end{aligned}$$

por otro lado,

$$\begin{aligned} \varphi(\lambda A) &= \sum_{i \in \mathbb{Z}_m} \xi^i (\lambda A_i) \\ &= \lambda \sum_{i \in \mathbb{Z}_m} \xi^i A_i \\ &= \lambda \varphi(A), \end{aligned}$$

así, φ es lineal.

III. Sean $A, B \in M_n(k)$, entonces

$$\begin{aligned}
 \varphi(AB) &= \sum_{l \in \mathbb{Z}_m} \xi^l (AB)_l \\
 &= \sum_{l \in \mathbb{Z}_m} \xi^l \left(\sum_{i+j=l} A_i B_j \right) \\
 &= \sum_{i,j \in \mathbb{Z}_m} \xi^{i+j} A_i B_j \\
 &= \left(\sum_i \xi^i A_i \right) \left(\sum_j \xi^j B_j \right) \\
 &= \varphi(A)\varphi(B).
 \end{aligned}$$

IV. Sea $\varphi(A) = 0$, entonces

$$\sum_{i \in \mathbb{Z}_m} \xi^i A_i = 0$$

Como cada uno de los A_i proviene de una descomposición única en componentes, y los coeficientes ξ^i son linealmente independientes sobre k , entonces cada $A_i = 0$, luego, $A = 0$ y así φ es inyectiva.

V. Note que φ es una transformación lineal entre dos espacios $(M_n(k))$ de la misma dimensión finita n^2 . Como $\ker(\varphi) = \{0\}$, se tiene que $\dim \ker(\varphi) = 0$, luego, $\dim \operatorname{Im}(\varphi) = n^2$ y como $\operatorname{Im}(\varphi) \subseteq M_n(k)$, y tiene dimensión máxima, entonces $\operatorname{Im}(\varphi) = M_n(k)$ y así, φ es sobreyectiva. Por lo tanto, φ es un automorfismo.

Luego, por el Teorema de Skolem-Noether existe una matriz invertible X tal que $\varphi(A) = XAX^{-1}$ para todo $A \in R$. Como φ^m es la identidad sobre $R = M_n(k)$, entonces $\varphi^m(A) = X^m AX^{-m} = A$ para todo $A \in R$, luego, $X^m \in Z(M_n(k))$ y así, $X^m = aI_n$ para algún $a \in k^*$.

Note que para $j \in \mathbb{Z}_m$ se cumple que

$$A_j = \frac{1}{m} (A + \xi^{-j} XAX^{-1} + \dots + \xi^{-(m-1)j} X^{m-1} AX^{-m+1}),$$

para cualquier $0 \leq i \leq m-1$.

En efecto, se consideran dos casos. Si $i = j$, se tiene que

$$\begin{aligned}
& \xi^{-j \cdot 0} \xi^{0 \cdot i} A_j + \xi^{-j} \xi^i A_j + \xi^{-j \cdot 2} \xi^{2i} A_j + \dots + \xi^{-j \cdot (m-1)} \xi^{i \cdot (m-1)} A_j \\
&= \xi^{-j \cdot 0} \xi^{0 \cdot j} A_j + \xi^{-j} \xi^j A_j + \xi^{-j \cdot 2} \xi^{2 \cdot j} A_j + \dots + \xi^{-j \cdot (m-1)} \xi^{j \cdot (m-1)} A_j \\
&= \xi^{0 \cdot (j-j)} A_j + \xi^{1 \cdot (j-j)} A_j + \xi^{2 \cdot (j-j)} A_j + \dots + \xi^{(m-1) \cdot (j-j)} A_j \\
&= \xi^0 A_j + \xi^0 A_j + \xi^0 A_j + \dots + \xi^0 A_j \\
&= A_j + A_j + A_j + \dots + A_j \\
&= mA_j.
\end{aligned}$$

Si $i \neq j$, entonces,

$$\begin{aligned}
& \xi^{-j \cdot 0} \xi^{0 \cdot i} A_i + \xi^{-j} \xi^i A_i + \xi^{-j \cdot 2} \xi^{2i} A_i + \dots + \xi^{-j \cdot (m-1)} \xi^{i \cdot (m-1)} A_i \\
&= \xi^{-j \cdot 0} \xi^{0 \cdot j} A_i + \xi^{-j} \xi^j A_i + \xi^{-j \cdot 2} \xi^{2 \cdot j} A_i + \dots + \xi^{-j \cdot (m-1)} \xi^{j \cdot (m-1)} A_i \\
&= \xi^{0 \cdot (i-j)} A_i + \xi^{1 \cdot (i-j)} A_i + \xi^{2 \cdot (i-j)} A_i + \dots + \xi^{(m-1) \cdot (i-j)} A_i.
\end{aligned}$$

Sea $i - j = s$, entonces

$$\xi^{0 \cdot s} A_i + \xi^{1 \cdot s} A_i + \xi^{2 \cdot s} A_i + \dots + \xi^{(m-1) \cdot s} A_i = A_i (1 + \xi^s + \xi^{2s} + \dots + \xi^{(m-1)s}),$$

donde $1 + \xi^s + \xi^{2s} + \dots + \xi^{(m-1)s} = 0$ por la Proposición 3.2.3. Sea $x_i = mA_i$ donde $1 \leq j \leq i$, entonces,

$$\sum_{i=0}^{m-1} x_i = x_0 + x_1 + \dots + x_j + \dots + x_{m-1} = x_j = mA_j$$

pues para $i \neq j$, $x_i = 0$. Por lo tanto,

$$A + \xi^{-j} \varphi(A) + \xi^{-2j} \varphi^2(A) + \dots + \xi^{-(m-1)j} \varphi^{m-1}(A) = mA_j$$

$$A_j = \frac{1}{m} (A + \xi^{-j} XAX^{-1} + \dots + \xi^{-(m-1)j} X^{m-1} AX^{-m+1}).$$

□

Observación 3.2.5. Sea X una matriz en $M_n(k)$ tal que $X^m = aI_n$ para algún $a \in k^*$ y $Y = bX$ para algún $b \in k^*$. Entonces $Y^m = b^m X^m = (b^m a)I_n$ y $C_i(X) = C_i(Y)$, donde,

$$C_i(X) = \{A \in M_n(K) \mid XA = \xi^i AX\},$$

y

$$C_i(Y) = \{A \in M_n(K) \mid YA = \xi^i AY\}$$

para todo $0 \leq i \leq m - 1$.

Note que para cualquier $A \in M_n(k)$ se tiene lo siguiente

$$YA = \xi^i AY.$$

Y, sustituyendo $Y = bX$, se tiene que,

$$bXA = \xi^i AbX$$

que se puede reordenar como

$$XA = \xi^i AX,$$

por tanto, para cada i , la condición para que $A \in C_i(Y)$ es la misma que la condición para que $A \in C_i(X)$.

Por lo tanto X y Y inducen a la misma \mathbb{Z}_m -graduación de $M_n(k)$. En particular, si k contiene una raíz m -ésima b de a , entonces existe una matriz Y tal que $Y^m = I_n$, y X y Y conducen a la misma \mathbb{Z}_m -graduación.

Definición 3.2.6. Se dice que una G -graduación de la k -álgebra $M_n(k)$ es **buena** si todas las matrices $e_{i,j}$ son elementos homogéneos.

Ejemplo 3.2.7. Sea $R = M_2(k)$ y $G = C_2 = \{e, g\}$. Consideremos la siguiente G -graduación sobre R :

$$R_e = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in k \right\}, R_g = \left\{ \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} : a, b \in k \right\}.$$

Note que esta G -graduación sobre $M_2(k)$ es una buena graduación.

En efecto, sea $A = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_2(k)$. Además, sea $A_e = \begin{bmatrix} x & 0 \\ 0 & w \end{bmatrix}$ y $A_g = \begin{bmatrix} 0 & y \\ z & 0 \end{bmatrix}$,

entonces,

$$\begin{aligned} A_e + A_g &= \begin{bmatrix} x & y \\ z & w \end{bmatrix} \\ &= A. \end{aligned}$$

Además, note que $R_e \cap R_g = \{0\}$, dado que la matriz que es simultáneamente diagonal y antidiagonal es la matriz 0 y, por lo tanto, $R = M_2(k) = R_e \oplus R_g$ como suma directa de subespacios.

I. El producto de dos matrices diagonales es diagonal, luego, $R_e R_e \subseteq R_e$.

II. Sea $A \in R_e$ y $B \in R_g$, entonces $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $B = \begin{bmatrix} 0 & c \\ d & 0 \end{bmatrix}$, entonces

$$\begin{aligned} AB &= \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} 0 & c \\ d & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & ac \\ bd & 0 \end{bmatrix} \in R_g. \end{aligned}$$

III. Sea $A \in R_e$ y $B \in R_g$, entonces, $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $B = \begin{bmatrix} 0 & c \\ d & 0 \end{bmatrix}$, entonces,

$$\begin{aligned} BA &= \begin{bmatrix} 0 & c \\ d & 0 \end{bmatrix} \cdot \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \\ &= \begin{bmatrix} 0 & cb \\ da & 0 \end{bmatrix} \in R_g. \end{aligned}$$

IV. Sea $B \in R_g$, entonces,

$$\begin{bmatrix} 0 & c \\ d & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & c' \\ d' & 0 \end{bmatrix} = \begin{bmatrix} cd' & 0 \\ 0 & dc' \end{bmatrix} \in R_e.$$

De esta manera, se tiene que $R = M_2(k)$ es una C_2 -graduación.

I. La matriz e_{11} es diagonal, por tanto, $e_{11} \in R_e$.

II. La matriz e_{22} es diagonal, por tanto, $e_{22} \in R_e$.

III. La matriz e_{12} tiene ceros en la diagonal y un valor fuera de la diagonal superior derecha, es decir, tiene la forma $\begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} \in R_g$ con $a = 1$ y $b = 0$, por lo tanto, $e_{12} \in R_g$.

IV. La matriz e_{21} tiene un valor fuera de la diagonal inferior izquierda y tiene la forma $\begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} \in R_g$ con $a = 0$ y $b = 1$, por lo tanto, $e_{12} \in R_g$.

Y así, los cuatro elementos de la base estándar $\{e_{11}, e_{12}, e_{21}, e_{22}\}$ son homogéneos y, por lo tanto, $R = M_2(k)$ es una buena C_2 -graduación.

Teorema 3.2.8. *Sea X una matriz con $X^m = aI_n$ para algún $a \in k^*$ y sea k un cuerpo que contiene una raíz m -ésima ξ de unidad, entonces $R = \bigoplus_{i=0}^{m-1} C_i(X)$ es una buena \mathbb{Z}_m -graduación de $M_n(k)$ si y sólo si X es una matriz diagonal. Además, en este caso,*

$$\alpha \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \eta_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \eta_n \end{bmatrix},$$

donde α es una raíz m -ésima de unidad de a en K y $\eta_2, \eta_3, \dots, \eta_n$ son raíces m -ésimas de unidad.

Demostración. Sea $X = (x_{ij})$ y supongamos que $R = \bigoplus_{i=0}^{m-1} C_i(X)$ es una buena \mathbb{Z}_m -graduación de $M_n(k)$, entonces $e_{ii} \in C_0(X)$ para todo $1 \leq i \leq n$. Por tanto, $Xe_{ii} = e_{ii}X$ para todo $1 \leq i \leq n$, luego, todas las entradas de la i -ésima fila y todas las entradas de la i -ésima columna de X son cero menos x_{ii} y así, X es una matriz diagonal. Recíprocamente, sea $X = (x_{ij})$ una matriz diagonal. Como $X^m = aI_n$ para algún $a \in k^*$, $x_{ii}^m = a$ para cada $i = 1, 2, \dots, n$. Sea $\eta_i = \frac{x_{ii}}{x_{11}}$ para cada $i = 2, \dots, n$, entonces $\eta_i^m = 1$ para cada $i = 1, 2, \dots, n$. Si se toma $\alpha = x_{11}$,

$$X = \alpha \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \eta_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \eta_n \end{bmatrix}.$$

Ahora, sea $Y = \alpha^{-1}X$, por la Observación 3.2.5, $C_i(X) = C_i(Y)$ para todo $0 \leq i \leq m-1$. Note que el elemento (i, j) de Ye_{ij} es η_i y el elemento (i, j) de $e_{ij}Y$ es η_j para cada

$1 \leq i, j \leq n$. Como η_i es una raíz m -ésima de unidad para cada $i = 1, 2, \dots, n$, entonces $\eta_i = \xi^l \eta_j$ para algún l , es decir, para cada $1 \leq i, j \leq n$, e_{ij} es un elemento de $C_l(X)$ para algún l y por lo tanto, $R = \bigoplus C_i(Y)$ es una buena \mathbb{Z}_m -graduación. \square

Teorema 3.2.9. *Sea Y una matriz con $Y^m = aI_n$ para algún $a \in k^*$ y sea k un cuerpo que contiene una raíz m -ésima ξ de unidad, $R = \bigoplus_{i=0}^{m-1} C_i(Y)$ es isomorfo a una buena \mathbb{Z}_m -graduación de $M_n(k)$ si y sólo si Y es la matriz diagonal.*

Demostración. Supongamos que $R = \bigoplus_{i=0}^{m-1} C_i(Y)$ es isomorfo a una buena \mathbb{Z}_m -graduación de $M_n(k)$. Sea $S = \bigoplus_{i=0}^{m-1} C_i(X)$. Note que S es una buena graduación de $M_n(k)$, pues toda buena \mathbb{Z}_m -graduación es de este tipo. Luego, existe un isomorfismo $\varphi : S = M_n(k) \rightarrow R = M_n(k)$. Por el Teorema de Skolem-Noether, existe una matriz invertible P tal que $\varphi(A) = PAP^{-1}$ para todo $A \in S$. Como $\varphi(C_0(X)) = C_0(Y)$, para cada $i = 1, 2, \dots, n$, entonces,

$$\begin{aligned} e_{ii} \in C_0(X) &\Leftrightarrow Pe_{ii}P^{-1} \in C_0(Y) \\ &\Leftrightarrow YPe_{ii}P^{-1} = Pe_{ii}P^{-1}Y \\ &\Leftrightarrow P^{-1}YPe_{ii}P^{-1} = P^{-1}Pe_{ii}P^{-1}Y \\ &\Leftrightarrow P^{-1}YPe_{ii}P^{-1} = e_{ii}P^{-1}Y \\ &\Leftrightarrow P^{-1}YPe_{ii}P^{-1}P = e_{ii}P^{-1}YP \\ &\Leftrightarrow P^{-1}YPe_{ii} = e_{ii}P^{-1}YP, \end{aligned}$$

por lo tanto, $P^{-1}YP$ es una matriz diagonal.

Recíprocamente, supongamos que existe una matriz invertible P tal que $P^{-1}YP$ es una matriz diagonal. Sea $S = \bigoplus C_i(P^{-1}YP)$, luego, se define $\varphi : R \rightarrow S$ por $\varphi(A) = P^{-1}YP$ para todo $A \in R$. φ es un automorfismo (Ver Teorema 3.2.4.) sobre $M_n(k)$ y $\varphi(C_i(Y)) = C_i(P^{-1}YP)$ para todo $i = 0, 1, \dots, m-1$. Por el Teorema 3.2.8, $S = \bigoplus C_i(P^{-1}YP)$ es una buena \mathbb{Z}_m -graduación y así, R es isomorfo a una buena graduación. \square

3.3. Graduaciones por grupos abelianos finitos

Sean G y H dos grupos finitos y $R = \bigoplus_{(g,h) \in G \times H} R_{(g,h)}$ una $(G \times H)$ -graduación de $M_n(k)$. Sea $S_g = \bigoplus_{h \in H} R_{(g,h)}$ y $T_h = \bigoplus_{g \in G} R_{(g,h)}$ para cada $g \in G$ y $h \in H$, entonces $S = \bigoplus_{g \in G} S_g$ y $T = \bigoplus_{h \in H} T_h$ son una G -graduación y H -graduación de $M_n(k)$, respectivamente. Estas graduaciones son llamadas **graduaciones asociadas a R** .

Note que $R_{(g,h)} = S_g \cap T_h$ para cada $g \in G$ y $h \in H$, luego, cada $(G \times H)$ -graduación de $M_n(k)$ inducen a una G -graduación y H -graduación natural de $M_n(k)$. No obstante, el recíproco no es cierto. Esto es, existen una G -graduación $S = \bigoplus S_g$ y una H -graduación $T = \bigoplus T_h$ de $M_n(k)$ tales que S y T no son graduaciones inducidas que son inducidas por una $(G \times H)$ -graduación de $M_n(k)$. En efecto, consideremos dos \mathbb{Z}_2 -graduaciones S y T . Sean,

$$S_0 = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in k \right\},$$

$$S_1 = \left\{ \begin{bmatrix} 0 & c \\ d & 0 \end{bmatrix} : c, d \in k \right\},$$

$$T_0 = \left\{ \begin{bmatrix} a & b-a \\ 0 & b \end{bmatrix} : a, b \in k \right\},$$

$$T_1 = \left\{ \begin{bmatrix} d & c \\ d & -d \end{bmatrix} : c, d \in k \right\},$$

$S = S_0 + S_1$ y $T = T_0 + T_1$, entonces $M_2(k) \neq S_0 \cap T_0 + S_0 \cap T_1 + S_1 \cap T_0 + S_1 \cap T_1$ y por lo tanto, $\bigoplus S_i \cap T_j$ no es una $(\mathbb{Z}_2 \times \mathbb{Z}_2)$ -graduación de $M_2(k)$, en este caso, $S_0 \cap T_0 + S_0 \cap T_1 \neq S_0$.

Para solventar lo anterior, se define la compatibilidad de dos graduaciones a continuación.

Definición 3.3.1. Sea G y H dos grupos finitos. Una G -graduación $S = \bigoplus S_g$ y una H -graduación $T = \bigoplus T_h$ de $M_n(K)$ son **compatibles** si $S_g = \bigoplus_{h \in H} (S_g \cap T_h)$ para todo $g \in G$ y $T_h = \bigoplus_{g \in G} (S_g \cap T_h)$ para todo $h \in H$.

Lema 3.3.2. Sea G y H dos grupos finitos y sean $S = \bigoplus S_g$ y $T = \bigoplus T_h$ G -graduación y H -graduación de $M_n(k)$, respectivamente, entonces S y T son compatibles si y sólo si existe una $(G \times H)$ -graduación R de $M_n(k)$ cuyos G y H -graduaciones asociados son S y T , respectivamente.

Demostración. Sea R una $(G \times H)$ -graduación de $M_n(k)$, entonces sus G y H -graduaciones son compatibles. Recíprocamente, supongamos que S y T son compatibles para cada $(g, h) \in G \times H$ y sea $R_{(g,h)} = S_g \cap T_h$, entonces $R = \bigoplus_{(g,h)} R_{(g,h)} = \bigoplus_{(g,h)} (S_g \cap T_h)$ es una $(G \times H)$ -graduación de $M_n(k)$.

En efecto, en primer lugar se tiene que $R_{(g,h)} \cdot R_{(g',h')} \subset S_{gg'} \cap T_{hh'} = R_{(gg',hh')}$. Ahora, sea $A \in S_g$. Como $S_g = \bigoplus_{h \in H} (S_g \cap T_h)$, entonces existe $A_{(g,h)} \in S_g \cap T_h$ para cada $h \in H$

tal que $A = \bigoplus_{h \in H} A_{(g,h)}$. Como cada elemento $A \in M_n(k)$ puede ser expresado como una suma de elementos en S_g , entonces cada elemento $A \in M_n(k)$ puede ser expresado como una suma de elementos en $S_g \cap T_h = R_{(g,h)}$. \square

El siguiente resultado presenta una caracterización de graduaciones compatibles.

Teorema 3.3.3. *Sean l y m dos enteros positivos y sean X y Y matrices con $X^l = bI_n$ y $Y^m = cI_n$ para algunos $b, c \in k^*$, $S = \bigoplus_{i=0}^{l-1} S_i = \bigoplus_{i=0}^{l-1} C_i(X)$ y $T = \bigoplus_{j=0}^{m-1} T_j = \bigoplus_{j=0}^{m-1} C_j(Y)$ \mathbb{Z}_l y \mathbb{Z}_m -graduaciones de $M_n(k)$, respectivamente y k que contiene una raíz primitiva l -ésima ξ y una raíz primitiva m -ésima η de unidad, entonces dos graduaciones S y T son compatibles si y sólo si $XY = aYX$ para algún $a \in k$ con $a^n = 1$.*

Demostración. Supongamos que S y T son compatibles. Sea $A \in S_i$, entonces $A = \bigoplus_{j=0}^{m-1} A_{(i,j)}$, donde $A_{(i,j)} \in S_i \cap T_j$ para cada $j = 0, 1, \dots, m-1$. Note que,

$$\begin{aligned} Y(XAX^{-1})Y^{-1} &= Y(\xi^i A)Y^{-1} \\ &= \xi^i \left(\bigoplus_{j=0}^{m-1} Y A_{(i,j)} Y^{-1} \right) \\ &= \xi^i \left(\bigoplus_{j=0}^{m-1} \eta^j A_{(i,j)} \right) \\ &= X \left(\bigoplus_{j=0}^{m-1} \eta^j A_{(i,j)} \right) X^{-1} \\ &= X(YAY^{-1})X^{-1}. \end{aligned}$$

Luego, $(YX)A(YX)^{-1} = (XY)A(XY)^{-1}$ para todo $A \in S_i$. Por tanto, $(YX)^{-1}(XY)A = A(YX)^{-1}(XY)$ para todo $A \in M_n(k)$. Como el centro de $M_n(k)$ es el conjunto $\{aI_n \mid a \in k\}$ de todas las matrices escalares de $M_n(k)$ y XY es invertible, se tiene que $(YX)^{-1}(XY) = aI_n$ para algún $a \in k^*$. Comparando los determinantes a ambos lados de $(YX)^{-1}(XY) = aI_n$, se tiene que $a^n = 1$. Recíprocamente, supongamos que $XY = aYX$ para algún $a \in k^*$. Sea $A \in S_i$ y $A = \bigoplus_{j=0}^{m-1} A_j$, donde $A_j \in T_j$ para cada $j = 0, 1, \dots, m-1$. Como $A_j = \frac{1}{m} \left(\sum_{k=0}^{m-1} \eta^{-kj} Y^k A Y^{-k} \right)$, entonces,

$$\begin{aligned} XA_jX^{-1} &= \frac{1}{m} \left(\sum_{k=0}^{m-1} \eta^{-kj} X(Y^k A Y^{-k})X^{-1} \right) \\ &= \frac{1}{m} \left(\sum_{k=0}^{m-1} \eta^{-kj} Y^k (XAX^{-1})Y^{-k} \right). \end{aligned}$$

Como $A \in S_i$, entonces $XAX^{-1} = \xi^i A$ y, por tanto, $XA_jX^{-1} = \xi^i A_j$. De ahí que, $A_j \in S_i \cap T_j$ y así $S_i \subset \bigoplus_{j=0}^{m-1} (S_i \cap T_j)$. Por otro lado, note que $\bigoplus_{j=0}^{m-1} (S_i \cap T_j) \subset S_i$ y así, $S_i = \bigoplus_{j=0}^{m-1} (S_i \cap T_j)$. Análogamente, se muestra que $T_j = \bigoplus_{i=0}^{l-1} (S_i \cap T_j)$. \square

Teorema 3.3.4. Sean l y m enteros positivos, $R = \bigoplus_{(i,j) \in \mathbb{Z}_l \times \mathbb{Z}_m} R_{(i,j)}$ una $(\mathbb{Z}_l \times \mathbb{Z}_m)$ -graduación de $M_n(k)$, $S = \bigoplus_{i=0}^{l-1} S_i$ y $T = \bigoplus_{j=0}^{m-1} T_j$ graduaciones asociadas con R tales que $S_i = C_i(X)$ donde $i = 0, 1, \dots, l-1$ y $T_j = C_j(Y)$ donde $j = 0, 1, \dots, m-1$ para algunas matrices X y Y con $X^l = bI_n$ y $Y^m = cI_n$ para algunos $b, c \in k^*$. Sea k que contiene una raíz l -ésima primitiva ξ y una raíz m -ésima primitiva η de unidad, entonces

$$R_{(i,j)} = \left\{ \frac{1}{lm} \bigoplus_{\substack{0 \leq r \leq l-1 \\ 0 \leq s \leq m-1}} \xi^{-ri} \eta^{-sj} X^r Y^s A Y^{-s} X^{-r} \mid A \in M_n(K) \right\} \\ = C_{ij}(X, Y),$$

para cada $i = 0, 1, \dots, l-1$ y $j = 0, 1, \dots, m-1$, donde

$$C_{ij}(X, Y) = \{A \in M_n(K) \mid XA = \xi^i AX, YA = \eta^j AY\}.$$

Demostración. Se sigue del Lema 3.3.2. y el Teorema 3.3.3. que si $S_i = \bigoplus_{k=0}^{l-1} R_{(i,k)}$ ($i = 0, 1, \dots, l-1$), $T_j = \bigoplus_{k=0}^{m-1} R_{(k,j)}$ ($j = 0, 1, \dots, m-1$) y $XY = aYX$ para algún $a \in k^*$ con $a^n = 1$, luego,

$$S_i = \left\{ \frac{1}{l} \bigoplus_{0 \leq r \leq l-1} \xi^{-ri} X^r A X^{-r} \mid A \in M_n(k) \right\}$$

y

$$T_j = \left\{ \frac{1}{m} \bigoplus_{0 \leq s \leq m-1} \eta^{-sj} Y^s A Y^{-s} \mid A \in M_n(k) \right\}.$$

Como $XY = aYX$, entonces $Y^s X^r A X^{-r} Y^{-s} = X^r Y^s A Y^{-s} X^{-r}$ para todo $A \in M_n(k)$ y todos los enteros r y s , se tiene que

$$R_{(i,j)} = S_i \cap T_j = \left\{ \frac{1}{l} \bigoplus_{0 \leq r \leq l-1} \xi^{-ri} X^r A X^{-r} \mid A \in T_j \right\}$$

$$R_{(i,j)} = S_i \cap T_j = \left\{ \frac{1}{m} \bigoplus_{0 \leq s \leq m-1} \eta^{-sj} Y^s A Y^{-s} \mid A \in S_i \right\}$$

$$R_{(i,j)} = S_i \cap T_j = \left\{ \frac{1}{lm} \bigoplus_{\substack{0 \leq r \leq l-1 \\ 0 \leq s \leq m-1}} \xi^{-ri} \eta^{-sj} X^r Y^s A Y^{-s} X^{-r} \mid A \in M_n(K) \right\}$$

para cada $i = 0, 1, \dots, l - 1$ y $j = 0, 1, \dots, m - 1$. □

Proposición 3.3.5. Sean G y H dos grupos finitos y sea $R = \bigoplus_{(g,h) \in G \times H} R_{(g,h)}$ una $(G \times H)$ -graduación de $M_n(k)$. Si S y T son dos graduaciones asociadas a R y además, buenas graduaciones, entonces R es una buena graduación.

Demostración. Supongamos que S y T son buenas graduaciones, entonces para cada $1 \leq i, j \leq n$, $e_{ij} \in S_g$ para algún $g \in G$, y $e_{ij} \in T_h$ para algún $h \in H$. Por lo tanto, $e_{ij} \in S_g \cap T_h$ para algún $g \in G$ y $h \in H$ y así, R es una buena graduación. □

Terminamos el trabajo con el siguiente ejemplo del resultado anterior.

Ejemplo 3.3.6. Sea $R = M_2(k)$, $G = \mathbb{Z}_2$ y $H = \mathbb{Z}_2$. Se definen las siguientes dos buenas graduaciones S y T de la siguiente manera,

- I. Para la graduación S por $G = \mathbb{Z}_2$ se define $S_0 = \langle e_{12}, e_{22} \rangle$, $S_1 = \langle e_{11}, e_{21} \rangle$. Note que cada e_{ij} está en un componente homogéneo, luego, S es una buena graduación.
- II. Para la graduación T por $H = \mathbb{Z}_2$ se define $T_0 = \langle e_{11}, e_{12} \rangle$, $T_1 = \langle e_{21}, e_{22} \rangle$. Note que las matrices de la primera fila están en grado 0, y las de la segunda fila en grado 1. Por otro lado, T es una buena graduación, pues cada e_{ij} pertenece solo a un componente.

Para cada e_{ij} , su grado R es (g, h) donde g es el grado de e_{ij} en S y h es el grado en T , luego,

I. $R_{(0,0)} = \langle e_{11} \rangle$,

II. $R_{(1,0)} = \langle e_{12} \rangle$,

III. $R_{(1,1)} = \langle e_{21} \rangle$,

IV. $R_{(0,1)} = \langle e_{22} \rangle$,

y así, cada e_{ij} están en un único componente homogéneo $R_{(g,h)}$ y, por lo tanto, R es una buena graduación por el grupo producto $(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

Bibliografía

- Bahturin, Yu. A., Sehgal, S. K., Zaicev, M. (2001). Group gradings on associative algebras. *J. Algebra* 241(2):677-698.
- Boboc, C. (2003). Gradings of matrix algebras by the Klein group. *Comm. Algebra* 31(5):2311-2326.
- Boboc, C., Dăscălescu, S. (2001). Gradings of matrix algebras by cyclic groups. *Comm Algebra* 29(11):5013-5021.
- Chun, J., Lee, J. (2007). Abelian Group Gradings on Full Matrix Rings. *Comm Algebra* 35(10):3095-3102.
- Dăscălescu, S., Ion, B., Năstăcescu, C., Rios Montes, J. (1999). Group gradings on full matrix rings. *J. Algebra* 220(2):709-728.
- Lee, G. (2018). *Abstract Algebra: An Introductory Course*. Archivo digital.
- Lezama, O. (2011a). Cuadernos de Algebra, No. 3: Módulos. Universidad Nacional de Colombia.
- Lizama, C. (2000). Producto Tensorial. *Apuntes de Álgebra III*. Universidad de Santiago de Chile.
- Orozco, L. (2020). Buenas graduaciones del anillo de matrices. [Tesis de pregrado, Universidad Industrial de Santander].
- Rotman, J. (2002). *Advanced Modern Algebra*. Prentice Hall.