BUENAS GRADUACIONES DEL ANILLO MATRICES

Laura Natalia Orozco García

Trabajo de Grado para optar al título de Matemática

Director

Héctor Edonis Pinedo Tapia

Doctor en ciencias

Universidad Industrial de Santander

Facultad de Ciencias

Escuela de Matemáticas

Bucaramanga

2020

Dedicatoria

A Dios, mis padres y Joan...

Agradecimientos

Son muchas las personas que han contribuido al proceso y conclusión de este trabajo. En primer lugar, quiero agradecer al Dr. Héctor Pinedo, director de esta tesis y mi maestro desde hace un par de años, por su apoyo, dedicación y paciencia ya que gracias a sus conocimientos y correcciones pude culminar este trabajo. Además, quiero agradecer a todos los profesores que contribuyeron a mi formación educativa con su sabiduría y conocimiento, todos ellos motivaron a desarrollarme como persona y profesional.

Quiero agradecer especialmente a mis padres quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir un sueño más. A mi hermana por su cariño y apoyo incondicional y finalmente a toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mi una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Tabla de Contenido

Lista de Apéndices

Resumen

Título: BUENAS GRADUACIONES DEL ANILLO DE MATRICES *

Autor: LAURA NATALIA OROZCO GARCÍA **

Palabras Clave: BUENAS GRADUACIONES, ANILLOS GRADUADOS, MÓDULOS GRADUADOS, ANILLOS FUERTEMENTE GRADUADOS, PRODUCTOS CRUZADOS.

Descripción: Este trabajo consiste en estudiar las graduaciones del anillo de matrices, en particular nos concentraremos en cierto tipo de graduación, llamadas buenas graduaciones, en la que las matrices elementales $e_{i,j}$, que son las matrices con 1 en la posición (i, j) y 0 en las demás posiciones, son elementos homogéneos. El objetivo de este trabajo es dar caracterizaciones a las buenas graduaciones que hacen que el álgebra de matrices sea un producto cruzado (ver Teorema 3.3.6) o un álgebra fuertemente graduada (ver Teorema 3.3.3).

En el primer capítulo mencionaremos conceptos y resultados básicos de la teoría de módulos, entre estos resultados está una caracterización de las sucesiones cindes que será de utilidad para establecer resultados a lo largo de este trabajo. En el capítulo siguiente daremos los conceptos de anillos graduados y módulos graduados, además hablaremos del anillo de endomorfismos graduado el cual es de suma importancia para establecer las graduaciones del anillo de matrices. Para finalizar, en el último capítulo mostraremos en primer aspecto como a partir de las graduaciones del anillo de endomorfismos construimos las buenas graduaciones del álgebra de matrices y en segundo aspecto mostraremos resultados que podemos obtener a partir de las buenas graduaciones, como por ejemplo cuantas buenas graduaciones existen en un anillo graduado por un grupo finito.

---

* Trabajo de grado

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

Abstract

Title: GOOD GRADINGS OF THE MATRIX RING [*]

Author: LAURA NATALIA OROZCO GARCÍA [**]

Keywords: GOOD GRADATIONS, GRADED RINGS, GRADED MODULES, STRONGLY GRADED RINGS, CROSSED-PRODUCT.

Description: This work consists in studying the gradations of the matrix ring, we will focus particularly on a certain type of gradation, the so called good gradations, in which the elementary matrices with 1 in position (i, j) and 0 in the other positions, are homogeneous elements. The purpose of this work is to characterize the good gradations that make matrix algebra a crossed product (see Theorem 3.3.6) or a strongly graded algebra (see Theorem 3.3.3).

In the first chapter we shall mention basic concepts and results of module theory, among these results is a characterization of the sequences cindes that will be useful to establish results throughout this work. In the next chapter we are gonna give the concepts of graded rings and graded modules, furthermore we shall talk about the graded endomorphism ring which is of great importance to establish the matrix ring gradations. To conclude this work, in the last chapter we will show to the first aspect how from the gradations of the ring of endomorphisms we induce good gradations on the matrix algebra and in the second aspect we will show results that we can obtain from the gradations, such as how many good graduations exist in a ring graduated by a finite group.

---

[*] Bachelor Thesis

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

Introducción

Los anillos graduados juegan un papel muy importante en la geometría algebraica un ejemplo de esto lo encontramos en (Borovik, 2010) y (Hazrat, 2016) donde estudian el anillo graduado $\mathbb{Z}[x_1x_1^{-1},\cdots,x_nx_n^{-1}]$ y en general el anillo graduado de polinomios de Laurent. También, los anillos graduados son de gran incidencia en el álgebra conmutativa un ejemplo de esto lo encontramos en el aclamado trabajo de Jean-Pierre Serre (Serre, 1955). Entre los anillos graduados se destaca una clase especial que son los anillos fuertemente graduados y una clase particular de estos son los productos cruzados. A pesar de que el anillo de matrices sobe un cuerpo K, es bastante conocido, determinar las G-graduaciones sobre el, donde G es un grupo fijo, es un problema bastante complicado. Este problema ha sido resuelto, en casos particulares como cuando G es un grupo cíclico (Dăscălescu et al., 1999, pág. 717), o $n = 2$ (Dăscălescu et al., 1999, sec. 4), o K es algebraicamente cerrado (Bahturin and Zaicev, 2002, pág. 504). Sin embargo, el caso general es aún un problema abierto. Un tipo interesante de graduación, son las llamadas buenas o elementales. Así las cosas, las buenas graduaciones pueden considerarse como un primer paso al estudio de clasificar todas las graduaciones de $M_n(K)$.

1. Módulos

En este primer capítulo mencionaremos definiciones, ejemplos y resultados que serán la base para desarrollar este trabajo. A menos de que se mencione lo contrario R denotará un anillo asociativo con unidad 1_R.

1.1. Módulos y submódulos

En esta sección mencionaremos las definiciones de módulos, submódulos y una serie de ejemplos enfocados en el tema. Necesarios para los capítulos siguientes.

Definición 1.1.1. *Sean $(M,+)$ un grupo abeliano y R un anillo. Decimos que M tiene estructura de **módulo** a derecha sobre R, si se ha definido un producto entre 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:

I. $(m_1+m_2)\cdot r = m_1\cdot r + m_2\cdot r$;

II. $m\cdot(r_1+r_2) = m\cdot r_1 + m\cdot r_2$;

III. $m\cdot(r_1r_2) = (m\cdot r_1)\cdot r_2$;

IV. $m\cdot 1_R = m$;

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

De manera similar se definen los módulos a izquierda sobre R. En adelante, si no se advierte lo contrario, la palabra módulo denotará módulo a derecha. También se dirá que M es un $R-$módulo.

Ejemplo 1.1.2. El $R-$módulo nulo es el grupo 0 provisto de la única acción a derecha de R sobre él.

Ejemplo 1.1.3. Cada anillo R es un $R-$módulo bajo la acción regular a derecha, dada por la multiplicación.

Ejemplo 1.1.4. Cada grupo abeliano $(M,+)$ es módulo a izquierda sobre su anillo $End(M)$ de endomorfismos con la siguiente operación:

$$f \cdot m := f(m), \quad m \in M, \quad f \in End(M).$$

Ejemplo 1.1.5. Sea R un anillo y sea $M_n(R)$ su anillo de matrices cuadradas de orden n. El producto

$$r \cdot F := r \cdot [f_{ij}] = [rf_{ij}]$$

da a $M_n(R)$ estructura de $R-$módulo a izquierda. De manera ánaloga se define la estructura de $R-$módulo a derecha.

Ejemplo 1.1.6. Todo espacio vectorial sobre un cuerpo K es un $K-$módulo.

Ejemplo 1.1.7. Sea $(M,+,0)$ un grupo abeliano. Los múltiplos enteros de elementos de M se definen inductivamente:

$$\left.\begin{array}{l} m\cdot 1 := m \\ \\ m\cdot k := m\cdot(k-1)+m, \quad k\geq 2 \\ \\ m\cdot 0 := 0 \\ \\ m\cdot(-k) := (-m)\cdot k \end{array}\right\} \quad m\in M, k\in\mathbb{Z}^{+};$$

se puede probar que M es un $\mathbb{Z}-$módulo. Así cada grupo abeliano es un $\mathbb{Z}-$módulo.

Los ejemplos 1.1.7 y 1.1.6 muestran que los grupos abelianos y los espacios vectoriales son casos particulares de módulos.

Definición 1.1.8. *Sea A un anillo conmutativo. Se dice que el anillo R es una $A-$álgebra si R tiene estructura de $A-$módulo, y además,*

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

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

Ejemplo 1.1.9. 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 1.1.10. Si K es un cuerpo y V es un $K-$espacio vectorial, entonces el anillo de transformaciones lineales de V, $End_K(V)$, es una $K-$álgebra. Esto es un caso particular del inciso *IV.* de la Proposición 1.2.2 que mencionaremos más adelante.

Definición 1.1.11. *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 $(M,+)$, y además*

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

para cada $n \in N$ y cada $r \in R$. Se escribe $N \leq M$.

Ejemplo 1.1.12. Los submódulos triviales de M son $\{0\}$ y M.

Definición 1.1.13. *Un submódulo de M que no coincide con él se dice propio. El módulo $M \neq \{0\}$ se dice simple si sus únicos submódulos son los triviales.*

Ejemplo 1.1.14. Considerando R como un $R-$módulo derecho, entonces sus submódulos son precisamente ideales derechos.

Ejemplo 1.1.15. Si K es un cuerpo y V un $K-$espacio vectorial, los submódulos de V son sus subespacios.

1.2. Homomorfismos

En esta sección introduciremos de una manera corta los homomorfismos de módulos ya que al igual que en anillos, es posible definir funciones entre módulos que preserven las operaciones.

Además, mencionaremos la estructura de la colección de homomorfismos entre módulos la cual forma un grupo abeliano.

Definición 1.2.1. *Sean M y N dos $R-$módulos. Una función $f : M \to N$ 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 cualesquiera elementos $m, m' \in M$ y $r \in R$.

Los conceptos de núcleo, imagen, homomorfismo inyectivo, homomorfismo sobreyectivo, isomorfismo y endomorfismo de módulos, se definen como en el caso de anillos. Notemos en particular que $ker(f) := \{m \in M \mid f(m) = 0\}$ es un submódulo de M e $Im(f) := \{f(m) \mid m \in M\}$ es un submódulo de N. Además, si $f : M \to N$ es homomorfismo, entonces f es inyectivo si y sólo si $ker(f) = \{0\}$ y f es sobreyectivo si y sólo si $Im(f) = N$. El homomorfismo identidad se define por $i_M : M \to M$, $i_M(m) = m$, para todo $m \in M$ y el homomorfismo nulo se define por $0 : M \to N$, $0(m) = 0$, para todo $m \in M$.

Es conocido que el conjunto de endomorfismos de un grupo abeliano M es un anillo en el cual la adición de dos endomorfismos $f, g : M \to M$ se define por $(f+g)(m) = f(m) + g(m)$, $m \in M$ y el producto $f \circ g(m) = f(g(m))$. Considerando dos grupos abelianos M y N se prueba, definiendo la adición como antes, que el conjunto $Hom(M,N)$ de homomorfismos de M en N es un grupo abeliano. Además, si M, N, L son grupos abelianos y $f, g : M \to N$, $h : N \to L$ son homomorfismos de grupos, entonces se cumple que

$$h(f+g)=hf+hg.$$

En efecto, para cada $m\in M$ se tiene que $(h(f+g))(m)=h((f+g)(m))=h(f(m)+g(m))=h(f(m))+h(g(m))$.

Consideraremos que M y N son además R-módulos. Es claro que cada $R-$homomor- fismo de M en N es un homomorfismo de grupos. Desde luego que para homomorfismos compatibles la distributiva por el lado derecho también se cumple.

Proposición 1.2.2. *Sean M y N módulos sobre un anillo R y $Hom_R(M,N)$ el conjunto de $R-$homomorfismos de M en N. Entonces,*

I. $Hom_R(M,N)$ es subgrupo de $Hom(M,N)$.

II. Si R es un anillo conmutativo, entonces $Hom_R(M,N)$ es además un $R-$módulo, con el producto definido para cada $f\in Hom_R(M,N)$ y $r\in R$ como

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

III. Si $M=N$, entonces $End_R(M):=Hom_R(M,M)$ es un subanillo del anillo $End(M)$ de endomorfismos del grupo abeliano M.

IV. Si R es un anillo conmutativo, entonces $End_R(M)$ es una $R-$álgebra.

Demostración. Ver (Lezama, 2011a, pág. 26–27). □

1.3. Suma directa

En esta sección estudiaremos la suma directa de una familia de submódulos de un módulo dado y daremos una caracterización de estas sumas mediante equivalencias. Esta sección será de suma utilidad en los capitulos siguientes, pues la mencionaremos en multiples ocasiones.

1.3.1. Suma directa externa. Dados M,N dos $R-$módulos, es posible obtener un nuevo $R-$módulo considerando el conjunto de todos los pares ordenados de la forma (m,n), donde $m \in M$ y $n \in N$, 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 $r \in R$.

Cuando consideramos familias eventualmente infinitas de $R-$módulos podemos generalizar la construcción anterior de la siguiente manera.

Sea $\{M_i\}_{i\in I}$ una familia de $R-$módulos y $M = \prod_{i\in I} M_i$ el producto cartesiano de los miembros de la familia (es decir, el conjunto de todas las familias de la forma $(m_i)_{i\in I}$, donde $m_i \in M_i$, para cada $i \in I$), podemos introducir una estructura de $R-$módulo con las siguentes 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 $r \in R$.

Definición 1.3.1. *El $R-$módulo construido arriba se dice producto directo o producto cartesiano de la familia $\{M_i\}_{i\in I}$.*

Si $I = \{1, \cdots, n\}$, denotamos

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

Definición 1.3.2. *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 $m_i \neq 0$ para un número finito de índices.*

En el conjunto de familias casi nulas podemos introducir una estructura de $R-$ módulo, por restricción de las operaciones de M, pues la suma de familias casi nulas es casi nula y el producto de un elemento del anillo por una familia casi nula es una familia casi nula.

Definición 1.3.3. *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

$$\dot{\bigoplus}_{i\in I} M_i.$$

Si el conjunto $I = \{1, \cdots, n\}$, denotaremos

$$\dot{\bigoplus}_{i\in I} M_i = M_1 \dot{\bigoplus} \cdots \dot{\bigoplus} M_n.$$

De la definición tenemos que la suma directa externa de una familia de $R-$módulos es un submódulo del producto directo y que

$$\dot{\bigoplus}_{i\in I} M_i = \prod_{i\in I} M_i,$$

si y sólo si, el conjunto de índices I es finito. Además, si en la familia de $R-$módulos $\{M_i\}_{i\in I}$ se tiene que $M_i = M$, para cada $i \in I$ denotamos la suma directa externa de dicha familia como sigue

$$\dot{\bigoplus}_{i\in I} M_i = \dot{\bigoplus}_{i\in I} M = \prod_{i\in I} M_i = M^n.$$

Ejemplo 1.3.4. La suma directa externa de cualquier par de matrices A de tamaño $m \times n$ y B de tamaño $p \times q$ es una matriz de tamaño $(m+p) \times (n+q)$ definida como

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & b_{11} & \cdots & b_{1q} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & b_{p1} & \cdots & b_{pq} \end{bmatrix}.$$

1.3.2. Suma directa interna. La noción de suma directa interna es conocida, por lo menos en el caso de espacios vectoriales. Existen varias formas de caracterizar la suma directa interna, esto lo veremos en esta sección.

Definición 1.3.5. *Sea S un subconjunto del $R-$módulo M, Denotamos por $\{S\rangle$ la intersección de todos los submódulos de M que contienen a S, es decir,*

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

Note que $\{S\rangle$ es el menor submódulo que contiene a S y $\{\emptyset\rangle = \{0\}$.

Decimos que S es un sistema de generadores para M si $\{S\rangle = M$.

Proposición 1.3.6. *Sea M un $R-$módulo y $\emptyset \neq S \subseteq M$. Entonces,*

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

Demostración. Ver (Lezama, 2011a, pág. 17–18). $\square$

Definición 1.3.7. *Sea $\{M_i\}_{i\in I}$ una familia no vacía de submódulos de un módulo M, se denomina suma de la familia dada, y se denota por $\sum_{i\in I} M_i$, al submódulo generado por el conjunto $\bigcup_{i\in I} M_i$.*

Según la Proposición 1.3.2,

$$\sum_{i\in I} M_i = \left\{ \sum_{j=1}^{n} m_j \mid m_j \in \bigcup_{i\in I} M_i, n \geq 1 \right\}.$$

Notemos 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 1.3.8. *Sean M un $R-$módulo y $\{M_i\}_{i\in I}$ una familia de submódulos de M. Se dice que M es suma directa interna de la familia si*

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

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

En tal caso se denota

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

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

Proposición 1.3.9. *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 $\{i_1, \cdots, i_n\}$ *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 $\{i_1, \cdots, i_n\}$ *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. Ver (Lezama, 2011a, pág. 45–46). □

Definición 1.3.10. *Sean* M *un* $R-$*módulo y* N *un submódulo de* M. *Se dice que* N *es un* ***sumando directo*** *de* M *si existe un submódulo* N' *de* M *tal que* $M = N \bigoplus N'$.

Ejemplo 1.3.11. Para cualquier $R-$módulo M, se tiene que $M = M \bigoplus \{0\}$. Los submódulos M y $\{0\}$ son llamados los sumandos directos triviales.

Ejemplo 1.3.12. Consideremos el $\mathbb{Z}-$módulo $\mathbb{Z}_6 = \{0, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Podemos verificar que los subconjuntos $H_1 = \{0, \bar{2}, \bar{4}\}$ y $H_2 = \{0, \bar{3}\}$ son submódulos tales que $H_1 \cap H_2 = \{0\}$. También podemos verificar que $\mathbb{Z}_6 = H_1 + H_2$, luego

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

por tanto H_1 es un sumando directo de $\mathbb{Z}_6$.

Ejemplo 1.3.13. Veamos quienes son los sumandos directos de $\mathbb{Z}$ como $\mathbb{Z}-$módulo. Vamos a suponer que $\mathbb{Z} = H_1 \oplus H_2$, donde H_1, H_2 son submódulos propios de $\mathbb{Z}$, por el Ejemplo 1.1.14 los submódulos de $\mathbb{Z}$ coinciden con sus ideales, es decir, $H_1 = \langle a \rangle$ y $H_2 = \langle b \rangle$ para $a, b \in \mathbb{Z}$. Desde que $H_1 \cap H_2 = \langle c \rangle \neq \{0\}$, donde $c = mcm(a, b)$, esto contradice que la suma de $H_1 + H_2$ sea directa, por tanto los únicos sumandos directos de $\mathbb{Z}$ como $\mathbb{Z}-$módulo son los triviales.

Es natural preguntarse si existe una relación entre la suma directa interna y la suma directa externa de una familia de submódulos. La siguiente proposición es una respuesta a esa pregunta.

Proposición 1.3.14. *Sea M un $R-$módulo y $\{M_i\}_{i\in I}$ una familia de submódulos de M tales que $M = \bigoplus_{i\in I} M_i$. Entonces,*

$$\bigoplus_{i\in I} M_i \cong \dot{\bigoplus}_{i\in I} M_i$$

Demostración. Ver (Milies, 1972, pág. 51). □

Puesto que existe esa correspondecia biyectiva entre la suma directa interna y la suma directa externa, es frecuente no distinguirlas y usar el símbolo $\bigoplus$ para ambas.

1.4. Sucesiones exactas

Las sucesiones exactas son un lenguaje que permite expresar ciertas relaciones entre homomorfismos mediante diagramas. Introducimos esta sección, pues nos interesa la relación que existe entre sumas directas y sucesiones exactas.

Definición 1.4.1. *Sean M,N,L, tres $R-$módulos y $f: M \to N$, $g: N \to L$ dos $R-$homomorfismos. Decimos que el diagrama*

$$M \xrightarrow{f} N \xrightarrow{g} L$$

es una sucesión de orden 2 en G si $Im(f) \subset Ker(g)$. En particular si $Im(f) = Ker(g)$ decimos que el diagrama es una sucesión exacta en G.

Se puede verificar que la condición $Im(f) \subset Ker(g)$ es equivalente a que $g \circ f = 0$. En efecto, vamos a suponer que $Im(f) \subset Ker(g)$. Sea $m \in M$, tenemos que $g \circ f(m) = g(f(m))$, pero $f(m) \in Im(f) \subset Ker(g)$, así $g(f(m)) = 0$. Recíprocamente, si $g \circ f = 0$ tenemos que para todo $m \in M$ $g(f(m)) = 0$, luego $f(m) \in Ker(g)$, desde que la elección de m fue arbirtraria se cumple que $Im(f) \subset Ker(g)$.

Ejemplo 1.4.2. Sean M,N dos $R-$módulos y f un homomorfismo. Entonces:

I. Una sucesión $0 \to N \xrightarrow{f} M$ es exacta, si y sólo si, f es un monomorfismo.

II. Una sucesión $N \xrightarrow{f} M \to 0$ es exacta, si y sólo si, f es un epimorfismo.

III. De los ejemplos anteriores tenemos que $0 \to N \xrightarrow{f} M \to 0$ es una sucesión exacta, si y sólo si, f es un isomorfismo.

Ejemplo 1.4.3. La sucesión $0 \to M \to 0$ es exacta, si y sólo si, $M = 0$.

Ejemplo 1.4.4. Si N es un submódulo de un $R-$módulo M e indicamos por $i : N \to M$ la inclusión y por $\pi : M \to M/N$ la proyección canónica, entonces la sucesión

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N$$

es exacta.

Ejemplo 1.4.5. Dado un homomorfismo de $R-$módulos $f : N \to M$, la siguiente sucesión es exacta:

$$0 \longrightarrow Ker(f) \xrightarrow{i} N \xrightarrow{f} M \xrightarrow{\pi} M/Im(f) \longrightarrow 0.$$

Ejemplo 1.4.6. Sean M_1, M_2 dos $R-$módulos la sucesión

$$0 \longrightarrow M_1 \xrightarrow{\iota_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0,$$

donde ι_1 es la inyección cánonica y π_2 la proyección cánonica, es una sucesión exacta.

A partir del ejemplo anterior es natural preguntarse cuando una sucesión $0 \to N \xrightarrow{f} M \xrightarrow{g} L \to 0$ es tal que $M \cong N \bigoplus L$. Para esto daremos el siguiente concepto.

Definición 1.4.7. *Decimos que una sucesión exacta de $R-$módulos $0 \to N \xrightarrow{f} M \xrightarrow{g} L \to 0$ es cinde si $N' = Im(f) = ker(g)$ es un sumando directo de M.*

Proposición 1.4.8. *Dada una sucesión exacta de $R-$módulos $0 \to N \xrightarrow{f} M \xrightarrow{g} L \to 0$ las siguientes afirmaciones son equivalentes:*

I. *La sucesión es cinde.*

II. *Existe un $R-$homomorfismo $\psi : M \to N$ tal que $\psi \circ f = i_N$.*

III. *Existe un $R-$homomorfismo $\varphi : L \to M$ tal que $g \circ \varphi = i_L$.*

Bajo estas condiciones $M \cong N \bigoplus L$.

Demostración. Ver (Milies, 1972, pág. 56–57). □

2. Anillos y módulos graduados

En este capítulo mencionaremos la definición de anillo y módulo graduado, resultados básicos de estos y algunos ejemplos, además finalizaremos estudiando el anillo de endomorfismos graduado el cual es importante para hablar de las graduaciones del anillo de matrices.

2.1. Anillos graduados

Los anillos graduados son cierto tipo de anillos a los cuales se les asocia una graduación por una familia de subgrupos aditivos. Entre los anillos graduados se destaca una clase especial que son los anillos fuertemente graduados y una clase particular de estos son los productos cruzados. En esta sección mostraremos las características básicas de estos anillos y sus propiedades.

Definición 2.1.1. *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 la igualdad en II se cumple, decimos que R es fuertemente graduado por G.

Un elemento distinto de cero $x \in R_g$ 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.

Definición 2.1.2. *El conjunto* $U(R)$ *denota el grupo multiplicativo de elementos invertibles de R, el conjunto* $h(R) = \cup_{g\in G} R_g$ *denota el conjunto de elementos homogéneos de R y el conjunto* $U^{gr}(R) = \cup_{g\in G}(U(R)\cap R_g)$ *denota al conjunto de elementos invertibles homogéneos de R.*

Notemos que la función $grad : U^{gr}(R) \to G$ la cual envía a un elemento $r \in U^{gr}(R)$ en $grad(r)$ es una función multiplicativa. En efecto, sean $r,s \in U^{gr}(R)$, por ser elementos homogéneos existen $g,h \in G$ tales que $grad(r) = g$ y $grad(s) = h$, luego $r \in R_g$ y $s \in R_h$, así $r\cdot s \in R_g R_h \subseteq R_{gh}$ lo anterior implica que $grad(rs) = gh = grad(r)grad(h)$.

Proposición 2.1.3. *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. La inversa r^{-1} *de un elemento* $r \in U(R)$ *es un elemento homogéneo.*

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

Demostración.

I. Veamos primero que R_e es un subanillo de R. En efecto, si $a,b \in R_e$, dado que R_e un subgrupo aditivo de R tenemos que $a-b \in R_e$ y $a \cdot b \in R_eR_e \subseteq R_e$ pues R es un anillo graduado, por tanto R_e es subanillo de R. Probaremos ahora que $1_R \in R_e$. 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 $h \in G$, tenemos que $s_h = s_h \cdot 1_R = \sum_{g\in G} s_h \cdot r_g$, con $s_h \cdot r_g \in R_{hg}$, desde que la descomposición de s_h como suma finita es única $s_h \cdot r_g = 0$ para cualquier $g \neq e$, es decir,

$$s_h \cdot r_e = s_h, \tag{1}$$

para todo $\lambda \in G$. Así

$$\begin{aligned} r_e = 1_R \cdot r_e &= \sum_{g\in G} r_g \cdot r_e \\ &= \sum_{g\in G} r_g \qquad \textit{por (2.1)} \\ &= 1_R \end{aligned}$$

por lo tanto $1_R = r_e \in R_e$.

II. Asumamos que $r \in U(R) \cap R_h$. Si $r^{-1} = \sum_{g\in G}(r^{-1})_g$ con $(r^{-1})_g \in R_g$, 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 $r \in U(R)$, tenemos 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 $R_g R_{g^{-1}} = R_e$ para todo $g \in G$ y por el item anterior $1 \in R_e = R_g R_{g^{-1}}$. Recíprocamente, se probará que para $g, h \in G$ arbitrarios se tiene $R_g R_h = R_{gh}$. En efecto, por ser R un anillo $G-$graduado $R_g R_h \subseteq R_{gh}$. Ahora veamos que $R_{gh} \subseteq R_g R_h$, para esto probaremos primero que

$$R_{gh} = R_e R_{gh}.$$

Puesto que R un anillo $G-$graduado, tenemos $R_e R_{gh} \subseteq R_{gh}$, por otra parte, si $x \in R_{gh}$, entonces $x = 1 \cdot x \in R_e R_{gh}$, de esta manera concluimos la igualdad. A continuación probaremos que

$$R_e = R_g R_{g^{-1}}$$

sabemos que $R_g R_{g^{-1}} \subseteq R_e$ por ser R un anillo $G-$graduado, por otra parte, si $x \in R_e$ por hipótesis tenemos que $x = x \cdot 1 \in R_e R_g R_{g^{-1}} \subseteq R_g R_{g^{-1}}$, por lo cual concluimos la igualdad. Por las pruebas anteriores tenemos

$$R_{gh} = R_e R_{gh} = (R_g R_{g^{-1}}) R_{gh} = R_g (R_{g^{-1}} R_{gh}) \subseteq R_g R_h.$$

De esta manera concluimos que R es un anillo fuertemente graduado.

□

La siguiente proposición muestra que el grado de los elementos idempotentes de un anillo graduado coincide con el elemento neutro del grupo.

Proposición 2.1.4. *Sean R un anillo $G-$graduado y $0 \neq r \in R$ un elemento homogéneo idempotente, entonces $grad(r) = e$.*

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 $g = e$. $\square$

Definición 2.1.5. *Sea R un anillo $G-$graduado. R es llamado un **producto cruzado** si $U(R) \cap R_g \neq \emptyset$ para cualquier $g \in G$, es decir, si existe un elemento invertible en cada componente homógenea.*

Note que la definición anterior es equivalente al hecho de que la función *grad* sea una función sobreyectiva.

Proposición 2.1.6. *Sea $R = \bigoplus_{g \in G} R_g$ un anillo $G-$graduado. Si R es un producto cruzado, entonces:*

I. R es fuertemente graduado.

II. $R_e \cong R_g$ como R_e-módulos para todo $g \in G$.

Demostración.

I. Si R es un producto cruzado existe $u_g \in U(R) \cap R_g$ para cada $g \in G$, por II. de la Proposición 2.1.3 tenemos que $u_g^{-1} \in R_{g^{-1}}$, luego $1_R = u_g \cdot u_{g^{-1}} \in R_g R_{g^{-1}}$, así por III. de la misma proposción concluímos que R es fuertemente graduado.

II. Por hipótesis sabemos que para cada $g \in G$ existe un elemento invertible $v_g \in R_g$. Consideremos las funciones R_e-lineales

$$\begin{aligned} \phi : R_e &\longrightarrow R_g \\ r_e &\longmapsto r_e \cdot v_g \end{aligned}$$

y

$$\begin{aligned} \varphi : R_g &\longrightarrow R_e \\ r_g &\longmapsto r_g \cdot v_g^{-1}. \end{aligned}$$

Veamos que $r_e \cdot v_g \in R_g$, en efecto puesto que R es un producto cruzado, por la parte I. probada anteriormente R es fuertemente graduado, luego $r_e \cdot v_g \in R_e R_g = R_g$, así $\phi(R_e) \subseteq R_g$. Por otra parte, por la Proposición 2.1.3 II. $v_g^{-1} \in R_{g^{-1}}$, por tanto $r_g \cdot v_g^{-1} \in R_g R_{g^{-1}} = R_e$ para todo $r_g \in R_g$, en consecuencia $\varphi(R_g) \subseteq R_e$. Ahora bien, si hacemos la composición de ambas funciones obtenemos

$$\phi \circ \varphi(r_g) = \phi(\varphi(r_g)) = \phi(r_g v_g^{-1}) = r_g v_g v_{g^{-1}} = r_g$$

y

$$\varphi \circ \phi(r_e) = \varphi(\phi(r_e)) = \varphi(r_e v_g^{-1}) = r_e v_g v_{g^{-1}} = r_e,$$

es decir, $\phi \circ \varphi = 1_{R_g}$ y $\varphi \circ \phi = 1_{R_e}$, de esta manera podemos concluir que $R_e \cong R_g$ para todo $g \in G$.

$\square$

Para finalizar esta sección mostraremos algunos ejemplos de anillos graduados.

Ejemplo 2.1.7. 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 2.1.8. Si A es un anillo, entonces el anillo de poliomios $R = A[X]$ es un anillo $\mathbb{Z}-$graduado con el grado estándar $R_n = AX^n$ para $0 \leq n$ y $R_n = 0$ para $n < 0$. Además R no es un un anillo fuertemente graduado, pues por ejemplo $R_{18} \nsubseteq R_{-3}R_{-6} = 0$.

Ejemplo 2.1.9. Si A es un anillo, sea $R = A[X, X^{-1}]$ el anillo de polinomios de Laurent. Un elemento de R es de la forma $\sum_{i \geq m} a_i X^i$ con $m \in \mathbb{Z}$ y un número finito de $a_i' s$ son distintos de cero. Entonces R tiene el $\mathbb{Z}-$grado estándar $R_n = AX^n$, $n \in \mathbb{Z}$. Note que R es un producto cruzado pues, para $n \in \mathbb{Z}$ basta considerar $r = 1_A \cdot X^n$ y $r^{-1} = 1_A \cdot X^{-n}$, luego $r \cdot r^{-1} = X^n X^{-n} = 1_R$.

Ejemplo 2.1.10. Sea A un anillo y $R = M_3(A)$ su anillo de matrices de orden 3 y con entradas en A, entonces

$$R_0 = \begin{pmatrix} A & A & 0 \\ A & A & 0 \\ 0 & 0 & A \end{pmatrix} \quad y \quad R_1 = \begin{pmatrix} 0 & 0 & A \\ 0 & 0 & A \\ A & A & 0 \end{pmatrix}$$

es una $\mathbb{Z}_2-$graduación en R, Además puesto que

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

tenemos que $1_R \in R_1R_1$ y por definición de R_0 se tiene que $1_R \in R_0R_0$, es decir $1_R \in R_gR_{g^{-1}}$ para todo $g \in \mathbb{Z}_2$ por lo que haciendo uso de la Proposición 2.1.3 *III*. concluimos que R es fuertemente graduado. Note que no es un producto cruzado pues no existen elementos invertibles en R_1.

Ejemplo 2.1.11. Sea $K \subseteq E$ una extensión del cuerpo K, y suponga que $E = K(\sigma)$, donde σ es algebraico sobre K de grado n, entonces los elementos $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ forma una base de E sobre K. Veamos que $E = \bigoplus_{i=0}^{n-1} E_i$, donde $E_i = K(\alpha^i)$ es una $\mathbb{Z}_n-$graduación. Primero veremos que $E = \bigoplus_{i=0}^{n-1} E_i$; puesto que los elementos $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ forman una base de E tenemos que

$E = \sum_{i=1}^{n} E_i$ veamos que dicha suma es directa, por la Proposición 1.3.8 debemos probar que

$$a_0 + \cdots + a_{n-1} = 0 \Leftrightarrow a_i = 0$$

con $a_i \in E_i$, $1 \leq i \leq n-1$. Note que cada a_i es de la forma $k_i\alpha^i$, luego $k_0 + k_1\alpha + \cdots k_{n-1}\alpha^{n-1} = 0$, si $k_i = 0$ para cada $0 \leq i \leq n-1$, pues es una combinación de la base, es decir $a_i = 0$ para cada $0 \leq i \leq n-1$, recíprocamente si $a_i = 0$ para todo $0 \leq i \leq n-1$, tenemos que $a_0 + \cdots + a_{n-1} = 0$. Ahora veamos que forma una $\mathbb{Z}_n-$graduación. Sean $m, r \in \mathbb{Z}_n$ mostraremos que $E_mE_r \subseteq E_{m+r}$ teniendo en cuenta que la suma $m+r$ es módulo n, sea $\sum_{i=0}^{n-1} a_i\alpha^m b_i\alpha^r \in E_mE_r$ entonces

$$\sum_{i=0}^{n-1} a_i\alpha^m b_i\alpha^r = \sum_{i=0}^{n-1} a_ib_i(\alpha^m\alpha^r) = \sum_{i=0}^{n-1} a_ib_i\alpha^{m+r} \in E_{m+r}$$

por tanto, se forma una $\mathbb{Z}_n-$graduación de E, además E es un producto cruzado con esta graduación pues para $m \in \mathbb{Z}_n$ sea $k_m\alpha^m \in E_m$, puesto que $k_m \in K$ existe $k_m^{-1} \in K$ tal que $k_mk_m^{-1} = 1_K$ consideremos $k_m^{-1}\alpha^{n-m} \in E_{n-m}$, luego $k_m\alpha^m \cdot k_m^{-1}\alpha^{n-m} = 1_K\alpha^{m+n-m} = 1_K\alpha^0 = 1_K$.

Definición 2.1.12. *Sean $R = \bigoplus_{g\in G} R_g$ y $S = \bigoplus_{g\in G} S_g$ anillos $G-$graduados y $f : R \to S$ un homomorfismo de anillos, entonces f es llamado homomorfismo $G-$graduado si $f(R_g) \subseteq S_g$, para todo $g \in G$. Si f es un isomorfismo decimos que f es un isomorfismo de anillos graduados.*

Como se mostrará en el Apéndice A, si G es un grupo, los anillos $G-$graduados junto con los homomorfismos $G-$graduados forman una categoría a la cual denotamos por $G-RING$.

2.2. Módulos graduados

Los módulos graduados de manera similar a los anillos graduados son cierto tipo de módulos a los cuales se les asocia una graduación por una familia de submódulos del módulo. Esta sección la ocuparemos para definir los módulos graduados y mostrar algunos ejemplos.

Definición 2.2.1. *Sea G un grupo con identidad $e \in G$. Un $R-$módulo $G-$graduado es un $R-$módulo a derecha M tal que:*

I. $M = \bigoplus_{h \in G} M_h$*; donde cada M_h es un subgrupo aditivo de M.*

II. $M_h R_g \subseteq M_{hg}$*, para cada $h, g \in G$.*

Un elemento distinto de cero $m \in M_h$ es llamado elemento homogéneo de grado h y se denota $grad(m) = h$. Además cada elemento $m \in M$ tiene representación única como $m = \sum_{h \in G} m_h$ con $m_h \in M_h$ y sólo un número finito de $m_h \neq 0$.

Definición 2.2.2. *Sea N un $R-$submódulo de M. Entonces, N es llamado **submódulo graduado** si para cada $n \in N$ todas sus componentes homogéneas también están en N, es decir, $N = \bigoplus_{g \in G}(N \cap M_g)$.*

A continuación presentaremos algunos ejemplos:

Ejemplo 2.2.3. Un anillo $G-$graduado R es un $R-$módulo $G-$graduado considerando

$$M = R, \quad M_g = R_g \quad \textit{para todo } g \in G.$$

Ejemplo 2.2.4. Sea M un $R-$módulo $G-$graduado, entonces el $R-$módulo M^n es $G-$graduado. En efecto, Veamos primero que $M^n = \bigoplus_{g\in G}(M_g)^n$. Sea $(m_i)_{i=1}^n \in M^n$, puesto que M es un módulo $G-$graduado tenemos que $m_i = \sum_{g\in G}(m_i)_g$ para todo $i \in \{1,\cdots,n\}$ con $(m_i)_g \in M_g$. Entonces, por definición de la operación suma en M^n se sigue que

$$\left(\sum_{g\in G}(m_i)_g\right)_{i=1}^n = \sum_{g\in G}((m_i)_g)_{i=1}^n \in \sum_{g\in G}(M_g)^n.$$

Ahora, probaremos que la suma anterior es directa. Fijemos $h \in G$, debemos verificar que

$$(M_h)^n \cap \sum_{\substack{g\in G \\ h\neq g}}(M_g)^n = \{0\}$$

sea $(m_i)_{i=1}^n \in (M_h)^n \cap \sum_{\substack{g\in G \\ h\neq g}}(M_g)^n$, entonces para cada m_i se tiene que $m_i \in M_h$ y $m_i \in \sum_{\substack{g\in G \\ h\neq g}}(M_g)^n$, pero M es un $R-$módulo $G-$graduado, por lo tanto $m_i = 0$ para todo $i \in I$, con lo anterior concluimos que $M^n = \bigoplus_{g\in G}(M_g)^n$. Por último, notemos que

$$(M_h)^n R_g = (M_h R_g)^n \subseteq (M_{hg})^n.$$

Ejemplo 2.2.5. Sea R un anillo $G-$graduado y $x \in R$ un elemento homogéneo de grado h, entonces el $R-$módulo $Rx = \{rx \mid r \in R\}$ es $G-$graduado. En efecto, veamos que

$$Rx = \bigoplus_{g\in G}(Rx)_g, \quad donde \quad (Rx)_g = R_g x.$$

Para lo anterior debemos probar primero que $Rx = \sum_{g\in G}(Rx)_g$. Sea $rx \in Rx$ con $r \in R$, puesto que R es $G-$graduado tenemos que r tiene descomposición en suma finita como sigue $r = \sum_{g\in G} r_g$ donde $r_g \in R_g$ para cada $g \in G$, luego $r_g x \in R_g x$ para cada $g \in G$, así

$$rx = \sum_{g\in G} r_g x \in \sum_{g\in G} R_g x = \sum_{g\in G}(Rx)_g,$$

por otra parte sea $\sum_{g\in G}(rx)_g \in \sum_{g\in G}(Rx)_g$, puesto que $(Rx)_g = R_g x$ tenemos que $\sum_{g\in G}(rx)_g = \sum_{g\in G} r_g x \in \sum_{g\in G} R_g x$, así como $\sum_{g\in G} r_g \in R$, concluimos que $\sum_{g\in G}(rx)_g \in Rx$. Ahora, probaremos que

$$(Rx)_g \cap \sum_{\substack{g'\in G\\ g'\neq g}}(Rx)_{g'} = \{0\},$$

sea $rx \in (Rx)_g = R_g x$ tenemos que $rx \in R_g R_h \subseteq R_{gh}$ vamos a suponer que $rx \in \sum_{\substack{g'\in G\\ g'\neq g}}(Rx)_{g'}$, entonces

$$rx = \sum_{\substack{g'\in G\\ g'\neq g}}(rx)_{g'} = \sum_{\substack{g'\in G\\ g'\neq g}} r_{g'} x \in \sum_{\substack{g'\in G\\ g'\neq g}} R_{g'} R_h \subseteq \sum_{\substack{g'\in G\\ g'\neq g}} R_{g'h},$$

pero por hipótesis R es suma directa, es decir, $R_{gh} \cap (\sum_{g'\in G} R_{g'h}) = \{0\}$, luego $rx = 0$. Note que la condición de que x sea un elemento homógeneo es necesaria para probar que la suma es directa, de lo contrario no podemos afirmarlo. Además, para $g,h \in G$ se satisface

$$R_g(Rx)_h = R_g(R_h x) \subseteq R_{gh} x = (Rx)_{hg}.$$

Ejemplo 2.2.6. Sea $R = \bigoplus_{g\in G} R_g$ un anillo $G-$graduado. Entonces, el anillo $M_n(R)$ de matrices cuadradas de tamaño $n \times n$ es $G-$graduado tomando la graduación definida por

$$M_n(R) = \bigoplus_{g\in G} M_n(R)_g, \quad \textit{donde } M_n(R)_g = M_n(R_g).$$

Consideremos $e_{i,i}$ la matriz elemental con 1_R en la posición (i,i) y cero en las demás posiciones. Notemos que $e_{i,i} \in M_n(R_e) = M_n(R)_e$, pues por la Proposición 2,1,3 tenemos que $1_R \in R_e$, y por ser R_e un subgrupo aditivo $0_R \in R_e$ es decir, la matriz $e_{i,i}$ tiene entradas en R_e por lo tanto $e_{i,i} \in M_n(R_e) = M_n(R)_e$ es un elemento homogéneo. Luego, $e_{i,i}M_n(R)$ es un $M_n(R)-$módulo a derecha tal que

$$e_{i,i}M_n(R) = \bigoplus_{g\in G} e_{i,i}M_n(R_g),$$

además, para todo $g,h \in G$ se verifica

$$(e_{i,i}M_n(R_g))M_n(R_h) = e_{i,i}(M_n(R_g)M_n(R_h)) \subseteq e_{i,i}M_n(R_{gh}).$$

Así $e_{i,i}M_n(R)$ es un $M_n(R)-$módulo a derecha $G-$graduado

Como se mostrará en el Apéndice A, si G es un grupo y R un anillo $G-$graduado, la categoría de módulos $G-$graduados a derecha, denotada por $gr-R$, es obtenida tomando los $R-$módulos $G-$graduados como objetos y como morfismos

$$Hom_{gr-R}(M,N) = \{f \in Hom_R(M,N) \mid f(M_g) \subseteq N_g, \quad \textit{para todo } g \in G\}$$

para N,M dos $R-$módulos $G-$graduados. Además, por la definición, es claro que $Hom_{gr-R}(M,N)$ es un subgrupo aditivo de $Hom_R(M,N)$.

Proposición 2.2.7. *Sean M,N,L módulos graduados y $f: M \to N$, $g: N \to L$ morfismos $G-$graduados, entonces $g \circ f$ es un morfismo graduado.*

Demostración. Debemos verificar que $g \circ f(M_g) \subseteq L_g$. En efecto, puesto que f,g son $G-$graduados, entonces

$$g \circ f(M_g) = g(f(M_g)) \subseteq g(N_g) \subseteq L_g.$$

Concluyendo así que la composición de morfismos graduados es un morfismo graduado. □

2.3. Anillo de endomorfismos graduado

En vista de que apartir de las graduaciones del anillo de endomorfismos podemos dar graduaciones al anillo de matrices, introducimos esta sección en la que estudiaremos algunas propiedades de este anillo como cuando es fuertemente graduado o cuando es un producto cruzado. De ahora en adelante, consideraremos a R un anillo $G-$graduado y M un $R-$módulo a derecha $G-$graduado.

Definición 2.3.1. *Definimos $(g)M$ como el $R-$módulo $G-$graduado a derecha que es justamente M, con la graduación definida como $(g)M_h = M_{gh}$ para todo $h \in G$.*

Veamos que el $R-$módulo $(g)M$ es un $R-$módulo $G-$graduado, para esto veamos que $(g)M = \bigoplus_{g' \in G}(g)M_{g'}$. Sea $m \in (g)M$, como $(g)M = M$ y M es un módulo $G-$graduado se tiene que $m = \sum_{g' \in G} m_{g'}$ con $m_{g'} \in M_{g'}$ para todo $g' \in G$, puesto que para cada g' existe un único $h \in G$

tal que $g' = gh$, tenemos que $m = \sum_{g' \in G} m_{g'} = \sum_{h \in G} m_{gh} \in \sum_{h \in G}(g)M_h$, la condición para que la suma anterior sea directa es consecuencia inmediata del hecho de ser M un módulo $G-$graduado. Ahora, veamos que $(g)M_h R_{g'} \subseteq (g)M_{hg'}$. En efecto,

$$(g)M_h R_{g'} = M_{gh} R_{g'} \subseteq M_{ghg'} = (g)M_{hg'}.$$

Así probamos que $(g)M$ es en efecto un módulo graduado.

A continuación vamos a definir el anillo de endomorfismos, como un anillo $G-$graduado.

Para cualquier $g \in G$ definimos

$$END(M)_g = \{f \in End_R(M) \mid f(M_h) \subseteq M_{gh},\ para\ todo\ h \in G\},$$

el cual es un subgrupo aditivo de $End_R(M)$. Note que $END(M)_g = Hom_{gr-R}(M, (g)M)$, en efecto,

$$\begin{aligned}
Hom_{gr-R}(M,(g)M) &= \{f \in Hom_R(M,(g)M) \mid f(M_h) \subseteq (g)M_h\ para\ todo\ h \in G\} \\
&= \{f \in Hom_R(M,M) \mid f(M_h) \subseteq (g)M_h = M_{gh}\ para\ todo\ h \in G\} \\
&= \{f \in End_R(M) \mid f(M_h) \subseteq M_{gh}\ para\ todo\ h \in G\} \\
&= END(M)_g.
\end{aligned}$$

Ahora veamos que $\sum_{g \in G} END(M)_g$ es una suma directa. En efecto, si suponemos por absurdo que no lo es tenemos

$$END(M)_g \cap \sum_{\substack{h\in G\\ h\neq g}} END(M)_h \neq \{0\},$$

es decir, existe $0 \neq f \in END(M)_g \cap \sum_{h\in G} END(M)_h$ tal que $f = \sum_{h\in G} f_h$ para $f_h \in END(M)_h$ y $f \in END(M)_g$. Así, por definición tenemos que para todo $g' \in G$

$$f(M_{g'}) = \sum_{\substack{h\in G\\ h\neq g}} f_h(M_{g'}) \subseteq \sum_{\substack{h\in G\\ h\neq g}} M_{hg'},$$

y $f(M_{g'}) \subseteq M_{gg'}$, luego $M_{gg'} \cap \sum_{\substack{h\in G\\ h\neq g}} M_{hg'} \neq \{0\}$, es decir, M no es un módulo $G-$graduado, lo cual es una contradicción.

Denotaremos por $END_R(M) = \bigoplus_{g\in G} END(M)_g$ el cual es un anillo $G-$graduado. Una construcción similar a la anterior se hace para módulos a izquierda.

Definición 2.3.2. *Sean $M,N \in gr-R$.*

I. Decimos que N divide a M en $gr-R$ si N es isomorfo como módulo graduado a un sumando directo de M.

II. Decimos que N divide débilmente a M en $gr-R$ si divide a una suma directa finita M^t de copias de M.

III. Decimos que M,N son débilmente isomorfos como módulos graduados en $gr-R$, si y sólo si, ellos se dividen débilmente entre si.

IV. Decimos que M es débilmente $G-$invariante si M y $(g)M$ son débilmente isomorfos en $gr-$

R, para todo $g \in G$.

La siguiente equivalencia será muy útil para los teoremas que siguen.

Proposición 2.3.3. *Sean $N, M \in gr - R$. Entonces, N divide débilmente a M en $gr - R$, si y sólo si, existen $f_1, \cdots, f_t \in Hom_{gr-R}(M,N)$ y $g_1, \cdots, g_t \in Hom_{gr-R}(N,M)$ tales que $i_N = f_1 \circ g_1 + \cdots + f_t \circ g_t$.*

Demostración. Vamos a suponer que N divide débilmete a M en $gr - R$, esto es, N divide a una suma directa finita M^t de copias de M, es decir, $M^t = N \bigoplus N'$, donde $N' \in gr - R$. Vamos a considerar

$$g_i : N \overset{\iota}{\hookrightarrow} M^t \overset{\pi_i}{\twoheadrightarrow} M \quad y \quad f_i : M \overset{\iota_i}{\hookrightarrow} M^t \overset{\pi}{\twoheadrightarrow} N$$

para $i \in \{1, \cdots t\}$, donde π_i y ι_i son las proyecciones e inyecciones canónicas respectivamente. Se puede verificar que tanto las proyecciones como las inclusiones canónicas $\pi, \pi_i, \iota, \iota_i$ son morfismos graduados donde la graduación de M^t es la graduación definida en el Ejemplo 2.2.4 y por la Proposición 2.2.7 la composición de morfismos graduados es un morfismo graduado, luego $g_i \in Hom_{gr-R}(N,M)$ y $f_i \in Hom_{gr-R}(M,N)$ para cada $i \in \{1, \cdots, t\}$. Note que,

$$\begin{aligned}
\sum_{i=1}^{t} f_i \circ g_i &= \sum_{i=1}^{t} (\pi \circ \iota_i \circ \pi_i \circ \iota) \\
&= \pi \circ \sum_{i=1}^{t} (\iota_i \circ \pi_i) \circ \iota \\
&= \pi \circ i_M \circ \iota \\
&= i_N.
\end{aligned}$$

Así, concluimos que existen $f_1, \cdots, f_t \in Hom_{gr-R}(M,N)$ y $g_1, \cdots, g_t \in Hom_{gr-R}(N,M)$ tales que $i_N = f_1 \circ g_1 + \cdots + f_t \circ g_t$.

Recíprocamente, vamos a suponer que existen $f_1, \cdots, f_t \in Hom_{gr-R}(M,N)$ y $g_1, \cdots, g_t \in Hom_{gr-R}(N,M)$ tales que

$$i_N = \sum_{i=1}^{t} f_i \circ g_i.$$

Consideremos la sucesión de orden 4

$$0 \longrightarrow N \xrightarrow{\widetilde{g}} M^t \xrightarrow{\pi} M^t/Im(\widetilde{g}) \longrightarrow 0,$$

donde

$$\begin{aligned} \widetilde{g} : N &\longrightarrow M^t \\ n &\longmapsto (g_1(n), \cdots, g_t(n)) \end{aligned}$$

es un homomorfismo graduado, pues

$$\widetilde{g}(N_g) = (g_1(N_g), \cdots, g_t(N_g)) \subseteq (M_g, \cdots, M_g) = (M_g)^t.$$

Veamos que la sucesión anterior es una sucesión exacta, para esto por el Ejemplo 1.4.2 dado que la función proyección π es un epimorfismo basta mostrar que la función $\widetilde{g}$ es un monomorfismo, para esto mostraremos que $ker(\widetilde{g}) = \{0\}$. Sea $n \in ker(\widetilde{g})$, entonces $\widetilde{g}(n) = (g_1(n), \cdots, g_t(n)) = (0, \cdots, 0)$, así si suponemos por contradicción que $n \neq 0$ tenemos que

$$f_1 \circ g_1(n) + \cdots + f_t \circ g_t(n) = f_1(0) + \cdots + f_t(0) = 0$$

lo cual contradice que $\sum_{i=1}^{t} f_i \circ g_i = i_N$. Así concluimos que la sucesión es exacta. Por otra parte veamos que existe $\widetilde{f} : M^t \longrightarrow N$ tal que $\widetilde{f} \circ \widetilde{g} = i_N$, para lo anterior basta considerar el homomorfismo

$$\begin{aligned} \widetilde{f} : M^t &\longrightarrow N \\ (m_i)_{i=1}^{n} &\longmapsto \sum_{i=1}^{t} f_i(m_i), \end{aligned}$$

el cual es graduado, pues

$$\widetilde{f}((M_g)^t) = \sum_{i=1}^{t} f_i(M_g) \subseteq \sum_{i=1}^{t} N_g = N_g$$

así,

$$\begin{aligned} \widetilde{f} \circ \widetilde{g}(N) &= \widetilde{f}(g_1(N), \cdots, g_t(N)) \\ &= \sum_{i=1}^{t} f_i \circ g_i(N) \end{aligned}$$

y lo anterior por hipótesis obtenemos que $\widetilde{f} \circ \widetilde{g} = i_N$, por lo tanto, haciendo uso de la Proposición

1.4.8 concluimos que $M^t \cong N \bigoplus M^t/Im(\widetilde{g})$ y esto por definición implica que N divide débilmente a M en $gr-R$. $\square$

Lema 2.3.4. *Sean M,N módulos $G-$graduados y $g,h \in G$. Entonces,*

I. $Hom_{gr-R}((g)M,(hg)M) = END(M)_h$.

II. $Hom_{gr-R}((g)M,N) = Hom_{gr-R}(M,(g^{-1})N)$.

III. $END_R(M)_{h^{-1}} = Hom_{gr-R}((gh)M,(g)M)$.

Demostración.

I. Veamos primero que $Hom_{gr-R}((g)M,(hg)M) \subseteq END(M)_h$, para esto sea $f \in Hom_{gr-R}((g)M,$ $(hg)M)$, por la Definición 2.3.1 se sigue que $(g)M = M = (hg)M$ por lo tanto tenemos que $f \in End_R(M)$, ahora verifiquemos que $f(M_{g'}) \subseteq M_{g'h}$ para todo $g' \in G$, por hipótesis $f((g)M_{h'}) \subseteq (hg)M_{h'}$, es decir, $f(M_{gh'}) = M_{hgh'}$, note que para todo $g' \in G$ existe $h' \in G$ tal que $g' = h'g$, así pues $f(M_{g'}) \subseteq M_{hg'}$, por tanto $f \in END(M)_h$. Ahora veamos que $END(M)_h \subseteq Hom_{gr-R}((g)M,(hg)M)$, sea $f \in END(M)_h$ por definición $f \in End_R(M) = Hom_R((g)M,(hg)M)$ y $f(M_{h'}) \subseteq M_{hh'}$, así como para todo $h' \in G$ existe $g' \in G$ tal que $h' = gg'$, tenemos que $f(M_{gg'}) \subseteq M_{hgg'}$, es decir, $f((g)M_{g'}) \subseteq (hg)M_{g'}$ con lo cual concluimos que $f \in Hom_{gr-R}((g)M,(hg)M)$.

II. Veamos primero que $Hom_{gr-R}(M,(g^{-1})N) \subseteq Hom_{gr-R}((g)M,N)$, para esto sea $f \in Hom_{gr-R}$ $(M,(g^{-1})N)$, por definición $f(M_h) \subseteq (g^{-1})N_h$, note que para todo $h \in G$ existe $h' \in G$ tal que $h = gh'$, así pues $f(M_{gh'}) \subseteq (g^{-1})N_{gh'} = N_{gg^{-1}h'} = N_{h'}$, es decir, $f \in Hom_{gr-R}((g)M,N)$.

Ahora sea $f \in Hom_{gr-R}((g)M,N)$ por definición tenemos que $f((g)M_h) \subseteq N_h$, es decir, $f(M_{gh}) \subseteq N_h = N_{g^{-1}gh} = (g^{-1})N_{gh}$, por lo tanto $f \in Hom_{gr-R}(M,(g^{-1})N)$.

III. Por el inciso anterior tenemos que

$$Hom_{gr-R}((hg)M,(g)M) = Hom_{gr-R}(M,(g^{-1}h^{-1})(g)M),$$

por lo tanto debemos verificar que

$$Hom_{gr-R}(M,(g^{-1}h^{-1})(g)M) = END_R(M)_{h^{-1}},$$

probaremos primero que $Hom_{gr-R}(M,(g^{-1}h^{-1})(g)M) \subseteq END_R(M)_{h^{-1}}$, sea $f \in Hom_{gr-R}(M,$ $(g^{-1}h^{-1})(g)M)$ por definición $f(M_{g'}) \subseteq (g^{-1}h^{-1})(g)M_{g'}$, para todo $g' \in G$, es decir, $f(M_{g'}) \subseteq$ $(g^{-1}h^{-1})(g)M_{g'} = (g)M_{g^{-1}h^{-1}g'} = M_{gg^{-1}h^{-1}g'} = M_{h^{-1}g'}$, por lo tanto $f \in END_R(M)_{h^{-1}}$. Recíprocamente, si $f(M_{g'}) \subseteq M_{h^{-1}g'}$, entonces $f(M_{g'}) \subseteq M_{h^{-1}g'} = M_{gg^{-1}h^{-1}g'} = (g)M_{g^{-1}h^{-1}g'} =$ $(g^{-1}h^{-1})(g)M_{g'}$, así pues $f \in Hom_{gr-R}(M,(g^{-1}h^{-1})(g)M) = Hom_{gr-R}((hg)M,(g)M)$.

$\square$

El siguiente teorema da una caracterización de las graudaciones que hacen que el anillo $END_R(M)$ sea un anillo fuertemente graduado.

Teorema 2.3.5. *Sea $M \in gr-R$. Entonces, el anillo $G-$graduado $END_R(M)$ es fuertemente graduado, si y sólo si, M es débilmente $G-$invariante.*

Demostración. Por el inciso III. de la Proposición 2.1.3 tenemos que $END_R(M)$ es fuertemente graduado, si y sólo si, $i_M \in END_R(M)_h END_R(M)_{h^{-1}}$ para todo $h \in G$. Lo anterior, por definición es equivalente a que existan $g_1, \cdots, g_n \in END_h(M)$ y $f_1, \cdots, f_n \in END_R(M)_{h^{-1}}$ tales que

$$i_M = \sum_{i=1}^{n} g_i \cdot f_i = \sum_{i=1}^{n} f_i \circ g_i, \tag{2}$$

pero por el Lema 2.3.4 inciso I.

$$Hom_{gr-R}((g)M, (hg)M) = END(M)_h,$$

y por el inciso III.

$$END_R(M)_{h^{-1}} = Hom_{gr-R}((hg)M, (g)M),$$

por las igualdades anteriores, el resultado $(2{,}2)$ es equivalente al hecho de que $(g)M$ divide débilmente a $(gh)M$, para todo $g, h \in G$. Así, si consideramos $g = e$ tenemos que M divide débilmente a $(h)M$ para todo $h \in G$. Además si consideramos $h = g^{-1}$ tenemos que $(g)M$ divide débilmente a M, para todo $g \in G$. Así que lo anterior es equivalente a que M sea débilmente $G-$invariante. $\square$

El siguiente teorema da una caracterización de las graudaciones que hacen que el anillo $END_R(M)$ sea un producto cruzado.

Teorema 2.3.6. *Sea $M \in gr - R$. Entonces $END_R(M)$ es un producto cruzado, si y sólo si, M es $G-$invariante.*

Demostración. Sabemos por definición que $END_R(M)$ es un producto cruzado, si y sólo si, existe un elemento invertible en $END_R(M)_g$ para cada $g \in G$. Dado que $END_R(M)_g = Hom_{gr-R}(M,(g)M)$ y $END_R(M)_{g^{-1}} = Hom_{gr-R}((g)M,M)$, lo anterior es equivalente a que existan $f \in Hom_{gr-R}(M,(g)M)$ y $f^{-1} \in Hom_{gr-R}((g)M,M)$ tales que $f \circ f^{-1} = i_M$ y por la Proposición 2.3.3 es equivalente a que M divida débilmente a $(g)M$ en $gr-R$ para todo $g \in G$, es decir, es equivalente a que M sea $G-$invariante. $\square$

3. Buenas graduaciones del álgebra de matrices

En este último capítulo estudiaremos las buenas graduaciones, comenzando por relacionar las buenas graduaciones del anillo de matrices con las graduaciones del anillo de endomorfismos y finalizando con propiedades y caracteriazaciones de estas buenas graduaciones. De aquí en adelante vamos a considerar K un cuerpo, G un grupo multiplicativo y denotaremos por $e_{i,j}$ a las matrices con 1_K en la posición (i,j) y 0_K en las demás posiciones.

3.1. Buenas graduaciones y el anillo de endomorfismos

Esta sección la dedicaremos a construir mediante isomorfismos buenas graduaciones para el álgebra de matrices.

Definición 3.1.1. *Decimos que una $G-$graduación de la $K-$álgebra $M_n(K)$ es buena si todas las matrices $e_{i,j}$ son elementos homogéneos.*

Definición 3.1.2 (Delta de Kronecker). *La función Delta de Kronecker es una función definida a* *trozos de la siguiente manera*

$$\delta_{i,j} = \begin{cases} 1 & si \quad i = j \\ \\ 0 & si \quad i \neq j \end{cases}$$

Lema 3.1.3. *Sea V un espacio vectorial de dimensión finita y $\{V_g\}_{g\in G}$ una familia de subespacios vectoriales de V. Si $V = \bigoplus_{g\in G} V_g$, entonces $\bigcup_{g\in G} \mathscr{B}_g$ es una base para V, donde $\mathscr{B}_g$ es una base de V_g para cada $g \in G$.*

Demostración. Sea $\mathscr{B}_g$ una base de V_g, para cada $g \in G$. Es claro que $\mathscr{B} = \bigcup_{g\in G} \mathscr{B}_g$ es un conjunto de generadores de $\sum_{g\in G} V_g = V$, por tanto

$$dim\left(\sum_{g\in G} V_g\right) \leq |\mathscr{B}|.$$

Por otro lado,

$$\begin{aligned} |\mathscr{B}| &\leq \sum_{g\in G} |\mathscr{B}_g| \\ &\leq \sum_{g\in G} dim(V_g) \\ &= dim\left(\sum_{g\in G} V_g\right). \end{aligned}$$

Note que la última igualdad es cierta pues $V = \bigoplus_{g\in G} V_g$, este hecho se probará más adelante (Ver

Lema 3.3.7. Inciso II.). Así pues,

$$|\mathscr{B}| = dim(\sum_{g\in G} V_g) = dim(V)$$

y como $\mathscr{B}$ genera a $\sum_{g\in G} V_g = V$, concluimos que $\mathscr{B}$ es base. □

Mostraremos como podemos formar buenas graduaciones para el anillo de matrices a partir de la graduaciones del anillo de endomorfismos. Sea V un espacio vectorial $G-$graduado, es decir, $V = \bigoplus_{g\in G} V_g$ para algunos subespacios $(V_g)_{g\in G}$. Recordemos que

$$END_K(V) = \bigoplus_{g\in G} END(V)_g,$$

donde

$$END(M)_g = \{f \in End_R(M) \mid f(M_h) \subseteq M_{gh},\ para\ todo\ h \in G\}.$$

Si V es un espacio vectorial de dimensión finita n, entonces $END_K(V) = End_K(V)$ ver (Năstăsescu and Oystaeyen, 2004, pág 27-28) y $End_K(V) \cong M_n(K)$, pues $End_K(V)$ y $M_n(K)$ tienen la misma dimensión. Si $(v_i)_{i=1}^n$ es una base de elemenos homogéneos de V, la cual existe por el Lema 3.1.3, denotamos $grad(v_i) = g_i$, para todo $1 \leq i \leq n$. Definamos $(E_{i,j})_{1\leq i,j\leq n}$ con cada $E_{i,j} \in End_K(V)$ como $E_{i,j}(v_t) = \delta_{t,j} v_i$ para todo $1 \leq i, j,t \leq n$ y veamos que $(E_{i,j})_{1\leq i,j\leq n}$ es una base para $End_K(V)$.

En efecto, basta notar que para ciertos escalares $\lambda_{i,j}$ se cumple que

$$\begin{aligned}\sum_{1\leq i,j\leq n}\lambda_{i,j}E_{i,j}(v_k)=0 &\Leftrightarrow \sum_{i=1}^{n}\lambda_{i,k}E_{i,k}(v_k)=0\\ &\Leftrightarrow \sum_{i=1}^{n}\lambda_{i,k}v_i=0,\end{aligned}$$

por ser $(v_i)_{i=1}^{n}$ una base de V cada $\lambda_{i,k}=0$ para todo $1\leq i\leq n$ y por ser k arbitrario $\lambda_{i,j}=0$, para todo $1\leq i,j\leq n$, con lo anterior y como hay tantos elementos en $(E_{i,j})_{1\leq i,j\leq n}$ como $dim(End_K(V))$ concluimos que es una base de $End_K(V)$. Por otra parte, mostraremos que $grad(E_{i,j})=g_ig_j^{-1}$, es decir mostraremos que $E_{i,j}\in End_K(V)_{g_ig_j^{-1}}$ para todo $1\leq i,j\leq n$, para esto veamos que si $g\in G$, entonces $E_{i,j}(V_g)\subseteq V_{g_ig_j^{-1}g}$. En efecto, si $V_g=\{0\}$, entonces $E_{i,j}(V_g)=0\subseteq V_{g_ig_j^{-1}g}$, caso contrario si $V_g\neq\{0\}$, entonces existe $v_k\in\{v_1,\cdots,v_n\}$ tal que $v_k\in V_g$, es decir $g=g_k$, por definición

$$E_{i,j}(v_k)=\delta_{k,j}v_i=\begin{cases}v_i & si\quad k=j\\ 0 & si\quad k\neq j\end{cases}$$

así, si $k=j$ se tiene que $E_{i,j}(v_j)=v_i\in V_{g_i}=V_{g_ig_j^{-1}g_j}$, en caso contrario $E_{i,j}(v_k)=\{0\}\subset V_{g_ig_j^{-1}g}$, concluyendo de esta manera que $grad(E_{i,j})=g_ig_j^{-1}$. Por tanto, si consideramos el homomorfismos de álgebras

$$\varphi: End_K(V)\longrightarrow M_n(K)$$

$$E_{i,j}\longmapsto e_{i,j}$$

el homomorfismo anterior es un isomorfismo pues tiene inversa, la cual envía al elemento de la base $e_{i,j}$ en $E_{i,j}$, así si definimos $M_n(K)_g = \varphi(End_k(V)_g)$ tenemos una buena $G-$graduación de $M_n(K)$. En efecto, veamos que $M_n(K) = \bigoplus_{g\in G} M_n(K)_g$, para esto note que

$$\begin{aligned}
\varphi(End_K(V)) &= \varphi\left(\sum_{g\in G} End_K(V)_g\right) \\
&= \sum_{g\in G} \varphi(End_K(V)_g) \\
&= \sum_{g\in G} M_n(K)_g
\end{aligned}$$

falta mostrar que dicha suma es directa para esto considere

$$[f_{i,j}] \in M_n(K)_g \cap \sum_{\substack{h\in G \\ h\neq g}} M_n(K)_h,$$

entonces, existen $f \in End_K(V)_g$ tal que $\varphi(f) = [f_{i,j}]$ y $g \in \sum_{\substack{h\in G \\ h\neq g}} End_K(V)_h$ tal que $\varphi(g) = [f_{i,j}]$, por lo tanto $\varphi(f) = \varphi(g)$ y por ser φ un monomorfismo concluimos que $f = g$, lo cual contradice que la suma $\sum_{g\in G} End_K(V)_g$ es directa. Veamos ahora que es una $G-$graduación, en efecto,

$$\begin{aligned}
M_n(K)_g M_n(K)_h &= \varphi(End_K(V)_g)\varphi(End_K(V)_h \\
&= \varphi(End_K(V)_g End_K(V)_h) \\
&= \varphi(End_K(V)_{gh})
\end{aligned}$$

$$= M_n(K)_{gh}.$$

Para finalizar, note que es una buena $G-$graduación pues, $e_{i,j} \in M_n(K)_{g_i g_j^{-1}}$ para todo $i, j \in \{1, \cdots, n\}$.

3.2. Construcción de buenas graduaciones para el anillo de matrices

En esta sección mostraremos que cualquier buena $G-$graduación de $M_n(K)$ se construye de la manera anterior, esto es, contruyendo un isomorfismo de álgebras graduadas entre el álgebra de endomorfismos y el álgebra de matrices. Para ver esto, comenzaremos probando el siguiente lema.

Lema 3.2.1. *Consideremos una buena $G-$graduación en $M_n(K)$. Entonces*

I. $grad(e_{i,i}) = e$,

II. $grad(e_{i,j}) = grad(e_{i,i+1})grad(e_{i+1,i+2}) \cdots grad(e_{j-1,j})$ *para* $i < j$,

III. $grad(e_{i,j}) = grad(e_{i-1,i})^{-1} grad(e_{i-2,i-1})^{-1} \cdots grad(e_{j,j+1})^{-1}$ *para* $i > j$.

Demostración.

I. Basta notar que $e_{i,i}e_{i,i} = e_{i,i}$, es decir, $e_{i,i}$ es un elemento homogéneo idempontente y por la Proposición 2.1.4 concluimos que $grad(e_{i,i}) = e$.

II. Las matrices elementales satisfacen la siguiente igualdad

$$e_{i,j} = e_{i,i+1}e_{i+1,i+2} \cdots e_{j-1,j}$$

para $i < j$. Por tanto, desde que la función *grad* es multiplicativa se tiene

$$\begin{aligned} grad(e_{i,j}) &= grad(e_{i,i+1}e_{i+1,i+2}\cdots e_{j-1,j}) \\ &= grad(e_{i,i+1})grad(e_{i+1,i+2})\cdots grad(e_{j-1,j}). \end{aligned}$$

$III.$ Note que $e_{i,i} = e_{i,j}e_{j,i}$, luego $e = grad(e_{i,i}) = grad(e_{i,j})grad(e_{j,i})$, entonces $grad(e_{j,i})^{-1} = grad(e_{i,j})$. Por la parte I se tiene que para $j < i$

$$grad(e_{j,i}) = grad(e_{j,j+1})grad(e_{j+1,j+2})\cdots grad(e_{i-1,i}),$$

luego,

$$grad(e_{i,j}) = grad(e_{j,i})^{-1} = grad(e_{i-1,i})^{-1}grad(e_{i,i+1})^{-1}\cdots grad(e_{j,j+1})^{-1}.$$

□

Proposición 3.2.2. *Sea una buena $G-$graduación en $M_n(K)$. Entonces, existe un espacio vectorial V el cual es $G-$graduado tal que el isomorfismo $End_K(V) \cong M_n(K)$ con respecto a una base homogénea de V es un isomorfismo de álgebras $G-$graduadas.*

Demostración. Debemos encontrar algunos $g_1,\cdots,g_n \in G$ tales que $grad(e_{i,j}) = g_ig_j^{-1}$ para cualesquiera $i,j \in \{1,\cdots,n\}$. El Lema 3.2.1 muestra que solo basta verificar los pares $(i,j) \in \{(1,2), (2,3),\cdots,(n-1,n)\}$, es decir, $g_ig_{i+1}^{-1} = grad(e_{i,i+1})$, para cualquier $1 \le i \le n-1$, para esto basta considerar

$$g_n = e \quad y \quad g_i = grad(e_{i,i+1})grad(e_{i+1,i+2})\cdots grad(e_{n-1,n}),$$

para cualquier $1 \leq i \leq n-1$, es claro que es un conjunto de elementos del grupo y que se satisface que $grad(e_{i,j}) = g_i g_j^{-1}$. Así, si V es un espacio vectorial de dimensión finita n y $(v_i)_{i=1}^n$ una base de V , definimos V_{g_i} como el subespacio de V generado por el elemento v_i de la base, para cada $1 \leq i \leq n$ y $V_g = \{0\}$ para todo $g \in G$ tal que $g \notin \{g_1, \cdots, g_n\}$. Consideremos la familia $\{V_g\}_{g\in G}$ y veamos que V es un espacio vectorial $G-$graduado por dicha familia. Es claro que $V = \sum_{g\in G} V_g$, además, si $\{h_1, \cdots, h_m\}$ un subconjunto finito de G se cumple que

$$v_{h_1} + \cdots + v_{h_m} = 0 \Leftrightarrow v_{h_k} = 0$$

con $v_{h_k} \in V_{h_k}$ para todo $1 \leq k \leq m$, pues $(v_i)_{i=1}^n$ es una base de V, así usando la Proposición 1.3.8 concluímos que $V = \bigoplus_{g\in G} V_g$. Por lo tanto, el isomorfimo $End_K(V) \cong M_n(K)$ que envía $E_{i,j}$ en $e_{i,j}$ es un isomorfismo de álgebras graduadas. □

Sabemos que una $G-$graduación de la $K-$álgebra de matrices es buena si cada $e_{i,j}$ es un elemento homogéneo. Sin embargo, como se mostrará en el siguiente ejemplo existen graduaciones que no son buenas, pero son isomorfas como álgebras graduadas a buenas graduaciones.

Ejemplo 3.2.3. Sea $R = M_2(K)$ con la $\mathbb{Z}_2-$graduación definida por

$$R_0 = \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix}, \quad R_1 = \begin{pmatrix} 0 & K \\ K & 0 \end{pmatrix}$$

y sea $S = M_2(K)$, veamos que la siguiente es una $\mathbb{Z}_2-$graduación de S

$$S_0 = \left\{ \begin{pmatrix} a & b-a \\ 0 & b \end{pmatrix} : a,b \in K \right\}, \quad S_1 = \left\{ \begin{pmatrix} d & c \\ d & -d \end{pmatrix} : c,d \in K \right\}$$

en efecto, probaremos que $S_0S_0 \subseteq S_0$

$$\begin{pmatrix} a & b-a \\ 0 & b \end{pmatrix} \begin{pmatrix} c & d-c \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & bd-ac \\ 0 & bd \end{pmatrix} \in S_0$$

probaremos ahora que $S_1S_1 \subseteq S_0$

$$\begin{pmatrix} a & b \\ a & -a \end{pmatrix} \begin{pmatrix} d & c \\ d & -d \end{pmatrix} = \begin{pmatrix} ac+bc & ad-bc \\ 0 & ad+ac \end{pmatrix} \in S_0$$

finalmente probaremos que $S_1S_0 \subseteq S_1$ y $S_0S_1 \subseteq S_1$

$$\begin{pmatrix} a & b \\ a & -a \end{pmatrix}\begin{pmatrix} c & d-c \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & ad-ac+bd \\ ac & -ac \end{pmatrix} \in S_1$$

$$\begin{pmatrix} a & b-a \\ 0 & b \end{pmatrix}\begin{pmatrix} d & c \\ d & -d \end{pmatrix} = \begin{pmatrix} bd & ac-bd+ad \\ bd & -bd \end{pmatrix} \in S_1.$$

Con lo anterior tenemos una $\mathbb{Z}_2-$graduación para S, así pues la función

$$f : R \to S, \quad f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} a+c & b+d-a-c \\ c & d-c \end{pmatrix}$$

es un homomorfismo de álgebras $G-$graduadas, pues para $a,b,c,d \in K$ se tiene que

$$f\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = \begin{pmatrix} a & b-a \\ 0 & b \end{pmatrix} \in S_0$$

y

$$f\left(\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}\right) = \begin{pmatrix} c & b-c \\ c & -c \end{pmatrix} \in S_1$$

así $f(R_0) \subseteq S_0$ y $f(R_1) \subseteq S_1$, además es un isomorfismo de álgeras $G-$graduadas pues la función

$$f^{-1} : S \to R, \quad f^{-1}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} a-c & b-d+a-c \\ c & d+c \end{pmatrix}$$

es la inversa de f. La graduación de S no es buena, pues $e_{1,1}$ no es un elemento homogéneo, pero es isomorfa a una buena graduación.

Note que en la graduación de S el elemento $e_{1,2}$ es homogéneo. El siguiente ejemplo muestra que existen graduaciones isomorfas a buenas graduaciones, pero que ningún elemento $e_{i,j}$ es homogéneo.

Ejemplo 3.2.4. Sea $R = M_2(K)$ con la $\mathbb{Z}_2-$graduación del ejemplo anterior

$$R_0 = \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix}, \quad R_1 = \begin{pmatrix} 0 & K \\ K & 0 \end{pmatrix}$$

y sea $S = M_n(K)$, veamos que la siguiente es una $\mathbb{Z}_2-$graduación para S,

$$S_0 = \left\{ \begin{pmatrix} 2a-b & -2a+2b \\ a-b & -a+2b \end{pmatrix} : a,b \in K \right\}$$

$$S_1 = \left\{ \begin{pmatrix} a-2b & -a+4b \\ a-b & -a+2b \end{pmatrix} : a,b \in K \right\}$$

en efecto, probaremos que $S_0S_0 \subseteq S_0$

$$\begin{pmatrix} 2a-b & -2a+2b \\ a-b & -a+2b \end{pmatrix} \begin{pmatrix} 2c-d & -2c+2d \\ c-d & -c+2d \end{pmatrix} = \begin{pmatrix} 2ac-bd & -2ac+2bd \\ ac-bd & -ac+2bd \end{pmatrix} \in S_0$$

probaremos ahora que $S_1S_1 \subseteq S_0$

$$\begin{pmatrix} a-2b & -a+4b \\ a-b & -a+2b \end{pmatrix} \begin{pmatrix} c-2d & -c+4d \\ c-d & -c+2d \end{pmatrix} = \begin{pmatrix} 2bc-ad & -2bc+2ad \\ bc-ad & -bc+2ad \end{pmatrix} \in S_0$$

por último verificaremos que $S_1S_0 \subseteq S_1$ y $S_0S_1 \subseteq S_1$

$$\begin{pmatrix} 2a-b & -2a+2b \\ a-b & -a+2b \end{pmatrix} \begin{pmatrix} c-2d & -c+4d \\ c-d & -c+2d \end{pmatrix} = \begin{pmatrix} bc-2ad & -bc+4ad \\ bc-ad & -bc+2ad \end{pmatrix} \in S_1$$

$$\begin{pmatrix} 2a-b & -2a+2b \\ a-b & -a+2b \end{pmatrix} \begin{pmatrix} c-2d & -c+4d \\ c-d & -c+2d \end{pmatrix} = \begin{pmatrix} ac-2bd & -ac+4bd \\ ac-bd & -ac+2bd \end{pmatrix} \in S_1.$$

Con lo anterior tenemos una $\mathbb{Z}_2-$graduación para S, así pues la función

$$f : R \to S, \quad f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} 2a+c-2b-d & -2a-c+4b+2d \\ a+c-b-d & -a-c+2b+2d \end{pmatrix}$$

es un homomorfismo de álgebras $G-$graduadas, pues para $a,b,c,d \in K$ se tiene que

$$f\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = \begin{pmatrix} 2a-b & -2a+2b \\ a-b & -a+2b \end{pmatrix} \in S_0$$

y

$$f\left(\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}\right) = \begin{pmatrix} c-2b & -c+4b \\ c-b & -c+2b \end{pmatrix} \in S_1$$

así $f(R_0) \subseteq S_0$ y $f(R_1) \subseteq S_1$ y además es un isomorfismo de álgeras $G-$graduadas pues la función

$$f^{-1} : S \to R, \quad f^{-1}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} 2a+b-2c-d & b+a-c-d \\ 4c+2d-2a-b & -a-b+2c+2d \end{pmatrix}$$

es la inversa de f. Por último, note que ningún elemento $e_{i,j}$ es homogéneo en S.

3.3. Buenas graduaciones de $M_n(K)$

En esta última sección estudiaremos las buenas $G-$graduaciones de $M_n(K)$, en particular veremos cuantas buenas $G-$graduaciones existen y cuantas hacen que $M_n(K)$ sea un álgebra fuertemente graduada, además mostraremos caracterizaciones de $M_n(K)$ que la hacen un álgebra fuertemente graduada o un producto cruzado.

Proposición 3.3.1. *Existe una correspondencia biyectiva entre el conjunto de las buenas $G-$graduaciones de $M_n(K)$ y el conjunto de todas las funciones $f : \{1, \cdots, n-1\} \to G$, talque a una buena $G-$graduación le asociamos la función definida por $f(i) = grad(e_{i,i+1})$ para cualquier $1 \leq i \leq n-1$.*

Demostración. El Lema 3,2,1 muestra que para definir una buena $G-$graduación en $M_n(K)$ es suficiente asignar grados a los elementos $e_{1,2}, \cdots, e_{n-1,n}$. La inversa de la función mencionada está dada al tomar $f : \{1, \cdots, n-1\} \to G$ y enviarla a la $G-$graduación de $M_n(K)$ tal que

$$grad(e_{i,i}) = e,$$

$$grad(e_{i,j}) = f(i)f(i+1)\cdots f(j-1)$$

y

$$grad(e_{j,i}) = f(j-1)^{-1}f(j-2)^{-1}\cdots f(i)^{-1}$$

para cualquier $1 \leq i \leq j \leq n$. Sea ϕ la correspondencia enunciada en la proposición y φ a la correspondencia que afirmamos ser su inversa. A continuación, vamos a verificar que en efecto esa función es su inversa. Si tomamos una buena $G-$graduación ϕ envía dicha buena graduación en la función

$$f:\{1,\cdots,n-1\}\longrightarrow G$$

$$i\longmapsto grad(e_{i,i+1}),$$

luego, φ envía la función en la buena $G-$graduación definida como sigue

$$grad(e_{i,i})=e,$$

$$grad(e_{i,j})=f(i)f(i+1)\cdots f(j-1)$$

y

$$grad(e_{j,i})=f(j-1)^{-1}f(j-2)^{-1}\cdots f(i)^{-1},$$

para cada $1\leq i\leq j\leq n$. Teniendo encuenta que dos buenas $G-$graduaciones son iguales si los grados de las matrices elementales de una coincide con el grado de las matrices elementales de la otra, denotaremos por $grad(e_{i,j})_1$ al $grad(e_{i,j})$ con la primer buena graduación y por $grad(e_{i,j})_2$ al $grad(e_{i,j})$ con la segunda buena graduación, por definición de la función f y por el Lema 3.2.1 tenemos que

$$gard(e_{i,i})_1=e=grad(e_{i,i})_2,$$

$$\begin{aligned} grad(e_{i,j})_2 &= f(i)f(i+1)\cdots f(j-1) \\ &= grad(e_{i,i+1})_1 \cdots grad(e_{j-1,j})_1 \\ &= grad(e_{i,j})_1 \end{aligned}$$

y de manera análoga probamos que

$$grad(e_{j,i})_2 = grad(e_{j,i})_1.$$

Por otra parte, sea $f : \{1, \cdots, n-1\} \to G$, la función φ envía a f en la buena $G-$graduación definida como

$$grad(e_{i,i}) = e,$$

$$grad(e_{i,j}) = f(i)f(i+1)\cdots f(j-1)$$

y

$$grad(e_{j,i}) = f(j-1)^{-1} f(j-2)^{-1} \cdots f(i)^{-1},$$

note que si despejamos obtenemos que

$$f(i) = grad(e_{i,j}) f(j-1)^{-1} \cdots f(i+1)^{-1}$$

y ϕ envía esta buena $G-$graduación en la función

$$g : \{1, \cdots, n-1\} \longrightarrow G$$
$$i \longmapsto grad(e_{i,i+1}).$$

Veamos que $f = g$, en efecto, sea $i \in \{1, \cdots, n-1\}$, entonces si $1 \leq i \leq j \leq n$ tenemos

$$\begin{aligned} g(i) &= grad(e_{i,i+1}) \\ &= grad(e_{i,j})grad(e_{j,i+1}) \\ &= grad(e_{i,j})f(j-1)^{-1} \cdots f(i+1)^{-1} \\ &= f(i). \end{aligned}$$

Concluimos así que dicha correspondecia actua como inversa de ϕ. □

Corolario 3.3.2. *Existen $|G|^{n-1}$ buenas graduaciones en $M_n(K)$.*

Demostración. Por la Proposición 3.3.1 tenemos una correspondencia biyectiva entre el conjunto de las buenas $G-$graduaciones de $M_n(K)$ y el conjunto de todas las funciones $f : \{1, \cdots, n-1\} \to G$, en consecuencia hay tantas buenas $G-$graduaciones como funciones $f : \{1, \cdots, n-1\} \to G$, y existen $|G|^{n-1}$ funciones. □

El siguiente teorema da una caracterización de las buenas $G-$graduaciones que hacen que el álgebra $M_n(K)$ sea un álgebra fuertemente graduada.

Teorema 3.3.3. *Consideremos el álgebra $End_K(V) \cong M_n(K)$ con una buena G-graduación tal que $grad(e_{i,i+1}) = h_i$ para $1 \leq i \leq n-1$, donde $V = \bigoplus_{g \in G} V_g$ es un espacio vectorial graduado. Las siguientes afirmaciones son equivalentes:*

I. *$M_n(K)$ es un álgebra fuertemente graduada.*

II. *$V_g \neq 0$ para todo $g \in G$.*

III. *Todos los elementos de G aparecen en la sucesión $e, h_1, h_1h_2, \cdots, h_1h_2\cdots h_{n-1}$.*

Demostración. Esta demostración se hará mostrando que la primera condición es equivalente a la segunda y la segunda es equivalente a la tercera.

$I \Rightarrow II$ Note que V es un objeto de $gr-K$, donde K es visto como un álgebra $G-$graduada con la graduación trivial. Por la Proposición 2.3.5, $End_K(V) \cong M_n(K)$ es fuertemente graduado, si y sólo si, V es débilmente $G-$invariante, es decir, si V divide débilmente a $(h)V$ para cualquier $h \in G$, lo cual por la Proposición 2.3.3, es equivalente a que existan $f_1, \cdots, f_t \in Hom_{gr-K}(V, (h)V)$ y $g_1, \cdots, g_t \in Hom_{gr-K}((h)V, V)$ tales que

$$i_V = f_1 \circ g_1 + \cdots + f_t \circ g_t, \tag{3}$$

para todo $h \in G$, lo anterior implica que $V_g \neq \{0\}$ para todo $g \in G$, pues de lo contrario, si existe $g \in G$ tal que $V_g = \{0\}$ se tiene que para cada $l \in G$, existe $h \in G$ tal que $l = hg$ y por la ecuación (3.1)

$$V_l = f_1 \circ g_1(V_l) + \cdots + f_t \circ g_t(V_l).$$

Puesto que cada g_i es un homomorfismo graduado tenemos que

$$g_i(V_l) = g_i(V_{hg}) \subseteq V_{h^{-1}hg} = V_g = \{0\}$$

y desde que cada $f_i(0) = 0$ concluimos que $V_l = \{0\}$ para todo $l \in G$, lo cual es absurdo.

$II \Rightarrow I$ Veamos que si $V_g \neq 0$, para todo $g \in G$, entonces $M_n(K)$ es un álgebra fuertemente graduada. Sea $\mathscr{B} = (v_i)_{1 \leq i \leq n}$ una base de elementos homogéneos de V y denotamos por $g_i = grad(v_i)$. Mostraremos que

$$G = \{g_1, \cdots, g_n\}. \tag{4}$$

Es claro que $\{g_1, \cdots, g_n\} \subseteq G$ pues los grados son elementos de G, por otra parte, supongamos que existe $g \in G$ tal que $g \notin \{g_1, \cdots, g_n\}$, definamos $G_i = \{g_1, \cdots, g_n\}$, desde que $\mathscr{B}$ es una base, tenemos que

$$V = \langle v_1, \cdots, v_n \rangle = \sum_{g_i \in G_i} V_{g_i},$$

por hipótesis, $V_g \neq \{0\}$ lo cual contradice que $V = \bigoplus_{g \in G} V_g$, pues

$$\begin{aligned} V_g &= V_g \cap V \\ &= V_g \cap \sum_{g \in G_i} V_{g_i} \\ &\neq \{0\}. \end{aligned}$$

Así obtenemos la ecuación (3.2). Ahora, Consideremos $g \in G$ y $j \in \{1, \cdots, n\}$, luego $gg_j \in G$, por (3.2) existe $i \in \{1, \cdots, n\}$ tal que

$$\begin{aligned} gg_j &= g_i \\ g &= g_i g_j^{-1} \\ g &= grad(E_{i,j}) \\ g &= grad(e_{i,j}) \\ g^{-1} &= grad(e_{j,i}) \end{aligned}$$

y como $e_{i,j}$, $e_{j,i}$ son elementos homogéneos de grado g, g^{-1} respectivamente, tenemos que $e_{i,j} \in M_n(K)_g$ y $e_{j,i} \in M_n(K)_{g^{-1}}$. Así

$$e_{i,i} = e_{i,j}e_{j,i} \in M_n(K)_g M_n(K)_{g^{-1}}$$

para todo $i \in \{1, \cdots, n\}$, luego

$$1_{M_n(K)} = e_{1,1} + \cdots + e_{n,n} \in M_n(K)_g M_n(K)_{g^{-1}}$$

de esta manera concluímos por la Proposición 2.1.3 *III*. que $M_n(K)$ es un álgebra fuertemente graduada.

$II \Leftrightarrow III$ Si $g_1, \cdots, g_n$ son los grados de los elementos de la base de V la cual induce el isomorfismo $End(V)_K \cong M_n(K)$, entonces por lo mostrado al inicio de este capítulo $grad(e_{i,j}) = grad(E_{i,j}) = g_i g_j^{-1}$, es decir,

$$h_1 = g_1 g_2^{-1}, h_2 = g_2 g_3^{-1}, \cdots, h_{n-1} = g_{n-1} g_n^{-1},$$

esto es

$$g_2 = h_1^{-1} g_1, g_3 = h_2^{-1} h_1^{-1} g_1, \cdots, g_n = h_{n-1}^{-1} \cdots h_1^{-1} g_1,$$

luego $V_g \neq 0$ para cualquier $g \in G$, si y sólo si, todos los elementos de G aparecen en la sucesión $g_1, \cdots, g_n$. En efecto, la condición necesaria se mostró en $II \Rightarrow I$ y la condición suficiente se obtiene, pues si todos los elementos de G aparecen en $g_1, \cdots, g_n$, entonces $V_g \neq \{0\}$, pues contiene almenos al elemento de la base de grado g. Con lo anterior, desde que

$$g_2 = h_1^{-1} g_1, g_3 = h_2^{-1} h_1^{-1} g_1, \cdots, g_n = h_{n-1}^{-1} \cdots h_1^{-1} g_1$$

esto es equivalente a probar III.

$\square$

Presentaremos a continuación unos corolarios del teorema anterior.

Corolario 3.3.4. *Si $M_n(K)$ tiene una buena $G-$graduación que la hace un álgebra fuertemente graduada, entonces $|G| \leq n$.*

Demostración. Por el Teorema anterior sabemos que todos los elementos de G aparece en el sucesión $e, h_1, h_1h_2, \cdots, h_1h_2\cdots h_{n-1}$, la cual tiene n elementos no necesariamente diferentes, por tanto $|G| \leq n$. □

Corolario 3.3.5. *Sea $|G| = m \leq n$. Entonces el número de buenas $G-$graduaciones sobre $M_n(K)$ que la hacen un álgebra fuertemente graduada es*

$$m^{n-1} + (m-1)^{n-1} - \sum_{i=1}^{m-1} (-1)^{i+1} \binom{m}{i} (m-i)^{n-1} -$$

$$\sum_{i=1}^{m-2} (-1)^{i+1} \binom{m-1}{i} (m-i-1)^{n-1}.$$

Demostración. Comenzaremos probando que existe una correspondencia biyectiva entre las buenas graduaciones sobre $M_n(K)$ que la hacen un álgebra fuertemente graduada y las funciones $f : \{1, \cdots, n-1\} \to G$ tales que $G - \{e\} \subseteq Im(f)$. En efecto, consideremos la función que toma una buena $G-$graduación sobre $M_n(K)$ que la hacen un álgebra fuertemente graduada y la enviamos a la función f definida como sigue

$$\begin{aligned} f : \{1, \cdots, n-1\} &\longrightarrow G \\ i \quad &\longmapsto h_1h_2\cdots h_i \end{aligned}$$

donde $h_i = grad(e_{i,i+1})$, para cada $i \in \{1, \cdots, n-1\}$, notemos que $G - \{e\} \subseteq Im(f)$, pues por el teorema anterior todos los elemento de $G - \{e\}$ aparecen en la sucesión $h_1, h_1h_2, \cdots, h_1h_2\cdots h_{n-1}$. La correspondencia anterior es biyectiva, pues la siguiente correspondencia es su inversa, sea g :

$\{1,\cdots,n-1\} \longrightarrow G$ una función tal que $G-\{e\} \subseteq Im(g)$. El Lema 3.2.1 muestra que para definir una buena $G-$graduación basta asignar los grados para los pares $(i,j) \in \{(1,2),\cdots,(n-1,n)\}$, así enviaremos a la función g en la graduación definida de la siguiente manera

$$\begin{cases} grad(e_{i,i+1}) = g(1) = h_1 & si \quad i=1 \\ grad(e_{i,i+1}) = f(i-1)^{-1}f(i) = h_i & si \quad 1 < i \leq n \end{cases}.$$

Lo anterior implica que existen tantas buenas graduaciones sobre $M_n(K)$ que la hacen un álgebra fuertemente graduada como funciones $f:\{1,\cdots,n-1\} \to G$ tales que $G-\{e\} \subseteq Im(f)$, por lo que debemos contar el número de funciones $f:\{1,2,\cdots,n-1\} \to G$ tal que $G-\{e\} \subseteq Im(f)$. Esto es, N_1+N_2, donde N_1 (respectivamente N_2) es el número de funciones sobreyectivas de $f:\{1,\cdots,n-1\} \to G-\{e\}$ (respectivamente $f:\{1,\cdots,n-1\} \to G$). Por un resultado clásico de combinatoria que podemos encontrar en (Isaacs, 2004, pág. 9–10) tenemos que

$$\begin{aligned} N_2 &= \sum_{i=0}^{m}(-1)^i\binom{m}{i}(m-i)^{n-1} \\ &= m^{n-1} + \sum_{i=1}^{m}(-1)^i\binom{m}{i}(m-i)^{n-1} \\ &= m^{n-1} + (1)^m\binom{m}{m}(m-m)^{n-1} + \sum_{i=1}^{m-1}(-1)^i\binom{m}{i}(m-i)^{n-1} \\ &= m^{n-1} + \sum_{i=1}^{m-1}(-1)^i\binom{m}{i}(m-i)^{n-1} \\ &= m^{n-1} - \sum_{i=1}^{m-1}(-1)^{i+1}\binom{m}{i}(m-i)^{n-1}, \end{aligned}$$

y

$$\begin{aligned}
N_1 &= \sum_{i=0}^{m-1} (-i)^i \binom{m-1}{i} (m-1-i)^{n-1} \\
&= (m-1)^{n-1} + \sum_{i=1}^{m-1} (-1)^i \binom{m-1}{i} (m-1-i)^{n-1} \\
&= (m-1)^{n-1} + (1)^{m-1} \binom{m-1}{m-1} (m-1-(m-1))^{n-1} + \sum_{i=1}^{m-2} (-1)^i \binom{m-1}{i} (m-1-i)^{n-1} \\
&= (m-1)^{n-1} - \sum_{i=1}^{m-2} (-1)^{i+1} \binom{m-1}{i} (m-1-i)^{n}.
\end{aligned}$$

Luego,

$$N_1 + N_2 = m^{n-1} + (m-1)^{n-1} - \sum_{i=1}^{m-1} (-1)^{i+1} \binom{m}{i} (m-i)^{n-1} -$$

$$\sum_{i=1}^{m-2} (-1)^{i+1} \binom{m-1}{i} (m-i-1)^{n-1}.$$

□

El siguiente teorema da una caracterización de las buenas $G-$graduaciones que hacen que el álgebra $M_n(K)$ sea un producto cruzado.

Teorema 3.3.6. *Sea $End_K(V) \cong M_n(K)$ con una buena G-graduación, donde $V = \bigoplus_{g\in G} V_g$ es un espacio vectorial graduado. Las siguientes afirmaciones son equivalentes:*

I. *$M_n(K)$ es un producto cruzado.*

II. *$dim(V) = |G| \cdot dim(V_g)$ para cualquier $g \in G$.*

III. $dim(M_n(K)_e) \cdot |G| = n^2$.

IV. $M_n(K)_e \cong M_t(K) \times \cdots \times M_t(K)$ *($|G|$ veces), donde* $t = \frac{n}{|G|}$.

Antes de demostrar este teorema, mostraremos unos resultados requeridos.

Lema 3.3.7. *Sean V, W espacios vectoriales sobre K de dimensión finita y sea $\{V_g\}_{g \in G}$ una familia de subespacios vectoriales de V. Entonces:*

I. *Si S, T son subespacios vectoriales de V, entonces* $dim(S+T) = dim(S) + dim(T) - dim(S \cap T)$.

II. *Si* $V = \bigoplus_{g \in G} V_g$, *entonces* $dim(\sum_{g \in G} V_g) = \sum_{g \in G} dim(V_g)$.

III. $V \cong W$, *si y sólo si,* $dim(V) = dim(W)$.

IV. *Si* $V = \bigoplus_{g \in G} V_g$, *entonces* $End_{K-gr}(V) \cong \bigoplus_{g \in G} End(V_g)$ *como espacios vectoriales.*

V. $dim(V \times W) = dim(V) + dim(W)$.

Demostración. A continuación probaremos cada item:

I. Sea $\mathscr{B} = \{b_1, \cdots, b_m\}$ una base de $S \cap T$. Esta base es linealmente independiente en S y T, extendamos $\mathscr{B}$ a una base $\mathscr{A} \cup \mathscr{B}$ para S donde $\mathscr{A} = \{a_1, \cdots, a_j\}$ es disjunta de $\mathscr{B}$ y a una base $\mathscr{B} \cup \mathscr{C}$ de T donde $\mathscr{C} = \{c_1, \cdots, c_k\}$ es disjunta de $\mathscr{B}$. Afirmamos que $\mathscr{A} \cup \mathscr{B} \cup \mathscr{C}$ es una base de $S+T$. Es claro que $\langle \mathscr{A} \cup \mathscr{B} \cup \mathscr{C} \rangle = S+T$. Veamos ahora que $\mathscr{A} \cup \mathscr{B} \cup \mathscr{C}$ es linealmente independiente, supongamos que

$$\sum_{i=1}^{m} \beta_i b_i + \sum_{i=1}^{j} \alpha_i a_i + \sum_{i=1}^{k} \gamma_i c_i = 0 \tag{5}$$

donde $\alpha_i, \beta_i, \gamma_i \in K$, para todo i. Si reescribimos la ecuación $(3,3)$

$$\sum_{i=1}^{k} \gamma_i c_i = -\sum_{i=1}^{m} \beta_i b_i - \sum_{i=1}^{j} \alpha_i a_i$$

concluimos con lo anterior que $\sum_{i=1}^{k} \gamma_i c_i \in S$, pues es una combinación lineal de la base $\mathscr{A} \cup \mathscr{B}$. Pero sabemos que los $c_i's$ están en T, luego $\sum_{i=1}^{k} \gamma_i c_i \in S \cap T$, como $\mathscr{B}$ es una base de $S \cap T$ y además disjunta de $\mathscr{C}$, tomemos $\lambda_i \in K$ tal que

$$\sum_{i=i}^{k} \gamma_i c_i = \sum_{i=1}^{m} \lambda_i b_i \Leftrightarrow \sum_{i=i}^{k} \gamma_i c_i - \sum_{i=1}^{m} \lambda_i b_i = 0,$$

pero sabemos que los $c_i's$ y $b_i's$ son linealmente independientes, luego $\gamma_i = \lambda_i = 0$. Por tanto, la ecuación $(3,3)$ se convierte en

$$\sum_{i=1}^{m} \beta_i b_i + \sum_{i=1}^{j} \alpha_i a_i = 0$$

y ya que los $b_i's$, $c_i's$ son linealmente independientes, tenemos que $\alpha_i = \beta_i = 0$. Así, conluimos que $\mathscr{A} \cup \mathscr{B} \cup \mathscr{C}$ es una base de $S+T$. Por lo anteror,

$$\begin{aligned} dim(S)+dim(T) &= |\mathscr{A} \cup \mathscr{B}| + |\mathscr{C} \cup \mathscr{B}| \\ &= |\mathscr{A}| + |\mathscr{B}| + |\mathscr{C}| + |\mathscr{B}| \\ &= |\mathscr{A}| + |\mathscr{B}| + |\mathscr{C}| + dim(S \cap T) \\ &= dim(S+T) + dim(S \cap T), \end{aligned}$$

con lo cual completamos la prueba.

II. Esta demostración la haremos por inducción sobre $|G|$

Base inductiva: Para $|G| = 2$ sea $G = \{e, g\}$, por I tenemos que

$$dim(V_e + V_g) = dim(V_e) + dim(V_g) - dim(V_e \cap V_g),$$

pero por ser V una suma directa $V_e \cap V_g = \{0\}$, así que

$$dim(V_e + V_g) = dim(V_e) + dim(V_g).$$

Hipótesis inductiva: Vamos a suponer que para $|G| = n$, tenemos

$$dim\left(\sum_{g \in G} V_g\right) = \sum_{g \in G} dim(V_g).$$

Paso inductivo: Consideremos $|G| = n+1$, luego

$$
\begin{aligned}
dim\left(\sum_{g\in G} V_g\right) &= dim\left(\sum_{g\in G-\{h\}} V_g + V_h\right) \\
&= dim\left(\sum_{g\in G-\{h\}} V_g\right) + dim(V_h) - dim\left(\sum_{g\in G-\{h\}} V_g \cap V_h\right) \qquad (6)\\
&= dim\left(\sum_{g\in G-\{h\}} V_g\right) + dim(V_h) \qquad (7)\\
&= \sum_{g\in G-\{h\}} dim(V_g) + dim(V_h) \\
&= \sum_{g\in G} dim(V_g) \qquad (8)
\end{aligned}
$$

note que la igualdad $(3{,}4)$ se da por $I.$, la igualdad $(3{,}5)$ se da pues V es suma directa y la igualdad $(3{,}6)$ por hipótesis inductiva.

$III.$ Sea $dim(V) = n$. Veamos que si $\mathscr{A} = \{a_1, \cdots, a_n\}$ es una base de V y $f : V \to W$ es un isomorfismo, entonces $\mathscr{B} = \{f(a_1), \cdots, f(a_n)\}$ es una base de W. Mostraremos que $\mathscr{B}$ es linealmente independiente, para esto tomemos escalares $\lambda_1, \cdots, \lambda_n \in K$ tales que

$$\sum_{j=1}^{n} \lambda_j f(a_j) = 0_W$$

por la linealidad de f, tenemos

$$f\left(\sum_{j=1}^{n} \lambda_j a_j\right) = 0_W$$

lo que significa que $\sum_{j=1}^{n} \lambda_j a_j \in Ker(f)$, pero f es inyectiva, lueo $Ker(f) = \{0\}$, así

$$\sum_{j=1}^{n} \lambda_j a_j = 0_V$$

y por la independencia lineal de $\mathscr{A}$, conluimos que $\lambda_1 = \cdots = \lambda_n = 0$. Además, note que por ser f un isomorfismo $\mathscr{B}$ es un conjunto generador. Reciprocamente, vamos a suponer que $dim(V) = dim(W) = m$, sean $\mathscr{B} = \{b_1, \cdots, b_m\}$ una base de V y $\mathscr{A} = \{a_1, \cdots, a_m\}$ una base de W, veamos que la función

$$\begin{aligned} f : V &\longrightarrow W \\ b_i &\longmapsto a_i \end{aligned}$$

es un isomorfismo.

Existencia: Dado $v \in V$, existen escalares únicos $\alpha_1, \cdots, \alpha_m \in K$ tales que

$$v = \sum_{i=1}^{m} \alpha_i b_i.$$

Definimos $f(v) = \sum_{i=1}^{m} \alpha_i a_i$. Veamos que f es una transformación lineal. Sean $v, v' \in V$, supongamos que

$$v = \sum_{i=1}^{m} \alpha_i b_i \quad y \quad v' = \sum_{i=1}^{m} \alpha_i' b_i',$$

entonces

$$v+v' = \sum_{i=1}^{m} \alpha_i b_i + \sum_{i=1}^{m} \alpha_i' b_i = \sum_{i=1}^{m} (\alpha_i + \alpha_i') b_i$$

y en consecuencia,

$$f(v+v') = \sum_{i=1}^{m} (\alpha_i + \alpha_i') a_i = \sum_{i=1}^{m} \alpha_i a_i + \sum_{i=1}^{m} \alpha_i' a_i = f(v) + f(v').$$

De manera análoga se prueba que $f(\lambda v) = \lambda f(v)$, para todo $v \in V$ y $\lambda \in K$.

Inyectividad: Veamos que $Ker(f) = \{0\}$. Sea $v \in Ker(f)$, entoces $f(v) = 0_W$, dado que $v \in V$ tenemos que $v = \sum_{i=1}^{m} \alpha_i b_i$, luego

$$f(v) = f(\sum_{i=1}^{m} \alpha_i b_i) = \sum_{i=1}^{m} \alpha_i f(b_i) = \sum_{i=1}^{m} \alpha_i a_i = 0_W$$

y por ser $\mathscr{A}$ una base $\alpha_i = 0$ para todo $\alpha_i \in K$. Por tanto, $v = \sum_{i=1}^{m} \alpha_i b_i = 0$.

Sobreyectividad: Sea $w \in W$, entonces existen $\alpha_1, \cdots \alpha_m \in K$ tales que

$$w = \sum_{i=1}^{m} \alpha_i a_i.$$

Así, consideremos el elemento en V tal que es generado por $\alpha_1, \cdots \alpha_m \in K$, es decir, $v = \sum_{i=1}^{m} \alpha_i b_i$, luego $f(v) = w$.

IV. Recordemos que

$$End_{gr-K}(V) = \{f \in End_K(V) \mid f(V_g) \subseteq V_g \; para \; cada \; g \in G\}.$$

Consideremos el homomorfismo

$$\begin{aligned} \varphi : End_{gr-K}(V) &\longrightarrow \bigoplus_{g\in G} End(V_g) \\ f &\longmapsto \sum_{g\in G} f_g \end{aligned}$$

donde $f_g \in End(V_g)$ para cada $g \in G$ se define como sigue

$$\begin{aligned} f_g : V_g &\longrightarrow V_g \\ v &\longmapsto f(v) \end{aligned}$$

note que la función anterior está bien definida, pues por definición de $End_{gr-K}(V)$ se tiene que $f(V_g) \subseteq V_g$, además note que la función $f = \sum_{g\in G} f_g$, en efecto, sean $v \in V = \bigoplus_{g\in G} V_g$ y $v = \sum_{g\in G} v_g$ la descomposición de v como suma finita, entonces

$$f(v) = f\left(\sum_{g\in G} v_g\right)$$

$$= \sum_{g\in G} f(v_g)$$

$$= \sum_{g\in G} f_g(v_g).$$

La función φ es un isomorfismo pues, el siguiente homomorfismo actúa como inversa

$$\varphi^{-1} : \bigoplus_{g\in G} End(V_g) \longrightarrow End_{gr-K}(V)$$

$$\sum_{g\in G} h_g \longmapsto h,$$

donde $h : V \to V$ envia a $v \in V$ cuya descomposición está dada por $v = \sum_{g\in G} v_g$ en

$$h\left(\sum_{g\in G} v_g\right) = \sum_{g\in G} h(v_g) = \sum_{g\in G} h_g(v_g).$$

V. Sean $\mathscr{B} = \{v_i\}_{i=1}^n$ una base de V y $\mathscr{W} = \{w_i\}_{i=1}^m$ una base de W. Vamos a mostrar que $(\mathscr{B} \times 0_W) \cup (0_V \times \mathscr{A})$ es una base de $V \times W$. En efecto, sea $(x,y) \in V \times W$ tenemos

$$(x,y) = (x, 0_V) + (0_W, y),$$

lo anterior para cada $x \in V$ y $y \in W$. Por otra parte, si $v_1, \cdots, v_n \in \mathscr{B}$, $w_1, \cdots, w_m \in \mathscr{W}$, entonces

$$r_1(v_1, 0_W) + \cdots + r_n(v_n, 0_W) + s_1(0_V, w_1) + \cdots + s_m(0_V, w_m)$$

$$= (r_1v_1 + \cdots + r_nv_n, s_1w_1 + \cdots + s_mw_m)$$

así pues, $w_1, \cdots, w_m \in \mathscr{W}$, luego

$$r_1(v_1, 0_W) + \cdots + r_n(v_n, 0_W) + s_1(0_V, w_1) + \cdots + s_m(0_V, w_m) = (0_V, 0_W),$$

si y sólo si,

$$r_1v_1 + \cdots + r_nv_n = 0_V \quad y \quad s_1(0_V, w_1) + \cdots + s_m(0_V, w_m) = 0_W.$$

De ahí que, $\mathscr{B} \times 0_W \cup 0_V \times \mathscr{A}$ es una base de $V \times W$, luego

$$dim(V \times W) = dim(V) + dim(W).$$

El resultado anterior, puede extenderse para k espacios vectoriales, es decir, si $V_1, \cdots, V_k$ son espacios vectoriales de dimensión finita, $dim(V_1 \times \cdots \times V_k) = \sum_{i=1}^{k} dim(V_i)$.

$\square$

Lema 3.3.8. *Sea V un espacio vectorial $G-$graduado. Si $V \cong (g')V$ con $g' \in G$ es un isomorfismo graduado, entonces $dim(V_g) = dim(V_{g'g})$ para todo $g \in G$.*

Demostración. Sea $\varphi : V \to (g')V$ un isomorfismo graduado, por definición $\varphi(V_g) \subseteq (g')V_g = V_{g'g}$ para todo $g \in G$. Veamos que $\varphi(V_g) = V_{g'g}$. Sea $w \in V_{g'g}$, entonces por ser φ un epimorfismo, existe $v \in V$ tal que $\varphi(v) = w$, si $v = \sum_{h \in G} v_h$ con $v_h \in V_h$, es la descomposición de v como suma finita, se sigue que

$$w = \varphi(v) = \varphi\left(\sum_{h\in G} v_h\right) = \sum_{h\in G} \varphi(v_h),$$

donde cada $\varphi(v_h) \in (g')V_h$. Puesto que w es un elemento homogéneo, tenemos que $\varphi(v_h) = 0$ para todo $h \in G$ con $g \neq h$, pero φ es un monomorfismo, esto es $v_h = 0$ para todo $h \neq g$, por lo tanto $w = \varphi(v_g) \in \varphi(V_g)$. Así, si tomamos una base $\mathscr{B}_g$ de V_g, siguiendo la demostración del Lema 3.3.7 inciso *III* $\varphi(\mathscr{B}_g)$ es una base de $V_{g'g}$, concluyendo así que $dim(V_g) = dim(V_{g'g})$. □

Lema 3.3.9 (*Desigualdad de Cauchy-Schwartz*)**.** *Si $a_1, \cdots, a_n$ y $b_1, \cdots, b_n$ son números reales arbitrarios, tenemos*

$$\left(\sum_{ik=1}^{n} a_k b_k\right)^2 \leq \left(\sum_{k=1}^{n} a_k^2\right)\left(\sum_{k=1}^{n} b_k^2\right).$$

Además, la igualdad se verifica, si y sólo si, existe un número real x tal que $a_k x + b_k = 0$ para cada $1 \leq k \leq n$.

Demostración. Ver (Apostol, 1992, pág. 17). □

Con los Lemas anteriores podemos dar paso a la demostración del Teorema 3.3.6.

Demostración. Esta demostración se hará mostrando las siguientes implicaciones $I \Leftrightarrow II$, $I \Rightarrow III$, $III \Rightarrow II$ Y $III \Leftrightarrow IV$.

$I \Leftrightarrow II$ Por definición y puesto que V es un espacio vectorial de dimensión finita tenemos que $END_K(V) = End_K(V) \cong M_n(K)$ es un producto cruzado, si y sólo si, $End(V)_{g'} = Hom_{gr-K}(V, (g')V)$ contiene un elemento invertible para cualquier $g' \in G$. Lo anterior es equivalente a que

$V \cong (g')V$ para todo $g' \in G$, pues $f \in End_K(V)$ es invertible, si y sólo si, f es un isomorfismo. Ahora, veamos que $V \cong (g')V$, si y sólo si, $dim(V_{g'g}) = dim(V_g)$, para todo $g', g \in G$. En efecto, si $dim(V_{g'g}) = dim(V_g)$, entonces

$$\sum_{g \in G} dim(V_{g'g}) = \sum_{g \in G} dim(V_g), \tag{9}$$

luego,

$$\begin{aligned} dim(V) &= dim\left(\sum_{g \in G} V_g\right) \\ &= \sum_{g \in G} (dim(V_g)) \qquad (10) \\ &= \sum_{gg' \in G} (dim(V_{g'g})) \qquad (11) \\ &= dim((g')V) \end{aligned}$$

note que la igualdad $(3{,}8)$ se da por II. del Lema 3.3.7 y que la igualdad $(3{,}12)$ se da por $(3{,}9)$. Así, concluimos por el inciso III. del Lema 3.3.7 que $V \cong (g')V$. Recíprocamente, si $V \cong (g')V$, por el Lema 3.3.8 $dim(V_g) = dim(V_{g'g})$, para todo $g' \in G$. Con lo anterior, sea $k \in G$ arbitrario, se sigue que $g^{-1}k \in G$, tomando $g' = kg^{-1}$, tenemos

$$\begin{aligned} dim(V_g) &= dim(V_{g'g}) \\ &= dim(V_{kg^{-1}g}) \end{aligned}$$

$$= dim(V_k)$$

lo anterior para todo $k \in G$. Luego, $dim(V) = dim(\sum_{g\in G} V_g) = \sum_{g\in G}(dim(V_g)) = |G| \cdot dim(V_g)$ para cualquier $g \in G$.

$I \Rightarrow III$ Si consideramos $M_n(K) = \bigoplus_{g\in G} M_n(K)_g$ como espacio vectorial graduado, tenemos por la Proposición 2.1.6 inciso II. que

$$M_n(K)_e \cong M_n(K)_g,$$

luego,

$$dim(M_n(K)_e) = dim(M_n(K)_g),$$

para todo $g \in G$. Así,

$$\begin{aligned} n^2 = dim(M_n(K)) = dim\left(\sum_{g\in G} M_n(K)_g\right) \\ &= \sum_{g\in G} dim(M_n(K)_g) \\ &= \sum_{g\in G} dim(M_n(K)_e) \\ &= |G| \cdot dim(M_n(K)_e) \end{aligned}$$

con lo cual concluimos III.

$III \Rightarrow II$ Supongamos que $dim(M_n(K)_e) \cdot |G| = n^2$. Notemos que

$$End(V)_e = \{f \in End_K(V) \mid f(V_g) \subseteq V_{eg} = V_g \text{ para todo } g \in G\} = End_{gr-K}(V),$$

Por el Lema 3.3.7 inciso *IV*.

$$End(V)_e = End_{gr-K}(V) = \bigoplus_{g\in G} End_K(V_g)$$

luego,

$$\begin{aligned} dim(M_n(K)_e) &= dim(End(V)_e) \\ &= dim(End_{gr-K}(V)) \\ &= dim(\sum_{g\in G} End_K(V_g)) \\ &= \sum_{g\in G} dim(End_K(V_g)) \\ &= \sum_{g\in G} (dim(V_g))^2 \end{aligned} \tag{12}$$

(la igualdad $(3{,}10)$ se da por el inciso II. del lema). Entonces por hipótesis

$$|G| \cdot dim(M_n(K)_e) = |G| \cdot \sum_{g\in G} (dim(V_g))^2 = n^2 = \left(\sum_{g\in G} dim(V_g)\right)^2$$

Tomemos $a_k = dim(V_g)$ y $b_k = 1$. Por la desigualdad de Cauchy-Shwartz tenemos

$$\begin{aligned}\left(\sum_{g\in G} dim(V_g)\right)^2 &\leq \sum_{g\in G} 1^2 \cdot \sum_{g\in G} (dim(V_g))^2 \\ &= |G| \cdot \sum_{g\in G} (dim(V_g))^2\end{aligned}$$

Como se satisface la igualdad existe un número real x tal que $dim(V_g) + x = 0$ para todo $g \in G$, luego $x = -dim(V_g)$, pero el número x es fijo, por lo tanto $dim(V_g) = dim(V_k)$ para todo $k \in G$, así concluimos que

$$\begin{aligned}dim(V) &= dim\left(\sum_{g\in G} V_g\right) \\ &= \sum_{g\in G} (dim(V_g)) \\ &= |G| \cdot dim(V_g).\end{aligned}$$

$III \Rightarrow IV$ Vamos a suponer que $dim(M_n(K)_e) \cdot |G| = n^2$. Por el Lema 3.3.7 inciso V.

$$\begin{aligned}dim(M_t(K) \times \cdots \times M_t(K)) &= \sum_{g\in G} dim(M_t(K)) \\ &= |G| \cdot dim(M_t(K)) \\ &= |G| \cdot \frac{n^2}{|G|^2} \\ &= \frac{n^2}{|G|}\end{aligned}$$

$$= \frac{dim(M_n(K)_e) \cdot |G|}{|G|}$$

$$= dim(M_n(K)_e)$$

así pues, por III. del Lema 3.3.7 concluimos que $M_n(K)_e \cong M_t(K) \times \cdots \times M_t(K)$.

$IV \Rightarrow III$ Comenzaremos por suponer que $M_n(K)_e \cong M_t(K) \times \cdots \times M_t(K)$, en consecuencia por el Lema 3.3.7 inciso III. e inciso V.

$$\begin{aligned} dim(M_n(K)_e) &= dim(M_t(K) \times \cdots \times M_t(K)) \\ &= \sum_{g \in G} dim(M_t)(K) \\ &= |G| \cdot \frac{n^2}{|G|^2} \\ &= \frac{n^2}{|G|} \end{aligned}$$

de ahí que, $dim(M_n(K)_e) \cdot |G| = n^2$.

$\square$

Para finalizar, mencionaremos un corolario resultado del Teorema 3.3.6 y unos ejemplos.

Corolario 3.3.10. *Cualesquiera dos estructuras de productos cruzados en $M_n(K)$ que tienen buenas $G-$graduaciones son isomorfas como álgebras graduadas.*

Demostración. Sabemos que las dos álgebras graduadas son isomorfas a $End_K(V)$ ($End_K(W)$ respectivamente) para dos espacios vectoriales $G-$graduados V,W de dimensión n. Por II. del Teorema 3.3.6 tenemos que

$$dim(V_g) = \frac{n}{|G|} \quad y \quad dim(W_g) = \frac{n}{|G|}$$

luego, $V \cong W$ como $K-$módulos graduados por tanto, $End_K(V) \cong End_K(W)$ como álgebras graduadas. □

Ejemplo 3.3.11. Sea $R = M_2(K)$, K un cuerpo arbitrario con una buena $C_2 = \{e,g\}-$graduación. Por el Corolario 3.3.2 existen $|C_2|^{2-1} = |C_2| = 2$ buenas graduaciones. Entonces las buenas C_2-graduaciones de R son siguintes

I. La graduación trivial

II. $R_e = \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix}, \quad R_g = \begin{pmatrix} 0 & K \\ K & 0 \end{pmatrix}.$

Ejemplo 3.3.12. Sea $R = M_3(K)$. Vamos a encontrar todas las buenas $C_2 - graduaciones$ de R. Por el Corolario 3.3.2 tenemos que existen $|G|^{3-1} = |G|^2 = 2^2 = 4$ buenas graduaciones. Por tanto, una buena graduación de R tiene una de las siguientes formas

I. La graduación trivial, $R_e = M_3(K)$, $R_g = 0$;

II. $R_e = \begin{pmatrix} K & K & 0 \\ K & K & 0 \\ 0 & 0 & K \end{pmatrix}, R_g = \begin{pmatrix} 0 & 0 & K \\ 0 & 0 & K \\ K & K & 0 \end{pmatrix};$

$$III.\ R_e = \begin{pmatrix} K & 0 & 0 \\ 0 & K & K \\ 0 & K & K \end{pmatrix}, R_g = \begin{pmatrix} 0 & K & K \\ K & 0 & 0 \\ K & 0 & 0 \end{pmatrix};$$

$$IV.\ R_e = \begin{pmatrix} K & 0 & K \\ 0 & K & 0 \\ K & 0 & K \end{pmatrix}, R_g = \begin{pmatrix} 0 & K & 0 \\ K & 0 & K \\ 0 & K & 0 \end{pmatrix}.$$

Mostraremos que las graduaciones $II.$, $III.$, $IV.$ son fuertemente graduadas. Para esto definimos $grad(e_{i,i+1}) = h_i$, por el Teorema 3.3.3 debemos verificar que todos los elementos de C_2 aparecen en la sucesión e, h_1, h_1h_2 para cada una de las graduaciones anteriores. En efecto, para la graduación II tenemos, $grad(e_{1,2}) = e$ y $grad(e_{2,3}) = g$, luego $e, h_1, h_1h_2 = e, e, g$, así todos los elementos de C_2 aparecen en dicha suceción, lo cual por el Teorema 3.3.3 equivale a que R con la graduación en $II.$ es fuertemente graduado.

Para la graduación en $III.$ tenemos, $grad(e_{1,2}) = g$ y $grad(e_{2,3}) = e$, luego $e, h_1, h_1h_2 = e, g, g$, así todos los elementos de C_2 aparecen en dicha suceción, lo cual por el Teorema 3.3.3 equivale a que R con la graduación en $III.$ es fuertemente graduado.

Para la graduación en $IV.$ tenemos, $grad(e_{1,2}) = e$ y $grad(e_{2,3}) = g$, y se concluye de manera ánaloga al primer item.

Por último note que ninguna de las graduaciones anteriores es un producto cruzado, para esto basta notar que $dim(M_3(K)_e) = 5$ para los ejemplos $II.$, $III.$ y $IV.$, así $dim(M_3(K)_e) \cdot |G| = 5 * 2 = 10$, pero por III. del Teorema 3.3.6 si dichas graduaciones fueran productos cruzados tendríamos que $dim(M_3(K)_e) \cdot |G| = 3^2 = 9$ por tanto, ninguno de los ejemplos anteriores es un producto cruzado.

Referencias Bibliográficas

Apostol, T. (1992). *Análisis matemático*. Editorial Reverte.

Bahturin, Y. A. and Zaicev, M. V. (2002). Group gradings on matrix algebras. *Canadian Mathematical Bulletin*, 45(4):499–508.

Borovik, A. (2010). *Mathematics under the microscope*. American Mathematical Society Publication, Providence.

Dăscălescu, S., Ion, B., Năstăsescu, C., and Montes, J. (1999). Group gradings on full matrix rings. *J. Algebra*, 220(2):709–728.

Guccione, J. and Guccione, J. (2011). *Álgebra : grupos anillos y módulos*. Universidad de Buenos Aires, sede Buenos Aires.

Hazrat, R. (2016). *Graded rings and graded Grothendieck groups*. Cambridge University Press.

Isaacs, R. (2004). *Relaciones, Funciones y Enumerabilidad*. Universidad Industrial de Santander.

Lezama, O. (2011a). *Cuadernos de Algebra, No. 3: Módulos*. Universidad Nacional de Colombia.

Lezama, O. (2011b). *Cuadernos de Algebra, No. 7: Categorías*. Universidad Nacional de Colombia.

Milies, C. P. (1972). *Anéis e módulos*. Instituto de Matematica e Estatistica da Universidade de São Paulo.

Năstăsescu, C. and Oystaeyen, F. (2004). *Methods of Graded Rings*. Lecture notes in Math, vol. 1836, Springer-Berlin.

Rocha, J. (2017). Uma sequência exata relacionada a uma extens*ão* de anéis e uma representaç*ão* parcial. Tesis de doctorado, Universidad de São Paulo, Brasil.

Roman, S., A. S. and Gehring, F. W. (2005). *Advanced linear algebra (Vol. 3)*. New York: Springer.

Serre, J. P. (1955). Faisceaux algébriques cohérents. *Annals of Mathematics*, pages 197–278.

Soler, Y. (2019). Anillos y módulos graduados por grupos. Tesis de maestría, Universidad Industrial de Santander, Colombia.

Apéndices

Apéndice A. Categorías

El tema que vamos a desarrollar en este apéndice se enfoca en las definiciones básicas de la teoría de categorías. Introducimos este anexo con el fin de especificar la categoría de anillos graduados y módulos graduados las cuales fueron mencionadas a lo largo de este trabajo.

Definición 3.3.13. *Una categoría $\mathscr{C}$ se define por:*

a) *Una colección no vacía cuyos elementos se llaman **objetos**. Esta colección se denota por $Ob(\mathscr{C})$.*

b) *Una colección no vacía de conjuntos disjuntos y eventualmente vacíos:*

$$\{Mor_{\mathscr{C}}(X,Y)\}_{X,Y\in Ob(\mathscr{C})}.$$

Los elementos del conjunto $Mor_{\mathscr{C}}(X,Y)$ se denominan morfismos del obejeto X en el objeto Y. Un elemento $f \in Mor_{\mathscr{C}}(X,Y)$ se representa por $f : X \longrightarrow Y$, donde X es el dominio del morfismo f y Y su codominio.

La reunión de todos de todos los conjuntos de morfismos de $\mathscr{C}$ se denota por

$$Mor(\mathscr{C}) := \cup_{X,Y\in Ob(\mathscr{C})} Mor(X,Y).$$

c) *Una operación entre morfismos llamada composición, tal que si X,Y,Z son objetos de $\mathscr{C}$,*

$f \in Mor(X,Y)$ y $g \in Mor(Y,Z)$, entonces existe un único morfismo $g \circ f \in Mor(X,Z)$:

$$Mor(X,Y) \times Mor(Y,Z) \longrightarrow Mor(X,Z)$$

$$(f,g) \longmapsto g \circ f$$

La operación $\circ$ cumple las siguientes condiciones:

I. *Es asociativa, es decir, si $f \in Mor(X,Y)$, $g \in Mor(Y,Z)$ y $h \in Mor(Z,W)$, entonces*

$$(h \circ g) \circ f = h \circ (g \circ f).$$

II. *Para cada objeto X en $\mathscr{C}$ existe un morfismo identidad $i_X \in Mor(X,X)$ tal que*

$$i_X \circ f = f \quad y \quad g \circ i_X = g$$

para todo $f \in Mor(Y,X)$, y todo $g \in Mor(X,Y)$.

Notemos que si en $c)$ $Mor(X,Y)$ o $Mor(Y,Z)$ son vacíos, la composición no se define.

Ejemplo 3.3.14. El ejemplo más sencillo de categoría es la de los conjuntos, la cual se denota por **Set**. Sus objetos son la colección de todos los conjuntos, las funciones conforman los morfismos y la operación entre éstos es la composición usual de funciones. Dado un conjunto X, el morfismo identidad es la función idéntica $i_X : X \to X$, $i_X(x) = x$. Se define $i_\emptyset := \emptyset$, $Mor(\emptyset,A) := \{\emptyset\}$, para cada conjunto A; $Mor(A,\emptyset)=\emptyset$ para cada conjunto $A\neq\emptyset$.

Ejemplo 3.3.15. A continuación enunciaremos las categorías más conocidas en álgebra:

I. La colección de todos los grupos junto con los homomorfismos constituyen una categoría denotada por **Gr**.

II. Los anillos con unidad junto con los homomorfismos de anillo que preservan la unidad conforman una categoría denotada por **Ring**.

III. Para un anillo con unidad A, Mod_A es la categoría de todos los $A-$módulos derechos cuyos objetos son los $A-$módulos derechos y los morfismos son los $A-$homomorfismos. De manera análoga definimos ${}_AMod$.

Categoría de anillos graduados. Si G es un grupo, la categoría de anillos graduados denotada por $G-RING$, es una categoría obtenida al tomar anillos $G-$graduados como objetos y como morfismos los homomorfismos entre anillos $G-$graduados definido como sigue:
Para cada R y S anillos $G-$graduados, definimos el homomorfismo graduado como

$$\varphi: R \longrightarrow S$$

tal que $\varphi(R_g)\subseteq S_g$ para cualquier $g\in G$.

En seguida mencionaremos unas observaciones:

I. Si $G=\{e\}$ tenemos que $G-RING=RING$.

II. Si R es un anillo $G-$graduado y X es un subconjunto no vacío de G denotaremos $R_X = \bigoplus_{x\in X} R_x$.

III. Si $H \leq G$ es un subgrupo, $R_H = \bigoplus_{h\in H}$ es un subanillo de R, de hecho R_H es un anillo $H-$graduado.

Categoría de módulos graduados. Sea R un anillo graduado por G denotaremos por $gr-R$ a la categoría de módulos graduados a derecha, donde los objetos de $gr-R$ son los $R-$módulos graduados y para los $R-$módulos $G-$graduados M y N definimos los morfismos de la categoría como:

$$Hom_{gr-R}(M,N) = \{f \in Hom_R(M,N) \mid f(M_g) \subseteq N_g \; para \; todo \; g \in G\}.$$

De manera ánaloga definimos $R-gr$.