Universidade Estadual do Sudoeste da Bahia
Departamento de Ciências Exatas e Tecnológicas

Graduações para a Álgebra $M_2(\mathbb{K})$

Vitória da Conquista - Bahia
2016

Pedro Souza Fagundes

Graduações para a Álgebra $M_2(\mathbb{K})$

Monografia apresentada ao Departamento de Ciências Exatas e Tecnológicas da Universidade Estadual do Sudoeste da Bahia - Campus Vitória da Conquista-BA, para obtenção do Título de Licenciado em Matemática, sob orientação do Prof. Dr. Júlio César dos Reis.

Vitória da Conquista - Bahia
2016

Folha de Aprovação

Pedro Souza Fagundes

Graduações para a Álgebra $M_2(\mathbb{K})$

Monografia apresentada ao Colegiado do Curso de Matemática como requisito parcial para aprovação na disciplina Seminário de Pesquisa II do Curso de Licenciatura em Matemática.

Aprovado em ____ / ____ / 2016.

BANCA EXAMINADORA

Dr. Júlio César dos Reis - UESB

Orientador

Ms. Altemar Brito Lima - UESB

2º Membro

Dr. Flaulles Boone Bergamaschi - UESB

3º Membro

Vitória da Conquista - BA

2016

Aos meus amados pais, Alice e Francisco.

Agradecimentos

Em primeiro lugar, agradeço a Deus pelo seu Amor, pela sua Presença e sua Força, que a cada dia me anima para seguir em frente.

Quero agradecer aos meus pais Alice Silva Souza e Francisco de Assis Fagundes Pereira, que sempre me incentivaram nos estudos e que sacrificaram alguns de seus desejos para que eu pudesse estar realizando o meu sonho de criança. Agradeço também à minha irmã Iasmin que sempre esteve do meu lado me animando. À eles minha gratidão.

Quero agradecer ao Prof. Dr. Júlio César dos Reis, que foi um pai me aconselhando e incentivando durante essa caminhada. Muito obrigado Júlio!!

Agradeço também aos amigos conquistados durante esse período da graduação. A cada um que com valiosas conversas me divertia, animava e ensinava. Em especial, os amigos com os quais tive o privilégio de dividir o espaço da sala de aula.

Sou grato aos professores do curso de Licenciatura em Matemática da UESB.

Agradeço também ao "tio" Geovani que nunca deixou ninguém desanimado nos corredores do módulo 04 e ao motorista do "bus" da UESB, Zelito, pelas caronas cedidas.

Resumo

Este trabalho tem como principal objetivo estudar o artigo *Group Gradings of* $M_2(\mathbb{K})$ produzido pelas autoras R. Khazal, C. Boboc e S. Dascalescu.

Basicamente o artigo descreve todas as graduações de $M_2(\mathbb{K})$, em que $\mathbb{K}$ é um corpo qualquer. O resultado principal diz que toda graduação é essencialmente uma boa graduação, ou uma graduação feita pelo grupo cíclico de ordem dois ou uma graduação feita pelo grupo de Klein.

O estudo é feito utilizando-se apenas conceitos básicos de Álgebra Linear, Álgebra Abstrata e alguns resultados iniciais de Graduações de Álgebras. Para o caso da álgebra graduada $M_2(\mathbb{K})$ são feitas algumas afirmações devidamente justificadas que são expostas como lemas e corolários.

Sumário

1 Conceitos Básicos **7**

1.1 Resultados de Álgebra Linear 7

1.2 Resultados de Álgebra Abstrata 9

1.3 Álgebras Graduadas 12

1.4 Por que estudar álgebras graduadas? 20

2 Graduações de $M_2(\mathbb{K})$ **21**

2.1 Graduações de suporte 2 25

2.2 Graduações de suporte 3 30

2.3 Graduações de suporte 4 33

Considerações Finais **35**

Referências Bibliográficas **38**

A Forma Canônica de Jordan **39**

Introdução

Dado um corpo $\mathbb{K}$ dizemos que um espaço vetorial A (sobre $\mathbb{K}$) é uma $\mathbb{K}$-álgebra se em A estiver definida uma multiplicação, que denotaremos por (*), se for válida a lei distribuitiva da multiplicação em relação à adição e a seguinte condição for satisfeita: $(\alpha v) * u = \alpha(v * u) = v * (\alpha u), \forall \alpha \in \mathbb{K}, \forall u, v \in A$.

Portanto toda álgebra é um espaço vetorial e sabemos que todo espaço vetorial pode ser decomposto em uma soma direta (no mínimo trivialmente). Então dada uma álgebra podemos "quebrá-la" em alguns pedaços de forma que estes mantenham parte da estrutura da álgebra. Para controlar o número de "quebras", utilizamos de alguma maneira os elementos de um grupo. Este fato, a grosso modo, é o que chamamos de graduar uma álgebra. Formalmente, se A é uma $\mathbb{K}$-álgebra e G é um grupo, dizemos que A é G-graduada se $A = \bigoplus_{g \in G} A_g$ e $A_g A_h \subseteq A_{gh}$, em que A_g são subespaços vetoriais de A.

Neste trabalho temos como principal objetivo apresentar um estudo do artigo de Khazal, Boboc e Dascalescu intitulado *Group Gradings of* $M_2(\mathbb{K})$ [9] sobre todas as graduações possíveis que podemos empregar na álgebra das matrizes de ordem dois. Aqui iremos apresentá-lo de uma forma mais extendida, expondo por exemplo as contas lá omitidas, e em alguns poucos casos apresentaremos demonstrações diferentes das expostas no referido artigo.

O texto foi dividido em dois capítulos, em que no primeiro fazemos uma revisão de alguns resultados de Álgebra Linear e Álgebra Abstrata que serão utilizados no capítulo posterior. Ainda nesse capítulo, introduzimos o conceito de álgebra bem como o de álgebras graduadas. Veja [1],[2], [5], e [10], por exemplo, para mais detalhes. Já no segundo capítulo discutimos o resultado principal do texto, que foi divido em três casos. Cada caso foi discutido em uma seção e esta divisão foi feita através do suporte da álgebra $M_2(\mathbb{K})$, para alguma graduação, que é o conjunto formado pelos elementos do grupo que indexam os subespaços não nulos na decomposição da álgebra.

Por fim, apresento uma tabela expondo de forma sucinta todas as graduações de $M_2(\mathbb{K})$ e em seguida um apêndice sobre a Forma Canônica de Jordan, ferramenta esta utilizada no decorrer do texto.

Capítulo 1

Conceitos Básicos

1.1 Resultados de Álgebra Linear

Esta seção está dedicada a apenas alguns tópicos de Álgebra Linear. O leitor interessado em rever os conceitos de espaço vetorial, base de um espaço vetorial, transformações lineares, autovalores, autovetores e diagonalização pode consultar [1] e [4].

Uma ferramenta que será muito usada aqui é a soma direta de subespaços vetoriais. Antes de expô-la, vejamos a seguinte definição.

Definição 1 *Sejam $W_1, \cdots, W_k$ subespaços do espaço vetorial V. Dizemos que $W_1, \cdots, W_k$ são independentes se*

$$w_1 + \cdots + w_k = 0, w_i \in W_i$$

implica em $w_i = 0, i = 1, \cdots, k$.

Uma consequência que segue desta definição é a seguinte:

Proposição 2 *Seja V um espaço vetorial finitamente gerado e $W_1, \cdots, W_k$ subespaços de V. Então*

$$W_1, \cdots, W_k \text{ são independentes}$$

$$\Updownarrow$$

$$W_i \cap (W_1 + \cdots W_{i-1} + W_{i+1} + \cdots + W_k) = \{0\}, \forall i = 1, \cdots, k.$$

Prova:

Suponha que $W_1, \cdots, W_k$ são independentes e seja $v \in W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_k)$ para algum $i \in \{1, \cdots, k\}$. Então $v \in W_i$ e $v = v_1 + \cdots + v_{i-1} + v_{i+1} + \cdots + v_k \in W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_k$. Portanto $v_1 + \cdots + v_{i-1} - v + v_{i+1} + \cdots + v_k = 0$ e usando a hipótese temos que $v = 0$, o que prova a igualdade $W_i \cap (W_1 + \cdots W_{i-1} + W_{i+1} + \cdots + W_k) = \{0\}$, já que a outra inclusão é óbvia. Reciprocamente, considere a soma $v_1 + \cdots + v_k = 0, v_i \in W_i$, mas com $v_j \neq 0$, para algum $j \in \{1, \cdots, k\}$. Segue que $v_j = -v_1 - \cdots - v_{j-1} - v_{j+1} - \cdots - v_k \in W_j \cap (W_1 + \cdots + W_{j-1} + W_{j+1} + \cdots + W_k) = \{0\}$, e assim $v_j = 0$, o que é uma contradição. ■

Como consequência deste resultado dizemos que

Definição 3 *Um espaço vetorial V é uma soma direta de subespaços $W_1, \cdots, W_k$ ($V = W_1 \oplus \cdots \oplus W_k$) quando $V = W_1 + \cdots + W_k$ e tais subespaços forem independentes.*

Uma consequência interessante das somas diretas é que além da equivalência dada na Proposição 2 , também temos $W_i \cap (W_{j_1} + \cdots + W_{j_l}) = \{0\}$, para quaisquer $i, j_1, \cdots, j_l \in \{1, \cdots, k\}$ distintos entre si. Basta notar que $W_{j_1} + \cdots + W_{j_l} \subseteq W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_k$.

Em álgebra linear temos um grande resultado envolvendo o polinômio característico de uma matriz que é o

Teorema 4 (Teorema de Cayley-Hamilton) *Sejam V um espaço vetorial finitamente gerado, $T : V \to V$ um operador linear e $p(t) \in \mathbb{K}[t]$ seu polinômio característico. Então $p(M_T) = 0$, em que M_T é a matriz associada a T.*

Para uma demonstração deste teorema, vide [3].

Então a pergunta que fica é a seguinte: existe um polinômio $m(t) \in \mathbb{K}[t]$ de menor grau, mônico como o característico, tal que $m(M_T) = 0$? A resposta é sim e a esse polinômio chamamos de polinômio minimal. Isto justifica a seguinte definição

Definição 5 *Dada uma matriz M, dizemos que $m_M(t)$ é o polinômio minimal de M, se $m_M(t)$ é o polinômio mônico de menor grau tal que $m_M(M) = 0$.*

O mundo das matrizes 2×2 nos fornece muitos resultados interessantes, justamente por conta de termos matrizes "pequenas" para trabalhar. Por exemplo, a partir de agora nosso objetivo é mostrar que qualquer matriz 2×2 é semelhante a uma de duas matrizes bem especiais.

Porém, antes iremos ver uma definição e um resultado que nos ajudarão a chegarmos ao nosso objetivo.

Definição 6 *Seja V um $\mathbb{K}$-espaço vetorial com $dim(V) = n$, e $T : V \to V$ um operador linear. Dizemos que V é T-cíclico, se existir $v \in V$ tal que $\{v, T(v), \cdots, T^{n-1}(v)\}$ é uma base de V.*

O seguinte resultado será considerado sem demonstração. A prova pode ser encontrada em [4].

Teorema 7 *Seja $T : V \to V$ um operador linear em que V é um $\mathbb{K}$-espaço vetorial finitamente gerado. Então existe um subespaço T-cíclico de V com dimensão igual ao grau do polinômio minimal de T.*

Com isso em mãos, vamos justificar a afirmação feita acima. Sabemos que dada uma matriz $A \in M_2(\mathbb{K})$, conseguimos calcular seus polinômios característico ($p(t)$) e minimal ($m(t)$). Sabemos que o polinômio característico tem grau 2, mas o mininal não necessariamente. Vamos supor inicialmente que o polinômio minimal tenha grau 2. Portanto $p(t) = m(t)$. Mas o teorema logo acima diz que existe um subespaço $W \subseteq \mathbb{K}^2 = \mathbb{K} \times \mathbb{K}$, T-cíclico, com $dim(W) =$ grau de $m(t) = 2$, o que nos fornece que $\mathbb{K}^2$ é T-cíclico. Então existe um vetor $v \in \mathbb{K}^2$ tal que $\{v, T_A(v)\}$ é uma base de $\mathbb{K}^2$, em que T_A é a transformação linear associada à matriz A. Portanto, se tivermos $m(t) = t^2 + a_1 t + a_0$, então

$$T_A^2 = -a_1 T - a_0 I_2.$$

Esta última equação nos ajuda ver que a matriz associada a T_A em relação à base $\{v, T_A(v)\}$ é

$$\begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix}.$$

Agora vamos supor que o polinômio minimal de A tenha grau 1. Então $m(t) = t - c$, para algum $c \in \mathbb{K}$. Portanto, temos $T_A = cI_2$ e assim a matriz associada à T_A em relação à base canônica de $\mathbb{K}^2$ é

$$\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}.$$

Logo, temos que dada uma matriz $A \in M_2(\mathbb{K})$, ela é semelhante à

$$\begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} \; ou \; \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}.$$

1.2 Resultados de Álgebra Abstrata

Nesta seção, nosso objetivo é a demonstração do seguinte lema

Lema 8 *Seja A um anel associativo com unidade. Para um ideal $J \subseteq A$, seja $J_n = M_n(J) = \{(a_{ij}) \in M_n(A); a_{ij} \in J\}$. Então J_n é um ideal de $M_n(A)$ e ainda mais, todo ideal de $M_n(A)$ é desta forma. Em particular, os únicos ideais de $M_n(\mathbb{K})$ são os triviais se $\mathbb{K}$ for um corpo.*

Mas antes vamos relembrar alguns conceitos de álgebra abstrata, que serão usados posteriormente no decorrer do texto.

Definição 9 *Seja G um conjunto não vazio e $*$ uma operação em G. Dizemos que $(G,*)$ é um grupo quando para quaisquer $a,b,c \in G$ tivermos*

- $(a*b)*c = a*(b*c)$;
- $\exists\ e \in G; a*e = e*a = a$;
- $\forall\ a \in G, \exists\ a' \in G; a*a' = a'*a = e$.

Dizemos que um grupo G é abeliano se $a*b = b*a, \forall\ a,b \in G$.

Dizemos que o número de elementos de um grupo G é a ordem deste grupo.

Dizemos que um grupo G é cíclico se existe $g \in G$ tal que dado um elemento qualquer $a \in G$, existe um inteiro não-negativo n de modo que

$$g^n = \underbrace{g*\cdots*g}_{\text{"}n\text{ vezes"}} = a.$$

Exemplo 10 *$\mathbb{Z}_5 \setminus \{\bar{0}\}$ com a multiplicação usual é um grupo abeliano de ordem 4. Agora note que $\mathbb{Z}_5 \setminus \{\bar{0}\} = \langle \bar{2} \rangle$, pois*

$$\bar{1} = \bar{2}^0,$$

$$\bar{2} = \bar{2}^1,$$

$$\bar{3} = \bar{8} = \bar{2}^3 \ e$$

$$\bar{4} = \bar{2}^2.$$

Logo $\mathbb{Z}_5 \setminus \{\bar{0}\}$ é cíclico.

Um importante grupo de ordem 4 é o chamado grupo de Klein. Basicamente, este é um grupo que tem a propriedade de todos os seus elementos serem auto-invertíveis, i.e.,

$$K = \{1,a,b,c\} \text{ grupo de Klein com a notação multiplicativa} \Rightarrow a^2 = b^2 = c^2 = 1.$$

Note que em um grupo de Klein $K = \{1,a,b,c\}$ devemos ter $ab = c$, pois se

$$ab = 1 \Rightarrow a = b \text{ (contradição)},$$

$$ab = a \Rightarrow b = 1 \text{ (contradição)},$$

$$ab = b \Rightarrow a = 1 \text{ (contradição)}.$$

Logo, $K = \{1, a, b, ab\}$, e assim podemos vê-lo como uma multiplicação, elemento por elemento, dos grupos cíclicos de ordem 2, $\{1, a\}$ e $\{1, b\}$. Por isso, vamos denotar $K := C_2 \times C_2$, em que C_2 denota um grupo cíclico de ordem 2.

Outra estrutura importante é a de anel, que difere de um grupo por ter uma operação a mais (e obviamente esta diferença irá trazer outras), mas em particular teremos que todo anel é um grupo abeliano com a notação aditiva.

Definição 11 *Seja A um conjunto não vazio e sejam $+$ e $*$ duas operações definidas em A. Dizemos que $(A, +, *)$ é um anel se para quaisquer $a, b, c \in A$ tivermos*

- *$(A, +)$ é um grupo abeliano;*
- *$a * (b + c) = a * b + a * c$ e $(a + b) * c = a * c + b * c$.*

Dizemos que A é associativo se $(a * b) * c = a * (b * c)$.

Dizemos que A tem unidade se existir $e \in A$ tal que $a * e = e * a = a$.

Dizemos que A é comutativo se $a * b = b * a$.

Um anel A associativo, comutativo, com unidade e que satisfaça a seguinte propriedade

$$\forall\ a \in A \setminus \{0\}, \exists\ a' \in A; a * a' = a' * a = e,$$

é dito corpo.

Por último definimos um ideal em um anel.

Definição 12 *Seja $I \neq \emptyset$ e $I \subseteq A$. I é dito ideal de A se para quaisquer $a, b \in I$ e para qualquer $c \in A$ tivermos $a + b \in I, ac \in I$ e $ca \in I$.*

Exemplo 13 *Seja $\mathcal{F}(\mathbb{R}; \mathbb{R}) := \{$todas as funções $f : \mathbb{R} \to \mathbb{R}\}$. Com as operações*

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

$$(f \cdot g)(x) = f(x) \cdot g(x),$$

é rotina provar que $\mathcal{F}(\mathbb{R}; \mathbb{R})$ é um anel associativo, comutativo e com unidade. Como $0 + 0 = 0$ e $a \cdot 0 = 0, \forall\ a \in \mathbb{R}$, temos que $I = \{f : \mathbb{R} \to \mathbb{R}; f(1) = 0\}$ é um ideal de $\mathcal{F}(\mathbb{R}; \mathbb{R})$.

Para o caso particular do Lema 8 usaremos a

Proposição 14 *Em um corpo $\mathbb{K}$, os únicos ideias são os triviais.*

Prova:

Seja $I \neq \{0\}$ um ideal de $\mathbb{K}$. Obviamente temos $I \subseteq \mathbb{K}$. Agora tome $a \in \mathbb{K}$ e $b_1 \in I - \{0\}$. Como $b_1 \neq 0$, então existe $b_2 \in \mathbb{K}$ tal que $b_1 b_2 = 1$. Logo, temos $a = a \cdot 1 = a(b_1 b_2) = (ab_2)b_1 \in I$. Logo $\mathbb{K} \subseteq I$, o que prova $I = \mathbb{K}$. ■

Agora sim, provemos o Lema 8.

Prova do Lema 8:

Primeiramente mostremos que J_n é um ideal de $M_n(A)$. De fato, se $(a_{ij}), (b_{ij}) \in J_n$, então $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \in J_n$, pois $a_{ij} + b_{ij} \in J$. E se $(a_{ij}) \in J_n$ e $(b_{ij}) \in M_n(A)$, então $(a_{ij}) \cdot (b_{ij}) = (\sum_{k=1}^{n} a_{ik} b_{kj}) \in J_n$, pois para cada $k = 1, \cdots, n$, temos $a_{ik} b_{kj} \in J$, além de J ser fechado em relação à adição. Análogo para $(b_{ij}) \cdot (a_{ij}) \in J_n$. Isto prova que J_n é um ideal de $M_n(A)$.

Agora considere J um ideal de $M_n(A)$ e defina $I = \{x \in A; \exists (a_{ij}) \in J \text{ com } a_{11} = x\}$ e $e_{pq}(x) = (a_{ij})$ tal que

$$a_{ij} = \begin{cases} x, & se\ i = p\ e\ j = q \\ 0, & se\ i \neq p\ ou\ j \neq q \end{cases},$$

isto é, $a_{pq} = x$ e $a_{ij} = 0$ nas demais entradas. Temos que I é um ideal de A. Com efeito, dados $x, y \in I$, existem matrizes (a_{ij}) e (b_{ij}) em J com $a_{11} = x$ e $b_{11} = y$. Então basta tomar $(c_{ij}) = (a_{ij} + b_{ij})$ e teremos que $x + y \in I$. Agora se $x \in I$, então existe uma matriz $(a_{ij}) \in J$ com $a_{11} = x$ e para $y \in A$, basta tomar a matriz $(a_{ij}) e_{11}(y) \in J$ e teremos que $xy \in I$. Analogamente prova-se que $yx \in I$. Isso prova que I é um ideal de A.

Afirmamos que $J = I_n = M_n(I)$. Seja $(a_{ij}) \in J$. Note que $e_{11}(a_{pq}) = e_{1p}(1)(a_{ij})e_{q1}(1) \in J, \forall p, q = 1, \cdots, n$. Logo $a_{pq} \in I, \forall p, q = 1, \cdots, n$, e assim $(a_{ij}) \in I_n$. Acabamos de provar então que $J \subseteq I_n$. Agora tome $(b_{ij}) \in I_n$. Então para cada entrada ij existe uma matriz $(c_{pq}^{ij}) \in J$ com $c_{11}^{ij} = b_{ij}$. Note que $e_{ij}(b_{ij}) = e_{i1}(1)(c_{pq}^{ij})e_{1j}(1) \in J$. Portanto, $(b_{ij}) = \sum_{i,j=1}^{n} e_{ij}(b_{ij}) \in J$, e assim $I_n \subseteq J$, o que prova a igualdade $J = I_n$. Para o caso particular em que todo corpo é um anel associativo com unidade basta utilizar a Proposição 14. ■

1.3 Álgebras Graduadas

Nesta terceira e última seção vamos defnir o que é uma álgebra e iremos entender o adjetivo graduada.

Definição 15 *Seja $\mathbb{K}$ um corpo. Dizemos que um espaço vetorial A (sobre $\mathbb{K}$) é uma $\mathbb{K}$-álgebra se em A estiver definida uma multiplicação, que denotaremos por (*), e as seguintes condições forem satisfeitas:*

- $(\alpha v) * u = \alpha(v * u) = v * (\alpha u), \forall \alpha \in \mathbb{K}, \forall u, v \in A;$

- $u * (v + w) = u * v + u * w, \forall u, v, w \in A;$
- $(u + v) * w = u * w + v * w, \forall u, v, w \in A.$

Em geral, usaremos uv em vez de $u * v$.

Caso ocorra $(uv)w = u(vw), \forall u, v, w \in A$, dizemos que A é **associativa.**

Se $uv = vu, \forall u, v \in A$, dizemos que A é **comutativa.**

E caso exista $e \in A$ tal que $ev = ve = v, \forall v \in A$, dizemos que A tem **unidade.**

O resultado principal irá focar apenas na álgebra $M_2(\mathbb{K})$ sobre um corpo $\mathbb{K}$ qualquer, que é uma álgebra associativa, não comutativa e com unidade.

Vejamos mais alguns exemplos de álgebras:

Exemplo 16 *Considere o conjunto dos números complexos $\mathbb{C}$ com a adição e multiplicação usuais. Sabemos que $\mathbb{C}$ é um $\mathbb{R}$-espaço vetorial. Agora basta notar que dados $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i \in \mathbb{C}$ e $\alpha \in \mathbb{R}$, temos*

$$(\alpha z_1) * z_2 = (\alpha a_1 + \alpha b_1 i) * (a_2 + b_2 i) = (\alpha a_1 a_2 - \alpha b_1 b_2) + (\alpha a_1 b_2 + \alpha a_2 b_1) i =$$

$$= \alpha((a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i) = \alpha(z_1 * z_2) = (a_1 \alpha a_2 - b_1 \alpha b_2) + (a_1 \alpha b_2 + a_2 \alpha b_1) i =$$

$$= (a_1 + b_1 i) * (\alpha a_2 + \alpha b_2 i) = z_1 * (\alpha z_2).$$

Isto prova a primeira condição da Definição 15. As outras duas condições seguem do fato de $\mathbb{C}$ ser um corpo. Com isso temos que $\mathbb{C}$ é uma $\mathbb{R}$-álgebra. Mais ainda, temos que $\mathbb{C}$ é uma $\mathbb{R}$-álgebra associativa, comutativa e com unidade.

Exemplo 17 *Seja $\mathbb{R}^3 = \{(x_1, x_2, x_3); x_i \in \mathbb{R}, i = 1, 2, 3\}$. Sabemos que $\mathbb{R}^3$ é um espaço vetorial sobre $\mathbb{R}$. Defina o produto vetorial usual em $\mathbb{R}^3$, i.e.,*

$$(x_1, x_2, x_3) * (y_1, y_2, y_3) = \begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix} \vec{i} - \begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix} \vec{j} + \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \vec{k}$$

lembrando que todo vetor $(a, b, c) \in \mathbb{R}^3$ pode ser representado na forma $a\vec{i} + b\vec{j} + c\vec{k}$. Utilizando algumas propriedades de determinantes para provar as três condições na definição acima, temos que $\mathbb{R}^3$ é uma $\mathbb{R}$-álgebra. E desde que o produto vetorial é anticomutativo e não associativo, temos então um exemplo de uma álgebra não comutativa, não associativa e sem unidade.

Agora vamos entender o que significa graduar uma álgebra. Vale ressaltar que para tal devemos ter em mãos um grupo, e para fixar as ideias vamos usar a notação multiplicativa. A teoria também pode ser escrita com o grupo em notação aditiva, tendo o cuidado de fazer os devidos ajustes.

Mas antes, se A é uma álgebra e A_g e A_h são subespaços de A, então definimos $A_gA_h = \{ab\,; a \in A_g \text{ e } b \in A_h\}$.

Definição 18 *Seja G um grupo. Dizemos que uma $\mathbb{K}$-álgebra A é G-graduada se tivermos uma família de subespaços $\{A_g \subseteq A : g \in G\}$ com $A = \bigoplus_{g\in G} A_g$ e $A_gA_h \subseteq A_{gh}$, quaisquer que sejam $g, h \in G$.*

Dada uma álgebra A, a G-graduação feita pondo $A_1 = A$ e $A_g = \{0\}$, para todo $g \in G - \{1\}$, é dita ser uma graduação trivial.

Algumas graduações da álgebra das matrizes tem a interessante propriedade de terem as matrizes elementares pertencentes aos subespaços que a compõe. Este fato nos motiva a seguinte definição.

Definição 19 *Seja $A = \bigoplus_{g\in G} A_g$ a álgebra de matrizes com alguma G-graduação. Dizemos que esta é uma boa graduação quando cada matriz elementar pertence a A_g para algum $g \in G$.*

Em alguns casos precisamos nos referir a algumas parcelas da decomposição de um elemento da álgebra. Para esta referência, temos a seguinte definição.

Definição 20 *Seja $A = \bigoplus_{g\in G} A_g$ uma graduação para uma álgebra A qualquer. Dado $a \in A$, temos que $a = a_{g_1} + \cdots + a_{g_k}$ com $a_{g_i} \in A_{g_i}$. Então para todo $i \in \{1, \cdots, k\}$ dizemos que a_{g_i} é a componente homogênea de grau g_i do elemento a.*

Um resultado importante no mundo das graduações é que a identidade da álgebra pertence ao subespaço da graduação cujo índice é o elemento neutro do grupo, i.e.,

Proposição 21 *Se A é uma álgebra com unidade e G-graduada, então $1 \in A_1$.*

Prova:

Sabemos que $1 = a_1 + a_{g_1} + \cdots + a_{g_n}$, com $a_1 \in A_1$ e $a_{g_i} \in A_{g_i}$. Então para quaisquer $h \in G$ e $a_h \in A_h$, temos

$$a_h = a_ha_1 + a_ha_{g_1} + \cdots + a_ha_{g_n} \Rightarrow a_h - a_ha_1 = a_ha_{g_1} + \cdots + a_ha_{g_n} \in A_h,$$

pois $a_ha_1 \in A_h$. Se $a_h - a_ha_1 \neq 0$, como $a_ha_{g_i} \in A_{hg_i}$ e $h, hg_1, \cdots, hg_n$ são distintos entre si, teremos então um absurdo de acordo com a última observação feita sobre somas diretas na seção 1.1. Portanto, devemos ter $a_h - a_ha_1 = 0 \Rightarrow a_h = a_ha_1$. Analogamente mostra-se que $a_h = a_1a_h$. Portanto $1 = a_1 \in A_1$. ∎

Quando graduamos uma álgebra, nem sempre usamos todos os elementos do grupo como índices para os subespaços não nulos. Por esse motivo temos a seguinte definição.

Definição 22 *Seja A uma álgebra G-graduada. Definimos suporte de A o conjunto $supp(A) = \{g \in G : A_g \neq 0\}$.*

Outro resultado interessante é o que diz que

Proposição 23 *Em uma álgebra G-graduada A, se $g \in supp(A)$ e existe $a \in A_g$ invertível, então $g^{-1} \in supp(A)$ e $a^{-1} \in A_{g^{-1}}$.*

Prova: Suponha $A = \bigoplus_{i=0}^{n} A_{g_i}$, com $g_0 = 1_G$ e A_{g_i}'s subespaços não nulos de A. Como $a^{-1} \in A$, então

$$a^{-1} = a_{g_0} + a_{g_1} + \cdots + a_{g_n}, a_{g_i} \in A_{g_i} \Rightarrow$$

$$\Rightarrow 1_A = aa_{g_0} + \cdots + aa_{g_n}.$$

Como a soma do lado direito da equação acima pertence à A_{1_G}, pois $1_A \in A_{1_G}$, então existe um $k \in \{0, 1, \cdots, n\}$ tal que

$$1_A = aa_{g_k} \text{ e } aa_{g_i} = 0, \forall i \neq k.$$

Analogamente provamos a existência de $l \in \{0, 1, \cdots, n\}$ tal que

$$1_A = a_{g_l}a \text{ e } a_{g_i}a = 0, \forall i \neq l.$$

Afirmamos que $k = l$. De fato,

$$a_{g_k} = (a_{g_l}a)a_{g_k} = a_{g_l}(aa_{g_k}) = a_{g_l}.$$

Como $A_{g_k} \cap A_{g_l} = \{0\}$, segue que $k = l$. Supondo que $a \in A_{g_p}$, para algum $p \in \{0, 1, \cdots, n\}$ temos então que $1_A = aa_{g_k} \in A_{g_p}A_{g_k} \subseteq A_{g_pg_k}$, o que nos fornece

$$g_pg_k = 1_G, a^{-1} = a_{g_k} \in A_{g_k} = A_{g_p^{-1}} \text{ e } g_p^{-1} \in supp(A).$$

■

Vejamos dois exemplos de graduação, em que no primeiro vamos trabalhar com suporte da graduação igual ao grupo e no segundo, com o suporte diferente do grupo.

Exemplo 24 *Considere o seguinte subconjunto de $\mathbb{Z}_{12}^*$, $G = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. É fácil ver que G é um grupo de Klein abeliano.*

Considere também $M_2(\mathbb{R})$ e as matrizes $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ e $Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Denote $A_{\overline{1}} = \mathbb{R}I_2$, $A_{\overline{5}} = \mathbb{R}X$, $A_{\overline{7}} = \mathbb{R}Y$ e $A_{\overline{11}} = \mathbb{R}XY$. Primeiramente vamos provar que $M_2(\mathbb{R}) = A_{\overline{1}} \oplus A_{\overline{5}} \oplus A_{\overline{7}} \oplus A_{\overline{11}}$.

Note que dada uma matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *em* $M_2(\mathbb{R})$ *temos*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{a+d}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{b+c}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{b-c}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \frac{d-a}{2}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

e a soma é direta pois os subespaços $A_{\overline{1}}, A_{\overline{5}}, A_{\overline{7}}$ *e* $A_{\overline{11}}$ *são independentes. De fato,*

$$\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} 0 & y \\ y & 0 \end{pmatrix} + \begin{pmatrix} 0 & w \\ -w & 0 \end{pmatrix} + \begin{pmatrix} -z & 0 \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, x, y, w, z \in \mathbb{R} \Rightarrow$$

$$\Rightarrow \begin{pmatrix} x-z & y+w \\ y-w & x+z \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{cases} x & & & - & z & = & 0 \\ & y & + & w & & = & 0 \\ & y & - & w & & = & 0 \\ x & & & + & z & = & 0 \end{cases} \Rightarrow$$

$$\Rightarrow x = y = w = z = 0.$$

Agora basta verificarmos a validade da propriedade $A_{\overline{g}}A_{\overline{h}} \subset A_{\overline{gh}}, \forall\ \overline{g}, \overline{h} \in G$.

Como o gerador de $A_{\overline{1}}$ *é a matriz identidade, então é fácil ver que* $A_{\overline{1}}A_{\overline{g}} \subset A_{\overline{g}}$. *As seguintes multiplicações justificam as demais inclusões.*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} (A_{\overline{5}}A_{\overline{7}} \subseteq A_{\overline{11}})$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} (A_{\overline{7}}A_{\overline{5}} \subseteq A_{\overline{11}})$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} (A_{\overline{5}}A_{\overline{11}} \subseteq A_{\overline{7}})$$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (A_{\overline{11}}A_{\overline{5}} \subseteq A_{\overline{7}})$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (A_{\overline{7}}A_{\overline{11}} \subseteq A_{\overline{5}})$$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} (A_{\overline{11}}A_{\overline{7}} \subseteq A_{\overline{5}})$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (A_{\overline{5}}A_{\overline{5}} \subseteq A_{\overline{1}})$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} (A_{\overline{7}}A_{\overline{7}} \subseteq A_{\overline{1}})$$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (A_{\overline{11}}A_{\overline{11}} \subseteq A_{\overline{1}})$$

Portanto este é um exemplo de uma graduação de $M_2(\mathbb{R})$. Note também que $|supp(M_2(\mathbb{R}))| = 4$, em relação a esta graduação.

No capítulo seguinte veremos que esta gradução pode ser considerada para qualquer corpo $\mathbb{K}$ com $char(\mathbb{K}) \neq 2$.

Agora iremos definir as chamadas matrizes elementares, que serão utilizadas nos dois exemplos seguintes.

Definição 25 *Em $M_n(\mathbb{K})$ as matrizes*

$$e_{pq} = \begin{cases} 1, & se\ i = p\ e\ j = q \\ 0, & se\ i \neq p\ ou\ j \neq q \end{cases}$$

são chamadas de matrizes elementares.

Exemplo 26 *Seja $M_2(\mathbb{R})$ e considere o grupo multiplicativo $\mathbb{Q}^*$. Para cada $k \in \mathbb{Q}^*$, faça*

$$A_k = \begin{cases} \{0\} & , se\ k \notin \{1, 2, 1/2\} \\ \langle e_{ij} | j/i = k \rangle & , se\ k \in \{1, 2, 1/2\} \end{cases}.$$

Note que assim temos

$$M_2(\mathbb{R}) = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix} \oplus \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix} = A_1 \oplus A_2 \oplus A_{\frac{1}{2}}.$$

Veja agora que

$$\begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}\begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix} (A_1A_2 \subseteq A_2),$$

$$\begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix} = \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix} (A_2A_1 \subseteq A_2)$$

$$\begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix} (A_1A_{\frac{1}{2}} \subseteq A_{\frac{1}{2}})$$

$$\begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix}\begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix} (A_{\frac{1}{2}}A_1 \subseteq A_{\frac{1}{2}})$$

$$\begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix} = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & 0 \end{pmatrix} (A_2 A_{\frac{1}{2}} \subseteq A_1)$$

$$\begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix}\begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{R} \end{pmatrix} (A_{\frac{1}{2}} A_2 \subseteq A_1).$$

As igualdades acima mostram que $A_g A_h \subseteq A_{gh}$, quaisquer que sejam $g, h \in \mathbb{Q}^*$. Observe que neste exemplo, apesar do grupo ser infinito, temos uma graduação com suporte finito, mais precisamente $|supp(M_2(\mathbb{R}))| = 3$.

Vejamos mais um exemplo de álgebra graduada considerando agora $M_3(\mathbb{R})$.

Exemplo 27 *Sejam $A = M_3(\mathbb{R})$, o grupo multiplicativo $\mathbb{Z}_3^* = \{\bar{1}, \bar{2}\}$ e $(g_1, g_2, g_3) = (\bar{1}, \bar{2}, \bar{1}) \in (\mathbb{Z}_3^*)^3$. Defina*

$$A_{\bar{1}} = \langle e_{ij}; g_i^{-1} g_j = \bar{1} \rangle \text{ e } A_{\bar{2}} = \langle e_{ij}; g_i^{-1} g_j = \bar{2} \rangle.$$

Desde que $(\bar{1})^{-1} = \bar{1}$ e $(\bar{2})^{-1} = \bar{2}$, é fácil ver que

$$A_{\bar{1}} = \langle e_{11}, e_{13}, e_{22}, e_{31}, e_{33} \rangle \text{ e } A_{\bar{2}} = \langle e_{12}, e_{21}, e_{23}, e_{32} \rangle,$$

isto é

$$A_{\bar{1}} = \begin{pmatrix} \mathbb{R} & 0 & \mathbb{R} \\ 0 & \mathbb{R} & 0 \\ \mathbb{R} & 0 & \mathbb{R} \end{pmatrix} \text{ e } A_{\bar{2}} = \begin{pmatrix} 0 & \mathbb{R} & 0 \\ \mathbb{R} & 0 & \mathbb{R} \\ 0 & \mathbb{R} & 0 \end{pmatrix}.$$

Obviamente temos $A = A_{\bar{1}} \oplus A_{\bar{2}}$.

Agora provemos $A_{h_1} A_{h_2} \subseteq A_{h_1 h_2}, \forall h_1, h_2 \in \mathbb{Z}_3^*$. Porém, note que basta provarmos tais inclusões para os elementos da base de cada subespaço envolvido. Assim,

$$e_{ij} \in A_{\bar{1}}, e_{pq} \in A_{\bar{2}} \Rightarrow e_{ij} e_{pq} \in A_{\bar{2}},$$

pois

$$e_{ij} e_{pq} = \begin{cases} 0, & \text{se } j \neq p \\ e_{iq}, & \text{se } j = p \end{cases},$$

e $e_{iq} \in A_{\bar{2}}$, já que $g_i^{-1} g_q = (g_i^{-1} g_j)(g_p^{-1} g_q) = \bar{1} \cdot \bar{2} = \bar{2}$. Isto prova que $A_{\bar{1}} A_{\bar{2}} \subseteq A_{\bar{2}}$. As outras inclusões são inteiramente análogas. Segue então que temos uma graduação para a álgebra das matrizes de ordem três sobre $\mathbb{R}$ com $|supp(A)| = 2$.

Por último, vamos definir o que é um homomorfismo e isomorfismo graduados entre álgebras graduadas pelo mesmo grupo.

Definição 28 *Sejam $A = \bigoplus_{g \in G} A_g$ e $B = \bigoplus_{g \in G} B_g$ álgebras G-graduadas. Dizemos que $\phi : A \to B$ é um homomorfismo graduado, se forem verificadas as seguintes condições:*

- *ϕ é uma transformação linear;*
- $\phi(xy) = \phi(x)\phi(y), \forall x, y \in A$;
- $\phi(1_A) = 1_B$;
- $\phi(A_g) \subseteq B_g, \forall g \in G$.

Caso ϕ seja um homomorfismo graduado bijetivo, então dizemos que ϕ é um isomorfismo graduado.

Um exemplo de isomorfismo graduado é o que segue:

Exemplo 29 *Sejam $M_2(\mathbb{R})$ e o grupo multiplicativo $\mathbb{Q}^*$. Conforme o exemplo 26, sejam as graduações*

$$A_1 = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}, A_2 = \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix}, A_{\frac{1}{2}} = \begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix}, A_p = 0, \forall p \notin \{1, 2, 1/2\} \text{ e}$$

$$B_1 = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}, B_2 = \begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix}, B_{\frac{1}{2}} = \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix}, B_p = 0, \forall p \notin \{1, 2, 1/2\}.$$

Vamos mostrar que a função $\phi : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ dada por $\phi(X) = UXU^{-1}$, em que $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, é um isomorfismo graduado. Primeiramente note que quaisquer que sejam $X, Y \in M_2(\mathbb{R})$,

- $\phi(X + Y) = U(X + Y)U^{-1} = UXU^{-1} + UYU^{-1} = \phi(X) + \phi(Y)$;
- $\phi(\alpha X) = U(\alpha X)U^{-1} = \alpha(UXU^{-1}) = \alpha\phi(X)$, $\forall\ \alpha \in \mathbb{R}$;
- $\phi(XY) = UXYU^{-1} = UX(U^{-1}U)YU^{-1} = (UXU^{-1})(UYU^{-1}) = \phi(X)\phi(Y)$;
- $\phi(I_2) = UI_2U^{-1} = I_2$;
- $\phi(A_1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix} = B_1$;
- $\phi(A_2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix} = B_2$;
- $\phi(A_{\frac{1}{2}}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix} = B_{\frac{1}{2}}$;

É fácil ver que $\ker(\phi) = \{0\}$, e portanto ϕ é injetora. Como ϕ é um operador linear, segue que ϕ é sobrejetora. Isto encerra a prova de que ϕ é um isomorfismo graduado.

1.4 Por que estudar álgebras graduadas?

Como vimos na seção precedente, graduar uma álgebra significa decompô-la em uma soma direta de subespaços vetoriais (tendo em vista que toda álgebra é um espaço vetorial) com um certa propriedade a ser verificada entre estes subespaços.

Portanto, quando graduamos uma álgebra podemos focar os estudos em seus "pedaços" e a partir daí termos uma noção do que ocorre com o todo. Esta é uma grande importância de se estudar graduações de álgebras.

Em PI-Teoria (Teoria das Álgebras com Identidades Polinomiais) é comum o estudo de identidades graduadas para álgebras graduadas, pois, em geral, a procura por identidades polinomiais para álgebras não graduadas se mostrou uma tarefa difícil.

Capítulo 2

Graduações de $M_2(\mathbb{K})$

Neste capítulo iremos apresentar as graduações existentes para a álgebra $M_2(\mathbb{K})$. Abaixo temos o resultado principal exposto na forma de um teorema que será demonstrado em três casos: $|supp(M_2(\mathbb{K}))| = 2$, $|supp(M_2(\mathbb{K}))| = 3$ e $|supp(M_2(\mathbb{K}))| = 4$. Aqui iremos representar a característica do corpo $\mathbb{K}$ por $char(\mathbb{K})$.

Teorema 30 *Seja G um grupo com unidade, $\mathbb{K}$ um corpo e $A = M_2(\mathbb{K})$.*

(I) Se $char(\mathbb{K}) \neq 2$ então qualquer G-graduação de A é isomorfa a um dos seguintes tipos.

(1) A graduação trivial, que é $A_1 = A, A_g = 0$ para qualquer $g \neq 1$.

(2) Uma boa graduação da forma $A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}$, $A_g = \begin{pmatrix} 0 & \mathbb{K} \\ \mathbb{K} & 0 \end{pmatrix}$, $A_h = 0$ para $h \in G - \{1, g\}$, onde $g \in G$ é um elemento de ordem 2.

(3) Uma graduação da forma $A_1 = \left\{ \begin{pmatrix} u & v \\ bv & u \end{pmatrix} | u, v \in \mathbb{K} \right\}$, $A_g = \left\{ \begin{pmatrix} u & v \\ -bv & -u \end{pmatrix} | u, v \in \mathbb{K} \right\}$, $A_h = 0$ para $h \in G - \{1, g\}$, onde $g \in G$ é um elemento de ordem 2 e $b \in \mathbb{K} - \mathbb{K}^2$.

(4) Uma graduação da forma $A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}$, $A_g = \begin{pmatrix} 0 & \mathbb{K} \\ 0 & 0 \end{pmatrix}$, $A_{g^{-1}} = \begin{pmatrix} 0 & 0 \\ \mathbb{K} & 0 \end{pmatrix}$, $A_h = 0$ para $h \in G - \{1, g, g^{-1}\}$, onde $g \in G$ é um elemento de ordem maior do que 2.

(5) Uma graduação da forma $A_1 = \mathbb{K}I_2, A_g = \mathbb{K}X, A_h = \mathbb{K}Y, A_{gh} = \mathbb{K}XY, A_u = 0$ para $u \in G - \{1, g, h, gh\}$, onde $g, h \in G$ tais que $\{1, g, h, gh\}$ é um subgrupo de G isomorfo à $C_2 \times C_2$, e X, Y são matrizes invertíveis tais que $X^2, Y^2 \in \mathbb{K}I_2$ e $XY = -YX$.

(II) Se $char(\mathbb{K}) = 2$, então qualquer graduação é isomorfa a uma das graduações do tipo $(1), (2), (4)$ em (I) ou a graduação da forma

(3') $A_1 = \left\{ \begin{pmatrix} x & x+y \\ b(x+y) & y \end{pmatrix} | x, y \in \mathbb{K} \right\}$, $A_g = \left\{ \begin{pmatrix} bx+y & x \\ y & bx+y \end{pmatrix} | x, y \in \mathbb{K} \right\}$, $A_h = 0$ *para* $h \in G - \{1, g\}$, *onde* $g \in G$ *é um elemento de ordem 2, e* $b \in \mathbb{K} - \{\alpha^2 + \alpha | \alpha \in \mathbb{K}\}$.

A seguir temos uma sequência de lemas que nos auxiliarão na demonstração do Teorema 30.

Lema 31 *Sejam* X, Y *elementos não nulos de* $M_2(\mathbb{K})$ *tais que* $X^2 \in \mathbb{K}I_2$ *e* $XY = YX = 0$. *Então* $X^2 = 0$, *e* X, Y *são linearmente dependentes.*

Prova:

Suponha, por absurdo, que $X^2 \neq 0$. Então $X^2 \in \mathbb{K}^* I_2$. Logo,

$$X \cdot X = kI_2, k \neq 0 \Rightarrow X \cdot \left(\frac{1}{k}X\right) = I_2 \Rightarrow X \text{ é invertível.}$$

Portanto, de $XY = 0$ temos $Y = 0$, o que contradiz nossa hipótese. Então devemos ter $X^2 = 0$.

Com isso em mãos, faça $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Note que $X^2 = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix}$, e desde que $X^2 = 0$, então devemos ter

$$a^2 + bc = 0 = bc + d^2 \tag{2.1}$$

$$ac + cd = 0 = ab + bd \tag{2.2}$$

Portanto, $a^2 = d^2 \Rightarrow a = -d$ ou $a = d$, além de $a^2 = -bc$. Assim, a partir deste momento iremos nos focar em dois casos.

1º caso: $a = d$. Das equações (2.2) temos $2ab = 0$ e $2ac = 0$. Se $a \neq 0$, então $b = c = 0$. Mas $a^2 = -bc = 0 \Rightarrow a = 0$, uma contradição. Logo devemos ter $a = d = 0$.

Portanto $X = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$. Agora faça $Y = \begin{pmatrix} x & y \\ w & z \end{pmatrix}$, e então de $XY = 0 = YX$ temos

(I) $bw = 0 = cy$

(II) $bz = 0 = bx$

(III) $cz = 0 = cx$

Se $b = 0$, então $c \neq 0$ (pois $X \neq 0$). Então por (I) e (III) temos $x = y = z = 0$. Logo, $Y = \begin{pmatrix} 0 & 0 \\ w & 0 \end{pmatrix}$ e $X = \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}$. Obviamente X e Y são l.d.

Se $c = 0$, então $b \neq 0$. Segue por (I) e (II) que $x = w = z = 0$. Daí, $Y = \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix}$ e $X = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$. Mais uma vez temos X e Y l.d.

Observe que não podemos ter o caso $b \neq 0$ e $c \neq 0$, pois senão Y seria a matriz nula, contradizendo a hipótese.

2º caso: $a = -d$. Neste caso $X = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ com $a^2 = -bc$. As equações $XY = 0 = YX$ nos fornecem as seguintes equações

(I) $ax + bw = 0 = ax + cy \Rightarrow bw = cy$

(II) $ay + bz = 0 = bx - ay \Rightarrow 2ay = bx - bz$

(III) $cx - aw = 0 = aw + cz \Rightarrow 2aw = cx - cz$

(IV) $cy - az = bw - az$

Se $w \neq 0$, então podemos escrever $b = \dfrac{c}{w}y$. Agora observe que

$$(III) \Rightarrow cx - aw = 0 \Rightarrow aw = cx \Rightarrow a = \frac{c}{w}x,$$

$$(III) \Rightarrow aw + cz = 0 \Rightarrow -aw = cz \Rightarrow -a = \frac{c}{w}z$$

$$\text{e obviamente } c = \frac{c}{w}w.$$

Logo, temos $X = \dfrac{c}{w}Y$, ou seja, X e Y são l.d.

Se $w = 0$, então em (I) temos $cy = bw = 0$. Se $c = 0$, então de $a^2 = -bc$, temos $a = 0$. Para $a = 0$, em (II) temos $b(x - z) = 0$. Se $b = 0$, então $X = 0$, o que é uma contradição. Por isso, $x = z$, e em (II), temos $ay + bz = 0 \Rightarrow bz = 0 \Rightarrow z = 0 = x$. Portanto, $Y = \dfrac{y}{b}X$. Agora se $c \neq 0$, então $y = 0$. Daí, em (III), temos $0 = c(x - z) \Rightarrow x = z$, mas também temos em (III) que $cx = aw = 0$ o que nos fornece $x = z = 0$. Logo $Y = 0$, o que é uma contradição.

Isto encerra a prova do lema.

■

Lema 32 *Seja* $A = \bigoplus_{g \in G} A_g$ *uma graduação da álgebra de matrizes. Se* $X \in A_g$ *para algum* $g \in G$, *então* $X^2 \in A_1$. *Em particular, se* $g^2 \neq 1$ *temos* $X^2 = 0$.

Prova:

Se $X = 0$, então $X^2 = 0 \in A_g, \forall g \in G$, em particular para $g = 1$. Suponha agora que $X \neq 0$. Sendo $X \in M_2(\mathbb{K})$, segue pelo Teorema de Cayley-Hamilton que

$$X^2 = -det(X)I_2 + tr(X)X \in A_1 + A_g.$$

Por outro lado, $X \cdot X \in A_{g.g} \Rightarrow X^2 \in A_{g^2}$. Caso $g = 1$, então a última pertinência nos fornece $X^2 \in A_1$. Se $g \neq 1$, então podemos ter $g^2 = 1$ ou $g^2 \neq 1$. No primeiro caso temos $X^2 \in A_1$. Já no segundo podemos afirmar que $X^2 \in A_{g^2} \cap (A_1 + A_g) = 0$. Logo, para $g^2 \neq 1$, temos $X^2 = 0$.

■

Corolário 33 *Se $A = \bigoplus_{g \in G} A_g$ é uma graduação tal que $A_1 = \mathbb{K}I_2$, então para qualquer $g, h \in G, g \neq h$ e quaisquer $X \in A_g, Y \in A_h$ não nulos, temos $XY \neq 0$ ou $YX \neq 0$.*

Prova:

Pelo Lema 32, $X^2 \in \mathbb{K}I_2$. Suponha então, por absurdo, que $XY = YX = 0$. Segue pelo Lema 31 que X e Y são L.D., o que contradiz o fato de $X \in A_g$ e $Y \in A_h$, $g \neq h$, com $X, Y \neq 0$. ■

Lema 34 *Seja $A = \bigoplus_{g \in G} A_g$ uma graduação tal que $A_1 \cap A_g A_h = \{0\}$ para qualquer $g, h \in supp(A) - \{1\}$ (em particular isso acontece quando $gh \neq 1$ para qualquer $g, h \in supp(A) - \{1\}$). Então a graduação é trivial.*

Prova:

Defina $\phi : A \to A_1$ por $\phi(X) = X_1$, onde X_1 é a componente homogênea de grau 1 de X. Provemos que ϕ é um homomorfismo de álgebras. De fato

- $\phi(X + Y) = (X + Y)_1 = X_1 + Y_1 = \phi(X) + \phi(Y)$;
- $\phi(\alpha X) = (\alpha X)_1 = \alpha X_1 = \alpha\phi(X)$, $\alpha \in \mathbb{K}$;
- $\phi(XY) = (XY)_1 = \sum_{g,h \in G, gh=1} X_g Y_h = \sum_{g,h \in supp(A), gh=1} X_g Y_h = X_1 Y_1$, já que $A_1 \cap A_g A_h = 0$;
- $\phi(I_2) = I_2$, pois $I_2 \in A_1$.

Como $\phi \neq 0$, então $\ker(\phi) \neq A$. Mas $\ker(\phi)$ é um ideal de $M_2(\mathbb{K})$, e com isso temos pelo Lema 8 que $\ker(\phi) = 0$, o que implica em ϕ ser injetivo. Desde que $A_1 \subseteq A$, segue então $dim(A_1) = dim(A)$ e daí $A_1 = A$. ■

2.1 Graduações de suporte 2

Nesta seção vamos apresentar as primeiras graduações da álgebra $M_2(\mathbb{K})$, mas restrita ao caso em que o suporte tenha apenas dois elementos. Primeiramente vamos mostrar as graduações feitas a partir de um grupo cíclico de ordem dois $C_2 = \{1, c\}$, i.e., $c^2 = 1$. Em seguida, mostramos que dada uma graduação de suporte dois, esta é essencialmente feita pelo grupo C_2.

Proposição 35 *Seja $\mathbb{K}$ um corpo e $C_2 = \{1, c\}$ um grupo cíclico de ordem 2. Então as C_2-graduações de $A = M_2(\mathbb{K})$ são descritas como segue:*

(I) Se $char(\mathbb{K}) \neq 2$, qualquer graduação é isomorfa a:

(1) A graduação trivial $A_1 = M_2(\mathbb{K})$ e $A_c = 0$;

(2) A boa graduação $A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}$, $A_c = \begin{pmatrix} 0 & \mathbb{K} \\ \mathbb{K} & 0 \end{pmatrix}$;

(3) A graduação $A_1 = \left\{ \begin{pmatrix} u & v \\ bv & u \end{pmatrix} | u, v \in \mathbb{K} \right\}$, $A_c = \left\{ \begin{pmatrix} u & v \\ -bv & -u \end{pmatrix} | u, v \in \mathbb{K} \right\}$, onde $b \in \mathbb{K} - \mathbb{K}^2$.

(II) Se $char(\mathbb{K}) = 2$, então qualquer graduação é isomorfa a graduação trivial, ou a boa graduação, ou a graduação da forma

(3') $A_1 = \left\{ \begin{pmatrix} x & x+y \\ b(x+y) & y \end{pmatrix} | x, y \in \mathbb{K} \right\}$, $A_c = \left\{ \begin{pmatrix} bx+y & x \\ y & bx+y \end{pmatrix} | x, y \in \mathbb{K} \right\}$, onde $b \in \mathbb{K} - \{\alpha^2 + \alpha | \alpha \in \mathbb{K}\}$.

Prova:

Seja $\mathbb{K}$ um corpo de característica qualquer e assuma que a graduação não é a trivial. Então temos os seguintes casos a considerar:

Caso 1: $dim(A_1) = 3$ e $dim(A_c) = 1$. Afirmamos que para qualquer matriz $Y \in A$ não invertível, temos $Y^2 = tr(Y)Y$. De fato, seja $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ com $det(Y) = ad - bc = 0$, i.e., não invertível e veja que

$$Y^2 = \begin{pmatrix} a^2 + bc & (a+d)b \\ (a+d)c & bc + d^2 \end{pmatrix} = \begin{pmatrix} a^2 + ad & (a+d)b \\ (a+d)c & ad + d^2 \end{pmatrix} = \begin{pmatrix} (a+d)a & (a+d)b \\ (a+d)c & (a+d)d \end{pmatrix} =$$

$$= (a+d)Y.$$

Agora seja $X \neq 0$ em A_c. Então $A_c = \mathbb{K}X$. Note que X é invertível. Com efeito, se $det(X) = 0$, pela afirmação anterior teríamos $X^2 = tr(X)X \in A_c$. Observe também que

podemos tomar $X^2 \neq 0$, pois se $X^2 = 0$ então pelo Lema 34, como $A_1 \cap A_cA_c = \{0\}$, a graduação em questão seria a trivial, o que é um absurdo. Logo concluímos que

$$0 \neq X^2 \in A_1 \cap A_c,$$

i.e.,$A_1 \cap A_c \neq \{0\}$, nos fornecendo mais uma vez um absurdo. Portanto para $B \in A_1 - \mathbb{K}I_2$, segue que $BX \in A_c$ e daí existe $\alpha \in \mathbb{K}$ tal que $BX = \alpha X \Rightarrow B = \alpha I_2 \in \mathbb{K}I_2$, o que é uma contradição. Logo não podemos ter este caso.

Caso 2: $dim(A_1) = 1$ **e** $dim(A_c) = 3$. Se $A_cA_c = 0$ então pelo Lema 34 a graduação é a trivial. Suponha então que existam $X, Y \in A_c$ tais que $XY \neq 0$. Como $dim(A_1) = 1$, então $A_1 = \mathbb{K}I_2$. Daí $XY \in \mathbb{K}^*I_2$. Segue que

$$XY \in \mathbb{K}^*I_2 \Rightarrow det(XY) \neq 0 \Rightarrow XY \text{ é invertível} \Rightarrow X \text{ e } Y \text{ invertíveis.}$$

Logo para $Z \in A_c - \mathbb{K}X$ temo que $XZ \in \mathbb{K}^*I_2$ (pois se $XZ = 0$, então $Z = 0$) e também $X^2 \in \mathbb{K}^*I_2$ (pois X^2 é invertível, logo $\neq 0$). Com isso, $XZ = \alpha I_2 \Rightarrow X^2Z = \alpha X \Rightarrow \beta I_2 Z = \alpha X \Rightarrow Z = \frac{\alpha}{\beta}X$, o que é uma contradição. Concluímos que esse caso também não é possível.

Caso 3: $dim(A_1) = dim(A_c) = 2$. Desde que $I_2 \in A_1$ e $dim(A_1) = 2$, então seja $\{I_2, B\}$ uma base de A_1. Logo $A_1 = \mathbb{K}I_2 + \mathbb{K}B$. Se considerarmos a graduação $A = A_1' \oplus A_c'$ (isomorfa a inicial), onde $A_1' = UA_1U^{-1}, A_c' = UA_cU^{-1}$ com U sendo uma matriz qualquer invertível, segue então que podemos trabalhar com matrizes semelhantes à B. Aqui iremos analisar todos os possíveis polinômios minimais que B pode assumir, lembrando da observação feita na seção 1.1 sobre matrizes semelhantes de ordem 2.

Começemos supondo que B seja uma matriz diagonal. Então $A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}$. Daí se $X = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \in A_c$, segue que $e_{11}Xe_{11} \in A_c \Rightarrow \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in A_c \Rightarrow x = 0$, pois $A_1 \cap A_c = \{0\}$. Analogamente mostra-se que $z = 0$ (basta utilizar a matriz e_{22}). Com isso temos a inclusão $A_c \subseteq \begin{pmatrix} 0 & \mathbb{K} \\ \mathbb{K} & 0 \end{pmatrix}$. A inclusão contrária é dada pela igualdade $A = A_1 \oplus A_c$. Logo temos $A_c = \begin{pmatrix} 0 & \mathbb{K} \\ \mathbb{K} & 0 \end{pmatrix}$, o que nos fornece uma graduação do tipo I-2. Note que essa análise sobre as matrizes diagonais eliminam todos os polinômios minimais de grau 1, já que dado o polinômio $m(t) = t + a, a \in \mathbb{K}^*$, basta considerar a matriz $\begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix}$, e assim $m(t)$ será minimal.

Agora suponha que o polinômio minimal de B seja da forma $m(t) = t^2 - b, b \notin \mathbb{K}^2$.

Essa última hipótese é posta, pois caso $b = c^2$, então teríamos $m(t) = (t+c)(t-c)$, que recai no caso das matrizes diagonais. Mais geralmente, para qualquer polinômio da forma $(t+a)(t+b), a \neq b$, podemos recair no caso das matrizes diagonais e aqui temos $a \neq b$, pois caso contrário B seria escalar, o que é um absurdo. Visto isso, segue que

$$B \sim \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}.$$

Portanto podemos susbstituir $B = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$ e como $A_1 = \mathbb{K}I_2 + \mathbb{K}B$, temos

$$A_1 = \left\{ \begin{pmatrix} u & v \\ bv & u \end{pmatrix} | u, v \in \mathbb{K} \right\}.$$

Agora seja $X \in A$ tal que $X^2 \in A_1$. Se fizermos $X = \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}$, para que $X^2 \in A_1$ devemos ter o seguinte sistema

$$\begin{cases} \lambda_1^2 & + & \lambda_2\lambda_3 & = & u \\ \lambda_4^2 & + & \lambda_2\lambda_3 & = & u \\ \lambda_1\lambda_2 & + & \lambda_2\lambda_4 & = & v \\ \lambda_1\lambda_3 & + & \lambda_3\lambda_4 & = & bv \end{cases}. \tag{2.3}$$

As duas primeiras equações de (2.3) nos dão $\lambda_1 = \pm\lambda_4$. Se $\lambda_1 = \lambda_4$, então das duas últimas equações de (2.3) temos $2\lambda_1\lambda_2 = v$ e $2\lambda_1\lambda_3 = bv$, i.e., $2\lambda_1\lambda_3 = 2b\lambda_1\lambda_2$. Para $\lambda_1 \neq 0$, temos $\lambda_3 = b\lambda_2$ e caso $\lambda_1 = 0$, então $\lambda_4 = 0$ e λ_2 e λ_3 serão variáveis livres. Se $\lambda_1 = -\lambda_4$, as duas últimas equações de (2.3) também nos fornece λ_2 e λ_3 como sendo variáveis livres.

Concluímos que se $X \in A$ tal que $X^2 \in A_1$, então $X = \begin{pmatrix} x & y \\ by & x \end{pmatrix}$ ou $X = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}, x, y, z \in \mathbb{K}$. Sendo assim, se tivermos $X \in A_c$, então $X = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}$. Desde que $BX \in A_c$ e $BX = \begin{pmatrix} z & -x \\ bx & by \end{pmatrix}$, segue que $z = -by$. Logo, mostramos que

$$A_c \subseteq H = \left\{ \begin{pmatrix} u & v \\ -bv & -u \end{pmatrix} | u, v \in \mathbb{K} \right\},$$

e como $dim(A_c) = dim(H) = 2$, segue que $A_c = H$.

Se $char(\mathbb{K}) = 2$, então $A_1 = A_c$, o que não pode ocorrer. Portanto devemos ter $char(\mathbb{K}) \neq 2$. Temos então uma graduação do tipo I-3.

Se o polinômio minimal de B for $m(t) = (t-\lambda)^2, \lambda \in \mathbb{K}$, então podemos substituir B por $B - \lambda I_2 \in A_1$ e obtermos uma nova matriz $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, pela forma de Jordan, veja o Exemplo 47 no Apêndice. Operando de forma análoga ao caso anterior, segue que

$$A_c \subseteq \left\{ \begin{pmatrix} u & v \\ 0 & -u \end{pmatrix} | u, v \in \mathbb{K} \right\}.$$

Mas assim $A_1 + A_c \subseteq \begin{pmatrix} \mathbb{K} & \mathbb{K} \\ 0 & \mathbb{K} \end{pmatrix} \neq A$, o que é uma contradição. Portanto, B não pode assumir tal polinômio minimal.

Por último, vamos ao caso em que o polinômio minimal de B seja irredutível da forma $m(t) = t^2 - \alpha t + \beta, \alpha \neq 0$. Suponha $char(\mathbb{K}) \neq 2$. Note então que as matrizes B e $\begin{pmatrix} \alpha/2 & 1 \\ b & \alpha/2 \end{pmatrix}$ possuem o mesmo polinômio minimal para algum $b \in \mathbb{K}$ adequado. Logo tais matrizes são semelhantes e por isso podemos supor $B = \begin{pmatrix} \alpha/2 & 1 \\ b & \alpha/2 \end{pmatrix}$. Substituindo esta por $B - (\alpha/2)I_2$ teremos $B = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$. Aqui devemos ter $b \notin \mathbb{K}^2$, pois se $b = c^2$, para algum $c \in \mathbb{K}$, então

$$m(t) = t^2 - \alpha t + \frac{\alpha^2}{4} - c^2 = (t^2 - \frac{\alpha}{2})^2 - c^2 = (t - \frac{\alpha}{2} - c)(t - \frac{\alpha}{2} + c),$$

o que é uma contradição. Mas note que nas condições acima, este caso já foi estudado.

Agora se $char(\mathbb{K}) = 2$, então vamos substituir B por $(1/\alpha)B \in A_1$, o que nos fornece um polinômio minimal da forma $t^2 + t + b$, para algum $b \in \mathbb{K}$. Vamos assumir então $B = \begin{pmatrix} 0 & 1 \\ b & 1 \end{pmatrix}$. Note que com isso devemos ter $b \notin \{\alpha^2 + \alpha | \alpha \in \mathbb{K}\}$, pois caso contrário, teríamos

$$m(t) = t^2 + t + \alpha^2 + \alpha = t^2 + \alpha^2 + t + \alpha = (t+\alpha)^2 + t + \alpha = (t+\alpha)(t+\alpha+1),$$

i.e., $m(t)$ seria redutível. Com isso temos

$$A_1 = \left\{ \begin{pmatrix} x & u \\ bu & x+u \end{pmatrix} | x, u \in \mathbb{K} \right\} = \left\{ \begin{pmatrix} x & x+y \\ b(x+y) & y \end{pmatrix} | x, y \in \mathbb{K} \right\},$$

fazendo $u = x + y$. Agora seja $X = \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix} \in A_c$. Desde que $X^2 \in A_1$, então devemos ter

$$\begin{cases} \lambda_1^2 & + & \lambda_2\lambda_3 & = & x \\ \lambda_4^2 & + & \lambda_2\lambda_3 & = & y \\ \lambda_1\lambda_2 & + & \lambda_2\lambda_4 & = & x+y \\ \lambda_1\lambda_3 & + & \lambda_3\lambda_4 & = & b(x+y) \end{cases} \tag{2.4}$$

Das duas primeiras equações de (2.2), temos $x + y = \lambda_1^2 + \lambda_4^2$. Portanto, na terceira equação segue que $\lambda_2(\lambda_1 + \lambda_4) = \lambda_1^2 + \lambda_4^2$, o que implica na quarta equação de (2.2) que,

$$\lambda_3(\lambda_1 + \lambda_4) = b(\lambda_1^2 + \lambda_4^2) = b\lambda_2(\lambda_1 + \lambda_4).$$

Se $\lambda_1 + \lambda_4 \neq 0$, então $\lambda_3 = b\lambda_2$, ou seja, $X = \begin{pmatrix} \lambda_1 & \lambda_2 \\ b\lambda_2 & \lambda_4 \end{pmatrix}$. Mas como $(BX)^2 \in A_1$ e

$$(BX)^2 = \begin{pmatrix} b^2\lambda_2^2 + b\lambda_4\lambda_1 + b\lambda_4\lambda_2 & \lambda_4^2 \\ b(\lambda_4\lambda_1 + \lambda_4\lambda_2) & b\lambda_4\lambda_1 + b\lambda_4\lambda_2 + b^2\lambda_2^2 + \lambda_4^2 \end{pmatrix}$$

segue que devemos ter $\lambda_4(\lambda_1 + \lambda_2) = \lambda_4^2$. Caso $\lambda_4 = 0$, então como $\lambda_1 + \lambda_4 \neq 0$, segue que devemos ter $\lambda_1 \neq 0$, e da equação $(\lambda_1 + \lambda_4)\lambda_2 = \lambda_1^2 + \lambda_4^2$ temos $\lambda_1 = \lambda_2$, ou seja,

$$X = \begin{pmatrix} \lambda_1 & \lambda_1 \\ b\lambda_1 & 0 \end{pmatrix} \in A_1,$$

o que é um absurdo. Caso $\lambda_4 \neq 0$, temos $\lambda_1 + \lambda_2 = \lambda_4$ e então

$$X = \begin{pmatrix} \lambda_1 & \lambda_2 \\ b\lambda_2 & \lambda_4 \end{pmatrix} \in A_1,$$

o que resulta novamente em uma contradição. Portanto devemos ter $\lambda_1 + \lambda_4 = 0$, i. e., $\lambda_1 = \lambda_4$. Logo $X = \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_1 \end{pmatrix}$ o que implica em

$$(BX)^2 = \begin{pmatrix} \lambda_3^2 + b\lambda_1^2 + \lambda_1\lambda_3 & \lambda_1\lambda_3 + b\lambda_1\lambda_2 + \lambda_1^2 \\ b\lambda_1\lambda_3 + \lambda_3^2 + b^2\lambda_1\lambda_2 + b\lambda_2\lambda_3 + b\lambda_1^2 + \lambda_1\lambda_3 & b\lambda_1^2 + \lambda_1\lambda_3 + b^2\lambda_2^2 + \lambda_1^2 \end{pmatrix}$$

e desde que $(BX)^2 \in A_1$, segue que $x_{11} + x_{22} = x_{12}$ e $x_{21} = bx_{12}$, onde aqui x_{ij} representa o elemento da i-ésima linha e j-ésima coluna da matriz $(BX)^2$. Dessas duas equações obtemos

$$\begin{aligned} &(I)\ \lambda_3^2 + b^2\lambda_2^2 = \lambda_1\lambda_3 + b\lambda_1\lambda_2 \\ &(II)\ \lambda_3^2 + b\lambda_2\lambda_3 + \lambda_1\lambda_3 = 0. \end{aligned}$$

Somando (I) e (II) membro a membro chegamos a $\lambda_2\lambda_3 = b\lambda_2^2 + \lambda_1\lambda_2$. Desta equação,

podemos ter $\lambda_2 = 0$ ou $\lambda_2 \neq 0$. Se $\lambda_2 = 0$, então de $(BX)^2 \in A_1$, devemos ter $\lambda_3^2 = \lambda_1\lambda_3$. Caso $\lambda_3 = 0$, então $X = \lambda_1 I_2 \in A_1$, o que é um absurdo. Logo $\lambda_3 \neq 0$ e assim

$$\lambda_3^2 = \lambda_1\lambda_3 \Rightarrow \lambda_3 = \lambda_1.$$

Portanto,

$$X = \begin{pmatrix} \lambda_1 & 0 \\ \lambda_1 & \lambda_1 \end{pmatrix} \in H' = \left\{ \begin{pmatrix} v & y \\ by+v & v \end{pmatrix} | y, v \in \mathbb{K} \right\}.$$

Agora se $\lambda_2 \neq 0$, então $\lambda_3 = b\lambda_2 + \lambda_1$. Podemos ver então que

$$A_c \subseteq H' = \left\{ \begin{pmatrix} v & y \\ by+v & v \end{pmatrix} | y, v \in \mathbb{K} \right\} = \left\{ \begin{pmatrix} bx+y & x \\ y & bx+y \end{pmatrix} | x, y \in \mathbb{K} \right\}.$$

Desde que $A_c \subseteq H'$ e $dimH' = 2 = dimA_c$, temos $A_c = H'$ e obtemos então uma graduação do tipo II-3'.

■

O que fizemos nesta última proposição foi apresentar uma graduação específica de $M_2(\mathbb{K})$ quando temos dois elementos no conjunto suporte, isto é, apenas dois subespaços não nulos na decomposição de $M_2(\mathbb{K})$ como espaço vetorial.

O que iremos fazer agora é mostrar que qualquer outra graduação da álgebra das matrizes de ordem dois com suporte dois é essencialmente uma C_2-graduação, ou seja, é isomorfa a alguma graduação apresentada na Proposição 35.

Proposição 36 *Seja G um grupo. Então qualquer G-graduação de $A = M_2(\mathbb{K})$ com $|supp(A)| = 2$ é do tipo C_2.*

Prova:

Seja $supp(A) = \{1, g\}$. Se $g^2 = 1$ (ordem dois), então a graduação já é do tipo C_2. Caso $g^2 \neq 1$, então $A_1 \cap A_g A_g \subset A_1 \cap A_{g^2} = \{0\}$. Pelo Lema 34 a graduação é a trivial, o que encerra a prova. ■

Com isso temos todas as graduações de $M_2(\mathbb{K})$ em suporte dois.

2.2 Graduações de suporte 3

Nesta seção iremos apresentar as graduações da álgebra $A = M_2(\mathbb{K})$ por um grupo G com $supp(A) = \{1, g, h\}$, $1, g, h \in G$. Dividiremos em dois casos: $dim(A_1) = 2$ e $dim(A_1) = 1$. Aqui iremos usar a notação $deg(X) = g$ para dizer que $X \in A_g$, em que A_g é um subespaço da decomposição da álgebra em questão.

Proposição 37 *Se $dim(A_1) = 2$, então $h = g^{-1}$ e a graduação é isomorfa à boa graduação dada por*

$$A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}, A_g = \begin{pmatrix} 0 & \mathbb{K} \\ 0 & 0 \end{pmatrix}, A_{g^{-1}} = \begin{pmatrix} 0 & 0 \\ \mathbb{K} & 0 \end{pmatrix}, A_p = 0, \forall p \in G - \{1, g, g^{-1}\}.$$

Prova:

Se $dim(A_1) = 2$, então existe $B \in A_1$ tal que $A_1 = [I_2, B]$. Do fato de $dim(A_g) = dim(A_h) = 1$, segue que existem $X, Y \in A$ com $A_g = \mathbb{K}X$ e $A_h = \mathbb{K}Y$. Como $A_1 A_g \subseteq A_g$ e $A_1 A_h \subseteq A_h$, segue que existem $\alpha, \beta \in \mathbb{K}$ tais que $BX = \alpha X$ e $BY = \beta Y$. Portanto, o mapa linear $\phi : A \to A$ dado por

$$\phi(Z) = BZ,$$

tem α e β como autovalores com autovetores X e Y, respectivamente. Suponha que $B = \begin{pmatrix} x & y \\ w & z \end{pmatrix}$, então considerando a base canônica de A, vemos que a matriz associada a transformação ϕ é

$$[\phi] = \begin{pmatrix} x & 0 & y & 0 \\ 0 & x & 0 & y \\ w & 0 & z & 0 \\ 0 & w & 0 & z \end{pmatrix}.$$

É fácil ver que

$$p_\phi = p_B^2, \tag{2.5}$$

em que p_ϕ é o polinômio característico de ϕ e p_B é o polinômio característico de B. Logo, desde que α e β sejam raízes de p_ϕ, então também serão de p_B, e portanto este pode ser fatorado em dois fatores lineares. Note que podemos considerar que B possui sua forma de Jordan. Primeiramente vamos supor $B = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}, b_1 \neq b_2$, diagonalizável. Então

$$A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}.$$

Portanto, podemos substituir B por qualquer matriz em A_1 que não seja escalar, e vamos escolher $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Segue que 0 e 1 são os autovalores de B e, por (2.5), 0 e 1 também são autovalores de ϕ. Daí em relação ao autovalor 0, temos autovetores da forma $\begin{pmatrix} 0 & 0 \\ r & s \end{pmatrix}$ e para o autovalor 1, temos os autovetores da forma $\begin{pmatrix} u & v \\ 0 & 0 \end{pmatrix}$. Logo

$A_g = \mathbb{K}\begin{pmatrix} u & 1 \\ 0 & 0 \end{pmatrix}$ e desde que $A_gA_1 \subseteq A_g$, então

$$\begin{pmatrix} u & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} u & 0 \\ 0 & 0 \end{pmatrix} \in A_g \Leftrightarrow u = 0.$$

Portanto,

$$A_g = \begin{pmatrix} 0 & \mathbb{K} \\ 0 & 0 \end{pmatrix}.$$

Analogamente mostra-se que

$$A_h = \begin{pmatrix} 0 & 0 \\ \mathbb{K} & 0 \end{pmatrix}.$$

Desde que $deg(e_{12}) = g$ e $deg(e_{21}) = h$, $0 \neq e_{12}e_{21} \in A_1$ e $A_gA_h \subseteq A_{gh}$, segue que devemos ter $gh = 1$. De forma análoga, também temos $hg = 1$ e portanto $g = h^{-1}$, o que nos fornece uma graduação.

Agora vamos supor B não diagonalizável. Então $\alpha = \beta = b \in \mathbb{K}$. Segue pela forma de Jordan (veja o Exemplo 47) que

$$B = \begin{pmatrix} b & 1 \\ 0 & b \end{pmatrix},$$

e portanto

$$A_1 = \left\{ \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} | c, d \in \mathbb{K} \right\},$$

e novamente podemos substituir B por uma matriz não escalar em A_1 e escolhemos $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. É fácil ver que os autovetores associados a 0 em relação à ϕ são da forma $\begin{pmatrix} m & n \\ 0 & 0 \end{pmatrix}, m, n \in \mathbb{K}$ e que 0 é o único autovalor de ϕ. Com isso conseguimos apenas dois autovetores L.I. Desde que $\mathbb{K}B + \mathbb{K}X + \mathbb{K}Y$ tem dimensão 3 e consiste de autovetores L.I., obtemos uma contradição.

Observação. Se $g \in G$ é um elemento do grupo com ordem maior que 2, então $A = B = M_2(\mathbb{K})$ são isomorfas como álgebras G-graduadas, em que

$$A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}, A_g = \begin{pmatrix} 0 & \mathbb{K} \\ 0 & 0 \end{pmatrix}, A_{g^{-1}} = \begin{pmatrix} 0 & 0 \\ \mathbb{K} & 0 \end{pmatrix}, A_p = 0, \forall p \notin \{1, g, g^{-1}\}$$

$$B_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}, B_g = \begin{pmatrix} 0 & 0 \\ \mathbb{K} & 0 \end{pmatrix}, B_{g^{-1}} = \begin{pmatrix} 0 & \mathbb{K} \\ 0 & 0 \end{pmatrix}, B_p = 0, \forall p \notin \{1, g, g^{-1}\}.$$

De fato, o mapa $\phi : A \to B, \phi(X) = UXU^{-1}$, onde $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, é um isomorfismo graduado.

■

Proposição 38 *Não existe graduação de A com $|supp(A)| = 3$ e $dim(A_1) = 1$.*

Prova:

Suponha, por absurdo, que tal graduação exista e sem perda de generalidade que $dim(A_g) = 2$ e $dim(A_h) = 1$. Sejam $X \in A_g, Y \in A_h$ elementos não-nulos. Então pelo Corolário 33 temos que $XY \neq 0$ ou $YX \neq 0$. Como $gh, hg \notin \{g, h\}$, pois caso contrário $g = 1$ ou $h = 1$, então devemos ter $gh = 1$, e desde que $A_1 = \mathbb{K}I_2$, isto implica que $YX = \lambda I_2$, para algum $\lambda \in \mathbb{K}$, i.e., Y é invertível à direita. Logo, de $A_gY \subseteq A_1 = \mathbb{K}I_2$, temos que $A_g \subseteq \mathbb{K}Y^{-1}$, uma contradição com $dim(A_g) = 2$. ■

Note que no caso de suporte três não especificamos um grupo para construir a graduação, o que nos permite afirmar que qualquer graduação de $M_2(\mathbb{K})$ com suporte três é basicamente a apresentada nesta seção.

2.3 Graduações de suporte 4

Inicialmente vamos decrever todas as graduações de $A = M_2(\mathbb{K})$ pelo grupo de Klein.

Proposição 39 *Seja $G = C_2 \times C_2 = \{1, g, h, gh\}$ o grupo de Klein. Então:*

(I) Se $char(\mathbb{K}) \neq 2$, qualquer G-graduação de A é isomorfa a uma das seguintes graduações.

(1) Uma graduação do tipo C_2.

(2) Uma graduação da forma $A_1 = \mathbb{K}I_2, A_g = \mathbb{K}X, A_h = \mathbb{K}Y, A_{gh} = \mathbb{K}XY$, onde X, Y são matrizes invertíveis tais que $X^2, Y^2 \in \mathbb{K}I_2$ e $XY = -YX$.

(II) Se $char(\mathbb{K}) = 2$, qualquer G-graduação de A é isomorfa a uma graduação do tipo C_2.

Prova:

Assuma que a graduação não é do tipo C_2. Então $|supp(A)| \neq 3$, pois senão deveríamos ter $a, b \in G$ com e $a \neq b$ e $ab = ba = 1$, o que não ocorre no grupo de Klein. Logo $|supp(A)| = 4$ e assim cada subespaço deverá ter dimensão 1, em particular $A_1 = \mathbb{K}I_2$. Seja $A_g = \mathbb{K}X$ e $A_h = \mathbb{K}Y$. Pelo Corolário 33 temos $XY \neq 0$ ou $YX \neq 0$. Suponha $XY \neq 0$. Então

$$A_{gh} = \mathbb{K}XY.$$

Se $X^2 = 0$, então $X(XY) = 0$ e ainda, pelo Corolário 33, $(XY)X \neq 0$ e como $A_{gh}A_g \subseteq A_h$, segue que $XYX = \alpha Y$ para algum $\alpha \in \mathbb{K} \setminus \{0\}$. Mas então $0 = X(XY)X = \alpha XY$, o que é uma contradição. Daí $X^2 \neq 0$. Analogamente, $Y^2 \neq 0$. Portanto X e Y são invertíveis.

Desde que $X^{-1} \in A_g$, temos $XYX^{-1} \in A_h$, i.e., $XYX^{-1} = \alpha Y$, para algum escalar α. Logo, $\alpha^2 Y = X\alpha YX^{-1} = XXYX^{-1}X^{-1}$ e como $X^2 \in \mathbb{K}I_2$, temos

$$\alpha^2 Y = \beta I_2 Y \beta^{-1} I_2 = Y.$$

Se $char(\mathbb{K}) \neq 2$, então $\alpha \in \{1, -1\}$. Para $\alpha = 1$ temos $XY = YX$. Afirmamos que conseguimos gerar A como uma álgebra através de X e Y. De fato, X e Y geram A_g e A_h, respectivamente. O produto XY gera A_{gh} e X^2 gera A_1. O resultado será uma álgebra A comutativa. Absurdo! Logo devemos ter

$$XY = -YX$$

e a graduação é do tipo I-2. Se $char(\mathbb{K}) = 2$, então $\alpha = 1$, e novamente obtemos que A é comutativa, uma contradição. Concluímos que o único caso possível de gradução com $char(\mathbb{K}) = 2$ é a do tipo C_2. ■

Como no caso de suporte dois temos aqui uma graduação feita através de um grupo específico, o grupo de Klein. O que iremos fazer agora é provar que qualquer outra graduação de $M_2(\mathbb{K})$ com quatro elementos em seu suporte é essencialmente uma $C_2 \times C_2$ graduação, ou seja, é a graduação que construímos acima pelo grupo de Klein.

Proposição 40 *Qualquer graduação de A com $supp(A) = 4$ é do tipo $C_2 \times C_2$.*

Prova: Seja $A = \bigoplus_{g \in G} A_g$ com $S = supp(A) = \{1, g, h, s\}$.

Iremos dividir esta demonstração em duas partes: na primeira vamos provar que se existe algum elemento invertível em S então este terá de ser auto-invertível e na segunda parte vamos mostrar que todos os elementos de S são invertíveis.

1ª parte: Notemos que $uv \neq 1$, quaisquer que sejam $u, v \in S, u \neq v$. De fato, suporemos que existam $u, v \in S, u \neq v$, com $uv = 1$. Então tomemos os elementos não nulos $X \in A_u$ e $Y \in A_v$. Desde que $A_1 = \mathbb{K}I_2$, usando o fato de que $A_uA_v \subseteq A_1$, $A_vA_u \subseteq A_1$ e o Corolário 33, temos que $XY \in \mathbb{K}^*I_2$ ou $YX \in \mathbb{K}^*I_2$. Por outro lado o Lema

32 nos fornece $X^2 = 0$, já que $u^2 \neq 1$. Segue daí que $XY = \alpha I_2 \Rightarrow X^2Y = \alpha X \Rightarrow X = 0$, pois $\alpha \neq 0$. Chegamos então a uma contradição!

2ª parte: Desde que a graduação não é a trivial, então pelo Lema 34 e pelo o que acabamos de provar, temos que existe $u \in S \setminus \{1\}$ tal que $A_uA_u \cap A_1 \neq 0$ e como $A_uA_u \subseteq A_{u^2}$, segue que $u^2 = 1$. Vamos dizer que $u = g$ e, sendo assim, seja $A_g = \mathbb{K}X$. Note que $X^2 \in \mathbb{K}^*I_2$ e assim, X é invertível. Então $A_gA_h = XA_h \neq 0$ (pois $A_h \neq 0$ e X é invertível) e então $gh \in S$ e a única possibilidade é $gh = s$. Analogamente, $A_hA_g \neq 0$ e então $gh = hg = s$. Daí temos $hs = sh$. Se $hs \notin S$, então devemos ter $A_hA_s = A_sA_h = 0$, já que $A_hA_s \subseteq A_{hs} = 0$. Então se tomarmos elementos não nulos $Y \in A_h$ e $Z \in A_s$, teremos $YZ = ZY = 0$, o que é uma contradição com o Corolário 33. Logo $h(hg) = (hg)h \in S$ e desde que estes não podem ser $1, h$ ou hg, resta apenas $h(hg) = g$, implicando em $h^2 = 1$, o que prova que $S = C_2 \times C_2$. ■

Portanto classificamos todas as graduações de $M_2(\mathbb{K})$ com suporte quatro.

Juntamente com as duas seções precedentes temos todas as graduações de $M_2(\mathbb{K})$.

Considerações Finais

Finalizo com a apresentação de uma tabela que apresenta o resultado principal deste trabalho.

Graduação de $M_2(\mathbb{K})$	**Característica de $\mathbb{K}$**
Trivial	Qualquer
$A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}$, $A_g = \begin{pmatrix} 0 & \mathbb{K} \\ \mathbb{K} & 0 \end{pmatrix}$ e $A_h = 0, \forall h \in G - \{1, g\}, g^2 = 1$	Qualquer
$A_1 = \left\{ \begin{pmatrix} u & v \\ bv & u \end{pmatrix} \mid u, v \in \mathbb{K} \right\}$, $A_g = \left\{ \begin{pmatrix} u & v \\ -bv & -u \end{pmatrix} \mid u, v \in \mathbb{K} \right\}$ e $A_h = 0, \forall h \in G - \{1, g\}, g^2 = 1, b \in \mathbb{K} - \mathbb{K}^2$	$\neq 2$
$A_1 = \left\{ \begin{pmatrix} x & x+y \\ b(x+y) & y \end{pmatrix} \mid x, y \in \mathbb{K} \right\}$, $A_g = \left\{ \begin{pmatrix} bx+y & x \\ y & bx+y \end{pmatrix} \mid x, y \in \mathbb{K} \right\}$ e $A_h = 0, \forall h \in G - \{1, g\}, g^2 = 1, b \in \mathbb{K} - (\mathbb{K}^2 + \mathbb{K})$	$= 2$
$A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}$, $A_g = \begin{pmatrix} 0 & \mathbb{K} \\ 0 & 0 \end{pmatrix}$, $A_{g^{-1}} = \begin{pmatrix} 0 & 0 \\ \mathbb{K} & 0 \end{pmatrix}$ e $A_h = 0, \forall h \in G - \{1, g, g^{-1}\}, g^2 \neq 1$	Qualquer
$A_1 = \mathbb{K}I_2, A_g = \mathbb{K}X, A_h = \mathbb{K}Y, A_{gh} = \mathbb{K}XY, A_u = 0, \forall u \in G - \{1, g, h, gh\}, X, Y$ invertíveis, $X^2, Y^2 \in \mathbb{K}I_2, XY = -YX, G \supset \{1, g, h, gh\} \simeq C_2 \times C_2$	$\neq 2$

Na tabela, a primeira coluna apresenta, a menos de isomorfismo, todas a graduações possíveis e imagináveis de $M_2(\mathbb{K})$. Na segunda coluna temos em qual característica a respectiva graduação existe. No texto vimos que a característica do corpo foi de fundamental importância, pois a depender desta tinhamos por exemplo grandes absurdos, como foi na última seção, em que chegamos na seguinte afirmação: $M_2(\mathbb{K})$ é comutativa.

Algumas contas foram feitas de forma diferente da apresentada na referência principal, o artigo [9], como por exemplo na segunda parte do Lema 31, bem como na primeira parte do caso 1 da construção das graduações de suporte 2.

No texto é utilizada uma ferramenta muito útil da Álgebra Linear, que é a Forma Canônica de Jordan. Sobre esta última fiz um apêndice cuja referência principal foi [3].

Referências Bibliográficas

[1] BOLDRINI, J. L.; COSTA, S. I. R.; FIGUEIREDO, V. L.; WETZLER, H. G., *Álgebra Linear*, Harbra ltda, São Paulo (1980).

[2] BRANDÃO JR., A. P., *Polinômios Centrais para Álgebras Graduadas*, Tese de Doutorado, Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica, São Paulo (2006).

[3] BUENO, H. P., *Álgebra Linear: um segundo curso*, UFMG (2002).

[4] COELHO, F. U.; LOURENÇO, M. L., *Um Curso de Álgebra Linear*, Editora da Universidade de São Paulo, São Paulo (2005).

[5] DOMINGUES, H. H.; IEZZI, G., *Álgebra Moderna,* Harbra ltda, São Paulo (2003).

[6] DUMMIT, D. S.; FOOTE, R. M., *Abstract Algebra*, John Wiley & Sons, Inc, Vermont (2004).

[7] GIAMBRUNO, A.; ZAICEV, M., *Polynomial Identities and Asymptotic Methods*, Mathematical Surveys and Monographs, vol. 122, (2005).

[8] HOFFMAN, K.; KUNZE, R., *Álgebra Linear*, Livros Técnicos e Científicos Editora, Rio de Janeiro (1979).

[9] KHAZAL, R.; BOBOC, C.; DASCALESCU, S., *Group Gradings of* $M_2(\mathbb{K})$, Bulletin of the Australian Mathematical Society, **68**, 285-293 (2003).

[10] REIS, J. C., *Graduações e Identidades Graduadas para Álgebra de Matrizes*, Tese de Doutorado, Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica, São Paulo (2012).

Apêndice A

Forma Canônica de Jordan

Considere uma transformação linear $T : V \to V$, em que V é um espaço vetorial finitamente gerado. Sabemos que existe uma matriz A que representa esta transformação, e que tal matriz pode mudar conforme mudemos a base do espaço V. Sabemos também que se conseguirmos uma base formada por autovetores de T, então tal matriz será diagonal. Isso é o que chamamos de diagonalizar a matriz A. Mas nem sempre é possível ter essa base de autovetores. Chegamos perto! Conseguimos obter uma base com alguns autovetores, e mais alguns vetores, que chamaremos de autovetores generalizados. A matriz associada a esta base não será diagonal, mas será tão especial quanto esta.

Comecemos nossos estudos definindo espaço quociente.

Seja V um $\mathbb{K}$-espaço vetorial e W um subespaço de V. Para $v_1, v_2 \in V$, dizemos que $v_1 \sim v_2$ se $v_1 - v_2 \in W$. É fácil ver que essa relação definida é uma relação de equivalência. Portanto, para cada $v \in V$, temos $\overline{v} = \{u \in V : u \sim v\} = v + W$. Seja $V/W = \{\overline{v} : v \in V\}$. Definindo as operações

$$\overline{v}_1 + \overline{v}_2 = \overline{v_1 + v_2} \text{ e } \lambda\overline{v}_1 = \overline{\lambda v}_1, \forall\ \overline{v}_1, \overline{v}_2 \in V/W,$$

e verificando que elas estão bem definidas, é fácil ver V/W é um $\mathbb{K}$-espaço vetorial, chamado espaço quociente de V por W. Observe que $\overline{0} = W$, i.e., $\overline{v} = \overline{0} \Leftrightarrow v \in W$.

Um resultado importante sobre os espaços qoucientes é o que segue:

Proposição 41 *Sejam V um $\mathbb{K}$-espaço vetorial com $dim(V) = n$ e W um subespaço de V. Então*

$$dim(V) = dim(W) + dim(V/W).$$

Prova:

De fato, seja $B' = \{v_1, \cdots, v_k\}$ uma base de W e complete-a até uma base de V $B = \{v_1, \cdots, v_k, v_{k+1}, \cdots, v_n\}$. Provemos que o conjunto $B'' = \{\overline{v}_{k+1}, \cdots, \overline{v}_n\}$ é uma base de V/W. Considere $\lambda_{k+1}\overline{v}_{k+1} + \cdots + \lambda_n\overline{v}_n = \overline{0}$. Segue que $\lambda_{k+1}v_{k+1} + \cdots + \lambda_n v_n \in W \Rightarrow$ $\exists\, \alpha_1, \cdots, \alpha_k \in \mathbb{K}$ tais que $\lambda_{k+1}v_{k+1} + \cdots + \lambda_n v_n = \alpha_1 v_1 + \cdots + \alpha_k v_k \Rightarrow \lambda_j = 0, \forall j = 1, \cdots, k,$

pois B é L.I. Isso prova que B'' é L.I. Agora seja $\overline{v} \in V/W$. Como $v \in V$, então existem $\beta_i, i = 1, \cdots, n$ tais que $v = \beta_1 v_1 + \cdots + \beta_n v_n \Rightarrow \overline{v} = \overline{\beta_1 v_1 + \cdots + \beta_n v_n} = \beta_{k+1}\overline{v}_{k+1} + \cdots + \beta_n \overline{v}_n$, o que prova que B'' gera V/W. ■

Definição 42 *Seja $p(t) \in \mathbb{K}[t]$ o polinômio característico do operador $T : V \to V$, em que V é um espaço vetorial finitamente gerado. Suponha que $p(t) = [p_1(t)]^{s_1} \cdots [p_j(t)]^{s_j}$ seja a decomposição de p em fatores irredutíveis, com $p_i \neq p_k$ quando $i \neq k$. Para cada $i = 1, \cdots, j$, dizemos que o conjunto $\ker[p_i(T)]^k$ para algum $k \in \mathbb{N}$ é o autoespaço generalizado associado ao polinômio $p_i(t)$.*

Desde que para qualquer $n \in \mathbb{N}$ e para qualquer $v \in \ker[p_i(T)]^n$ temos $[p_i(T)]^{n+1}v = p_i(T)[p_i(T)]^n v = p_i(T) \cdot 0 = 0$, segue então as seguintes inclusões,

$$\ker[p_i(T)] \subset \ker[p_i(T)]^2 \subset \ker[p_i(T)]^3 \subset \cdots \subset V.$$

Como V é finitamente gerado, então para alguma potência os núcleos acima deverão estabilizar, i.e., serão iguais. Seja d_i o menor natural com esta propriedade. Então

$$\ker[p_i(T)]^{d_i} = \ker[p_i(T)]^{d_i+1} = \cdots, \text{mas} \ker[p_i(T)]^{d_i-1} \subsetneq \ker[p_i(T)]^{d_i}.$$

Para referências futuras, chamaremos o inteiro positivo d_i acima mencionado de índice de $p_i(T)$ e denotaremos $W_i = \ker[p_i(T)]^{d_i}$.

Aqui iremos assumir o Teorema da Decomposição Primária sem demonstração. Uma justificativa para este resultado pode ser encontrada em [3] ou [8], por exemplo.

Teorema 43 *Seja $T : V \to V$ um operador linear e $p(t) \in \mathbb{K}[t]$ seu polinômio característico. Se $p(t) = [p_1(t)]^{s_1} \cdots [p_j(t)]^{s_j}$ é a decomposição de p em fatores primos, com $p_i \neq p_k$ para $i \neq k$. Então, se d_i é o índice de $p_i(T)$, o polinômio minimal de T é $m(t) = [p_1(t)]^{d_1} \cdots [p_j(t)]^{d_j}$. Além disso, $V = \bigoplus_{i=1}^{j} W_i$, em que $W_i = \ker[p_i(T)]^{d_i}$, com $T(W_i) \subset W_i$, $\forall i = 1, \cdots, j$.*

Um corolário do teorema acima que será de fundamental importância no cálculo da Forma Canônica de Jordan de um matriz é o

Corolário 44 *O subespaço $W_i = \ker[p_i(T)]^{d_i}$ tem dimensão igual ao grau de $[p_i(t)]^{s_i}$, em que s_i é a multiplicidade de p_i como fator irredutível de $p(t)$.*

Prova:

Como o polinômio característico de uma matriz $n \times n$ tem grau n, então basta provar que o polinômio característico de T restrito à W_i é $[p_i(t)]^{s_i}$. Para isso, considere B_i uma

base para W_i. Como $V = \bigoplus_{i=1}^{j} W_i$, então a representação de T em relação à base $B = \bigcup_{i=1}^{j} B_i$ é dada pela matriz

$$[T]_B = A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_j \end{pmatrix}$$

em que A_i é um bloco de tamanho $k_i \times k_i$, onde k_i é a dimensão de W_i. Mais precisamente A_i é a matriz que representa a aplicação linear $T|_{W_i}$. Usando a definição de determinante dada em [1] é fácil ver que

$$det(tI_{n\times n} - A) = \prod_{i=1}^{j} det(tI_{k_i\times k_i} - A_i) \tag{A.1}$$

Note que $det(tI_{k_i\times k_i} - A_i)$ é o polinômio característico de $T|_{W_i}$. Pela definição do índice d_i, vemos que o polinômo minimal de $T|_{W_i}$ é dado por $[p_i(t)]^{d_i}$. Pelo Teorema da Decomposição Primária, segue o que polinômio característico de $T|_{W_i}$ é uma potência de $p_i(t)$ e pela igualdade A.1 acima temos que o característico de $T|_{W_i}$ deve ser $[p_i(t)]^{s_i}$.

■

A seguir, temos um lema que será usado na demonstração do teorema principal deste anexo.

Lema 45 *Sejam a matriz $A \in M_n(\mathbb{C})$, λ_i um autovalor de A e $W_i = \ker[p_i(A)]^{d_i}$. Então a aplicação*

$$A - \lambda_i I : \ker[p_i(A)]^{k+1}/\ker[p_i(A)]^k \to W_i$$

tem imagem contida em $\ker[p_i(A)]^k/\ker[p_i(A)]^{k-1}$ e é injetiva.

Prova:

Seja $0 \neq x \in \ker[p_i(A)]^{k+1}/\ker[p_i(A)]^k$, i.e., $x \in \ker[p_i(A)]^{k+1}$ e $x \notin \ker[p_i(A)]^k$. Segue que $x \in \ker[p_i(A)]^{k+1}$ e $x \notin \ker[p_i(A)]^k$. Como A tem entrada no conjunto dos números complexos, então podemos supor $p_i = t - \lambda_i I$. Portanto, $(A-\lambda_i I)^{k+1}x = 0$ e $(A-\lambda_i I)^k x \neq 0$. Considere agora $(A-\lambda_i I)x$. Desde que $(A-\lambda_i I)^k(A-\lambda_i I)x = (A-\lambda_i I)^{k+1}x = 0$, temos que $(A-\lambda_i I)x \in \ker[p_i(A)]^k$. Como $(A-\lambda_i I)^{k-1}(A-\lambda_i)x = (A-\lambda_i I)^k x \neq 0$, o que prova que $(A-\lambda_i I)x \in \ker[p_i(A)]^k/\ker[p_i(A)]^{k-1}$, para qualquer $x \in \ker[p_i(A)]^{k+1}/\ker[p_i(A)]^k$.

Agora sejam $x \neq y \in \ker[p_i(A)]^{k+1}/\ker[p_i(A)]^k$ com $(A-\lambda_i I)x = (A-\lambda_i I)y$. Daí temos $(A-\lambda_i I)(x-y) = 0 \Rightarrow (A-\lambda_i I)^k(x-y) = (A-\lambda_i I)^{k-1}(A-\lambda_i I)(x-y) = 0$, i.e., $x - y \in \ker[p_i(A)]^k$ o que é uma contradição. Isso prova que a aplicação linear $A - \lambda_i I$ acima definida é injetiva. ■

Agora vamos ao teorema principal

Teorema 46 *Sejam $A, B \in M_n(\mathbb{C})$ duas matrizes semelhantes. Então,*

(1) A e B têm os mesmos autovalores;

(2) os espaços $\ker(A-\lambda_i)^j$ *e* $\ker(B-\lambda_i)^j$ *têm a mesma dimensão para todo* $j \in \mathbb{N}$ *todo autovalor* λ_i.

Reciprocamente, se (1) e (2) valem, então A e B são semelhantes.

Prova:

Começemos a demonstração com uma afirmação: os núcleos de duas matrizes semelhantes têm a mesma dimensão. De fato, se C e D são semelhantes então existe uma matriz invertível Q tal que $C = Q^{-1}DQ$. Considere $\{x_1, \cdots, x_k\}$ uma base de $\ker C$. Então $Cx_i = 0, i = 1, \cdots, k$. Segue que $(Q^{-1}DQ)x_i = 0 \Rightarrow (DQ)x_i = 0 \Rightarrow D(Qx_i) = 0 \Rightarrow Qx_i \in \ker D, i = 1, \cdots, k$. Aqui temos que o conjunto $\{Qx_1, \cdots, Qx_k\}$ é uma base de $\ker D$. Com efeito, este conjunto é L.I., pois dado $\sum_{i=1}^{k} \alpha_i Qx_i = 0$, obtemos $\sum_{i=1}^{k} \alpha_i x_i = 0$ e consequentemente, $\alpha_1 = \cdots = \alpha_k = 0$, e tal conjunto também gera $\ker D$, pois dado $x \in \ker D$, temos $Dx = 0 \Rightarrow QCQ^{-1}x = 0 \Rightarrow CQ^{-1}x = 0 \Rightarrow C(Q^{-1}x) = 0 \Rightarrow Q^{-1}x = \sum_{i=1}^{k} \beta_i x_i \Rightarrow x = \sum_{i=1}^{k} \beta_i Qx_i$. Isso prova a afirmação. Agora, se A e B são semelhantes, então existe $P \in M_n(\mathbb{C})$ invertível tal que $A = P^{-1}BP$. Assim, qualquer que seja $a \in \mathbb{C}$, temos $A - aI = P^{-1}BP - aI = P^{-1}BP - aP^{-1}P = P^{-1}(B - aI)P$, o que prova que $A - aI$ é semelhante à $B - aI$. Com isso é fácil ver que também são semelhantes as matrizes $(A - aI)^m$ e $(B - aI)^m$, para qualquer $m \in \mathbb{N}$. Juntamente com a afirmação povada no início do texto, temos a justificação do item *(2)*. Para provar *(1)*, vamos supor sem perda de generalidade que λ_i seja um autovalor de A. Provemos então que λ_i também é um autovalor de B. Temos

$$Av_i = \lambda_i v_i \Leftrightarrow Q^{-1}BQv_i = \lambda_i v_i \Leftrightarrow B(Qv_i) = \lambda_i(Qv_i),$$

o que prova que λ_i também é um autovalor de B. Reciprocamente, lembrando que $W_i = \ker(A - \lambda_i I)^{d_i}$, vamos construir uma interessante base deste subespaço, a chamada **base de Jordan**.

Seja $\{x_1, \cdots, x_l\}$ uma base de $\ker(A - \lambda_i I)^{d_i} / \ker(A - \lambda_i I)^{d_i - 1}$. Pelo Lema 45 temos que $(A - \lambda_i I)x_1, \cdots, (A - \lambda_i I)x_l \in \ker(A - \lambda_i I)^{d_i - 1} / \ker(A - \lambda_i I)^{d_i - 2}$ e são L.I. Com isso, completamos o conjunto $\{(A - \lambda_i I)x_1, \cdots, (A - \lambda_i I)x_l\}$ até termos uma base deste último subespaço. Continuamos assim até chegarmos a uma base de $\ker(A - \lambda_i I)$. Note que desta forma temos uma base de W_i, e a união destas bases para todo $i = 1, \cdots, n$ nos fornece uma base para V, pelo Teorema da Decomposição Primária, que é a base desejada.

Agora, usando a hipótese *(2)*, temos $dim(\ker(A - \lambda_i I)^j) = dim(\ker(B - \lambda_i I)^j), \forall j \in \mathbb{N}$, e assim as dimensões de $\ker(A - \lambda_i I)^j / \ker(A - \lambda_i I)^{j-1}$ e $\ker(B - \lambda_i I)^j / \ker(B - \lambda_i I)^{j-1}$ também são as mesmas, pelo teorema da dimensão de espaços quocientes feito no início

do apêndice. Se denotarmos

$$N_j = \ker(A - \lambda_i I)^j \ e \ M_j = \ker(B - \lambda_i I)^j,$$

então existe uma única aplicação linear P que leva os elementos da base de Jordan em N_j/N_{j-1} para os respectivos em outra base em M_j/M_{j-1}. Como P leva base em base, segue que P é invertível. Portanto, de $P(A - \lambda_i I)x = (B - \lambda_i I)y = (B - \lambda_i I)Px$, temos $P(A - \lambda_i I) = (B - \lambda_i I)P \Rightarrow PA = BP \Rightarrow A = P^{-1}BP \Rightarrow A$ e B são semelhantes. ■

Vejamos alguns exemplos:

Exemplo 47 *Seja $\mathbb{K}$ um corpo qualquer, $A \in M_2(\mathbb{K})$ e $p(t) = (t - \lambda)^2$ o polinômio característico de A. Se para o único autovalor de $p(t)$, λ, tivermos dois autovetores l.i., então teremos uma base de autovetores para $\mathbb{K}^2$, e portanto A será diagonalizável. Suponha agora que para o autovalor λ tenhamos apenas um autovetor $v_1 \in \mathbb{K}^2$. Então $dim(\ker(A - \lambda I)) = 1$ e como W_1 tem dimensão 2, segue que*

$$\mathbb{K}^2 = W_1 = \ker(A - \lambda I)^2.$$

Seja $\overline{v_2} \in \ker(A - \lambda I)^2/\ker(A - \lambda I)$. Logo $(A - \lambda I)v_2 = \alpha v_1$, para algum $\alpha \in \mathbb{K}$. Desta última equação, obtemos $Av_2 = \lambda v_2 + \alpha v_1$. Portanto a base de Jordan procurada é $B = \{\alpha v_1, v_2\}$ e note que

$$Av_1 = \lambda v_1 \Rightarrow A(\alpha v_1) = \lambda(\alpha v_1) + 0 \cdot v_2,$$

$$Av_2 = 1 \cdot (\alpha v_1) + \lambda v_2.$$

Logo, a forma de Jordan de A é

$$J_A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Exemplo 48 *Ache a forma canônica de Jordan da matriz*

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ -3 & 5 & 2 \end{pmatrix}.$$

O polinômio característico de A é dado por $p(t) = (t - 1)(t - 2)^2$. Defina então $p_1(t) = t - 1$ e $p_2(t) = t - 2$. Note agora que $\ker[p_1(A)] = \{(-x, x, -8x); x \in \mathbb{R}\}$ e como $dim(W_1) = 1$, temos então $W_1 = \ker[p_1(A)]$. Daí conseguimos nosso primeiro vetor da

base de Jordan,

$$v_1 = (1, -1, 8) \in W_1.$$

Sabemos que $dim(W_2) = 2$ e que

$$\ker[p_2(A)] = \{(0, 0, y); y \in \mathbb{R}\} \text{ e}$$

$$\ker[p_2(A)]^2 = \{(0, w, z); w, z \in \mathbb{R}\}.$$

Portanto $W_2 = \ker[p_2(A)]^2$. Agora note que $v_3 = (0, 1, 0) \in \ker[p_2(A)]^2 / \ker[p_2(A)]$. Logo, $(A - 2I)v_3 = (0, 0, 5) = v_2$. Segue que o conjunto $B = \{v_1, v_2, v_3\}$ é a nossa base de Jordan para a matriz A. Desde que

$$\begin{cases} Av_1 &= v_1 \\ Av_2 &= 2v_2 \\ Av_3 &= v_2 + 2v_3 \end{cases}$$

segue que

$$J_A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$