UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA
UESB

Bruno Reis Ramos

G-GRADUAÇÕES PARA ÁLGEBRA $M_3(\mathbb{K})$

Vitória da Conquista - Bahia
Maio de 2021

Bruno Reis Ramos

G-graduações para a álgebra $M_3(\mathbb{K})$

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
2021

Folha de aprovação

Bruno Reis Ramos

G-graduações para a álgebra $M_3(K)$

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:

BANCA EXAMINADORA

Prof. Dr. Júlio César dos Reis - UESB
Orientador

Prof. Dr. Fernanda Gonçalves de Paula
UESC

Prof. Dr. Flaulles Boone Bergamaschi
UESB

Vitória da Conquista-BA
2021

Agradeço primeiramente à Deus por tudo. Sem ele, não teria chegado até aqui. “Pois dele, por ele e para ele são todas as coisas”.

Agradeço aos meus pais, Sueli dos Santos Reis e Denis Silvera Ramos, que são verdadeiros guerreiros e fizeram o possível me incentivando sempre em meus estudos. Também, aos meus demais familiares que sempre estiveram comigo durante essa jornada acadêmica me ajudando, cada um à sua forma. Em especial, ao meu tio Márcio, que como professor de matemática me influenciou bastante para que eu pudesse seguir nessa área, muito obrigado pelas nossas conversas.

Agradeço ao professor Júlio César dos Reis por tudo, creio que apresentar essa gratidão em apenas um parágrafo não é possível. Contudo, resumidamente, agradeço à ele por ter me apresentado esse mundo lindo da álgebra abstrata, pela sua paciência e seu carisma. A sua forma de falar sobre matemática é muito contagiante, dá para perceber seu amor e alegria em falar sobre a rainha das ciências. Muito obrigado por ter sido como um pai durante a minha caminhada acadêmica, pelas nossas conversas e por me motivar com todo o seu entusiasmo.

Agradeço aos meus colegas da turma 2017.1, bem como meus veteranos e calouros. Em especial, à Gislaine pelas nossas discussões em álgebra, à Debóra por seu entusiasmo em nossas conversas e à Marcos Paulo pelas suas discussões e observações sempre muito inteligentes. Por fim, à Kleber e Diógenes que não foram apenas amigos, mas quase irmãos durante esse período, jamais os esquecerei.

Agradeço à UESB por ter me proporcionado tantos bons momentos, ao corpo docente do curso de matemática, em especial, ao professor Altemar por ter me apresentado a belíssima teoria dos números que aumentou ainda mais minha paixão pela matemática, aos ensinamentos de cálculo diferencial e integral do professor Sérgio e à professora Tânia pelos seus incentivos.

"Pois dele, por ele e para ele são todas as coisas. (...)"
(Romanos 11:36)

Resumo

G-graduações são decomposições de espaços vetoriais como somas diretas da forma: $A = \oplus_{g \in G} A_g$, onde A é uma álgebra e G é um grupo. Descreveremos nesse trabalho todas as G-graduações para a álgebra das matrizes de ordem 3, $M_3(\mathbb{K})$, onde $\mathbb{K}$ é um corpo qualquer. Mostraremos que todas as G-graduações possíveis nessa álgebra se resumem à 3 graduações específicas: Boas graduações, $\mathbb{Z}_3$-graduações e $\mathbb{Z}_3 \times \mathbb{Z}_3$-graduações.

As boas graduações são caracterizadas pela existência de todas as matrizes elementares nas componenetes homogêneas da graduação, de fato, é suficiente que apenas uma matriz elementar atue como elemento homogêneo, resultado demonstrado por Bathurin. Em $M_3(\mathbb{K})$ é suficiente para uma G-graduação receber o adjetivo de boa graduação a existência de um elemento de ordem 2 ou de ordem 4 contidos no suporte. Portanto, as demais graduações ocorrem apenas quando o suporte consiste de elementos de ordem 3.

Um grande resultado que será mostrado ao longo do trabalho classifica essas novas graduações a partir do seu suporte, veremos que o suporte é um subgrupo abeliano de G cujos elementos tem ordem 3, nesse caso, as únicas possibilidades são $\mathbb{Z}_3$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Por meio da teoria de Galois construíremos uma $\mathbb{Z}_3$-graduação denotada por $A(a)$ e, por fim, mostraremos que todas graduações nesse suporte são isomorfas à alguma dessa classe.

Para o caso $\mathbb{Z}_3 \times \mathbb{Z}_3$, construiremos uma graduação a partir de matrizes $X, Y \in M_3(\mathbb{K})$; $X^3, Y^3 \in \mathbb{K}I_3$ e $YX = \xi XY$. E, assim como em suporte isomorfo à $\mathbb{Z}_3$, mostraremos sua unicidade, nesse suporte, a menos de isomorfismos.

Conteúdo

Introdução

Um dos problemas clássicos de matemática, numa perspectiva combinatória, é de contagem e, eventualmente, de classificação de certos objetos inseridos em alguma área específica. Por exemplo, números naturais podem ser decompostos como soma de dois outros números, para elucidar, tomemos o número 4, que pode ser escrito como 4=1+3 e 4=2+2, ou seja, existem duas formas de decompor o 4 como soma de outros naturais, a dizer: (1,3) e (2,2), a menos de comutatividade.

Agora tome A uma álgebra, que é uma estrutura que se comporta, à grosso modo, como um anel e um espaço vetorial. Vamos formular um problema parecido com o apresentado no parágrafo anterior, dada uma álgebra A: de quantas formas a podemos decompor como soma direta de seus subespaços vetorias? E mais ainda, quais são essas formas. Desse modo, nosso problema é muito geral, pois o conjunto dos números reais, complexos, o conjunto dos $\mathbb{Z}_p$; (p primo) e o conjunto das matrizes, munidos de certas operações, são álgebras. É nesse último exemplo de álgebra que o nosso trabalho se concentra, buscando determinar todas essas decomposições possíveis, no que se conhece como o problema de Zelmanov.

Como tal problema se encontra ainda em aberto, iremos apresentar a solução para o caso de $M_3(\mathbb{K})$. Inspirados num artigo de 2007 intitulado: "Group Gradings on $M_3(\mathbb{K})$", apresentaremos a solução do problema de Zelmanov, de modo a explorar esse trabalho e tratá-lo numa abordagem mais elementar, a fim de que um estudante de graduação com os pré-requisitos necessários possa compreender a prova completa de um trabalho de pesquisa recente em matemática.

Para tal, faremos a divisão desse trabalho em quatro capítulos. No capítulo 1, iremos introduzir as definições e resultados necessários de álgebra abstrata e álgebra linear elementares, tais como grupos, anéis e álgebras. Veremos que essas decomposições específicas são chamadas de G-graduações e são explicitadas na forma: $A = \oplus_{g \in G} A_g$, em que os subespaços vetorias são indexados por elementos de um grupo. No capítulo seguinte, apresentaremos alguns resultados, que embora elementares, serão de grande relevância, pois "filtram"as graduações possíveis.

No capítulo 3, enunciaremos e demonstraremos um resultado muito importante que classificará todas as graduações quando o conjunto dos elementos g associados à um subespaço

A_g, não nulo (chamado de suporte da graduação), for um subgrupo de G isomorfo ao grupo $\mathbb{Z}_3$, a menos de isomorfismos. Não apenas os descreveremos, como também apresentaremos sua representação matricial concreta.

No capítulo 4, mostraremos a última classe de G-graduações em $M_3(\mathbb{K})$, que ocorre quando o suporte é um subgrupo de G isomorfo à $\mathbb{Z}_3 \times Z_3$. Para finalizar, faremos uma breve discussão sobre resultados futuros.

Capítulo 1

Estruturas algébricas

Nesse capítulo, iremos trabalhar com as nossas ferramentas bases para o desenvolvimento de toda teoria ao longo do trabalho: estruturas algébricas. Além de apresentarmos a definição das estrutura que nos serão úteis ao longo do trabalho, bem como alguns exemplos, falaremos um pouco sobre teoria de Galois e, finalmente, sobre a definição e propriedades das estruturas adicionais que chamamos de G-graduações. A abordagem que escolhemos se concentra em apresentar definições básicas e algumas propriedades necessárias para um leitor que não tenha cursado alguma disciplina de álgebra, portanto, ao leitor mais habituado com tais termos, recomendamos pular para a última seção deste capítulo em diante.

1.1 Estruturas álgebricas

1.1.1 Grupos

Grupos tem uma das estruturas dentre as mais "simples" entre todas as que iremos citar aqui, pois exige menos propriedades e operações em relação às demais. O estudo de grupos tem uma vasta aplicação em várias áreas da matemática, que vão desde a ferramenta relevante no estudo de soluções de equações algébricas, bem como tem suas aplicações em simetrias de figuras geométricas (este chamado grupo das simetrias de uma figura, nas quais a simetrias preservam a "estrutura da figura") e, além disso, pode ser aplicada em teorias combinatórias como veremos no exemplo 1.1.4 a seguir.

Definição 1.1.1 ***Grupos:*** *Seja G um conjunto não vazio e $\times : G \times G \to G$ uma função, que denominaremos eventualmente de adição ou de multiplicação. Suponha que, para quaisquer $a, b, c \in G$, vale :*

$$1. a \times (b \times c) = (a \times b) \times c$$

$$2.\exists e \in G; a \times e = e \times a = a$$

$$3.\exists y \in G; a \times y = y \times a = e$$

Ou seja, G munido da operação $\times$ tem a propriedade associativa, existências de elementos neutro e simétricos (a esquerda e à direita). Então G será dito um grupo.

Definição 1.1.2 ***ordem:*** *Seja G um grupo e $g \in G$, chamamos de ordem de g o número $n \in \mathbb{N}$, tal que $g^n = e$, onde e é o elemento neutro de G.*

Definição 1.1.3 *Seja $S \subseteq G$ um conjunto que munido da mesma operação que dota G de um grupo que é também um grupo, diremos que S é um subgrupo de G.*

No caso em que G munido de $\times$ tem ainda a propriedade comutativa, dizemos que G é um grupo abeliano em relação à $\times$. Além disso, quando estivermos trabalhando com operações entre elementos de um grupo denotaremos ab ao invés de $a \times b$

Exemplo 1.1.4 ***Grupos das permutações:*** *Seja $X = \{x_1, x_2, ..., x_n\}$, o conjunto de todas as funções bijetoras: $f : X \to X$ forma um grupo munido da operação de composição de funções. Sem muita surpresa, o nome dado à esse grupo é o grupo das permutacões no conjunto X. Denotaremos esse conjunto por S_n.*

O grupo das permutacões terá um importante papel em alguns resultados em teoria de Galois, no que se refere, em particular, ao chamado grupo de Galois.

Exemplo 1.1.5 ***Classes residuais em módulo 3:*** *Tome $\mathbb{Z}$ o conhecido conjunto dos números inteiros, analisando todos os possíveis restos da divisão euclidiana entre os elementos de $\mathbb{Z}$ por 3 podemos construir um conjunto $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, onde $\overline{0}, \overline{1}$ e $\overline{2}$ denotam os restos (é como se estivessemos, a grosso modo, reduzindo $\mathbb{Z}$ à um conjunto com 3 elementos). Sobre a operação usual de produto ou soma dos elementos $\overline{0}, \overline{1}, \overline{2}$, $\mathbb{Z}_3$ se torna um grupo.*

Exemplo 1.1.6 ***O grupo diedral*** *Seja P_n um polígono regular. Chamamos de D_n o conjunto de todas as transformações geometricas que preservam essa estrutura de polígono regular. Munido da operação de composição de tranformações geométricas, D_n se torna um grupo.*

Dados esses exemplos, iremos apresentar a definição de ordem de um grupo.

Definição 1.1.7 *Seja G um grupo, dizemos que G é finito se $G = \{x_1, ..., x_n\}; x_i \in G$. Chamamos de ordem de G e denotamos por $|G|$ a quantidade de elementos de G, ou seja, $|G| = n$.*

1.1.2 Corpos

O conjunto dos números reais possui diversas propriedades que nos dão muitos resultados interessantes acerca de seus elementos. As propriedades de ordenação e completude de $\mathbb{R}$, por exemplo, nos dizem que toda sequência de Cauchy na reta é convergente. Além disso, as propriedades das operações de multiplicação e adição (usuais) nesse conjunto nos fornece algumas informações sobre o comportamento das soluções de um sistema linear a partir da matriz dos coeficientes desse sistema. Estendendo as propriedades operatórias obtidas com as operações de $\mathbb{R}$ para um conjunto qualquer, chegamos na definição de corpo, que é essencialmente um conjunto que se comporta como grupo abeliano tanto na adição como na multiplicação.

Como nem tudo é um mar de rosas, o conjunto dos números reais não tem todas as propriedades que gostaríamos que tivesse, um exemplo disso reside no fato de que nem todo polinômio de coeficientes reais tem todas as suas raízes em $\mathbb{R}$, como no caso do polinômio: $p(x) = x^2 + 1$. Em casos como esse, apelamos para a construção de um novo corpo que contenha as raízes de polinômios desse tipo, conhecido como o corpo dos complexos ($\mathbb{C}$). Para encontrar corpos que contenham as raízes de um polinômio tal como $p(x)$ sem necessitar de usar $\mathbb{C}$, apelamos para a construção de um corpo especial, chamado de Corpo de decomposição.

Definição 1.1.8 ***Característica*** *Seja $\mathbb{K}$ um corpo, o menor número $n \in \mathbb{N}$ tal que $n \times a = 0$, para todo $a \in \mathbb{K}$ é chamado de característica de $\mathbb{K}$, denotado por $a = char(\mathbb{K})$.*

Exemplo 1.1.9 ***Corpos de Decomposição:*** *Dado um polinômio f de coeficientes reais, chamamos de corpo de decomposição de f, denotado por $Gal(f, \mathbb{R})$, o menor corpo em $\mathbb{C}$ que contenha todas as raízes de f.*

De fato, tal corpo existe, basta tomar a interseção (interseção qualquer de corpos é corpo) de todos os corpos em $\mathbb{C}$ que contenham todas as raízes de f, Na pior das hipóteses, $Gal(f, \mathbb{R}) = \mathbb{C}$.

Naturalmente, a mesma idéia pode ser estendida para um corpo qualquer $\mathbb{K}$ contido em um outro corpo $\mathbb{L}$ que contenha todas as raízes de qualquer polinômio com coeficientes em $\mathbb{K}$. Essas idéias serão retomadas posteriormente na nossa seção sobre teoria de Galois.

1.1.3 Anéis

Diferente dos grupos, um anel A é uma estrutura munida de duas operações, chamadas de adição e de multiplicação, $+ : A \times A \to A, \times : A \times A \to A$, respectivamente. Além disso, A é um grupo abeliano em relação à adição e a operação de multiplicação deve ser associativa em A e distributiva sobre a adição , ou seja, $a \times (b + c) = a \times b + a \times c$. No caso em que a segunda operação obedece à algumas propriedades adicionais, o anel recebe, naturalmente, seus adjetivos, por exemplo, se cada elemento de A possui inverso multiplicativo, então A é dito anel de divisão.

Exemplo 1.1.10 ***Anel dos Polinômios:*** *Seja $\mathbb{K}$ um corpo , o conjunto dos polinômios ($\mathbb{K}[x]$) da forma $p(x) = a_0 + a_1x + ... + a_nx^n$, onde $a_i \in \mathbb{K}$ e $n \in \mathbb{N}$ com as operações usuais de multiplicação e adição determinam um anel, chamado anel dos polinômios em $\mathbb{K}$. Desde que $a_n \neq 0$, dizemos que o grau de p é igual à n.*

Observação 1.1.11 *Também será comum usarmos a notação $\mathbb{K}[B]$ para denotar o conjunto dos polinômios avaliados na constante B.*

Os polinômios também serão de enorme relevância em nosso trabalho. Como trabalharemos com matrizes, nomes como: "polinômio minimal"ou "polinômio caracteristico"serão bem comuns. Apesar de suas propriedades interessantes, o conjunto dos polinômios não formam um anel de divisão, isso não quer dizer que não podemos efetuar uma espécie de divisão e, assim como em $\mathbb{Z}$, é possível determinar uma divisão euclidiana, ou seja, dados $p, q \in \mathbb{K}[x]$, existem $g, r \in \mathbb{K}[x]$ tais que $p = qg + r$, com o grau de r menor que o grau de q. Quando $r \neq 0, \forall q \in \mathbb{K}[x]$, dizemos também que p é irredútivel sobre $\mathbb{K}$.

1.1.4 Espaços vetoriais

Uma das ferramentas fundamentais no estudo de geometria analítica são os vetores. São a partir deles que somos capazes de trabalhar com equações de reta e plano mais convenientes. Além disso, eles possuem algumas propriedades que tem significados geométricos muito interessantes, por exemplo, em cálculo no $\mathbb{R}^n$ o chamado vetor gradiente da curva em um ponto é ortogonal à curva. Aqui, o uso desses conceitos tem interesse mais algébrico, no qual faremos uso das propriedade operatórias do conjunto de vetores , que munido dessas operações recebe o nome de espaço vetorial. Em outras palavras, iremos generalizar a idéia de vetores da geometria análitica e do cálculo para casos mais gerais.

Definição 1.1.12 *Seja $\mathbb{K}$ um corpo e E um conjunto. Considere ainda as seguintes operações: $+ : E \times E \to E, * : \mathbb{K} \times E \to E$. Se:*
I. *$(E, +)$ é um grupo abeliano.*
II. *São válidas as seguintes propriedades:*
II'. $1 * v = 1; 1 \in \mathbb{K}, v \in E$
II$''.\lambda * (u + v) = \lambda * u + \lambda * v, (\mu + \lambda) * u = \mu * u + \lambda * u; \mu, \lambda \in \mathbb{K}, u \in E$
II$'''.\lambda * (\mu * v) = \mu * (\lambda * v) = (\lambda * \mu) * v$ ***Com essas operações,*** E ***se torna um espaço vetorial sobre*** $\mathbb{K}$***, e os elementos*** $v \in E$ ***são chamados de vetores.***

Definição 1.1.13 ***Vetores L.I e L.D:*** *Seja E um espaço vetorial sobre um corpo $\mathbb{K}$. Um conjunto de vetores $\{v_1, v_2, v_3, ..., v_n\} \subset E$ são ditos L.I se qualquer equação: $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0; \alpha_i \in \mathbb{K}$ implica em cada $\alpha_i = 0$.Em caso contrário, dizemos que esses vetores são L.D.*

Definição 1.1.14 ***Geradores:*** *Seja E um espaço vetorial sobre um corpo $\mathbb{K}$. Sejam $\{v_1, v_3, ..., v_n\}$ vetores, o conjunto: $< v_1, v_3, ..., v_n >= \{\alpha_1 v_1 + \alpha_2 v_2 +, ..., \alpha_n v_n; \alpha_i \in \mathbb{K}\}$ é dito conjunto gerado por esses vetores. Vale ressaltar que esse conjunto tem sempre estrutura de espaço vetorial. Caso o espaço vetorial seja gerado por esse conjunto, dizemos que o primeiro é gerado pelo segundo.*

Observação 1.1.15 *Vale ressaltar que toda a base de um espaço vetorial sempre tem a mesma quantidade de elementos.*

Definição 1.1.16 ***Base:*** *Seja V um espaço vetorial, dizemos que $B = \{v_1, v_3, ..., v_n\}$ é uma base para V se:*
I. *Os elementos de B são L.I.*
II. *$V =< B >$.*

Definição 1.1.17 ***Dimensão:*** *Seja V um espaço vetorial (de dimensão finita) sobre um corpo $\mathbb{K}$ e $B = \{v_1, v_3, ..., v_n\}$ uma base para V. Chamamos de dimensão de V sobre $\mathbb{K}$ o número de elementos de B, e denotamos por: $dim(V)_{\mathbb{K}} = n$*

Observação 1.1.18 *Até o fim desse capítulo, mencionaremos alguns resultados relevantes para o nosso trabalho, dos quais optaremos por omitir as provas a fim de não deixar esse trabalho enfadonho. Para o leitor interessado, recomendamos o livro "Algebra: A graduate course"de Serge Lang.*

Definição 1.1.19 ***Subespaços vetoriais:*** *Seja E um espaço vetorial sobre um corpo $\mathbb{K}$, se $S \subseteq E$ é tal que S sobre $\mathbb{K}$ tem também estrutura de espaço vetorial, então dizemos que S é um subespaço vetorial de E.*

Definição 1.1.20 ***Soma direta:*** *Sejam $\mathcal{P} = \{S_\lambda\}$ uma família de subespaços vetoriais, cuja interseção dois à dois seja apenas o elemento neutro, de um espaço vetorial E, onde λ são elementos de uma família de índices. Se $E = \sum_\lambda S_\lambda$, dizemos que E é decomposto como soma direta desses espaços S_λ. Será mais comum usarmos a notação: $E = \oplus_\lambda A_\lambda$*

1.1.5 Álgebra

Essa estrutura exige que o conjunto seja munido de três operações e , como podemos perceber a seguir, se comporta , a grosso modo, como um anel e um espaço vetorial. Logo, não há muito o que dizer sobre suas propriedades, visto que as que precisaremos decorrem imediatamente das propriedades de anéis e espaços vetoriais. Por outro lado, ela terá uma importante atuação nesse trabalho visto que nosso objeto de estudo aqui (as matrizes) serão abordados sob a perspectiva dessa estrutura.

Definição 1.1.21 *Um espaço vetorial* $(R, +, *)_{\mathbb{K}}$ *(onde* $\mathbb{K}$ *é um corpo) é chamado de uma álgebra (ou de uma* $\mathbb{K}$*-álgebra) se* R *é munido de uma operação binária:* $\times : R \times R \to R$*, chamada de multiplicação, tal que para todo* $a,\ b,\ c \in R$ *e* $\alpha \in \mathbb{K}$ *as seguintes condições são satisfeitas:*
I. $(a + b) \times c = a \times c + b \times c$;
II. $a \times (b + c) = a \times b + a \times c$;
III. $\alpha * (a \times b) = (\alpha * a) \times b = a \times (\alpha * b)$.

Exemplo 1.1.22 ***A álgebra das matrizes:*** *Seja* $\mathbb{K}$ *um corpo e* $n \in \mathbb{N}$*.O espaço das matrizes de ordem* n *de entradas em* $\mathbb{K}$ *define uma álgebra sobre* $\mathbb{K}$ *com as operações usuais de multiplicação, adição e produto por escalar de matrizes. Denotaremos essa álgebra por* $M_n(\mathbb{K})$*.*

Vamos mencionar sucintamente duas definições importantes que decorrem desse objeto.

Definição 1.1.23 ***O polinômio característico:*** *O polinômio característico de uma matriz* $M \in M_n(\mathbb{K})$ *é o polinômio da forma:* $C(\lambda) = det(\lambda I_n - M)$*, onde* I_n *é a matriz identidade.*

Definição 1.1.24 ***O polinômio minimal:*** *Seja* $M \in M_n(\mathbb{K})$*, chamamos de polinômio minimal de* M*, o polinômio mônico* P *de menor grau tal que* $\mu(\lambda) = 0$

Dadas essas duas definições, enunciaremos a seguir o belíssimo teorema de Caley-Hamilton, que faz uma relação entre as duas definições dadas acima.

Teorema 1.1.25 *Seja* $M \in M_n(\mathbb{K})$*,* $C(\lambda)$ *e* $\mu(\lambda)$ *seus polinômios característico e minimal, respectivamente. Então* $\mu(\lambda)$ *divide* $C(\lambda)$ *.*

1.2 Morfismos

Dedicaremos essa seção para discutir o conceito de morfismos e suas propriedades, que é um tema clássico de qualquer curso de álgebra. Em álgebra linear, eles recebem o nome de transformações lineares e, em teoria de grupo e teoria de anéis, é conhecido como homomorfismo. Trazer uma definição geral para essas funções nos será muito útil, uma vez que estamos lidando com mais de um tipo de estrutura.Sem mais delongas, vamos apresentar esses conceitos cruciais para o nosso trabalho.

Definição 1.2.1 ***Morfismos:*** *Sejam A e B duas estruturas álgebricas de mesma estrutura. Chamamos de um morfismo μ de A em B uma função que preserva a estrutura dos mesmos, ou seja, dadas duas operações correspondentes τ e ω em A e B, respectivamente, deve-se valer que $\mu(a\tau b) = \mu(a)\omega\mu(b), \forall a, b \in A$.*

Faremos, eventualmente, o uso do seguinte resultado:

Teorema 1.2.2 *O conjunto dos morfismos $\mu : A \to B$, onde A e B são estruturas de mesma definiçao, tem a mesma estrura álgebrica que A e B.*

Definição 1.2.3 ***Isomorfismos:*** *Sejam A e B estruturas de mesmo comportamento, se μ é um morfismo e, como função de A em B, é bijetora, então dizemos que μ é um isomorfismo.*

Definição 1.2.4 ***Automorfismos:*** *Seja A uma estrutura álgebrica munida de certas operações, o conjunto de todos os ismorfismos de A em A é dito o conjunto dos automorfismos de A*

Observação 1.2.5 *Dada A uma estrutura álgebrica, o conjunto (que também é uma estrutura álgebrica de mesma natureza) de todos os automorfismos de A é chamado de conjunto dos automorfismos em A.*

1.3 Um pouco de teoria de Galois

O francês Évariste Galois, talvez seja a figura mais polêmica na história da matemática. Prodígio matemático de morte precoce, desenvolveu alguns dos manuscritos que iriam mudar o percurso da álgebra abstrata, fazendo com que florescesse uma etapa da matemática chamada de "libertação da álgebra". Dentre seu trabalho matemático, se destaca a teoria de grupos que ele criou para demonstrar quais eram e quais não eram as equações álgebricas solúveis por meio de radicais.

Alguns conceitos importantes de álgebra recebem seu nome, como por exemplo grupo de Galois, extensões de Galois, entre outros. Alguns desses objetos serão muito usados em nosso trabalho, principalmente no capítulo 3. Portanto, vamos à essas definições. Iremos fazer uso de alguns dos resultados dessa teoria sem demonstração, das quais o leitos interessado pode encontrá-las em [3].

Definição 1.3.1 ***Extensões:*** *Seja $\mathbb{K}$ um corpo, dizemos que um corpo $\mathbb{L}$ é uma extensão de $\mathbb{K}$ se, e somente se, $\mathbb{K} \subset \mathbb{L}$*

Veja que se considerarmos $\mathbb{K}$ um corpo de escalares, $\mathbb{L}$ se torna um espaço vetorial sobre o primeiro. Como espaço vetorial, $\mathbb{L}$ tem direito à uma dimensão sobre $\mathbb{K}$.

Definição 1.3.2 *(* ***Grau de uma extensão:*** *) Seja $\mathbb{L}$ uma extensão de um corpo $\mathbb{K}$, chamamos de grau da extensão $\mathbb{L}$ sobre $\mathbb{K}$, o número $[\mathbb{L} : \mathbb{K}] = dim_{\mathbb{K}}(\mathbb{L})$.*

Observação 1.3.3 *Quando essa dimensão é finita, dizemos ainda que $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$*

Nesse ponto, iremos retomar um exemplo apresentado na seção de anéis, o qual chamamos de corpo de decomposições. Vamos estender esse conceito para corpos quaisquer e o usaremos para apresentar e definir extensões de Galois.

Definição 1.3.4 *(**Corpos de decomposição:**) Dado um polinômio f de coeficientes em um corpo $\mathbb{K}$, chamamos de corpo de decomposição de f , denotado por $Gal(f, \mathbb{K})$, o menor corpo em $\mathbb{L}$ (onde $\mathbb{L}$ é uma extensão que contém as raízes de qualquer polinômio com coeficientes em $\mathbb{K}$) tal que contenha todas as raízes de f.*

Exemplo 1.3.5 *Seja $\mathbb{Q}$ o corpo dos racionais e $p(x) = x^2 - 2 \in \mathbb{Q}[x]$. O corpo $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ é o corpo de decomposição de $p(x)$, uma vez que, tomando-se $b = 0$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ e, das propriedades de fechamento de adição e multiplicação de corpos, quaisquer que sejam $\mathbb{L}$ extensões de $\mathbb{Q}$ que contém $\sqrt{2}$ deve valer que $a + b\sqrt{2} \in \mathbb{L}, \forall a, b \in \mathbb{Q}$, ou seja, $\mathbb{Q}(\sqrt{2}) \subset \mathbb{L}$. Por definição, esse é o corpo de decomposição de $p(x)$.*

Observação 1.3.6 *Esse processo é conhecido em álgebra abstrata como a "adjunção"de raízes, que consiste em construir uma extensão envolvendo operações entre multiplicação das raízes do polinômio e elementos do corpo base com a soma de todos esses fatores.*

Definição 1.3.7 *Dizemos que uma extensão finita* $\mathbb{L}$ *de um corpo* $\mathbb{K}$ *é uma extensão de Galois de* $\mathbb{K}$ *se* $\exists f(x) \in \mathbb{K}[x]$ *tal que* $\mathbb{L} = Gal(f, \mathbb{K})$

Observação 1.3.8 *Apenas vamos observar que* $\mathbb{K}[x]$ *é o conjunto de polinômios com coeficientes em* $\mathbb{K}$

Observação 1.3.9 *O grau dessa extensão finita será também o grau da extensão de Galois. Por exemplo, se a extensão tiver grau 3, a chamaremos de extenão cúbica de Galois.*

Agora daremos duas definições de extensões específicas que serão importantes para o grande teorema dessa seção.

Definição 1.3.10 ***Extensões normais:*** *Dizemos que uma extensão* $\mathbb{L}$ *de* $\mathbb{K}$ *é normal se* $\forall g(x) \in \mathbb{K}[x]$*, irredutível sobre* $\mathbb{K}$ *que possui uma raiz* $\alpha \in \mathbb{L}$*, possui todas suas raízes em* $\mathbb{L}$ *e, além disso, todo elemento de* $\mathbb{L}$ *é raiz de algum polinômio de* $\mathbb{K}[x]$*.*

Exemplo 1.3.11 $\mathbb{C}$ *é uma extensão normal sobre* $\mathbb{R}$*. Isso decorre imediatamente do teorema fundamental da álgebra, que diz que todo polinômio com coeficientes em* $\mathbb{C}$ *possui todas as suas raízes em* $\mathbb{C}$*.*

Definição 1.3.12 ***Elementos separáveis:*** *Seja* $\mathbb{K}$ *um corpo,* $\mathbb{L}$ *uma extensão de* $\mathbb{K}$ *e* $\alpha \in \mathbb{L}$*, dizemos que* α *é separável sobre* $\mathbb{K}$ *se* $\exists f(x) \in \mathbb{K}[x]$ *tal que* $f(\alpha) = 0$ *e* $f(x)$ *não possui raízes múltiplas.*

Exemplo 1.3.13 *2 é separável sobre* $\mathbb{Q}$*, uma vez que é raiz do polinômio* $f(x) = x - 2$*.*

Definição 1.3.14 ***Extensões separáveis*** *Uma extensão* $\mathbb{L}$ *de um corpo* $\mathbb{K}$ *é dita separável, se todo elemento de* $\mathbb{L}$ *é separável sobre* $\mathbb{K}$*.*

Exemplo 1.3.15 $\mathbb{C}$ *é uma extensão separável sobre* $\mathbb{R}$*. Isso decorre de uma propriedade que diz que todo corpo de característica zero tem extensões finitas separáveis. Damos à esses corpos bases o adjetivo de corpos perfeitos.*

Agora vamos enunciar um resultado formidável em teoria de Galois sem a demonstração, resultado este que será ferramenta chave para resultados no trabalho:

Teorema 1.3.16 *Seja $\mathbb{L}$ uma extensão de um corpo $\mathbb{K}$, $\mathbb{L}$ é uma extensão de Galois de $\mathbb{K}$ se, e somente se $\mathbb{L}$ é normal e separável.*

Corolário 1.3.17 *$\mathbb{C}$ é uma extensão de Galois de $\mathbb{R}$. Mais geralmente, toda extensão finita e normal de um corpo de característica zero é uma extensão de Galois.*

A partir desse ponto, passamos a definir o grupo de Galois, que fará a ligação dessas idéias com a teoria dos grupos já mencionada.

Definição 1.3.18 *(**O grupo de Galois:**) Seja $\mathbb{L}$ uma extensão de um corpo $\mathbb{K}$, chamamos do grupo de Galois da extensão $\mathbb{L}_{\mathbb{K}}$ o conjunto:*

$$Aut_{\mathbb{K}}(\mathbb{L}) = \{\sigma \in Aut(\mathbb{L}); \sigma(a) = a, \forall a \in \mathbb{K}\}$$

munido da operação de composição de funções.

Uma propriedade muito relevante que decorre imediatamente dessa definição se encontra enunciada a seguir:

Teorema 1.3.19 *Seja $f(x) \in \mathbb{K}[x]$, $\sigma \in Aut_{\mathbb{K}}(\mathbb{L})$ e $\alpha \in \mathbb{L}$ raiz de $f(x)$, então $\sigma(\alpha)$ é outra raiz de $f(x)$.*

Esse teorema caracteriza o grupo de Galois como um conjunto de permutadores das raízes de um polinômio de coeficientes em $\mathbb{K}$. Os próximos resultados concretizam esse fato de forma muito elegante.

Teorema 1.3.20 *A quantidade de elementos do grupo de Galois (que denotamos por $|Aut_{\mathbb{K}}(\mathbb{L})|$) é igual ao grau da extensão $\mathbb{L}$ sobre $\mathbb{K}$, ou seja, $|Aut_{\mathbb{K}}(\mathbb{L})| = [\mathbb{L} : \mathbb{K}]$.*

Teorema 1.3.21 *$Aut_{\mathbb{K}}(\mathbb{L})$ é um subgrupo de S_n, para algum $n \in \mathbb{N}$*

Como S_n é um grupo de permutações, vale o que mencionamos anteriormente.

O resultado que daremos maior ênfase dessa seção é o teorema 1.3.19, pois iremos aplicar esse resultado para fazermos "permutações de matrizes".

1.4 G-graduações

1.4.1 Do que estamos falando?

O que iremos falar no início dessa seção parece destoar um pouco com tudo o que foi trabalhado até aqui, visto que faremos comentários combinatórios entre objetos das estruturas já estudadas. Vamos considerar o anél dos inteiros $\mathbb{Z}$ e o grupo das transformações geométricas D_3, conhecido como o grupo diedral das transformações em um triângulo equilátero. Como um anel, $\mathbb{Z}$ deve ter duas operações definidas, que são a adição e a multiplicação usuais, e, como já citamos, D_3 tem como operação do grupo as transformações geométricas possíveis em um triângulo que preservam sua estrutura de triângulo equilátero, a menos da posição dos seus vértices. À essas operações chamamos de simetrias.

Agora que já vimos a estrutura dos conjuntos munidos das operações, podemos analisar dois problemas que podem sugir de modo natural:

I. Dado um número inteiro, de quantas e quais são as formas de reescrevê-lo como soma de outros dois números inteiros?. Por exemplo, o número 2 pode ser escrito como (a+2)-a, mas esses casos são elementares, é mais interessante analisar os casos em que essa soma é decomposta em $\mathbb{N}$, dessa forma: 2=1+1, apenas. Quando estendemos para o número 4, vemos que suas decomposições em naturais são 2, a dizer, 4=2+2 ou 4=1+3.

II. No caso dos grupos podemos formular um problema de mesma natureza. Por exemplo, o grupo D_3 pode ser escrito como $D_3 = \{R_0, R_{120}, R_{240}\}\{R_0, a\}$. Note que essa decomposição não é feita de qualquer maneira, pegamos dois subconjuntos que também tem estrutura de grupo, que chamamos de subgrupo. Falando em grupos finitos, uma pergunta natural a se fazer é, de quantas formas e quais são os subgrupos que o decompõe.

Agora, vamos pensar em álgebras. Como vimos, essas estruturas tem um comportamento de espaço vetorial sobre um corpo $\mathbb{K}$, e um conceito que apresentamos anteriormente foi o de soma direta de subespaços vetoriais de um espaço vetorial dado. Veja que no item **II** decompomos grupos como produtos de subgrupos, dessa forma, se torna interessante analisar para as álgebras com a operação de soma direta, pois cada componente da soma direta tem uma estrutura de subespaço vetorial. Então, dada uma álgebra A, de quantos modos podemos escrevê-la como:

$$A = \Sigma V; V \subset A$$

com V espaço vetorial. A pergunta se parece com as feitas anteriormente, porém temos um problema aqui: "E como fica a operação de multiplicação da álgebra?". Da forma como escrevemos é possível que, dados $v \in V$ e $u \in U$, podemos eventualmente ter que vu não pertença à nenhum dos subespaços que decompõe a álgebra em soma direta. Portanto, precisamos de uma forma de “amarrar”essas componentes.

Uma forma eficaz de reparar esse problema é indexar os espaços vetoriais e exigir um bom comportamento entre os indíces e o produto entre os elementos da álgebra vistos como espaços vetoriais. Estamos acostumados à olhar índices de conjuntos como números naturais, assim teríamos que essas decomposições seriam da forma:

$$A = \oplus_{n \in \mathbb{N}} A_n$$

A forma natural de se “amarrar”esses produtos seria exigir que se $u \in A_k$ e $v \in A_p$, então uvA_{kp}. Porém, isso limita a generalidade da nossa construção, dado que não poderíamos ter uma dessas decomposições em que a soma direta seja composta por uma família não enumerável de subespaços vetoriais. Em seu livro Real Analysis, o autor Halsey Royden apresenta uma generalização para o conjunto de índices associadas à uma família de outros conjuntos, nesse caso o conjunto de índices será formado por elementos de um conjunto escolhido.

Como queremos ter uma boa relação entre os índices de cada componente da soma direta, bem como uma boa relação entre o produto de elementos da álgebra, podemos pensar em

$$A = \oplus_{g \in G} A_g,$$

no qual G é um grupo. Assim, para o bom comportamento esperado, vamos exigir que, se $a \in A_g$ e $b \in A_h$, então $ab \in A_{gh}$. Com isso, nossos elementos estão “amarrados”pelos índices e podemos “quebrar”a álgebra como soma direta de espaços vetoriais, assim como “quebramos”números naturais como soma de outros números naturais em **I.** . Veja ainda que a nossa escolha de índices foi bem estratégica, visto que grupos tem menos propriedades algébricas que as demais estruturas apresentadas e, além disso, existe um fechamento entre as operações envolvidas.

Essas discussões preliminares nos levam a seguinte definição:

Definição 1.4.1 *Seja $\mathbb{K}$ um corpo, A uma $\mathbb{K}$-álgebra e G um grupo. Uma G-graduação em A é uma decomposição $A{=}\oplus_{g \in G} A_g$ como soma direta de $\mathbb{K}$-subespaços vetoriais de A, tal que $A_g A_h \subseteq A_{gh}$, para quaisquer g e $h \in G$.*

Os passos naturais agora são: encontrar exemplos de G-graduações e tentar formular um problema geral análogo ao que vimos em **I** e **II**.

1.4.2 Exemplos e o Problema de Zelmanov

Inicialmente, vamos apresentar alguns exemplos de G-graduações em álgebras, . Para isso, é necessario ressaltarmos que tomaremos a nossa álgebra sempre como a álgebra de matrizes. Temos a seguir dois exemplos, ambos em $M_2(\mathbb{K})$ para visualisar como funciona na prática esse conceito.

Exemplo 1.4.2 *Seja $\mathbb{K}$ um corpo qualquer de característica diferente de 2. Seja $G = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ como grupo aditivo. Os seguintes subespaços formam uma graduação para $M_2(\mathbb{K})$:*

$$A_{\overline{0}} = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix} A_{\overline{1}} = \begin{pmatrix} 0 & \mathbb{K} \\ \mathbb{K} & 0 \end{pmatrix}$$

É fácil de ver que $A_{\overline{0}}$ e $A_{\overline{1}}$ são subespaços vetoriais que decompõe $M_2(\mathbb{K})$ em soma direta. Além disso, precisamos mostrar que, de fato, os elementos $\overline{0}$ e $\overline{1}$ "amarram"o produto de elementos da graduação, ou seja, devemos mostrar que $A_{\overline{0}}A_{\overline{0}} \subseteq A_{\overline{0+0}} = A_{\overline{0}}$, $A_{\overline{1}}A_{\overline{0}} \subseteq A_{\overline{1+0}} = A_{\overline{1}}$ e como $M_2(\mathbb{K})$ não é comutativa, devemos também analisar que $A_{\overline{0}}A_{\overline{1}} \subseteq A_{\overline{0+1}} = A_{\overline{1}}$. Então vamos analisar separadamente cada uma das condições:

I. $A_{\overline{0}}A_{\overline{0}} \subseteq A_{\overline{0}}$*:*

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

Dessa forma, temos como resultante uma matriz diagonal composta por elementos de $\mathbb{K}$, portanto, vale o fechamento acima.

II. $A_{\overline{1}}A_{\overline{0}} \subseteq A_{\overline{1}}$*:*

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

Temos que esse produto gera uma matriz diagonal secundária, ou seja, o produto entre elementos de $A_{\overline{1}}$ com elementos de $A_{\overline{0}}$ pertencem à $A_{\overline{1}}$, como já esperávamos.

Resta analisar o caso $A_{\overline{0}}A_{\overline{1}} \subseteq A_{\overline{1}}$. De fato:

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

Como podemos perceber, a única diferença entre esse caso e o seu antecessor são os produtos que aparecem na diagonal secundária. Isso não vai mudar o fato de que essa operação também é bem comporda em relação ao produto de elementos da álgebra e a adição de elementos em $\mathbb{Z}_2$*. Com isso, podemos, portanto, afirmar que* $A = A_{\bar{0}} \oplus A_{\bar{1}}$ *é uma* $\mathbb{Z}_2$*-graduação em* $M_2(\mathbb{K})$*.*

Dado esse exemplo que elucida os passos de verificação para que uma decomposição da álgebra em soma direta possa ser considerada uma G-graduação, podemos começar a definir alguns objetos básicos, como por exemplo, qual nome damos às “partes”que compõem a soma direta, ou ainda,qual o nome que damos aos elementos do grupo associados à essas partes.

Definição 1.4.3 *Dada* A *uma álgebra,* G *um grupo e uma* G*-graduação em* A *da forma* $A = \oplus_{g\in G} A_g$*, chamamos de* ***componente homogênea de grau*** g *o subespaço vetorial de índice* g*,* A_g*.*

Definição 1.4.4 *Dada* A *uma álgebra,* G *um grupo e uma* G*-graduação em* A *da forma:* $A = \oplus_{g\in G} A_g$*. Chamamos de* ***elemento homogêneo de grau*** g *qualquer elemento de* $A \cap A_g$*.*

Definição 1.4.5 *Dada* A *uma álgebra,* G *um grupo e uma* G*-graduação em* A *da forma:* $A = \oplus_{g\in G} A_g$*. Chamamos de* ***suporte de A*** *e denotamos por* $Supp(A)$ *o conjunto de todos os elementos de* G *associados à um subespaço vetorial não nulo, ou seja,* $Supp(A) = \{g \in G; A_g \neq 0\}$*.*

Definição 1.4.6 ***Homomorfismo*** G***-graduado*** *Sejam* A *e* B *duas álgebras* G*-graduadas. Se* $f : A \to B$ *é um homomorfismo de álgebras, tal que* $f(A)_g = B_g$*, diremos que* f *é um homomorfismo* G*-graduado*

Dito isso, podemos fazer uma analogia a decomposição de grupos em subgrupos simples e nos perguntarmos quais são todas as G-graduações em uma álgebra dada. No exemplo das matrizes de ordem 2, além da graduação apresentada existe uma outra graduação que pode ser assim definida:

$$A_1 = \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix} A_g = \begin{pmatrix} 0 & \mathbb{K} \\ 0 & 0 \end{pmatrix} A_{g^{-1}} = \begin{pmatrix} 0 & 0 \\ \mathbb{K} & 0 \end{pmatrix}$$

Em que G é um grupo múltiplicativo e $A_h = 0$ para $h \in G - \{1, g, g^{-1}\}$, onde g é um elemento de ordem maior do que 2. Então descrever todas as G-graduações já se mostra uma tarefa um pouco complexa para o caso da álgebra das matrizes de ordem 2. De modo geral, o problema de encontrar todas as G-graduações de uma álgebra dada depende muito da escolha da própria Álgebra. Se restringirmos a questão para a álgebra das matrizes, chegamos no conhecido como o problema de Zelmanov, que se encontra enunciado abaixo.

O problema de Zelmanov: "Dada a álgebra das matrizes de ordem n sobre um corpo qualquer $\mathbb{K}$ e G um grupo qualquer qualquer, determinar todas as G-graduações da álgebra $M_n(\mathbb{K})$ ".

1.4.3 Um Pouco do Contexto Histórico

Efim Isaakovich Zelmanov é um matemático russo naturalizado americano que trabalha especialmente nas áreas de álgebras não-associativas e conceitos combinatórios de álgebras. É muito conhecido por ter resolvido o problema restrito de Burnside. Suas pesquisas o levaram à ser um dos premiados da medalha fields em 1994.

Tal como foi enunciado, o problema de Zelmanov despertou um certo interesse nos matemáticos que trabalham com álgebras associativas. Ocupando uma certa parte de teóricos em álgebras e Anéis associativos no fim do século passado até os dias de hoje, esse trabalho árduo ainda continua em andamanento, visto que o problema ainda não foi resolvido de modo geral.

Para termos uma noção da complexidade do problema, vamos citar brevemente alguns trabalhos que foram feitos para, enfim, apresentar o nosso foco de pesquisa deste trabalho.

Um primeiro artigo que obteve resultados de graduações em álgebras matriciais foi Knus (1969). Em Green (1983) e Green e Marcos (1994), certas graduações foram construídas em álgebras matriciais a partir de funções-peso no gráfico completo em n pontos. Em um estudo sistemático de graduações em álgebras matriciais iniciado por Dascalescu (1999), uma classe especial de graduações, chamadas de boas graduações (também chamadas de graduações elementares em Bahturin (2001)) foram investigadas. Uma graduação é dita boa graduação se toda matriz unitária e_{ij} é um elemento homogêneo. Sob certas condições, qualquer graduação na álgebra de matrizes é isomorfa à uma boa graduação. Dascalescu (1999) e Sehgal and Zaicev (2001), mostram que isso acontece em algumas das seguintes situações:

I. G é cíclico e $\mathbb{K}$ é algebricamente fechado.

II. G é livre de torção.

III, $G = Z_p$ onde p é um número primo. $\mathbb{K}$ tem uma raiz p-enésima primitiva da unidade e p não divide n. As boas G-graduações em $M_n(\mathbb{K})$ foram classificadas por Caenepeel(2002) via órbitas da biação do grupo simétrico S_n à esquerda e G à direita no conjunto G_n. Usando teoria da "descent", graduações via grupos cíclicos foram descritas por Caenepeel (2002) em termos cohomológicos.

Para outras casos, podemos citar os seguintes resultados: se $\mathbb{K}$ for algebricamente fechado, todas as graduações por um grupo abeliano foram descritas em Bahturin (2001), onde ficou provado que tais graduações são isomorfas à um produto tensorial de uma boa graduação com outro tipo de graduação, chamado de graduação fina, definida pelo fato de que a dimensão de qualquer componente homogêneo é no máximo 1. Um resultado semelhante foi provado em Bahturin (2002) para graduações por grupos finitos arbitrários, desde que $\mathbb{K}$ seja algebricamente fechado e tenha característica zero.

Em Khazal (2003) foram descritas todas as G-graduações em $M_2(\mathbb{K})$, onde $\mathbb{K}$ é um corpo arbitrário e G um grupo qualquer.E, foi provado que quaisquer destas graduações ou são isomorfas a uma boa graduação ou se reduz a uma graduação por $\mathbb{Z}_2$ ou por $\mathbb{Z}_2 \times \mathbb{Z}_2$. Tais fatos também podem ser encontrados em Boboc (2002, 2003) e Boboc e Dascalescu (2001).

Infelizmente, de acordo com esse breve histórico, a única álgebra que tem todas as G-graduações classificadas para $\mathbb{K}$ e G genéricos é a álgebra $M_2(\mathbb{K})$, no trabalho realizado por Crina Boboc e Dascalescu em 2002. Em 2016, Pedro Souza Fagundes, em sua monografia intitulada: "G-graduações para $M_2(\mathbb{K})$", fez uma análise detalhada do artigo "Group grandings on $M_2(\mathbb{K})$"(Boboc e Dascalescu), no qual é feita uma discussão e exploração das idéias e tem como o grande resultado o seguinte teorema:

Teorema 1.4.7 *Seja G um grupo com elemento neutro 1, $\mathbb{K}$ 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:

$$A_1 = \left\{ \begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix} \right\}, A_g = \left\{ \begin{pmatrix} 0 & \mathbb{K} \\ \mathbb{K} & 0 \end{pmatrix} \right\}, A_h = 0$$

Para $h \in G - \{1, g\}$, onde 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 $A_1 = \left\{\begin{pmatrix} \mathbb{K} & 0 \\ 0 & \mathbb{K} \end{pmatrix}\right\}, A_g = \left\{\begin{pmatrix} 0 & \mathbb{K} \\ 0 & 0 \end{pmatrix}\right\}, A_{g^{-1}} = \left\{\begin{pmatrix} 0 & 0 \\ \mathbb{K} & 0 \end{pmatrix}\right\}$ $A_h = 0$ *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* $g, h \in G$ *são tais que* $\{1, g, h, gh\}$ *é um subgrupo de* G *isomorfo ao grupo de Klein, 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* $b \in \mathbb{K} - \{\alpha^2 + \alpha; \alpha \in \mathbb{K}\}$*.*

Para se mostrar esse teorema, usaram-se muitos conceitos de álgebra linear, principalmente no que se refere à polinômios característicos e minimais, autovetores e autovalores. Dividindo o resultado em casos em que o suporte tem 2, 3 ou 4 elementos, e o resultado foi completamente demonstrado.

1.4.4 G-graduações para $M_3(\mathbb{K})$

Diante a tudo que foi citado, chegamos agora ao pricipal objetivo do presente trabalho, que é determinar todas as G-graduações para a álgebra $M_3(\mathbb{K})$. Para isso, vamos nos basear no artigo "Group gradings on $M_3(\mathbb{K})$"dos autores Crina Boboc e Dascaslescu de 2007, que enuncia o seguinte teorema a ser provado:

Teorema 1.4.8 *Seja* $\mathbb{K}$ *um corpo e* G *um grupo. Então qualquer* G*-graduação* $A = \oplus_{g\in G} A_g$ *em* $M_3(\mathbb{K})$ *é isomorfa à algumas das seguintes graduações:*

I*: Uma boa graduação.*

II*: Uma graduação com supp(A)* $\simeq \mathbb{Z}_3$*, não isomorfa à uma boa graduação. Tal graduação é descrita a seguir:*

II'*: Se char*$(\mathbb{K}) \neq 3$*, essa graduação será da forma* $A(a)$ *para algum* $a \in \mathbb{K}$ *tal que* $a \neq \frac{t^3-3t+1}{t^2-t}$ *para qualquer* $t \in \mathbb{K} - \{0, 1\}$ *tal que* $A(a)_e = \mathbb{K}[B_a] = \{\alpha(B_a)^2 + \beta B_a + \gamma I_3; \alpha, \beta, \gamma \in \mathbb{K}\}$,

$A(a)_c = X\mathbb{K}[B_a]$ *e* $A(a)_{c^2} = X^2\mathbb{K}[B_a]$ *com:*

$$B_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix}, X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix}$$

.

II': *Se* $char(\mathbb{K}) = 3$ *essa graduação será da forma* $A_3(a)$ *para algum* $a \in \mathbb{K}$ *tal que* $a \neq t^3 - t$, *para todo* $t \in \mathbb{K}$, *onde* $A_3(a)_e = K[C_a] = \alpha(C_a)^2 + \beta C_a + \gamma I_3 | \alpha, \beta, \gamma \in \mathbb{K}$, $A_3(a)_c = XK[C_a]$ *e* $A_3(a)_{c^2} = X^2K[C_a]$, *com* $C_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & 1 & 0 \end{pmatrix}, X = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

E temos que $A_3(a) \simeq A_3(b)$ *se e somente se* $a - b = t^3 - t$ *para algum* $t \in \mathbb{K}$.

Para ambos os casos, se A *é uma graduação, temos que* A_e *é uma extensão cúbica de Galois de* $\mathbb{K}$, A *é um anel de divisão graduado e, quando considerado como álgebra* Z_3*-graduada, temos que* $A \simeq A_e * Z_3$, A *será um anel de grupo torcido.*

III: *Uma graduação cujo* $supp(A) = \mathbb{Z}_3 \times \mathbb{Z}_3 =< \sigma > \times < \tau >$, *não isomorfa à uma boa graduação. Essa graduação é isomorfa à uma das seguintes:*

III': $A(X, Y_a)$, *onde* $X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^2 \end{pmatrix}$ eY$_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & 0 & 0 \end{pmatrix}$; a$\in \mathbb{K}$

III": $A(X_d, Y(x, y, z))$, onde

$$X_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ d & 0 & 0 \end{pmatrix}, Y(x, y, z) = \begin{pmatrix} x & y & z \\ \xi^2 dz & \xi^2 x & \xi^2 y \\ \xi dy & \xi^2 dz & \xi x \end{pmatrix}$$

, onde $d \in \mathbb{K}^* - (\mathbb{K}^*)^3$, e $x, y, z \in \mathbb{K}$, não todos nulos.

Aqui ξ é uma raiz cúbica primitiva da unidade de $\mathbb{K}$. Para qualquer par de matrizes X, Y como em (III') ou (III''), a graduação $A(X,Y)$ é definida por $A(X,Y)_{\sigma^i\tau^j} = kX^iY^j$.

Esse teorema é o tema central do trabalho, os próximos capítulos serão dedicados à prova em detalhes do mesmo.

Capítulo 2

Resultados Preliminares

2.1 Princípios

Nessa seção, o nosso objetivo é usar alguns resultados importantes que nos levarão à condições suficientes para a existência da chamada "boa graduação". Essas graduações são caracterizatas por terem matrizes elementares atuando como elementos homogêneos. Para encontrá-las, faremos apenas exigências sobre o suporte, de modo que $\mathbb{K}$ e G é um corpo qualquer e um grupo qualquer, respectivamente.

Lema 2.1.1 *Seja $A = \oplus A_g$ uma G-graduação numa álgebra A, então $1_A \in A_e$*

Demonstração: A demonstração de tal fato pode ser encontrada em [8]. ■

Lema 2.1.2 *Seja $A{=}\oplus_{g\in G} A_g$ uma graduação e seja B um elemento homogêneo de grau g. Então essa graduação é isomorfa à uma graduação tal que a forma de Jordan J_B de B é um elemento homogêneo de grau g.*

Demonstração:

Sabemos que a forma de Jordan de uma dada matriz é um tipo especial de matriz semelhante à ela, logo usemos a seguinte caracterização para J_B: $J_B = UXU^{-1}$;, onde U é invertível. Agora provaremos que a seguinte função: $\phi : A \to A, \phi(X) = UXU^{-1}$ é um automorfismo na álgebra A. Vamos dividir a prova em 3 passos habituais: (1) mostraremos que ϕ é um homomorfismo de álgebras, (2) que ϕ é injetora e, finalmente, que (3) ϕ é sobrejetora.

(1) Note que apenas devemos avaliar se ϕ preseverva a nossa estrutura de álgebra, de fato isso ocorre como podemos ver nas 3 igualdades a seguir:

$$1.\phi(X+Y) = U(X+Y)U^{-1} = UXU^{-1} + UYU^{-1} = \phi(X) + \phi(Y)$$

$$2.\phi(XY) = U(XY)U^{-1} = UX(U^{-1}U)YU^{-1} = (UXU^{-1})(UYU^{-1}) = \phi(X)\phi(Y)$$

$$3.\phi(\alpha X) = U(\alpha X)U^{-1} = \alpha(UXU^{-1}) = \alpha\phi(X)$$

(2) Veja que $\phi(X) = 0 \Leftrightarrow UXU^{-1} = 0 \Leftrightarrow X = 0 \Rightarrow Ker(\phi) = 0$, usando o teorema do homomorfismo para álgebras temos que ϕ é um homomorfismo injetor em A.

(3) A sobrejetividade de ϕ é garantida pelo fato de U ser invertível, pois se $X \in M_3(K)$ basta tomar $Y = U^{-1}XU$ e teremos $\phi(Y) = X$.

De acordo com a definição de homomorfismo G-graduado, vale que J_B será um elemento homogêneo de grau g. ∎

Lema 2.1.3 *Seja A=$\oplus_{g\in G}A_g$ uma graduação de tal forma que exista uma matriz inversível $U \in A_g$ para algum $g \in G$. Então $dim(A_h) = dim(A_{gh})$ para todo $h \in G$.*

Demonstração: Vamos tomar a seguinte função $\phi : A_h \to A_{gh}, \phi(X) = UX$ é uma bijeção de A_h em A_{gh}. Veja que ϕ é uma transformação linear (embora não seja um homomorfismo de álgebras) e a demonstração desse fato é análoga aos passos 1 e 3 da prova do Lema 2.1.2. A prova da injetividade e da sobrejetividade de ϕ são análogas, respectivamente, aos passos **2** e **3** do Lema 2.1.2, logo $dim(im(\phi)) = dim(A_{gh})$, do Teorema do núcleo e da imagem, segue-se que $dim(A_h) = dim(A_{gh})$. ∎

Observação 2.1.4 *Caso G não seja abeliano ainda temos que $dim(A_h) = dim(A_{hg})$, e a demonstração é análoga.*

Corolário 2.1.5 *Suponha que G tenha um elemento g de ordem 2 e seja $M_3(\mathbb{K})$=$\oplus_{g\in G}A_g$ uma G-graduação. Se existe um elemento homogêneo B de grau g, então B não é invertível.*

Demonstração: Vamos supor, por absurdo, que B seja invertível, nesse caso vale o Lema 2.1.3. Por outro lado podemos escrever:

$$M_3(\mathbb{K}) = (A_e \oplus A_g) \oplus (A_{h_1} \oplus A_{gh_1}) \oplus ... \oplus (A_{h_n} \oplus A_{gh_n}); h_i \in \{Supp(A) - g\}$$

Observemos que $Supp(A)$ é finito, visto que $M_3(\mathbb{K})$ tem dimensão finita. Além disso, $gh_j \neq h_j, \forall j \in (1, ..., n)$, pois $g \neq e$. E, caso, $h_i = gh_j$ para alguns $i, j \in (1, ..., n)$,vale que $gh_i = h_j$ pelo fato de g ter ordem 2. Ora, nesse caso teríamos que: $A_{h_i} \oplus A_{gh_i} = A_{gh_j} \oplus A_{h_j}$. Podemos, assim, dizer que $M_3(\mathbb{K})$ está decomposta como união disjunta de conjuntos da forma gh_i, h_i. Como $dim(A_{h_i}) = dim(A_{gh_i})$ segue que $dim(M_3(\mathbb{K}))$ é par, absurdo. ∎

Agora que já vimos esses resultados, no qual daremos maior enfâse ao resultado 2.1.5, desenvolveremos uma pequena sequência de resultados na próxima seção que reduziram em muito a quantidade e a caracterizações possíveis dos elementos de $G \cap Supp(A)$. Veremos que para grupos com elementos de ordem 4 ou 2 as graduações possíveis são isomorfas à um tipo especial de graduações que recebe o nome de boas graduações.

2.2 Boas graduações

Definição 2.2.1 ***Matrizes elementares:*** *Dizemos que uma matriz $M \in M_n(\mathbb{K})$ é elementar se uma das suas componentes $a_{ij} = 1$ e as demais são nulas. Nesse caso, iremos denotar essas matrizes por e_{ij}.*

Definição 2.2.2 *Uma graduação $A{=}\oplus_{g\in G}A_g$ tal que e_{ij} é um elemento homogêneo para alguns i, j é dita uma boa graduação.*

Lema 2.2.3 *Seja $A{=}\oplus_{g\in G}A_g$ uma graduação tal que exista um elemento homogêneo B diferente de zero tal que $B^3 = 0$. Então a graduação é isomorfa à uma boa graduação.*

Demonstração: Pelo lema 2.1.2 podemos assumir que B está em sua forma de Jordan J_B já que as graduações associadas à B serão isomorfas às associadas à J_B. Considere os 3 possíveis blocos de Jordan para $M_3(\mathbb{K})$,em seguida analisemos separadamentamente cada um dos casos:

$$(1) \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} (2) \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 0 & \alpha \end{pmatrix} (3) \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix}$$

Aplicando-se B^3 para cada uma das formas obtemos as seguintes, respectivamente:

$$(1') \begin{pmatrix} \lambda^3 & 0 & 0 \\ 0 & \lambda^3 & 0 \\ 0 & 0 & \lambda^3 \end{pmatrix} (2') \begin{pmatrix} \lambda^3 & 0 & 0 \\ 3\lambda^2 & \lambda^3 & 0 \\ 0 & 0 & \alpha^3 \end{pmatrix} (3') \begin{pmatrix} \lambda^3 & 0 & 0 \\ 3\lambda^2 & \lambda^3 & 0 \\ 3\lambda & 3\lambda^2 & \lambda^3 \end{pmatrix}$$

Em todos os casos os valores da diagonal principal de J_B deverão ser todos nulos pois $B^3 = 0$, então substituindo (1'),(2'),(3') em (1),(2),(3), respectivamente, B deverá ser de alguma das 3 seguintes formas:

$$(i) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} (ii) \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} (iii) \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

(i) Não é possível pois B é não nula por hipótese.
(ii) $B = e_{21}$ que será um elemento homogêneo de grau g. Por definição, A será uma boa graduação.
(iii) $B^2 = e_{31}$ como B^2 é um elemento homogêneo de grau g^2, novamente, pela definição A será uma boa graduação. ■

Agora começaremos a “filtrar”as possíveis graduações da nossa álgebra através dos elementos do seu suporte. Até agora não colocamos condições sobre $Supp(A)$.

A seguir mostraremos duas condições suficientes para A ser uma boa graduação. A primeira é a existência de um elemento $g \in Supp(A)$ de ordem maior ou igual que 4 e a segunda a existência de um elemento $g \in Supp(A)$ de ordem 2.

Teorema 2.2.4 *Seja $A = \oplus_{g\in G} A_g$ uma graduação tal que $supp(A)$ contenha um elemento g de ordem pelo menos 4. Então a graduação é isomorfa à uma boa graduação.*

Demonstração: Seja $g \in Supp(A)$ tal que $ord(g) \geq 4$, pelo Teorema de Caley-Hamilton, existem $\alpha, \beta, \lambda \in \mathbb{K}$ tais que $B^3 + \alpha B^2 + \beta B + \lambda I_3 = 0$. Por outro lado, $I_3 \in A_e, B \in A_g, B^2 \in A_{g^2}, B^3 \in A_{g^3}$, como $ord(g) \geq 4$ vale que esses termos são componentes homogênios de grau distinto, então: $B^3 = \alpha B^2 = \beta B = \lambda I_3 = 0$. Como $B^3 = 0$, do Lema 2.2.3 A é isomorfa à uma boa graduação. ■

Teorema 2.2.5 *Seja $A = \oplus_{g\in G} A_g$ uma graduação tal que $supp(A)$ contenha um elemento de ordem 2. Então essa graduação é isomorfa à uma boa graduação.*

Demonstração: Seja $g \in Supp(A)$ tal que $ord(g) = 2$ e seja $B \in A_g$ não nula, pelo Lema 2.1.2 ,vamos assumir que B tenha a forma de Jordan. O Teorema de Cayley-Hamilton nos diz que $B^3 - Tr(B)B^2 + cB - det(B)I_3 = 0$, para algum $c \in \mathbb{K}$. Como $ord(g) = 2$ vale que $B^2 \in A_e$ e $B^3 \in A_g$. Logo $B^3, B \in A_g$ e $Tr(B)B^2, det(B)I_3 \in A_e$, com isso $Tr(B)B^2 + det(B)I_3 = 0$ e $B^3 + cB = 0$.
Além disso, pelo Corolário 2.1.5, temos que $det(B) = 0$, pois nesse caso B não é invertível, portanto, $Tr(B)B^2 = 0$. Essa igualdade em um espaço vetorial é válida se, e somente se, $Tr(B) = 0$ ou $B^2 = 0$. Se $B^2 = 0$ então $B^3 = 0$ e o resultado decorre do Lema 2.2.3. Agora, caso $Tr(B) = 0$, então: $B^3 - Tr(B)B^2 + cB - det(B)I_3 = B^3 + cB = 0$, assim, o polinômio característico de B é da forma $P(t) = t^3 + ct = t(t^2 + c)$. Vamos novamente considerar a forma de Jordan de B, na qual dividiremos em 3 casos novamente como no Lema 2.2.3:

$$(1) \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} (2) \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 0 & \alpha \end{pmatrix} (3) \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix}$$

O caso (1) não deve ser levado em conta pois $B \notin A_e$, aplicando o polinômio característico em (2) e em (3) temos as seguintes relações:

$$(i)B(B^2+c) = \begin{pmatrix} \lambda\left(\lambda^2+c\right) & c\lambda & c\lambda \\ \lambda^2+\lambda\left(2\lambda+c\right)+c & \lambda\left(\lambda^2+c\right)+c & c\lambda+c \\ c\alpha & c\alpha & \alpha\left(\alpha^2+c\right) \end{pmatrix} = 0$$

$$(ii)B(B^2+c) = \begin{pmatrix} \lambda\left(\lambda^2+c\right) & c\lambda & c\lambda \\ \lambda^2+\lambda\left(2\lambda+c\right)+c & \lambda\left(\lambda^2+c\right)+c & c\lambda+c \\ \left(c+1\right)\lambda+2\lambda+c & \lambda^2+\lambda\left(2\lambda+c\right)+c & \lambda\left(\lambda^2+c\right)+c \end{pmatrix} = 0$$

Em (i), devemos ter que $\lambda c = \alpha c = 0 \Leftrightarrow \lambda, \alpha = 0$ ou $c = 0$, mas se $c = 0$, então $P(\lambda) = \lambda^3$, onde $B^3 = 0$ e, novamente, pelo Lema 2.2.3 A será uma boa graduação. Considerando que apenas $\alpha = \lambda = 0$, nossa matriz B é da forma:

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

Ou seja, $B = e_{21}$. Por definição, A é isomorfa à uma boa graduação.

Analisando o caso seguinte (ii), observamos novamente a equação $\lambda c = 0$ que terá solução para $\lambda = 0$, pois o caso $c = 0$ já foi analisado em (i). Assim B será escrita sob a forma:

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

E sabemos que $B^2 = e_{31}$. E assim B^2 é um elemento homogêneo de grau e. De qualquer modo, acabamos de mostrar que a ordem de g ser 2 leva a graduação a ser isomorfa à uma boa graduação. ■

E assim concluímos a nossa seção com um resultado formidável. A partir da análise do comportamento dos polinômios característicos,conseguimos deduzir uma relação entre a ordem dos elementos do $Supp(A)$ com a estrutura da álgebra G-graduada, mostrando duas condições suficientes para se ter uma boa graduação: a existência de um elemento de ordem 2 no suporte ou de ordem maior ou igual que 4. Veja que fomos muito cautelosos ao enfatizar a palavra suficiente, isso porque podem existir boas graduações em um cenário onde todos os elementos do suporte não tenham ordem 2 ou 3, basta tomar como exemplo a graduação trivial.

Além disso, o resultado tem uma consequência imediata quanto à ordem dos elementos do suporte. Ou seja, ou todos os elementos podem ter ordem 1, nesse caso a graduação será trivial, ou todos os elementos tem ordem 3. Toda graduação trivial é uma boa graduação, pois $e_{ij} \in M_3(\mathbb{K}); \forall i, j \in (1, 2, 3)$, portanto, nos resta a seguinte pergunta: **Toda graduação em $M_3(\mathbb{K})$ é uma boa graduação?** Para responder essa pergunta basta analisar qual o comportamento da graduação quando o seu suporte consiste de elementos de ordem 3.

Na seção seguinte iremos construir duas G-graduações quando o $Supp(A)$ é constituído de elementos de ordem 3. A primeira delas é um exemplo de uma boa graduação, a segunda é um exemplo de uma G-graduação que não faz parte dessa classe.

2.3 Existem apenas boas graduações?

Exemplo 2.3.1 ***Uma Boa graduação:***

Considere $G = \mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ e $\mathbb{K}$ um corpo qualquer. Defina as seguintes partes homogêneas da graduação:

$$A_{\overline{0}} = \left\{ \begin{pmatrix} \mathbb{K} & \mathbb{K} & 0 \\ \mathbb{K} & \mathbb{K} & 0 \\ 0 & 0 & \mathbb{K} \end{pmatrix} \right\} A_{\overline{1}} = \left\{ \begin{pmatrix} 0 & 0 & \mathbb{K} \\ 0 & 0 & \mathbb{K} \\ 0 & 0 & 0 \end{pmatrix} \right\} A_{\overline{2}} = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \mathbb{K} & \mathbb{K} & 0 \end{pmatrix} \right\}$$

Agora vamos fazer a verificação de praxe para o fechamento da operação de multiplicação quanto ao fechamento do grupo, ou seja verificar se $A_g A_h \subset A_{gh}, \forall g, h \in \mathbb{Z}_3$. Nesse caso, como o grupo é abeliano, basta analisar se o produto de componentes de $\overline{0}$ e $\overline{1}$ ou $\overline{2}$ funcionam de forma adequada, além de analisar o produto de componentes de $\overline{1}$ e $\overline{2}$ sob a mesma óptica.

Vamos apenas verificar para os casos $A_{\overline{0}}A_{\overline{0}} \subset A_{\overline{0}}$, $A_{\overline{2}}A_{\overline{2}} \subset A_{\overline{1}}$ e $A_{\overline{1}}A_{\overline{2}} \subset A_{\overline{0}}$:

$$A_{\overline{0}}A_{\overline{0}} = \left\{ \begin{pmatrix} \mathbb{K} & \mathbb{K} & 0 \\ \mathbb{K} & \mathbb{K} & 0 \\ 0 & 0 & \mathbb{K} \end{pmatrix} \right\}$$

$$A_{\overline{2}}A_{\overline{2}} = \left\{ \begin{pmatrix} 0 & 0 & \mathbb{K} \\ 0 & 0 & \mathbb{K} \\ 0 & 0 & 0 \end{pmatrix} \right\}$$

$$A_{\overline{1}}A_{\overline{2}} = \left\{ \begin{pmatrix} \mathbb{K} & \mathbb{K} & 0 \\ \mathbb{K} & \mathbb{K} & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\}$$

O último passo para se verificar que essa decomposição é uma graduação é mostrar que $M_3(\mathbb{K}) = A_{\overline{0}} \oplus A_{\overline{1}} \oplus A_{\overline{2}}$. Esse fato é trivial dada a caracterização de cada espaço que foi definido no exemplo.

Não podemos afirmar, portanto, que uma boa graduação é equivalente à não existência de elementos de ordem 3 em $Supp(A)$. Além disso, nem toda G-graduação é isomorfa à uma boa graduação em $M_3(\mathbb{K})$, como veremos no seguinte exemplo:

Exemplo 2.3.2 ***Uma graduação misteriosa***

Seja $G = \mathbb{Z}_3$ e $\mathbb{K} = \mathbb{Z}_3$ também, vamos agora construir as 3 partes homogêneas da graduação da seguinte forma, onde $x, y, z \in \mathbb{K}$:

$$A_e = \begin{pmatrix} \overline{2}y + z & x + y & x \\ x & x + \overline{2}y + z & x + y \\ x + y & \overline{2}x + y & x + \overline{2}y + z \end{pmatrix}$$

$$A_c = \begin{pmatrix} \overline{2}y + z & x + y & x \\ x + y + \overline{2}z & y + z & y \\ \overline{2}x + z & x + y + z & z \end{pmatrix}$$

$$A_{c^2} = \begin{pmatrix} \overline{2}y + z & x + y & x \\ x + \overline{2}y + z & \overline{2}x + z & \overline{2}x + y \\ z & \overline{2}x + \overline{2}z & x + y + z \end{pmatrix}$$

Não faremos a demonstração das condições que essa decomposição deve ter para ser um graduação, tal fato poderá ser considerado verdadeiro com base em resultados futuros. Nesse *instante, vamos mostrar apenas a impossibilidade da existência de componentes homogêneos elementares.*

Para existir uma matriz elementar de grau e, deveríamos ter que $x = \overline{0}$*, pois se não o fosse teríamos duas de suas compomentes não nulas a dizer* $e_{21} + e_{13}$ *ou* $\overline{2}(e_{21} + e_{13})$*, por motivo análogo* $y = \overline{0}$*. Com* $x = y = \overline{0}$ *teríamos:*

$$A_e = \begin{pmatrix} z & \overline{0} & \overline{0} \\ \overline{0} & z & \overline{0} \\ \overline{0} & \overline{0} & z \end{pmatrix}$$

Assim, A_e *não contém elementos homogêneos.*

Em A_c*, a existênicia de uma matriz elementar exige que entre* x, y, z *dois deles sejam nulos. Digamos, sem perda de generalidade, que* $x = y = \overline{0}$*, assim* $x + y + z = \overline{0} \Rightarrow z = \overline{0}$*, logo a matriz em questão, que depende totalmente das variáveis* x, y *e* z *deve ser nula, portanto, não é elementar.Mas ainda não excluimos a possibilidade da matriz ser igual* e_{32} *podendo-se ter* $x + y + z = \overline{1} \Rightarrow z = \overline{1}$*, porém* $\overline{2}y + z = \overline{1}$ *o que mostra que ainda assim não temos uma matriz elementar.*

Na última parte homogênea podemos avaliar as possíveis matrizes elementar atribuindo valores para x*,* y *e* z*.*

Vamos supor que $x = \overline{1}$ *e tentar construir* e_{13}*, em particular* $z = \overline{o}$ *e* $x + y = \overline{o} \Rightarrow y = \overline{2}$*, dai* $\overline{2}y + z = \overline{1}$ *e não temos a matriz elementar apropriada.*

Para $z = \overline{1}$ *queremos construir a matriz elementar* e_{31}*, assim, vale que* $\overline{2}y + \overline{1} = \overline{2}y = \overline{2} \Rightarrow y = \overline{1}$*, de* $x + y + z$ *encontramos que* $x = \overline{1}$ *e não teremos, novamente, uma matriz elementar.*

Das duas análises anteriores podemos concluir que $x = y = \overline{0}$*, por* $x + y + z = \overline{0}$ *teremos* $y = \overline{0}$ *e assim a matriz será nula, portanto, não elementar.*

Desse modo, não existem componentes homogêneos elementares e isso significa que tal como foi definida, $A_{\overline{0}}, A_{\overline{1}}$ *e* $A_{\overline{2}}$ *não decompõem* $M_3(\mathbb{K})$ *na forma de uma boa graduação, embora as mesmas formem uma estrutura* G *graduada para a nossa álgebra.*

Os dois exemplos acima mostram que as boas graduações atuam de modo muito denso no conjunto das possíveis graduações em $M_3(\mathbb{K})$, visto que em todas as ordens possíveis dos elementos de $Supp(A)$ podem existir boas graduações associada à esse suporte. Por outro lado, vemos que existem graduações que não são isomorfas às primeiras e mais ainda, em suportes iguais podem existir graduações de diferentes classes associadas ao suporte. Isso elucida o comportamento complexo inerente à estrutura de álgebras G-graduadas.

Com essa discussão que tivemos até o momento, sabemos que quando o suporte não tem elementos apenas de ordem 3 teremos uma boa graduação, porém, mesmo no caso contrário à esse podem existir boas e outros tipos de graduações. Veja que nos exemplos pegamos apenas graduações em $\mathbb{Z}_3$ como suporte e corpo base, mas ainda não respondemos qual a estrutura de $Supp(A)$, nem mesmo sabemos ainda se esse conjunto tem uma estrutura de grupo. Na próxima seção apresentaremos 3 teoremas que responderão algumas perguntas relacionadas ao comportamento dessas classes de graduações não isomorfas à uma boa graduação.

2.4 Um importante resultado

Nessa seção apresentaremos 3 teoremas que serão fundamentais para o estudo das graduações em que o suporte associado seja composto apenas por elementos de ordem 3.Já vimos nas duas seções anteriores que as boas graduações determinam as graduações nos demais casos, porém, podem ainda aparecer nesse caso. O que faremos nos capítulos subsequentes é classificar essas outras graduações "misteriosas". Veremos que estudo dessas graduações estará associado ao tipo de suporte que iremos trabalhar. Com o próximo resultado seremos capazes de identificar qual o comportamento desse suporte, para em seguida começar o trabalho de classificar as demais graduações.

Considere nos enunciados a seguir: $A=\oplus_{g\in G}A_g$ uma graduação não isomorfa à uma boa graduação, e tal que $supp(A)-\{e\}$ consista apenas em elementos de ordem 3.

Teorema 2.4.1 *A é um anel de divisão graduado, ou seja, qualquer elemento homogêneo não-nulo é invertível.*

Demonstração: Vamos provar que dado qualquer elemento homogêneo não nulo da graduação ,este será invertível. Seja $B \in A_g(g \neq e)$ não nula, por Caley Hamilton, temos que existem $\alpha, \beta \in K$ tais que $B^3+\alpha B^2+\beta B-det(B)I_3=0$. Considere o seguinte diagrama, onde $x=B^2$ e $y=B^3$:

$$\begin{tikzcd}
 & A_g \arrow[r, "x"] & A_{g^2} \arrow[dr, "y"] & \\
B \arrow[ur] \arrow[r] \arrow[dr] & A_e \arrow[r, "x"] & A_e \arrow[r, "y"] & A_e \\
 & A_{g^2} \arrow[r, "x"] & A_g \arrow[ur, "y"] &
\end{tikzcd}$$

Analisando o caso em que $B \notin A_e$ vale que B e $x = B^2$ são elementos homogêneos de grau diferentes, bem como $y = B^3 \in A_e$. Por serem elementos homogêneos de diferentes graus, vale que a equação acima tem solução se, e somente se, $B^3 - det(B)I_3 = \alpha B^2 = \beta B = 0$. Portanto, se $det(B) = 0$, então $B^3 = 0$ e teremos uma graduação isomorfa à uma boa graduação pelo Lema 2.2.3. Concluímos que todo elemento homogêneo de grau g ou g^2 é invertível.

Agora seja $X \in A_e; X \neq 0$, assim dada $B \in A_g$ não nula, vale que $XB \in A_g$, ora, $XB \neq 0$, pois caso contrário $X = 0$ (da condição de B ser invertível), assim, XB é invertível. Como $det(XY) = det(X)det(Y) \neq 0$ tem-se, em particular, que $det(X) \neq 0$, logo X é invertível também. ■

Com esse teorema, podemos aproximar as componentes homogêneas da graduação para um corpo.

Teorema 2.4.2 *Seja G um grupo e $A = M_3(\mathbb{K})$, então $Supp(A)$ é um subgrupo de G.*

Demonstração: Vamos fazer a verificação de praxe: (i) mostrar que $Supp(A)$ é não vazio, (ii) se dado $g \in Supp(A)$, então $g^{-1} \in Supp(A)$ e, finalmente, (iii) dados $g, h \in Supp(A)$, então $gh^{-1} \in Supp(A)$:

(i) $Supp(A)$ não é vazio, visto que $e \in Supp(A)$;

(ii) Vamos tomar $X \in A_g$, como X é invertível, vale que $X^2 \neq 0$, mas $X^2 \in A_{g^2}$, logo $g^2 = g^{-1}$ (por hipótese $ord(g) = 3$) pertence à $Supp(A)$

(iii) Assim, seja $X \in A_g$ e $Y \in A_{h^{-1}}$, sabemos que $det(XY) = det(X)det(Y)$, onde $det(X) \neq 0, det(Y) \neq 0$, então $det(XY) \neq 0$, pois $\mathbb{K}$ é um corpo e, assim, $gh^{-1} \in Supp(A)$. Por tanto, $Supp(A)$ é um subgrupo de G ■

Agora sabemos que o suporte dadas essas condições tem uma estrutura bem comportada de grupo e isso decorre imediatamento da estrutura de anel de divisão graduado das componentes homogêneas da graduação. Tal fato é óbvio quando estamos trabalhando em G-graduação em corpos, porém o anel das matrizes tem divisores de zero, como por exemplo:

$$X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

São matrizes não nulas, porém:

$$XY = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Esses exemplos mostram que nem sempre o $Supp(A)$ tem essa propriedade de fechamento e que existe a possibilidade do produto de dois elementos do suporte não pertencer necessariamente ao suporte. No caso de anéis de divisões não existem essas matrizes divisoras de zero.

Assim, resolvemos o problema do fechamento e mostramos que em suportes de elementos de ordem 3 "ganhamos" uma estrutura de grupo. Mais ainda, esses resultados ainda implicam num terceiro resultado que será o nosso "pontapé" de saída em buscas das novas graduações. Ele fará uma relação entre esse suporte com a estrutura dos componentes homogêneos, mostrando que até mesmo estes preservam uma boa estrutura para os nossos estudos seguintes.

Teorema 2.4.3 *Seja G um grupo, $A = M_3(\mathbb{K})$. Ou temos que: (i) $supp(A) \simeq \mathbb{Z}_3$ e $dim(A_h) = 3, \forall h \in Supp(A)$ ou: (ii) $supp(A) \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ e $dim(A_h) = 1$ para todo $h \in supp(A)$.*

Demonstração: Da nossa hipótese sabemos que, no mínimo, $Supp(A) = \{e, g, g^2\}$. Se o suporte conter apenas esses elementos então ele será um subgrupo de G isomorfo à $\mathbb{Z}_3$ (único grupo de ordem 3 a menos de isomorfismos) e pelo Lema 2.1.3, como todo elemento homogêneo de A_e é invertível, temos que $dim(A_e) = dim(A_{ge=g}) = dim(A_{g^2e=g^2})$. Como $M_3(\mathbb{K}) = A_e \oplus A_g \oplus A_{g^2}$ tem dimensão 9, devemos ter que $dim(A_e) = dim(A_{ge=g}) = dim(A_{g^2e=g^2}) = 3$ e cairemos no primeiro caso (i).

Se existir $h \in Supp(A) - \{e, g, g^2\}$, vale que $ord(h) = 3$ e , portanto, $h^2 \notin \{e, g, g^2\}$, pois se $h^2 = g \Rightarrow hg = e$ e se $h^2 = g^2 \Rightarrow h^2 g = e$. Em ambos os casos temos uma contradição pela unicidade do elemento inverso no grupo.Logo, $h^2 \in Supp(A)$, pelo teorema anterior. Além disso, $gh, gh^2 \in Supp(A)$ e, utilizando de racíocinio análogo à prova anterior, temos que $gh, gh^2 \notin \{e, g, g^2, h, h^2\}$. Por fim, $g^2h, g^2h^2 \in Supp(A)$ e são diferentes dos demais elementos, e a justificativa, novamente, se repete. Temos, por enquanto, que $Supp(A) = \{e, g, g^2, h, h^2, gh, gh^2, g^2h, g^2h^2\} =< g, h >$. Mas $g^{n-1}h^{m-1} \neq e$, onde m, n não são simultaneamente iguais à 1. Devido a unicidade dos inversos e da ordem de g e de h, temos $gh = hg$. Nesse caso, $M_3(\mathbb{K})$ é decomposta por nove componentes, portanto dim(A_g)=1 (com $g \in Supp(A)$). ■

Com isso, completamos nossa prova que implica em um bom comportamento dessas novas graduações que iremos encontrar, principalmente no que se refere ao suporte das mesmas. Mostramos que elas obedecem à uma estrutura de grupo, mais ainda, ela é isomorfa à grupos cujo o comportamento é bem conhecido no caso $\mathbb{Z}_3$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$. A dimensão das componentes dessas graduações são também conhecidas, sendo iguais à 1 e a 3. Dito isso podemos inciar a nossa busca pelas graduações restantes da nossa álgebra ($M_3(\mathbb{K})$).

Na nossa próxima seção analisaremos quais são as graduações possíveis para um suporte isomorfo ao $\mathbb{Z}_3$, cuja as dimensões das componentes homogêneas são todas iguais à 3. Na seção subsequente, faremos a análise do segundo caso resultante desses teoremas.

Capítulo 3

As $\mathbb{Z}_3$-Graduações

Agora que já classificamos algumas graduações como boas graduações e no final do capítulo anterior deduzimos um grande resultado a respeito do suporte das G-graduações restantes, iremos descrever nesse capítulo todas as graduações em que o suporte é o grupo $\mathbb{Z}_3$. Faremos uma construção de uma G-graduação sob essas condições e, por fim, mostraremos que essa construção de fato é a única $\mathbb{Z}_3$-graduação, a menos de isomorfismos.

3.1 Resultados preliminares

Seja $A = M_3(\mathbb{K})$, $G \simeq \mathbb{Z}_3$ e $A = \oplus_{g\in\mathbb{Z}_3} A_g$, uma G-graduação em A. Nessa seção, vamos mostrar que numa $\mathbb{Z}_3$-graduação temos que a componente homogênea A_e é um corpo e, mais ainda, A_e é também uma extensão de Galois de $\mathbb{K}$.

Teorema 3.1.1 *A_e é um corpo.*

Demonstração: Seja B um elemento homogêneo em A_e cujo o polinômio minimal μ_B tem grau 3, vamos mostrar que $A_e = \mathbb{K}(B)$. Como A_e é um anel de divisão graduado, provar essa afirmação garante à A_e uma estrutura de corpo, uma vez que dados $X, Y \in \mathbb{K}(B)$, tem-se que $XY = YX$. Como queremos mostrar a igualdade de dois conjuntos, provaremos que: $(i)\mathbb{K}(B) \subset A_e$ e $(ii) A_e \subset \mathbb{K}(B)$.

(i) seja $\mathbb{K}(B) = \{f(B); f(x) \in \mathbb{K}(x)\} = \{a_0 + a_1B + ... + a_nB^n; a_i \in \mathbb{K}, \forall i \in (0, 1, ..., n)\}$. Veja que $\forall n \in \mathbb{N}$ temos que $B^n \in A_e$. De fato, $I_d, B \in A_e$ e dado que $B^n \in A_e$ então $B^nB \in A_e$ por definição de graduação, e assim $B^{n+1} \in A_e$, e, por indução, o resultado se segue. Dito isso, basta usar o fato de que $a_iB^i \in A_e$, pois A_e é espaço vetorial e, pelo mesmo motivo, $a_0 + a_1B + ... + a_nB^n \in A_e, \forall n \in \mathbb{N}$. Assim, $\mathbb{K}(B) \subset A_e$.

(ii) Para provar a inclusão contrária, mostramos que o seguinte conjunto: $\{I_d, B, B^2\}$ é uma base para A_e. Veja que dada a equação $\alpha I_d + \beta B + \lambda B^2 = 0$, temos solução apenas para $\alpha = \beta = \lambda = 0$, visto que $\delta(\mu_B) = 3$ (aqui δ denota o grau do polinômio μ_B). Agora, do Teorema do Núcleo e da Imagem temos que $A_e \simeq \mathbb{K}^3$. Seja $T : A_e \to \mathbb{K}^3$ a transformação linear bijetiva entre os espaços vetoriais tal que: $T(I_d) = a, T(B) = b, T(B^2) = c$. Assim, $xa + yb + zc = 0; x, y, z \in \mathbb{K}^3$ se, e somente se, $xT^{-1}(I_d) + yT^{-1}(B) + zT^{-1}(B^2) = 0$. Usando o fato de que T^{-1} é uma transformação linear bijetiva, vale que $T^{-1}(xI_d + yB + zB^2) = 0$, portanto, $xI_d + yB + zB^2 = 0$ (pois $Ker(T^{-1}) = 0$), e daí a, b, c são L.I. Dessa forma, a matriz dos coeficientes dos vetores a, b, c tem determinante diferente de 0. Isso significa que $\mathbb{K}^3 =< a, b, c >$.

Para concluírmos, seja $M \in A_e$, então $M = T^{-1}(d); d \in \mathbb{K}^3 \Rightarrow M = T^{-1}(xa + yb + zc)$ com $x, y, z \in \mathbb{K}$, isto é, $xT^{-1}(a) + yT^{-1}(b) + zT^{-1}(c) = M \Rightarrow xI_d + yB + zB^2 = M$, portanto, $A_e =< I_d, B, B^2 >$. Logo, $\{I_d, B, B^2\}$ é base para A_e e o resultado se segue.

■

Teorema 3.1.2 *A_e é uma extensão normal de $\mathbb{K}$*

Demonstração: Conforme a definição de extensão normal, devemos mostrar que dado um polinômio irredutível em $\mathbb{K}[x]$ que contenha, pelo menos uma raiz em A_e, têm todas as suas raízes em A_e. No nosso caso vamos analisar essa propriedade para μ_B e o resultado se seguirá para os demais polinômios que contenham raízes em A_e, visto que $\mathbb{K}[B] = A_e$.

Tome $X \in A_c$ não nulo, temos pela proposição 1.8 que X é invertível. Mostremos agora que $A_c = XA_e$ e $A_{c^2} = X^2 A_c$:

$A_c = XA_e$ se, e somente se, $X^{-1}A_c = A_e$. De fato, seja $M \in A_e$, veja que $XM = N \in A_c$, assim $M = X^{-1}N \in X^{-1}A_c$, portanto $A_e \in X^{-1}A_c$. Além disso, como consequência da definição de G-graduações, vale que $X^{-1}A_c \subseteq A_c A_{c^{-1}} \subseteq A_{cc^{-1}} = A_e$, isso completa o nosso argumento de que $X^{-1}A_c = A_e$ e, com isso, temos que $A_c = XA_e$. De modo análogo, obtemos $A_{c^2} = X^2 A_c$.

Portanto, $\phi_X : A_e \to A_e$, definido por $\phi_X(U) = XUX^{-1}$ é um automorfismo de A_e pelo Lema 2.1.2. ϕ leva elementos de A_e em A_e da própria definição de graduação, uma vez que se $X \in A_c \to X^{-1} \in A_{c^{-1}}$ e $A_c A_e \subset A_c$ e $A_c A_{c^{-1}} \subseteq A_{cc^{-1}} = A_e$. Visto que A_e tem estrutura de corpo, dadas $M, N \in A_e$ vale que $MN = NM$. Por outro lado, se $Y, Z \in M_3(\mathbb{K})$ então existem matrizes $u_i, u_i^{'} \in A_e$ tais que: $Y = u_1 + Xu_2 + X^2 u_3$ e $Z = u_1^{'} + Xu_2^{'} + X^2 u_3^{'}$. Se ϕ_X é identidade, então isso significa que X comuta com todas as matrizes de A_e, donde A_e é comutativo. Daí concluímos que $YZ = ZY$ implicando que nossa álgebra é comutativa, absurdo. Logo, $\phi_x \neq I_d$

Por outro lado, $\mu(UBU^{-1}) = X\mu(B)X^{-1} = 0$, leva B em uma matriz semelhante, ou seja, ϕ leva uma raiz de μ_B em uma outra raiz do mesmo. Em particular, $\phi \in Aut_{\mathbb{K}} A_e$,ou seja leva B em XBX^{-1} que é uma outra raiz. Com $|Aut_{\mathbb{K}}A_e| = 3$ e $Aut_{\mathbb{K}}A_e \simeq S_n$, deve valer que $Aut_{\mathbb{K}}A_e = \{id, \phi, \phi^2\}$, por outro lado, $\phi^2 = XB^2X^{-1}$ que é a terceira raiz de μ_B. Logo todas as raízes desse polinomio estão em A_e.

Como $\mathbb{K}[B] = A_e$, vale que A_e é uma extensão normal de $\mathbb{K}$ ■

Teorema 3.1.3 *A_e é uma extensão separável de $\mathbb{K}$.*

Demonstração: A_e é separável se, e somente se, $\forall M \in A_e; \exists f(x) \in \mathbb{K}[X]; f(M) = 0$ e $f(M)$ é decomposto em raízes simples em qualquer extensão. Já sabemos que A_e é uma extensão normal pelo item anterior, ou seja, se tal f existe ele será decomposto totalmente em A_e, nossa trabalho é mostrar a existência de f bem como a sua decomposição simples em A_e.

Suponha, por absurdo, que A_e não é separável. Assim, deve existir $M \in A_e$, tal que $\forall f(x) \in \mathbb{K}[x]; f(M) = 0$ no qual f tem raízes múltiplas em A_e. Em particular, μ_M tem raízes múltiplas em A_e. Sabemos que as matrizes da forma λI_3 não entram nessa hipótese, visto que nesse caso μ_M tem grau 1. Também não devemos analisar o caso em que μ_B tem grau 2, pois nesse caso usando a função ϕ da demonstração anterior teríamos que $\mu_M = (T - M)(T - XMX^{-1})$ e seria totalmente decomposto em raízes simples. Por tanto, nos atentemos ao caso em que μ_M tem grau 3.

Para o caso em que $Char(\mathbb{K}) = 3$, temos que $\mu_M = T^3 + \alpha T^2 + \beta T + \lambda$, se esse polinômio tem a raiz M com multiplicidade 2 ou 3, vale, por propriedades da derivada formal, que: $\mu'_M = 3M^2 + 2\alpha M = 0$, então μ_M tem grau 2, um absurdo.

Para o caso em $Char(\mathbb{K}) \neq 3$ é suficiente analisar a condição de separável para os polinômios minimais de M (onde $M \in A_e$). Para isso, como $char(\mathbb{K}) \neq 3$, note que a função ϕ definida na demonstração anterior é um elemento de $Aut_{\mathbb{K}}A_e$, então todas as raízes de μ_M são simples, pois o grupo de Galois associado à A_e é o $\mathbb{Z}_3$. Pelo fato de μ_M ter grau três sua decomposição deve ser simples. ■

Nessa primeira seção mostramos que essa componente homogênea detém propriedades muito específicas. O primeiro resultado implicou que A_e atende a todas as propriedades de corpo, qualquer. Pelo fato de $A_e = \mathbb{K}[B], B \in A_e$. Em seguida provamos um belo fato: que dado um polinômio de coeficientes em $\mathbb{K}$ que tenha uma raiz em A_e então ele é totalmente decomposto em A_e e essa análise foi feita sobre os polinômios minimais, visto que se $P(B) = 0 \Rightarrow P(\lambda) = Q(\lambda)\mu_B(\lambda)$. E mais ainda, essa decomposição não ocorre de qualquer maneira, ela determina um produto de monômios em suas raízes e, como vimos, a análise foi feita sobre os polinômios minimais, uma vez que se P tem uma raiz e , portanto todas, as raízes em A_e ele deve ser escrito como $P = \mu_{N_1}\mu_{N_2}...\mu_{N_k}; N_i \in A_e$. A estratégia de mostrar essa decomposição simples em cada minimal mostra que a decomposição de P deverá certamente ser simples, logo a extensão é também separável.

Essa particularidade de A_e mostra que ele é uma extensão normal e separável. Esses tipos de extensões assim construídas, como podemos perceber, são corpos extremamente "pequenos"e que contém todas as raízes de um polinômio em $\mathbb{K}$ desde que ele contenha pelo menos uma. Quando isso ocorre, a extensão recebe um nome especial: "extensão de Galois". Durante as demonstrações dessa seção, utilizamos muito o grupo de Galois $Aut_{\mathbb{K}}A_e$ e de fato, para cada extensão de Galois existe sempre um desses grupos que fazem o papel de "permutadores"das raízes do polinômio simplesmeste decomposto. Por isso dizemos que $Aut_{\mathbb{K}}A_e$ é o "grupo de Galois associado à A_e "e como estamos trabalhando em dimensão 3, $Aut_{\mathbb{K}}A_e = 3$.

Dados esses comentários e resultados da seção, estamos aptos a construir uma $\mathbb{Z}_3$-graduação em $M_3(\mathbb{K})$.

3.2 Construindo uma $\mathbb{Z}_3$-graduação ($char(\mathbb{K}) \neq 3$)

Agora iremos começar a trabalhar com as nossas graduações em $\mathbb{Z}_3 \times \mathbb{Z}_3$ e em $\mathbb{Z}_3$ em termos da teoria de Galois. . Em um artigo de 1987 intitulado : "A characterization of Galois field extensions of degree 3", os autores Kersten e Miachalicek provam que uma extensão cúbica L de Galois de um corpo $\mathbb{K}$ é o corpo de divisão do polinômio : $P_a = T^3 - aT^2 + (a-3)T + 1$, onde $a \in \mathbb{K} - \{\frac{t^3-3t+1}{t^2-t}, \forall t \notin \{0,1\}\}$. Em outras palavras, P_a é irredútivel.

Tal como foi definido, se α for uma raiz de P_a então as suas outras raízes são: $\frac{1}{1-\alpha} = 2 + (a-1)\alpha - \alpha^2$ e $\frac{\alpha-1}{\alpha} = \alpha^2 - a\alpha + (a-2)$. Como a extensão de Galois é cúbica, seu grupo de Galois associado é $S_3 = \{i_d, \sigma, \sigma^2\}$, onde $\sigma(\alpha) = \frac{1}{1-\alpha}$.

A partir desse resultado que iremos admitir sem a sua demonstração enfadonha, iremos construir uma $\mathbb{Z}_3$-graduação com uma raiz de P_a sendo a seguinte matriz: $B_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix}$.

Teorema 3.2.1 *Seja* $B_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix}$, *então* B_a *é uma raiz de* P_a

Demonstração: Para isso basta mostrar que: $(B_a)^3 - a(B_a)^2 + (a-3)(B_a) + 1 = 0$. De fato, o polinômio característico $C_{Ba} = -P_a$. A menos do sinal, vamos considerar P_a seu polinômio característico, pelo fato de ser o polinômio característico e irredútivel ele também é o minimal. ■

Dessa forma, sendo B_a uma raiz de P_a, vamos usar o resultado de Kersten e Michalicek sobre as raízes de P_a, ou seja, que $\sigma(B_a) = (I_3 - B_a)^{-1} = 2I_3 + (a-1)B_a - (B_a)^2 =$

$-B^2+(a-1)B_a+2I_3$, onde $\sigma(B_a)=(I_3-B_a)^{-1}=2I_3+(a-1)B_a-(B_a)^2=\begin{pmatrix}2 & a-1 & -1\\ 1 & a-1 & -1\\ 1 & a-2 & -1\end{pmatrix}$.

Observação 3.2.2 *Dada uma matriz qualquer em $M_3(\mathbb{K})$ podemos escrevê-la na notação de matriz composta em colunas de vetores de 3 elementos (dizemos que estes são elementos de V_3). Por exemplo, a matriz:*

$$\begin{pmatrix}2 & a-1 & -1\\ 1 & a-1 & -1\\ 1 & a-2 & -1\end{pmatrix}$$

Pode ser escrita sob a forma $(V_1|V_2|V_3)$, onde:

$$V_1=\begin{pmatrix}2\\1\\1\end{pmatrix},V_2=\begin{pmatrix}a-1\\a-2\\a-2\end{pmatrix}V_3=\begin{pmatrix}-1\\-1\\-1\end{pmatrix},$$

Como $[B_a]=\{\alpha I_3+\beta B_a+\gamma B_a^2\}$ é um corpo e uma extensão de $\mathbb{K}$ ele deverá ser, consequentemente, o corpo de divisão de P_a pelo resultado dos autores citados. A partir desse corpo, aparentemente inóquo, construiremos uma componente homogênea de grau e e, com as demais raízes de P_a, construiremos uma componente de grau c e uma de grau c^2. Sabemos que $dim(\mathbb{K}[B_a])=3$, e veremos que o mesmo vale para as demais componentes que serão definidas.

Lema 3.2.3 *Assuma que $char(\mathbb{K})\neq 3$. Seja $a\in\mathbb{K}$ tal que $a\neq\frac{t^3-3t+1}{t^2-t}$ para todo $t\in\mathbb{K}-[0,1]$. Então*

$$\mathbb{K}[B_a]=\{(V|(aB_a-(B_a)^2)V|-B_aV);V\in V_3\}$$

Demonstração: Vamos denotar por $\Delta_a=\{(V|(aB_a-B_a^2)V|-B_aV);V\in V_3(\mathbb{K})\}$. Vale que:

$$aB_a-B_a^2=\begin{pmatrix}0 & a & 0\\ 0 & 0 & a\\ -a & (3-a)\,a & a^2\end{pmatrix}-\begin{pmatrix}0 & 0 & 1\\ -1 & 3-a & a\\ -a & (3-a)\,a-1 & a^2-a+3\end{pmatrix}=\begin{pmatrix}0 & a & -1\\ 1 & a-3 & 0\\ 0 & 1 & a-3\end{pmatrix}$$

Se considerarmos $V=\begin{pmatrix}x\\y\\z\end{pmatrix}$, temos as seguintes relações:

$$(i)(aB_a - B_a^2)V = \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & a \\ -a & (3-a)\,a & a^2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ay - z \\ x + (a-3)y \\ y + (a-3)z \end{pmatrix}$$

$$(ii) - B_aV = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & a-3 & -a \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -y \\ -z \\ x + (a-3)y - az \end{pmatrix}$$

Como $\Delta_a = \{(V|(aB_a - B_a^2)V| - B_aV); V \in V_3(\mathbb{K})\}$, poderemos reescrevê-lo sob a forma: $\Delta_a = \{U_{x,y,z}; x, y, z \in K\}$, onde

$$U_{x,y,z} = \begin{pmatrix} x & ay - z & -y \\ y & x + (a-3)y & -z \\ z & y + (a-3)z & x + (a-3)y - az \end{pmatrix}$$

Com isso, vale que $I_3 = U_{1,0,0}, B_a = U_{0,0,-1}$ e $B_a^2 = U_{0,-1,-a}$, portanto, temos que $\mathbb{K}[B_a] \subseteq \Delta_a$. Por outro lado $\mathbb{K}[B_a] =< I_3, B_a, B_a^2 >$, visto que o grau de P_a é igual à 3. Como $\mathbb{K}[B_a]$ e Δ_a tem dimensão 3 sobre $\mathbb{K}$, podemos concluir que $\mathbb{K}[B_a] = \Delta_a$

$\blacksquare$

Essa caracterização de $\mathbb{K}[B_a]$ será muito útil quando estivermos trabalhando com sistemas lineares devido ao vetor V ser "livre"na primeira coluna dessa matriz. Em seguida, iremos construir uma $\mathbb{Z}_3$-graduação em que cada componente será dada em termos semelhantes à essa caracterização de $\mathbb{K}[B_a]$. O próximo resultado trará à luz do nosso trabalho uma nova graduação não isomorfa à uma boa graduação. Assim como veremos, essas componentes homogêneas são determinadas pelas raízes de P_a, ou seja, B_a (que já temos definida), $\sigma(B_a)$ e $\sigma^2(B_a)$.

Lembremos que:

$$B_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix}, \sigma(B_a) = \begin{pmatrix} 2 & a-1 & -1 \\ 1 & a-1 & -1 \\ 1 & a-2 & -1 \end{pmatrix}$$

Teorema 3.2.4 *Assuma que char*$(\mathbb{K}) \neq 3$. *Seja* $a \in \mathbb{K}$ *tal que* $a \neq \frac{t^3-3t+1}{t^2-t}$ *para todo* $t \in$

$\mathbb{K} - \{0, 1\}$. *Seja*

$$A_e = \{(V|(aB_a - (B_a)^2)V| - B_aV); V \in V_3\}$$

$$A_c = \{(V|(a\sigma B_a - \sigma(B_a)^2)V| - \sigma(B_a)V); V \in V_3\}$$

$$A_{c^2} = \{(V|(a\sigma^2 B_a - (\sigma^2(B_a))^2)V| - \sigma^2(B_a)V); V \in V_3\}$$

Então $A(a)_e + A(a)_c + A(a)_{c^2} = M_3(\mathbb{K})$*, que é uma soma direta e* $A(a) = \oplus_{g\in Z_3} A(a)_g$ *é uma estrutura algébrica* $\mathbb{Z}_3$*-graduada em* $M_3(\mathbb{K})$*, que não é isomorfa a boa graduação.*

Demonstração: Pelo Lema 3.2.3, $A(a)_e = \mathbb{K}[B_a]$. Seja $X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix}$. Veja que $X^3 = I_3$.

Além disso, vale a seguinte igualdade:

$$XB_aX^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix} \begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & a-1 & -1 \\ 1 & a-1 & -1 \\ 1 & a-2 & -1 \end{pmatrix} = \sigma(B_a)$$

E teremos que: $(XB_aX^2)X = \sigma(B_a)X \implies XB_a = \sigma(B_a)X(1)$.

Se $U \in \mathbb{K}[B_a]$ devemos ter que $U = \alpha I_3 + \beta B_a + \lambda B_a^2 \implies XU = X(\alpha I_3 + \beta B_a + \lambda B_a^2) = \alpha X I_3 + \beta X B_a + \lambda X B_a B_a$. Por (1), devemos ter que: $XU = \alpha X I_3 + \beta\sigma(B_a)X + \lambda\sigma(B_a)XB_a$, como $I_3 \in K$, então: $XU = \alpha X\sigma(I_3) + \beta\sigma(B_a)X + \lambda\sigma(B_a)XB_a = \alpha\sigma(I_3)X + \beta\sigma(B_a)X + \lambda\sigma(B_a)\sigma(B_a)X = \alpha\sigma(I_3)X + \beta\sigma(B_a)X + \lambda\sigma(B_a)^2X = \alpha\sigma(I_3)X + \beta\sigma(B_a)X + \lambda\sigma(B_a)^2X = (\alpha\sigma(I_3) + \beta\sigma(B_a) + \lambda\sigma(B_a)^2)X$, como σ é um automorfismo vale, finalmente, que: $XU = (\sigma(\alpha I_3 + \beta(B_a) + \lambda(B_a)^2))X = \sigma(U)X; \forall U \in \mathbb{K}[B_a]$. Assim, $XK[B_a] = K[B_a]X$ e, consequentemente, $\forall V \in V_3(\mathbb{K})$ temos que:

$$X(V|(aB_a - B_a^2)V| - B_aV) =$$

$$(XV|X(aB_a - B_a^2)V|X(-B_aV)) =$$

$$(XV|(aXB_a - XB_a^2)V|((-XB_a)V) =$$

$$(XV|((a\sigma(B_a)X - \sigma(B_a)^2X)V|((-\sigma(B_a)X)V) =$$

$$(XV|(a\sigma(B_a) - \sigma(B_a)^2)XV|((-\sigma(B_a))XV) = X(V|(a\sigma(B_a) - \sigma(B_a)^2)V|((-\sigma(B_a))V) = XA_e$$

Como $XV \in V_3(\mathbb{K})$ temos que $A(a)_c = XA(a)_e$. Como σ é automorfismo, vale que $\sigma(U) \in A_e; \forall U \in A_e \implies XA_e = A_eX$ (a igualdade decorre da bijetividade de σ).

Devemos ter que $\sigma^2(B_a) = (B_a - I_3)B_a^{-1}$, já que $\sigma^2 \in Aut_{\mathbb{K}}(\mathbb{L})$. Logo σ leva uma raiz de P_a em uma outra raiz tal que $\sigma^2(B_a) \neq \sigma(B_a)$, caso contrário teríamos $\sigma(B_a) = B_a$, o que é uma contradição.

De modo análogo, teremos que $A(a)_{c^2} = X^2A(a)_e = A(a)_eX^2$. Consequentemente, $X^2A(a)_e = A(a)_eX^2$. Assim, $A_eA_e = K[B_a]K[B_a] \subseteq K[B_a] = A_e; A_cA_e = (XA(a)_e)A(a)_e \subseteq XA_e = A_c; A_{c^2}A_c = (X^2A(a)_e)XA(a)_e = X^2(A_eX)A_e = X^2(XA(a)_e)A_e = (X^3)(A_eA_e) = (A_eA_e) \subseteq A_e$. Nesse ponto, concluímos uma parte da demonstração, ou seja, que $A(a)_e, A(a)_c, A(a)_{c^2}$ tem um "bom comportamento"em relação à multiplicação de componentes da graduação.

Resta, portanto, mostrar que a soma: $A(a)_e + A(a)_c + A(a)_{c^2} = M_3(K)$ é direta.

Veja que $dim(A(a)_e) = dim(A(a)_c) = dim(A(a)_{c^2}) = 3$, logo nosso dever agora é mostrar que são partes disjuntas, isso equivale à mostrar que na equação:

$$Z_e + Z_c + Z_{c^2} = 0$$

onde $Z_e = (V_1|(aB_a - (B_a)^2)V_1| - B_aV_1) \in A(a)_e, Z_c = (V_2|(a\sigma(B_a) - \sigma(B_a)^2)V_2| - \sigma(B_a)V_2) \in A(a)_c$ e $Z_{c^2} = [(V_3|(a\sigma^2B_a - (\sigma^2(B_a))^2)V_3| - \sigma^2(B_a)V_3) \in A_{c^2}$. Ao efetuarmos essa soma, devemos ter a seguinte expressão:

$$Z_e + Z_c + Z_{c^2} = 0 \Leftrightarrow$$

$$(V_1+V_2+V_3|(aB_a-(B_a)^2)V_1+(a\sigma(B_a)-\sigma(B_a)^2)V_2+(a\sigma^2B_a-(\sigma^2(B_a))^2)V_3|(B_a)^2V_1+\sigma(B_a)^2V_2+\sigma^2(B_a)V_3) =$$

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

Tal igualdade matricial tem solução se, e somente se:

$$V_1 + V_2 + V_3 = 0$$

$$(aB_a - (B_a)^2)V_1 + (a\sigma(B_a) - \sigma(B_a)^2)V_2 + (a\sigma^2B_a - (\sigma^2(B_a))^2)V_3 = 0$$

$$(B_a)^2V_1 + \sigma(B_a)^2V_2 + \sigma^2(B_a)V_3 = 0$$

Reescrevendo nosso sistema sob a forma matricial:

$$\begin{pmatrix} I_3 & I_3 & I_3 \\ aB_a - (B_a)^2 & a\sigma B_a - \sigma(B_a)^2 & a\sigma^2B_a - (\sigma^2B_a)^2 \\ B_a & \sigma B_a & \sigma^2B_a \end{pmatrix} \begin{pmatrix} V_1 \\ V_2 \\ V_3 \end{pmatrix} = 0$$

A primeira matriz M, via operações de linha (-al_3+l_2) é equivalente a seguinte matriz N:

$$\begin{pmatrix} I_3 & I_3 & I_3 \\ -(B_a)^2 & a-\sigma(B_a)^2 & -(\sigma^2 B_a)^2 \\ B_a & \sigma B_a & \sigma^2 B_a \end{pmatrix}$$

Como o determinante é invariante por operações linha-operações, vale que $det(M) = det(N)$. Por outro lado $det(N) = (\sigma(B_a) - B_a)(\sigma^2(B_a) - B_a)(\sigma^2(B_a) - \sigma(B_a))$. Lembremos que $B_a, \sigma(B_a), \sigma^2(B_a)$ são distintas e que todas pertencem à A_e, mas A_e é um anel de divisão graduado (como já mostramos), então $det(N) = (\sigma(B_a)-B_a)(\sigma^2(B_a)-B_a)(\sigma^2(B_a)-\sigma(B_a)) \neq 0$. Da condição de A_e ter estrutura de corpo, vale que o sistema possui solução única e determinada, a saber: $V_1 = V_2 = V_3 = 0$, e isso significa que $A_e + A_c + A_{c^2}$ é uma soma direta. Portanto, $A(a)$ é uma estrutura algébrica $\mathbb{Z}_3$-graduada em $M_3(\mathbb{K})$.

Para concluir essa demonstração resta mostrar que, de fato, tal graduação não é isomorfa à uma boa graduação, para isso vamos usar, inicialmente, o fato que X é invertível e todo elemento de $A(a)_e$ também é. Como $A(a)_c = XA(a)_e$ vale que todo elemento de $A(a)_c$ também é invertível, além disso, $A(a)_{c^2} = X^2A(a)_e$, donde $X^2 = X^{-1}$, logo todo elemento de $A(a)_{c^2}$ é invertível. Ora, então $A(a)_e, A(a)_c$ e $A(a)_{c^2}$ são anéis de divisão graduados, em particular e_{11} não é invertivel, portanto $A(a)$ não pode ser uma boa graduação, e será, portanto, uma $\mathbb{Z}_3$-graduação por um resultado anterior. ∎

Agora que já construímos uma $\mathbb{Z}_3$-graduação não isomorfa à uma boa graduação da forma $A(a)$ com $a \neq \frac{t^3-3t+1}{t^2-t}$, iremos mostrar na próxima proposição um fato ainda mais profundo, que cada $\mathbb{Z}_3$-graduação não isomorfa à uma boa graduação deve ser isomorfa à uma do tipo $A(a)$, sob essas mesmas condições. Dividiremos a discussão para o caso em que $char(\mathbb{K}) \neq 3$ e, posteriormente, para o caso contrário, visto que o fato de A_e ser uma extensão cúbica de Galois dividiu a discussão para esses dois casos.

Teorema 3.2.5 *Assuma que $char(\mathbb{K}) \neq 3$. Seja $A = \oplus_{g\in\mathbb{Z}_3} A_g$ uma $\mathbb{Z}_3$-graduação de $M_3(\mathbb{K})$ não isomorfa à uma boa graduação. Então existe $a \in \mathbb{K}, a \neq \frac{t^3-3t+1}{t^2-t}$ para todo $t \in K - [0,1]$, tal que $A \simeq A(a)$.*

Demonstração: Como queremos mostrar que a graduação será isomorfa à uma graduação da forma $A(a)$, lembremos que essa última é definida pelas componentes:

$$A_e = \{(V|(aB_a - (B_a)^2)V| - B_aV); V \in V_3\}$$

$$A_c = \{(V|(a\sigma B_a - \sigma(B_a)^2)V| - \sigma(B_a)V); V \in V_3\}$$

$$A_{c^2} = \{(V|(a\sigma^2 B_a - (\sigma^2(B_a))^2)V| - \sigma^2(B_a)V); V \in V_3\}$$

Pelo Teorema 2.4.3, A_e é um anel de divisão, logo $dim(A_g) = 3, \forall g \in Supp(A)$, pela Proposição 3.1.2 A_e é uma extensão de Galois de $\mathbb{K}$, então, $A_e = \mathbb{K}[B]; \delta(\mu_B) = 3$. Usando novamente o resultade de Kersten e Machaliceck, se $A_e = \mathbb{K}[B]$ é uma extensão cúbica de Galois de , então $A_e = Gal(P_a(T), \mathbb{K})$, com $P_a(T) = \mu_B$. Da Proposição 3.1.2, vimos que: $A_e = K[B]$, como já mostramos, as propriedades do conjunto A_e uma das raízes do minimal de B, nesse caso caracterizado como $P_a(T)$, é a sua forma de Jordan J_B, então se $B_a \neq B$ deve valer a igualdade para a forma de Jordan correspondente, então $J_B = B_a$, consequentemente, $A_e = K[B_a]$.

Para todo elemento homogêneo não nulo X de A seja $\phi_X : A_e \to A_e, \phi_X(U) = XUX^{-1}$. Ainda pela proposição citada no parágrafo anterior, sabemos que $\phi_X \neq Id$ para todo $X \in A_c \cup A_{c^2}$, do caso contrário como vimos na prova desse resultado, teríamos que $M_3(\mathbb{K})$ é uma álgebra comutativa. Veja que $\phi(K) = XKX^{-1} = XX^{-1}K = K, \forall K \in \mathbb{K}$, como já mostramos, vale também que ϕ é um automorfismo em A_e, então $\phi \in Aut_{\mathbb{K}}(A_e) = \{I_d, \sigma, \sigma^2\}$. Se para alguns $X, Y \in A_c - \{0\}$ tivermos que $\phi_X = \sigma$ e $\phi_Y = \sigma^2$, então $\phi_{XY}(U) = XYU(XY)^{-1} = (XY)U(Y^{-1}X^{-1}) = X(YUY^{-1})X^{-1} = \phi_x \circ \phi_y = Id$.

Assim, podemos considerar: $A_c^2 = XYA_e$ e $A_c = (XY)^2 A_e$, isso se deve ao fato de que A_c^2 é um anel de divisão graduado e a prova é análoga à que usamos para mostrar que se $X \in A_c \implies A_c = Xa_e$ e $A_c^2 = X^2 A_e$. Dessa forma, dados $u \in M_3(\mathbb{K})$ e U_i, U_i' elementos das componentes da graduação sabemos que: $U = U_1 + (XY)^2 U_2 + (XY)U_3, U' = U_1' + (XY)^2 U_2' + (XY)U_3'$, como A_e é corpo, segue imediatamente que $UU' = U'U$. Novamente, $M_3(\mathbb{K})$ seria comutativa, um absurdo. Concluímos que ou $\phi = \sigma$ ou $\phi = \sigma^2, \forall X \in A_c$.

A partir desse momento, vamos analisar o que ocorre em cada um dos casos separadamente. Vamos começar pelo caso em que $\phi_X = \sigma$, para todo $X \in A_c$.

Assuma, incialmente que $\phi_X = \sigma$ para todo $X \in A_c$, Portanto $XB_a = \sigma(B_a)X$ para todo $X \in A_g$, visto que $\phi_x(B_a) = XB_aX^{-1}$. Como $\phi_X = \sigma$, vale que $\phi_x(B_a) = \sigma(B_a)$, assim $Xb_aX^{-1} = \sigma(B_a) \Leftrightarrow XB_a = \sigma(B_a)X$. Seja $X = (V_1|V_2|V_3)$ onde:

$$V_1 = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, V_2 = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}, V_3 = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}$$

Lembrando que $B_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix}$, devemos ter que:

$$XB_a = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix} = \begin{pmatrix} -z_1 & (3-a)\; z_1 + x_1 & a\, z_1 + y_1 \\ -z_2 & (3-a)\; z_2 + x_2 & a\, z_2 + y_2 \\ -z_3 & (3-a)\; z_3 + x_3 & a\, z_3 + y_3 \end{pmatrix} =$$

$$(-V_3|V_1 + (3-a)V_3|V_2 + aV_3)$$

.

Por outro lado, $\sigma(B_a)X = (\sigma(B_a)V_1|\sigma(B_a)V_2|\sigma(B_a)V_3)$. Portanto, $XB_a = \sigma(B_a)X \Leftrightarrow V_3 = -\sigma(B_a)V_1$, dai segue que $V_2 = -aV_3 + \sigma(B_a)V_3 = a\sigma(B_a)V_1 - \sigma(B_a)^2V_1 = (a\sigma(B_a) - \sigma(B_a)^2)$. Assim, obtemos a seguinte relação entre A_c e $A(a)_c$:

$$A_c \subseteq [(V|(a\sigma(B_a) - \sigma(B_a)^2)V| - \sigma(B_a)V; V \in V_3] = A(a)_c.$$

Assim, $dim(A_c) = 3 \implies A_c = A(a)_c$. Usando argumentos análogos, encontramos que: $A_{c^2} = XA_c = A(a)_c = A(a)_{c^2}$ mostrando que $A = A(a)$.

Agora vamos analisar o segundo caso: $\phi_X = \sigma^2, \forall X \in A_c$. Sabemos que $A_e = A(a)_e$ e, com cálculos análogos aos feitos com σ, temos as mesmas propriedades para σ^2 e, consequentemente, $A_c = A(a)_c^2$ e $A_c^2 = A(a)_c$.

Seja $H = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ e $f : A(3-a) \to A; f(Z) = HZH$

Note que:

$$H^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Dessa forma, $H^2 = I_3$, e a função assim definida é um isomorfismo pelo Lema 2.1.2. Assim, Podemos caracterizar f como um automorfismo de $M_3(\mathbb{K})$ associado à H.

Veja que as seguintes relações são válidas:

$$B_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix} \Rightarrow B_{(3-a)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & a & 3-a \end{pmatrix}$$

Então:

$$HB_{3-a}H = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & a & 3-a \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 3-a & a & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = B_a^{-1}$$

Como $\mathbb{K}[B_{3-a}] =< I_3, B_{3-a}, (B_{3-a})^2 >$, deve valer que: $HYH = H(\alpha I_3 + \beta B_{3-a} + (B_{3-a})H = H\alpha I_3 H + H\beta B_{3-a}H + H(B_{3-a}H$, para $Y \in \mathbb{K}[B_a], \alpha, \beta, \lambda \in \mathbb{K}$. Usando o fato de que $H^2 = I_3 \Rightarrow H = H^{-1}$ e que $HB_{3-a}H = B_a^{-1}$. Devemos ter $HYH = \alpha I_3 + \beta B_a^{-1} + \lambda(H(B_{3-a}H)(H(B_{3-a}H) = \alpha I_3 + \beta B_a^{-1} + \lambda B_a^{-2}$. Ora $\mathbb{K}[B_a]$ é um corpo, portanto, B_a^{-1} e B_a^{-2} são elementos de $\mathbb{K}[B_a]$, o que implica que $Y \in \mathbb{K}[B_a]$. Logo, podemos afirmar que $H\mathbb{K}[B_{3-a}]H \subseteq \mathbb{K}[B_a]$.

Vale que $dim(\mathbb{K}[B_a]) = 3 = dim(H\mathbb{K}[B_{3-a}]H)$ pelo fato de f ser um isomorfismo. Portanto, obtemos a seguinte igualdade: $H\mathbb{K}[B_{3-a}]H = \mathbb{K}[B_a]$, ou seja, $f(A(3-a)_e) = A_e$, dada a caracterização de $A_e = \mathbb{K}[B_a]$ e $\mathbb{K}[B_{3-a}] = A(3-a)$.

Vamos definir: $X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix}$

A matriz X assim definida determina as componentes homogêneas $A(a)_c$ e $A(a)_{c^2}$, como vimos no Teorema 3.2.4. Como $A(3-a)$ também é uma $\mathbb{Z}_3$-graduação, X determina também as demais componentes além de $A(3-a)_e$.

Dessa forma, vemos que:

$$HXH = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = X^2$$

Em particular vale que $HX = X^2H$. A partir dessa relação, podemos deduzir,dada definição de f, que $f(A(3-a)_c) = HA(3-a)_cH$, retomando que $A(3-a)_c = XA(3-a)_e$, então $HA(3-a)_cH = HXA(3-a)_eH = X^2HA(3-a)_eH$, e como já demonstramos $HA(3-a)_eH = A_e$, logo $HA(3-a)_cH = X^2A_e = A_{c^2}$.

Assim mostramos que para $\phi_x = \sigma^2$ definida dessa forma temos que $A(3-a)_e \simeq A(a)_e$ e $A(3-a)_c \simeq A(a)_{c^2}$, pela f. Baseado em manipulações algébricas como no passo anterior a componente $A(3-a)_{c^2} \simeq A(a)_c$ e daí segue que $A(3-a)$ é uma $\mathbb{Z}_3$-graduação em $M_3(\mathbb{K})$ isomorfa à uma graduação da forma $A(a)$.

Isso conclui, finalmente, a demonstração desse teorema. ■

Acabamos de demonstrar um resultado muito forte no Teorema anterior. Já haviamos construído uma $\mathbb{Z}_3$-graduação pelo Teorema 3.2.4, e agora mostramos que, a menos de isomorfismos, essas são todas as graduações dessa classe, exceto as boas graduações. Diante à esse grande resultado cuja a prova é um tanto longa, criamos um esquema que resume os passos da prova.

I. Ultilizando um resultado de Kersten e Michaliceck, definimos uma matriz $B_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 3-a & a \end{pmatrix}$, cujo o polinômio característico irredútivel era: $P_a = T^3 - aT^2 + (a-3)T + 1$, onde $a \in \mathbb{K} - \{\frac{t^3-3t+1}{t^2-t}, \forall t \notin \{0,1\}\}$. Mostramos que o conjunto $\mathbb{K}[B_a]$ era um corpo e que, além disso, $A_e = \mathbb{K}[B_a]$

II. Com isso, no Teorema 3.2.4, construímos uma $\mathbb{Z}_3$-graduação de $M_3(\mathbb{K})$ a partir dessa matriz B_a. A qual chamamos de $A(a)$ e descrevemos as suas componentes homogêneas como:

$$A_e = \{(V|(aB_a - (B_a)^2)V| - B_aV); V \in V_3\}$$

$$A_c = \{(V|(a\sigma B_a - \sigma(B_a)^2)V| - \sigma(B_a)V); V \in V_3\}$$

$$A_{c^2} = \{(V|(a\sigma^2 B_a - (\sigma^2(B_a))^2)V| - \sigma^2(B_a)V); V \in V_3\}$$

Do Teorema 3.1.2 vimos que dado A_e, as demais componentes eram dadas por: $A_c = XA_e$ e $A_{c^2} = X^2A_e$. Para esse fato particular, encontramos uma matriz X da forma: $X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix}$. Essa matriz foi fundamental na prova desse resultado e no resultado seguinte.

III. Mostramos que, de fato, $A(a)$ determina uma estrutura de álgebra graduada para $M_3(\mathbb{K})$. Ainda no Teorema 3.2.4 mostramos que essa estrutura não é isomorfa à uma boa graduação, devido ao fato de que e_{11} não era um elemento homogêneo.

IV. Apresentamos o maior resultado dessa seção no Teorema 3.2.5, onde conseguimos demonstrar que a nossa construção anterior determina todas as graduações sobre $\mathbb{Z}_3$, a menos de isomorfismos. A partir do grupo $Aut_{\mathbb{K}}A_e \simeq S_3$, fizemos uma análise da função $\phi_X(U) = XUX^{-1}$ e tivemos que dividir a prova em duas partes essenciais.

IV'. Analisamos as possibilidades para o automorfismo ϕ_X que foram: I_d, σ, σ^2. Claramente, ϕ_X não pôde admitir o primeiro valor, pois caso admitisse, concluiríamos que $M_3(\mathbb{K})$ seria comutativa, o que é um absurdo, então verificamos as duas últimas possibilidades.

IV". No caso em que $\phi_X = \sigma$, provamos que a componente homogênea A_c era igual à $A(a)_c$. Com a matriz X as seguintes relações $A_{c^2} = XA_c = XA(a)_c = A(a)_{c^2}$ foram possíveis devido ao Teorema 3.1.2, mostrando assim que $A(a)_{c^2} = A(a)_c$. Com isso $A = A(a)$

IV"'. No último caso, $\phi_X = \sigma^2$, não tivemos uma igualdade imediata, então criamos um isomorfismo de $A(3-a)$ em A definido por: $f(Z) = HZH$, onde: $H = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ com a propriedade: $H^2 = I_3$. Por meio de algumas manipulações matriciais, mostramos uma igualdade "indireta"entre as componentes de $A(3-a)$ e A, tal como se segue: $A(3-a)_e \simeq A_e$, $A(a)_{c^2} \simeq A_c$ e, finalmente, $A(a)_c \simeq A_{c^2}$.

E isso conclui a nossa seção, não apenas com a construção de uma nova graduação não isomorfa à uma boa graduação, como também com um resultado que classifica essas novas graduações como da forma $A(a)$, ou seja, elas são únicas, a menos de isomorfismos. Claro que esse resultado, embora muito forte, ainda é bastante abstrato, pois a seguinte caracterização:

$$A_e = \{(V|(aB_a - (B_a)^2)V| - B_aV); V \in V_3\}$$

$$A_c = \{(V|(a\sigma B_a - \sigma(B_a)^2)V| - \sigma(B_a)V); V \in V_3\}$$

$$A_{c^2} = \{(V|(a\sigma^2 B_a - (\sigma^2(B_a))^2)V| - \sigma^2(B_a)V); V \in V_3\}$$

é muito bela numa perspectiva limitada à solução do nosso problema de Zelmanov. Porém, em termos computacionais e de aplicação em outras áreas, é mais razoável se trabalhar com uma definição concreta das matrizes, ou seja, é necessário descrever as matrizes que atuam como elementos homogêneos. Felizmente, é possível fazer essa descrição e dedicaremos a última seção deste capítulo para tal.

Antes de descrever os elementos homogêneos de forma concreta, resta ainda analisar o comportamento das $\mathbb{Z}_3$-graduações para corpos de característica 3, e faremos isso na nossa seção seguinte.

3.3 Construindo uma $\mathbb{Z}_3$-graduação ($char(\mathbb{K}) = 3$)

Nessa penúltima seção, iremos construir uma $\mathbb{Z}_3$-graduação para o caso em que $char(\mathbb{K}) = 3$. Vale ressaltar que não há nada que seja fortemente diferente dos resultados da seção anterior para esse caso. De fato, os passos são os mesmos com leves diferenças. Portanto, vamos incialmente lembrar o que fizemos resumidamente na seção anterior:

I. Construímos um corpo base $\mathbb{K}[B_a]$ pelo resultado de Kersten e Michaliceck.

II. Construímos uma $\mathbb{Z}_3$-graduação que chamamos de $A(a)$, onde impomos certas condições sobre o a.

III. Mostramos que, a menos de isomorfismos, toda $\mathbb{Z}_3$-graduação era isomorfa à uma graduação da forma $A(a)$ (quando a consideramos não isomorfa à uma boa graduação).

Esses passos vão nos nortear para a nossa conclusão análoga. Por isso, optamos por não apresentá-los em forma de teoremas, apenas indicando as principais diferenças para característica diferente de 3, e as explorando.

I. No livro "Algebra: A Graduate Course", de Serge Lang, o autor cita e prova um teorema conhecido como o Teorema de Artin-Schreier, que afirma que uma extensão cúbica de Galois de $\mathbb{K}$ é o corpo de decomposição de um polinômio da forma: $Q_a = T^3 - T - a; a \in \mathbb{K}, a \neq t^3 - t (t \in \mathbb{K})$. Assim como no resultado de Kersten e Michalicek em característica diferente de 3, aqui encontramos também uma matriz que tenha como polinômio caracterísiсo Q_a e a matriz, a saber, é:

$$C_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & 1 & 0 \end{pmatrix}$$

Como $det(C_a) \neq 0$, então $\mathbb{K}[C_a]$ é um corpo. Ele também determina a componente homogênea A_e, ou seja, $A_e = \mathbb{K}[C_a]$.

Outra propriedade relevante é que as demais raízes de Q_a são $C_a + I_3$ e $C_a + 2I_3$, onde no grupo $Aut_{\mathbb{K}}(A_e)$ $\sigma(C_a) = C_a + I_3$.

II. Agora que já definimos nossa componente homogênea A_e, vamos determinar as demais componentes em função da mesma. No caso de característica diferente de 3, $A_c = X\mathbb{K}[B_a]$ e $A_{c^2} = X^2\mathbb{K}[B_a]$, onde $X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix}$. Aqui usaremos uma matriz diferente, a dizer:

$$X_3 = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Com isso, as relações entre as componentes homogêneas em característica diferente de 3 também se seguram no caso em característica 3, ou seja: $A_e = \mathbb{K}[C_a], A_c = X\mathbb{K}[C_a]$ e $A_{c^2} = X^2\mathbb{K}[C_a]$.

O próximo passo será reconstruir o Teorema 3.2.4 para esses corpos.

No Teorema 3.2.4 dada a definição da matriz B_a e as relações entre as componentes homogêneas, construímos uma graduação que chamamos de $A(a)$, cujas componentes homogêneas eram definidas como:

$$A_e = \{(V|(aB_a - (B_a)^2)V| - B_aV); V \in V_3\}$$

$$A_c = \{(V|(a\sigma B_a - \sigma(B_a)^2)V| - \sigma(B_a)V); V \in V_3\}$$

$$A_{c^2} = \{(V|(a\sigma^2 B_a - (\sigma^2(B_a))^2)V| - \sigma^2(B_a)V); V \in V_3\}$$

onde σ e σ^2 eram os automorfismos de $Aut_{\mathbb{K}}(A(a)_e)$ que levavam B_a nas demais raízes de P_a, a dizer: $(I_3 - B_a)^{-1} = 2I_3 + (a-1)B_a - (B_a)^2$ e $(B_a - I_3)(B_a)^{-1} = (B_a)^2 - aB_a + (a-2)I_3$.

Em característica 3 vimos que essas raízes se reduzem à $C_a + I_3$ e $C_a + 2I_3$ e a nossa graduação a ser construída $A(a)$ será determinada da seguinte forma:

$$A_3(a)_e = \{((C_a^2 + 2I_3)V|C_aV|V); V \in V_3\} = \mathbb{K}\{C_a\}$$

$$A_3(a)_c = \{((C_a^2 + 2C_a)V|(C_a + I_3)V|V); V \in V_3\}$$

$$A_3(a)_c = [((C_a^2 + C_a)V|(C_a + 2I_3)V|V); V \in V_3]$$

Retomando a matriz X, que tem a propriedade de $X^3 = I_3$, faremos uma relação análoga à feita no Teorema 3.2.4. Estamos fazendo referência à conclusão de que $A(a)_c = XA(a)_e = A(a)_eX$ e $A(a)_{c^2} = X^2A(a)_e = A(a)_eX^2$, aqui ficamos com: $XC_a = (C_a + I_3)X, A_3(a)_c = XA_3(a)_e = A_3(a)_eX$.

Agora adaptaremos o Teorema 3.2.5 associado à esses corpos.

III. Como vimos, o Teorema 3.2.5 foi construído a partir do grupo dos automorfismos $Aut_{\mathbb{K}}(A_e)$ tomando $\phi_X = \sigma$, que qualquer $\mathbb{Z}_3$-graduação é da forma $A(a)$. No caso em que $\phi_X = \sigma^2$, não tivemos a mesma sorte, mas ainda conseguimos ganhar um isomorfismo entre $A(a)$ (a $\mathbb{Z}_3$-álgebra graduada em questão), definido por: $f : A(3-a) \to A; f(Z) = HZH$, onde: $H = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ com a propriedade: $H^2 = I_3$. Por meio de algumas manipulações matriciais, mostramos uma igualdade "indireta"entre as componentes de $A(3-a)$ e A, tal como se segue: $A(3-a)_e \simeq A_e$, $A(a)_{c^2} \simeq A_c$ e, finalmente, $A(a)_c \simeq A_{c^2}$.

No primeiro caso, não trabalhamos em momento algum com elementos da forma: $nx; n \in \mathbb{Z}, x \in \mathbb{K}$, em outras palavras não se fez necessária a análise da característica de $\mathbb{K}$. Portanto, o resultado se segue de modo totalmente análogo.

Em contrapartida, no segundo caso estamos falando de um isomorfismo entre $A(3-a)$ e A, mas a operação $3-a$ é uma operação em $\mathbb{K}$, isso significa que em corpos de característica 3 o isomorfismo deve ser entre $A(-a)$ e A. Agora vamos tomar uma matriz H e relembrar a configuração de C_a:

$$H_3 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} C_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & 1 & 0 \end{pmatrix}$$

Daí segue-se que:

$$C_{-a} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & 1 & 0 \end{pmatrix}$$

Note que:

$$H_3 C_{-a} H_3 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -2 & -1 \\ 3-a & -1 & 1 \end{pmatrix} \quad (3.1)$$

Por outro lado:

$$I_3 - C_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - C_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & 1 & 0 \end{pmatrix} = C_a = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ -a & -1 & 1 \end{pmatrix} \tag{3.2}$$

Nesse instante, se afirmarmos que as equações 3.1 e 3.2 são equivalentes, pode parecer a princípio algo um tanto quanto suspeito, uma vez que deveríamos ter $3-a = -a$ e $-2 = 1$, mas essas igualdades decorrem imediatamente do fato do corpo ter característica 3, assim $3-a = -a$ e $(3)(1) = 1+1+1 = 0 \Rightarrow -2 = 1$, e, de fato, as igualdades se seguem.

Assim, ao construirmos um homomorfismo $f : A(-a) \to A$, definido por $f(Z) = H_3 Z H_3$, deveremos ter que $f(\mathbb{K}[C_a]) = \mathbb{K}[C_a]$, além disso vamos usar a matriz X_3, definida como: $X_3 = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

Logo:

$$H_3 X_3 H_3 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 4 & -1 & 1 \end{pmatrix}$$

Mas temos ainda que:

$$X_3^2 = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix}$$

Novamente, de modo aparentemente audacioso, afirmamos que $H_3 X_3 H_3 = X_3^2$. Já vimos que em característica 3, -2=1, mas também, pelo mesmo motivo deve valer que $(4)(1) = 1+1+1+1 = (1+1+1)+1 = (3)(1)+1 = 1$, e a igualdade se segue.

Finalmente, observemos que:

$$H_3^2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix}$$

Pela característica de $\mathbb{K}$, podemos afirmar que $H_3^2 = I_3$. Dito isso, vemos que $H_3X_3H_3 = X_3^2 \Rightarrow H_3X_3 = X_3^2H_3$. Nesse ponto, podemos fazer uma comparação dos resultados obtidos com os resultados do teorema 3.2.5.

Lá encontramos uma certa matriz $H; H^2 = I_3$, da qual tínhamos $XH = X^2H$ para uma matriz X que fora definida. A função f do isomorfismo entre a dada $\mathbb{Z}_3$-graduação e a graduação construída (naquela ocasião f associava A com $A(3-a)$), tinha a propriedade de que $H\mathbb{K}[B_{3-a}]H = f(\mathbb{K}[B_{3-a}]) = \mathbb{K}[B_a]$. Aqui, nossas manipulações algébricas nos levaram a concluir os mesmos resultados. Construímos, inicialmente, $f(\mathbb{K}[C_a]) = \mathbb{K}[C_a]$ e por fim, vimos que $H_3X_3 = X_3^2H_3$. Naturalmente tudo segue de modo análogo como acontece em característica diferente de 3.

Portanto, podemos concluir que, assim como ocorre em característica diferente de 3, o argumento de que $A(-a)_e \simeq A_e$, $A(a)_{c^2} \simeq A_c$ e, finalmente, $A(a)_c \simeq A_{c^2}$, também valerá para esse caso.

Com isso, concluímos essa seção, mostrando que o comportamento de $\mathbb{Z}_3$-graduações em características 2 e 3, tem suas particularidades, porém o resultado segue de forma análoga em ambos os casos. Ou seja, todas as $\mathbb{Z}_3$-graduações, não isomorfas à uma boa graduação, devem ser todas da forma $A(a)$, a menos de isomorfismos. Como prometido, finalizaremos esse capítulo com uma descrição concreta dessa classe de graduações, isso irá nos permitir identificar melhor os elementos de cada uma de suas componentes homogêneas.

3.4 Uma descrição concreta das $\mathbb{Z}_3$-graduações

É muito comum em áreas de matemática pura, nos depararmos em algum momento com teoremas sobre a existência ou a unicidade de alguns objetos inerentes à mesma. A exemplo disso podemos citar o famoso Teorema do Valor Médio da análise que diz que: "Se f é uma função contínua em $[a, b]$ e derivável em $]a, b[$, então existe um número real c pertencente à $]a, b[$, tal que a reta tangente ao gráfico de f traçada pelo ponto $(c, f(c))$ é paralela à reta que passa por $(a, f(a))$ e $(b, f(b))$, isto é, $f'(c) = \frac{f(b)-f(a)}{b-a}$". O Teorema do valor médio garante um resultado esteticamente belo, uma vez que diz que existe um ponto no intervalo de definição da função no qual a variação média dela no intervalo inteiro é a variação instântanea da mesma nesse ponto. Porém ele não afirma nada sobre qual seja esse ponto, daí se torna necessária uma análise mais númerica e menos analítica.

O que fizemos nas duas últimas seções se encaixa nesse espírito de teoremas dessa natureza. Garantimos com as graduações da forma $A(a)$ a existência de $\mathbb{Z}_3$-graduações, não isomorfas às chamadas boas graduações e, em seguida, mostramos a sua unicidade, sempre enfatizando a questão de ser a menos de isomorfismos. Veja que seguimos a receita de bolo do Teorema do Valor Médio, e assim como nesse teorema, é natural se perguntar , quais são as matrizes de fato que pertencem às componentes. E nessa seção descreveremos todas as matrizes que atuam como elementos homogêneos nessa graduação. Mais ainda, daremos uma expressão não apenas aproximada (como ocorre com os métodos numéricos para encontrar o valor médio), mas precisa e exata da caracterização dessas matrizes. Novamente, dividiremos nossa conversa nas situações de característica diferente de 3, bem como em característica 3.

3.4.1 Caso em que $Char(\mathbb{K}) \neq 3$

A idéia por trás da busca pela caracterização dos elementos homogêneos reside em, essencialmente, explorar a seguinte relação obtida no Teorema 3.2.4 :

$$A_e = \{(V|(aB_a - (B_a)^2)V| - B_aV); V \in V_3\}$$

$$A_c = \{(V|(a\sigma B_a - \sigma(B_a)^2)V| - \sigma(B_a)V); V \in V_3\}$$

$$A_{c^2} = \{(V|(a\sigma^2 B_a - (\sigma^2(B_a))^2)V| - \sigma^2(B_a)V); V \in V_3\}$$

Como conhecemos a matriz B_a, bem como $\sigma(B_a)$ e $\sigma^2(B_a)$, poderíamos considerar um vetor coluna V genérico e determinar os valores das demais colunas das matrizes em função de V e B_a. A fim de seguir os passos dos autores do artigo, iremos usar a matriz $\sigma(B_a)$, determinando, assim, a forma das matrizes em $A(a)_c$. Para tal, sejam:

$$V = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \sigma(B_a) = \begin{pmatrix} 2 & a-1 & -1 \\ 1 & a-1 & -1 \\ 1 & a-2 & -1 \end{pmatrix}$$

Dada a caracterização de $A(a)_c$, vamos determinar todos os vetores colunas que compõem as matrizes dessa componente, respectivamente: V, $(a\sigma B_a - \sigma(B_a)^2)V$ e $-\sigma(B_a)V$:

$$V = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$$(a\sigma B_a - \sigma(B_a)^2)V = \left[\begin{pmatrix} 2a & a(a-1) & -a \\ a & a(a-1) & -a \\ a & a(a-2) & -a \end{pmatrix} - \begin{pmatrix} a+2 & a^2-a+1 & -a \\ a & a^2-2a+2 & 1-a \\ a-1 & a^2-3a+3 & 2-a \end{pmatrix}\right]\begin{pmatrix} x \\ y \\ z \end{pmatrix} =$$

$$= \left[\begin{pmatrix} a-2 & -1 & 0 \\ 0 & a-2 & -1 \\ 1 & a-3 & -2 \end{pmatrix}\right]\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} (a-2)x - y \\ (a-2)y - z \\ x + (a-3)y - 2z \end{pmatrix}$$

Com isso, já temos a configuração da segunda coluna das nossas matrizes, resta analisar o comportamento da última coluna.

$$-\sigma(B_a)V = \begin{pmatrix} -2 & 1-a & 1 \\ -1 & 1-a & 1 \\ -1 & 2-a & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -2x - (a-1)y + z \\ -x - (a-1)y + z \\ -x - (a-2)y + z \end{pmatrix}$$

Agora que determinamos a caracterização de cada coluna que compõe os elementos de $A(a)_c$, podemos determinar a caracterização de todo o conjunto, que será dada por:

$$A(a)_c = \left\{ \begin{pmatrix} x & (a-2)x - y & -2x - (a-1)y + z \\ y & (a-2)y - z & -x - (a-1)y + z \\ z & (a-3)y - 2z & -x - (a-2)y + z \end{pmatrix}; x, y, z \in \mathbb{K} \right\}$$

Note que ainda restaram as componentes A_e e A_{c^2}. Claramente, poderíamos fazer uso dessa mesma estratégia e determinar suas respectivas caracterizações, porém lembremos que no Teorema 3.2.4, mostramos que $A_c = XA_e$ e $A_{c^2} = X^2A_e = XA_c$, no qual, $X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix}$ tem a propriedade de que $X^3 = I_3$.

Com isso, valem as seguintes propriedades:

I.

$$A(a)_c = XA(a)_e \Leftrightarrow X^2A(a)_c = A(a)_e$$

II.

$$A(a)_{c^2} = XA(a)_c$$

Ora, dado que já descobrimos a expressão concreta de $A(a)_c$, basta efetuar a multiplicação dela pelas matrizes X e X^2, respectivamente, para obter a caracterização de $A(a)_e$ e $A(a)_{c^2}$. Então, segue-se que:

I.

$$A(a)_e = \begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x & (a-2)x-y & -2x-(a-1)y+z \\ y & (a-2)y-z & -x-(a-1)y+z \\ z & (a-3)y-2z & -x-(a-2)y+z \end{pmatrix} =$$

$$= \begin{pmatrix} x-2y+z & (a-1)x-ay & -x+y \\ x-y & (a-2)x-(a-1)y+z & -x \\ x & (a-2)x-y & -2x-(a-1)y+z \end{pmatrix}$$

E esse resultado significa que:

$$A(a)_e = \left\{ \begin{pmatrix} x-2y+z & (a-1)x-ay & -x+y \\ x-y & (a-2)x-(a-1)y+z & -x \\ x & (a-2)x-y & -2x-(a-1)y+z \end{pmatrix} ; x, y, z \in \mathbb{K} \right\}$$

Por outro lado, temos ainda:

II.

$$A(a)_{c^2} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} x & (a-2)x-y & -2x-(a-1)y+z \\ y & (a-2)y-z & -x-(a-1)y+z \\ z & (a-3)y-2z & -x-(a-2)y+z \end{pmatrix} =$$

$$= \begin{pmatrix} z & x+(a-3)y-2z & -x-(a-2)y+z \\ -y+z & x-y-z & y \\ x-2y+z & (a-1)x-ay & -x+y \end{pmatrix}$$

Novamente, como no caso anterior, a caracterização da nossa última componente homogênea será dada por:

$$A(a)_{c^2} = \left\{ \begin{pmatrix} z & x+(a-3)y-2z & -x-(a-2)y+z \\ -y+z & x-y-z & y \\ x-2y+z & (a-1)x-ay & -x+y \end{pmatrix} ; x,y,z \in \mathbb{K} \right\}$$

Esses resultados que vimos completam metade da nossa afirmação, de que poderiamos determinar uma descrição concreta das $\mathbb{Z}_3$-graduações, que são todas da forma $A(a)$, a menos de isomorfismos. Apenas com base na definição em forma de colunas de $A(a)_c$ e das relações entre as demais componentes a partir da matriz X, conseguimos realizar esse trabalho com algum esforço computacional.Ainda estamos devendo a segunda parte, ou seja, devemos mostrar ainda uma caracterização análoga para o caso em que a característica do corpo é igual à 3. Mas antes, segue resumidamente as componenetes homogêneas dessas $\mathbb{Z}_3$-graduações em forma matricial.

São essas todas as $\mathbb{Z}_3$-graduações em $M_3(\mathbb{K})$:

$$A(a)_c = \left\{ \begin{pmatrix} x & (a-2)x-y & -2x-(a-1)y+z \\ y & (a-2)y-z & -x-(a-1)y+z \\ z & (a-3)y-2z & -x-(a-2)y+z \end{pmatrix} ; x,y,z \in \mathbb{K} \right\}$$

$$A(a)_e = \left\{ \begin{pmatrix} x-2y+z & (a-1)x-ay & -x+y \\ x-y & (a-2)x-(a-1)y+z & -x \\ x & (a-2)x-y & -2x-(a-1)y+z \end{pmatrix} ; x,y,z \in \mathbb{K} \right\}$$

$$A(a)_{c^2} = \left\{ \begin{pmatrix} z & x+(a-3)y-2z & -x-(a-2)y+z \\ -y+z & x-y-z & y \\ x-2y+z & (a-1)x-ay & -x+y \end{pmatrix}; x,y,z \in \mathbb{K} \right\}$$

3.4.2 Caso em que $Char(\mathbb{K}) = 3$

Uma vez encontrada a caracterização das $\mathbb{Z}_3$-graduações para corpos de característica diferente de 3, vamos encontrar essa mesma caracterização para corpos de característica 3. Vale ressaltar, que os passos serão todos análogos aos feitos no caso anterior, ou seja, primeiramente determinaremos a forma concreta de $A_3(a)_c$ e fazendo-se uso das relações (que se seguram aqui também) **I.** $X^2A(a)_c = A(a)_e$ e **II.** $A(a)_{c^2} = XA(a)_c$, determinaremos as caracterizações das demais componentes. Relembremos que em característica 3, foi mostrado que toda $\mathbb{Z}_3$-graduação é determinada pelas seguintes componentes:

$$A_3(a)_e = \{((C_a^2 + 2I_3)V|C_aV|V); V \in V_3\}$$

$$A_3(a)_c = \{((C_a^2 + 2C_a)V|(C_a + I_3)V|V); V \in V_3\}$$

$$A_3(a)_c = \{((C_a^2 + C_a)V|(C_a + 2I_3)V|V); V \in V_3\}$$

Além disso,

$$V = \begin{pmatrix} x \\ y \\ z \end{pmatrix} X = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} C_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & 1 & 0 \end{pmatrix}$$

Com isso, se M é uma matriz de $A_3(a)_e$, então, as suas colunas serão dadas por: $(C_a^2 + 2C_a)V$:

$$(C_a^2+2I_3)V = \left[\begin{pmatrix} 0 & 0 & 1 \\ a & 1 & 0 \\ 0 & a & 1 \end{pmatrix} + \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 2a & 2 & 0 \end{pmatrix} \right] \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 & 2 & 1 \\ a & 1 & 2 \\ 2a & a+2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} z+2y \\ 2z+y+ax \\ z+(a+2)\,y+2ax \end{pmatrix}$$

$(C_a + I_3)V$:

$$(C_a + I_3)V = \left[\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right]\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x+y \\ y+z \\ ax+y+z \end{pmatrix}$$

V :

$$V = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Com esses resultados, podemos compor a nossa primeira componente homogênea em característica 3 (note que em momento algum usamos o fato de que o corpo tenha característica 3) A saber:

$$A_3(a)_c = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax+y+2z & y+z & y \\ 2ax+(a+2)y+z & ax+y+z & z \end{pmatrix}; x, y, z \in \mathbb{K} \right\}$$

Agora, de modo análogo ao que fizemos em característica diferente de 3, vamos determinar $A_3(a)_e$ e $A_3(a)_{c^2}$, que indicaremos por **I** e **II**, respectivamente.

I.

$$X^2(A_3(a)_c) = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 2y+z & x+y & x \\ ax+y+2z & y+z & y \\ 2ax+(a+2)y+z & ax+y+z & z \end{pmatrix} =$$

$$\begin{pmatrix} z+2y & y+x & x \\ ax-3y & z-y-2x & y-2x \\ 6z+(a+6)\,y+4ax & 3z+4y+x+ax & z+2y+x \end{pmatrix}$$

Usando o fato de que estamos em um corpo de característica 3, deve valer que:

$$\begin{cases} -3y = 0 \\ -y = 2y \\ -2x = x \\ 6z = 0 \\ (a+6)y = ay \\ 4y = y \end{cases}$$

Com esse resultado podemos, enfim, concluir que:

$$A_3(a)_e = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax & x+2y+z & x+y \\ ax+ay & (a+1)x+y & x+2y+z \end{pmatrix} ; x,y,z \in \mathbb{K} \right\}$$

Resta identificar a caracterização de $A_3(a)_{c^2}$, e ela será dada por:

II.

$$A_3(a)_{c^2} = XA(a)_c = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2y+z & x+y & x \\ ax+y+2z & y+z & y \\ 2ax+(a+2)y+z & ax+y+z & z \end{pmatrix} =$$

$$= \begin{pmatrix} z+2y & y+x & x \\ z-y+ax & z-x & y-x \\ 4z+(a+5)\,y+3ax & 2z+3y+(a+1)x & z+y+x \end{pmatrix}$$

Vamos novamente simplificar a expressão pela característica do corpo:

$$\begin{cases} -y = 2y \\ -x = 2x \\ 4z = z \\ (a+5)y = (a+2)y \\ 3ax = 0 \\ 3y = 0 \end{cases}$$

Então devemos ter que:

$$A_3(a)_{c^2} = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax+2y+z & 2x+z & 2x+y \\ (a+2)y+z & (a+1)x+2z & x+y+z \end{pmatrix} ; x,y,z \in \mathbb{K} \right\}$$

E assim, como em característica diferente de 3, temos a seguinte caracterização para uma $\mathbb{Z}_3$-graduação em $M_3(\mathbb{K})$, que pode ser explicitada da seguinte forma:

$$A_3(a)_e = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax & x+2y+z & x+y \\ ax+ay & (a+1)x+y & x+2y+z \end{pmatrix} ; x,y,z \in \mathbb{K} \right\}$$

$$A_3(a)_c = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax+y+2z & y+z & y \\ 2ax+(a+2)y+z & ax+y+z & z \end{pmatrix} ; x,y,z \in \mathbb{K} \right\}$$

$$A_3(a)_{c^2} = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax+2y+z & 2x+z & 2x+y \\ (a+2)y+z & (a+1)x+2z & x+y+z \end{pmatrix} ; x,y,z \in \mathbb{K} \right\}$$

E esse dois grandes resultados concluem o nosso capítulo de $\mathbb{Z}_3$-graduações, para quaisquer corpos de quaisquer características.

3.5 Comentários finais sobre o capítulo

Podemos dizer até o momento que 2/3 do nosso trabalho foi concluído, e, reservamos essa seção para discutir a respeito de algumas idéias que foram inseridas ao longo do mesmo, bem como comentar resumidamente as relações que essas idéias têm entre si.

O primeiro resultado, o Teorema 3.1.2, tratava sobre extensões cúbicas de Galois e a sua relação com uma das componentes homogêneas da nossa $\mathbb{Z}_3$-graduação, que era justamente $A_e = \mathbb{K}[B_a]$, onde o polinômio minimal de B_a tinha grau 3. O primeiro adjetivo que A_e recebeu foi o de extensão de corpos. Quando trabalhamos com extensão de racionais é fácil de ver a multiplicação entre os escalares e os elementos da extensão, já que estamos falando de produto com elementos de subconjuntos de $\mathbb{C}$. Em matrizes é necessário identificar uma imersão de corpos, a saber $\mathbb{K} \hookrightarrow M_3(\mathbb{K})$, que é identificada por $\mathbb{K} \simeq kI_3; k \in \mathbb{K}$. Além disso, falar sobre extensões de Galois no contexto de polinômios de variáveis complexas já não é algo tão elementar e aqui trabalhamos com esses conceitos em um caso mais geral, das matrizes. Ou seja, todas aquelas definições que são dadas em um curso de teoria de Galois podem ser generalizadas para corpos quaisquer.

Como $\mathbb{K}[B_a]$ tinha dimensão 3 sobre $\mathbb{K}$, então a extensão de Galois também teve grau 3. Pelo fato da idéia de extensão de Galois estar associada à idéia do corpo de decomposição de um polinômio, usamos uma caracterização de $\mathbb{K}[B_a]$ no qual a mesma era um corpo de decomposição desse polinômio.

Também nesse capítulo, em algum momento da prova do Teorema 3.1.2, usamos a idéia de derivada para um polinômio em $\mathbb{K}[B_a]$, apesar de ambas as noções parecerem nada convencionais, tanto polinômios com coeficientes matriciais quanto a derivada do mesmo, vale ressaltar que a derivada polinomial que vemos no cálculo diferencial e integral se comporta essencialmente como a regra da potência para cada monômio, então, mesmo sem uma topologia definida, podemos axiomatizar essa regra para derivada de polinômios em álgebra, no qual chamamos de derivada formal:

Definição 3.5.1 *Seja $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, dizemos que sua derivada formal é o polinômio: $p'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + a_1$.*

Além disso, todas as propriedades de funções polinomiais que decorrem da noção de derivadas (como a relação das raízes múltiplas) também se aplicam à esse caso.

Capítulo 4

As graduações finas

Nesse quarto e último capítulo, iremos encontrar as demais graduações em $M_3(\mathbb{K})$. No segundo capítulo encontramos condições suficientes para determinar as chamadas boas graduações. Ao fim desse mesmo capítulo, apresentamos e provamos o Teorema 2.4.3, que nos indicou onde procurar as demais graduações. Vimos que elas seriam graduações cujo suporte é o $\mathbb{Z}_3$ ou $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Designamos o capítulo anterior para estudar e deduzir quais eram as graduações sobre um suporte isomorfo à $\mathbb{Z}_3$. Para tal, construímos inicialmente uma família de subespaços de $M_3(\mathbb{K})$ que decompôs a mesma em uma G-graduação não isomorfa à uma boa graduação. A idéia de construir essa graduação foi voltada inteiramente para mostramos em seguida que, a menos de isomorfismo, ela era, de fato, única.

Visando descrever todas as graduações de suporte isomorfo à $\mathbb{Z}_3 \times \mathbb{Z}_3$, usaremos de tática análoga, ou seja, construiremos, inicialmente, uma graduação sobre esse suporte não isomorfa à uma boa graduação. Em seguida, iremos demonstrar que, a menos de isomorfismos, tais graduações são únicas sobre $\mathbb{Z}_3 \times \mathbb{Z}_3$. Essas graduações que serão denotadas por $A(X, Y)$, serão chamadas de "graduações finas", terminologia usada por Yurin Bathurin em seu artigo "Gradings of matrix algebras by cyclic groups".

Dadas essas considerações, vamos definir essas graduações da forma $A(X, Y)$ e mostrar a sua "unicidade".

4.1 Construindo uma $\mathbb{Z}_3 \times \mathbb{Z}_3$-Graduação

Seja $A = \oplus_{g \in \mathbb{Z}_3 \times \mathbb{Z}_3} A_g$ uma graduação em $M_3(\mathbb{K})$ não isomorfa à uma boa graduação. Pela Teorema 2.4.3, temos que ou o suporte é um subgrupo de $\mathbb{Z}_3$ de ordem 3, e essas graduações foram discutidas na Seção 2, ou que $supp(A) = \mathbb{Z}_3 \times \mathbb{Z}_3$, com $dim(A_g) = 1$ para qualquer $g \in \mathbb{Z}_3 \times \mathbb{Z}_3$, e A é um anel de divisão graduado. Nessa seção vamos construir um tipo de tal graduação a partir de dois teoremas, um deles será um objeto auxiliar para o outro. Antes de enunciar e demonstrá-los, vamos definir as matrizes que determinaram as nossas componentes homogêneas, bem como elas próprias.

Suponha que $\mathbb{K}$ contenha uma raiz cúbica primitiva da unidade ξ. Sejam $X, Y \in M_3(\mathbb{K})$ tal que $X^3, Y^3 \in \mathbb{K}^* I_3$ e $YX = \xi XY$. Vamos mostrar que se $A_{\sigma^i \tau^j} = kX^iY^j$ para qualquer $0 \leq i, j \leq 2$, então $A{=}\oplus_{g \in Z_3 X Z_3} A_g$ é uma graduação em $M_3(\mathbb{K})$. Note que a combinatória funciona, visto que teremos nove componentes homogêneas que serão todas de grau 1.

Teorema 4.1.1 *O polinômio minimal f_X de X é da forma $f_X(T) = T^3 - d$ para algum $d \in \mathbb{K}^*$.*

Demonstração: Como $X^3 \in \mathbb{K}I_3$, então $X^3 - dI_3 = 0$. Vamos denotar essa expressão sucintamente por $X^3 - d = 0$, para algum $d \in \mathbb{K} - \{0\}$. Dessa forma $f_X|(T^3 - d)$. Vamos então dividir a nossa análise em dois casos: (i) $d \notin \mathbb{K}^3$ e (ii) $d \in \mathbb{K}^3$:

(i) Nesse caso, o polinômio $T^3 - d$ é irredútivel e portanto, deve coincidir com f_X.

(ii) Se $d \in \mathbb{K}^3$, então $d = a^3; a \in \mathbb{K}$. Vamos usar o fato de que ξ é uma raíz cúbica primitiva da unidade em $\mathbb{K}$, portanto, $\xi^3 = 1$ e $\xi^n \neq 1$, para $n \in \{0, 1, 2\}$. Daí segue que, como $\xi^3 - 1 = (\xi - 1)(\xi^2 + \xi + 1) = 0$, então $\xi^2 + \xi + 1 = 0$. Assim deve valer que:

$$(T - a)(T - \xi a)(T - \xi^2 a) = (T^2 + (-a - \xi a)T + a^2\xi)(T - \xi^2 a) =$$

$$T^3 - (\xi^2 a + \xi a + a)T^2 + (\xi^2 a^2 +^2 + a^2)T - a^3 =$$

$$T^3 - a(\xi^2 + \xi + 1)T^2 + a^2(\xi^2 + \xi + 1)T - a^3 = T^3 - a^3$$

Isso, em particular, implica que $f_X|(T - a)(T - \xi a)(T - \xi^2 a)$. Assim, é fácil ver que f_X é escrito como produto de monômios lineares da forma $f_X = (T - a)^i (T - \xi a)^j (T - \xi^2 a)^k$, onde $i, j, k \in \{0, 1\}$.

Sabe-se que se f_X é escrito de tal forma, então X é diagonalizável e sua forma de Jordan correspondente será dada por:

$$X = \begin{pmatrix} a\xi_1 & 0 & 0 \\ 0 & a\xi_2 & 0 \\ 0 & 0 & a\xi_3 \end{pmatrix}$$

.

Da forma como apresentamos não é explícito que os elementos da diagonal sejam distintos dois a dois. E é isso que iremos mostrar agora a partir da relação fornecida na hipótese: $YX = \xi XY$. Vamos considerar $Y = (V_1|V_2|V_3)$, onde:

$$V_1 = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} V_2 = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} V_3 = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} .$$

Desse modo obtemos:

$$YX = \begin{pmatrix} x_1\xi_1 & y_1\xi_2 & z_1\xi_3 \\ x_2\xi_1 & y_2\xi_2 & z_2\xi_3 \\ x_3\xi_1 & y_3\xi_2 & z_3\xi_3 \end{pmatrix}, \xi XY = \begin{pmatrix} x_1\xi\,\xi_1 & y_1\xi\,\xi_1 & z_1\xi\,\xi_1 \\ x_2\xi\,\xi_2 & y_2\xi\,\xi_2 & z_2\xi\,\xi_2 \\ x_3\xi\,\xi_3 & y_3\xi\,\xi_3 & z_3\xi\,\xi_3 \end{pmatrix}$$

O leitor deve ter percebido a ausência do coeficiente a na matriz X, isso se deve ao seguinte fato: da condição $YX = \xi XY$ o termo a se cancela na igualdade, portanto, é mais conveniente e fácil trabalhar com X de tal forma, e é o que faremos a partir de agora. Assim, decorrem as seguintes relações:

$$\begin{cases} x_1\xi_1 = \xi^{-1}\xi_1 x_1 \\ x_2\xi_2 = \xi^{-1}\xi_1 x_2 \\ x_3\xi_3 = \xi^{-1}\xi_1 x_3 \end{cases}, \begin{cases} y_1\xi_1 = \xi^{-1}\xi_2 y_1 \\ y_2\xi_2 = \xi^{-1}\xi_2 y_2 \\ y_3\xi_3 = \xi^{-1}\xi_2 y_3 \end{cases}, \begin{cases} z_1\xi_1 = \xi^{-1}\xi_3 z_1 \\ z_2\xi_2 = \xi^{-1}\xi_3 z_2 \\ z_3\xi_3 = \xi^{-1}\xi_3 z_3 \end{cases}$$

Isso nos permite deduzir que $XV_i = \xi^{-1}\xi_i V_i; i \in \{1, 2, 3\}$. Vamos provar rapidamente que esse sistema tem solução única se, e somente se, $\xi^{-1}\xi_i \in \{\xi_1, \xi_2, \xi_3\}$.

Sabemos que $Y^3 \in \mathbb{K}I_3$, logo, Y é invertível. Então nenhuma linha da matriz Y pode ser inteiramente nula. Vamos supor sem perder generalidade que $x_2y_3z_1 \neq 0$ para respeitar o fato de ξ ser uma raiz cúbica da unidade. Desse modo:

$$x_2\xi_2 = \xi^{-1}\xi_1 x_2 \Rightarrow \xi^{-1}\xi_1 = \xi_2$$

$$y_3\xi_3 = \xi^{-1}\xi_2 y_3 \Rightarrow \xi^{-1}\xi_2 = \xi_3$$

$$z_1\xi_1 = \xi^{-1}\xi_3 z_1 \Rightarrow \xi^{-1}\xi_3 = \xi_1$$

E, assim, vale que $\xi^{-1}\xi_i \in \{\xi_1, \xi_2, \xi_3\}$.

Reciprocamente, devemos mostrar que qualquer sistema do tipo:

$$\begin{cases} \xi_1 x = \xi^{-1}\xi_3 x \\ \xi_2 y = \xi^{-1}\xi_3 z_2 y \\ \xi_3 z = \xi^{-1}\xi_3 z \end{cases}$$

tem solução. Sabemos que $\xi^{-1}\xi_i \in \{\xi_1, \xi_2, \xi_3\}$. Então em alguma das três relações podemos fazer uma escolha de um elemento não nulo de $\mathbb{K}$ que seja solução da mesma. E isso conclui esse pequeno resultado.

Uma consequência imediata desse fato, agregado à Y não ter todas as linhas nulas $\xi^{-1}\{\xi_1, \xi_2, \xi_3\} = \{\xi_1, \xi_2, \xi_3\}$. Para isso, basta dividir, respeitando o fato de que ξ é raiz cúbica primitiva, o fator não-nulo em cada um dos sistemas. ■

Nesse ponto, estamos aptos à enunciar o teorema que descreve uma graduação nesses suportes.

Teorema 4.1.2 *Se $A_{\sigma^i\tau^j} = kX^iY^j$ para qualquer $0 \leq i, j \leq 2$, então $A{=}\oplus_{g\in\mathbb{Z}_3\times\mathbb{Z}_3} A_g$ é uma graduação em $M_3(\mathbb{K})$.*

Demonstração: Seja:

$$\sum_{0\leq i,j\leq 2} \alpha_{ij} X^i Y^j = 0 \tag{4.1}$$

Considere $Z_j = \sum_{0\leq i\leq 2} \alpha_{ij} X^i$. Ou seja:

$$\begin{aligned} Z_0 &= \alpha_{00} + \alpha_{10}X + \alpha_{20}X^2 \\ \textit{Como}\ \ Z_1 &= \alpha_{01}Y + \alpha_{11}X + \alpha_{21}X^2 \\ Z_2 &= \alpha_{02} + \alpha_{12}X + \alpha_{22}X^2 \end{aligned}$$

Ao fazer isso, estamos apenas reescrevendo a soma geral em partes das quais podemos colocar os fatores Y e Y^2 em evidência posteriormente. Queremos mostrar que cada $\alpha_{ij} = 0$, pois assim teremos que Z_0, Z_1, Z_2 são LI, como eles geram cada uma de suas componentes homogêneas correspondentes, teremos uma soma direta de $M_3(\mathbb{K})$. Com isso, a equação 4.1 se torna:

$$Z_0 + Z_1 Y + Z_2 Y^2 = 0 \tag{4.2}$$

Multiplicando-se essa nova igualdade por X à direita e X^2 à esquerda e usando a relação

$YX = \xi XY$, obtemos as novas relações:

$$Z_0 + \xi Z_1 Y + \xi^2 Z_2 Y^2 = 0 \tag{4.3}$$

De modo análogo, podemos também deduzir que $Z_0 + \xi^2 Z_1 + \xi Z_2 = 0$, bastando multiplicar por X^2 à direita da equação 4.2 e depois por X à esquerda na mesma.

Colocando os termos Y em evidência em cada uma dessas relações, obtemos o sistema:

$$Z_0 + \xi Z_1' Y + \xi^2 Z_2' Y^2 = 0$$
$$Z_0 + \xi^2 Z_1' Y + \xi Z_2' Y^2 = 0$$

Onde $Z_0 = \alpha_{00} + \alpha_{10}X + \alpha_{20}X^2, Z_1' = \alpha_{01} + \alpha_{11}X + \alpha_{21}X^2, Z_2' = \alpha_{02} + \alpha_{12}X + \alpha_{22}X^2$

E com isso, temos que $\xi(Z_1Y - Z_2Y^2) = \xi^2(Z_1Y - Z_2Y^2)$, que tem solução única para $Z_1Y - Z_2Y^2 = 0$. Como ambos são elementos homogêneos de componentes homogêneas distintas, vale que $Z_1Y = Z_2Y^2 = 0$. Como $Y \in kI_3$, vale em particular que $det(Y^3) \neq 0 \Rightarrow [det(Y)]^3 \neq 0$, ou seja, $det(Y) \neq 0$, assim Y é invertível. Isso implica que $Z_1 = Z_2 = 0$, assim $Z_0 = 0$. Então obtemos as relações:

$$\alpha_{00} + \alpha_{10}X + \alpha_{20}X^2 = 0 \alpha_{01} + \alpha_{11}X + \alpha_{21}X^2 = 0 \alpha_{02} + \alpha_{12}X + \alpha_{22}X^2 = 0 \tag{4.4}$$

Do teorema anterior, temos que f_X que é o polinômio minimal de X, tem grau 3, portanto, para que essas relações ocorram é necessário que $\alpha_{ij} = 0$. Ou seja, a equação 4.1 é uma soma direta de $M_3(\mathbb{K})$, como queríamos mostrar.

Para demonstrar que $A(X,Y)$ é uma G-graduação, resta mostrar o bom comportamento do produto matricial em relação ao produto de elementos do suporte, mas para isso basta perceber que $X^iY^jX^kY^n = \xi^m X^{i+k}Y^{j+n}$. ■

Seguindo os mesmos passos para os suportes isomorfos à $\mathbb{Z}_3$, iremos mostrar que essa graduação construída é, de fato, a única graduação com suporte isormorfo à $\mathbb{Z}_3 \times \mathbb{Z}_3$, a menos de isomorfismos. Esse resultado se encontra enunciado a seguir.

Teorema 4.1.3 *Seja $A = \oplus_{g \in \mathbb{Z}_3 \times \mathbb{Z}_3} A_g$ uma graduação em $M_3(\mathbb{K})$ não isomorfa à uma boa graduação, e tal que $supp(A) \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$. Então, $A \simeq A(X,Y)$ para alguns $X, Y \in M_3(\mathbb{K})$ tais que $X^3, Y^3 \in k^*I_3$ e $YX = \xi XY$, onde ξ é uma raiz cúbica primitiva da unidade em $\mathbb{K}$.*

Demonstração: Veja que numa $\mathbb{Z}_3 \times \mathbb{Z}_3$-graduação, vale que a dimensão de cada componente homogênea é igual à 1. E nesse caso, $A_e = A_{\overline{00}} = \mathbb{K}I_3$, $A_\sigma = \mathbb{K}X$ e $A_\tau = \mathbb{K}Y$. Como $supp(A) = \sigma^i\tau^j$, devemos ter que $A_{\sigma^i\tau^j} = \mathbb{K}X^iY^j$.

Agora, vamos mostrar que $X, Y \in \mathbb{K}I_3$. Essa propriedade decorre de X^3 e Y^3 serem, respectivamente, elementos homogêneos de A_{σ^3} e A_{τ^3}, ora, $supp(A) \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$, ou seja $A_{\sigma^3} = A_{\overline{0}}$ e $A_{\tau^3} = A_{\overline{0}}$, como $A_{\overline{0}} = I_3$, o resultado se segue.

Para concluir a nossa prova, resta mostrar que existe uma raiz cúbica primitiva da unidade ξ tal que $YX = \xi XY$. Para isso, seja $Y \in A_\tau$ e $X \in A_\sigma$, em particular, $Y^{-1} \in A_{\tau^{-1}}$. Com isso, devemos ter que $YXY^{-1} \in A_\tau A_\sigma A_{\tau^{-1}} \subset A_{\tau\sigma\tau^{-1}}$. Lembremos que $\sigma = \overline{1}, \tau = \overline{2}$, então $\tau\sigma\tau^{-1} = \overline{2} + \overline{1} + \overline{1} = \overline{1}$, logo $YXY^{-1} = \xi X$, para $\xi \in \mathbb{K}^*$, ou seja, $YX = \xi XY$.

Por outro lado, essa igualdade também implica que $(YXY^{-1})^3 = \xi^3X^3$, logo $Y^{-3}X^3Y^3 = \xi^3X^3$. Como $Y^3 \in \mathbb{K}I_3$, teremos que $Y^3 = d \in \mathbb{K}$, logo teremos $\frac{1}{d}X^3d = \xi^3X^3$, daí decorre que $\xi^3 = 1$. Veja que $\xi \neq 1$, caso contrário valeria que $XY = YX$, como as componentes homogêneas dependem exclusivamente dessas variáveis teríamos que $M_3(\mathbb{K})$ é comutativa, um absurdo.

Com isso, acabamos de provar que $A_{\sigma^i\tau^j}$ é uma graduação da forma $A(X, Y)$, para alguns X e Y em $\mathbb{K}$, que atendem às condições inicialmente impostas. ■

4.2 Comentários finais sobre o capítulo

Nesse capítulo, tentamos "recriar" a prova feita no caso anterior, que foi, inicialmente, construir uma graduação em suporte isomorfo à $\mathbb{Z}_3 \times \mathbb{Z}_3$, e em seguida mostramos essa unicidade a menos de isomorfismos. Para tal usamos um resultado muito sutil, mas relevante, exibimos uma caracterização do polinômio minimal da matriz X. Lembrando que em graduações de suporte isomorfo à $\mathbb{Z}_3$, caracterizamos uma componente homogênea como uma extensão cúbica de Galois e aqui optamos por caracterizar o polinômio minimal. Esse tipo de artifício contorna um problema geral em um caso mais específico em que os elementos envolvidos na demonstração se tornam mais "concretos". Essa engenhosidade também pode ser encontrada em "Group grandings of $M_2(\mathbb{K})$", no qual os mesmos autores usam das caracterizações dos polinômios minimais e característicos dessas matrizes geradoras das componentes.

O termo curioso "graduações finas" foi introduzido em um artigo de Bathurin. Esse nome criativo se refere à graduações nas quais a dimensão das componentes homogêneas são todas iguais à 1, pois nesse caso é como se o "filtro" que a graduação faz na álgebra torna a segunda dividida em componentes muito "pequenas".

Conclusão

Ao fim desse trabalho, que foi dividido em boas graduações, $\mathbb{Z}_3$-graduações e $\mathbb{Z}_3 \times \mathbb{Z}_3$-graduações, mencionaremos cada tipo de graduação abaixo:

I. Boas graduações, que sempre ocorrem quando o suporte tem elementos de ordem 2 ou 4. Eventualmente, podem ocorrer em suporte de elementos de ordem 3, como vimos ao fim do capítulo 2.

II. $\mathbb{Z}_3$-graduações, que são explicitamente dadas na forma:

(i) $Char(\mathbb{K}) \neq 3$:

$$A(a)_c = \left\{ \begin{pmatrix} x & (a-2)x - y & -2x-(a-1)y+z \\ y & (a-2)y-z & -x-(a-1)y+z \\ z & (a-3)y-2z & -x-(a-2)y+z \end{pmatrix} ; x, y, z \in \mathbb{K} \right\}$$

$$A(a)_e = \left\{ \begin{pmatrix} x-2y+z & (a-1)x-ay & -x+y \\ x-y & (a-2)x-(a-1)y+z & -x \\ x & (a-2)x-y & -2x-(a-1)y+z \end{pmatrix} ; x, y, z \in \mathbb{K} \right\}$$

$$A(a)_{c^2} = \left\{ \begin{pmatrix} z & x+(a-3)y-2z & -x-(a-2)y+z \\ -y+z & x-y-z & y \\ x-2y+z & (a-1)x-ay & -x+y \end{pmatrix} ; x, y, z \in \mathbb{K} \right\}$$

(ii) $char(\mathbb{K}) = 3$:

$$A_3(a)_e = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax & x+2y+z & x+y \\ ax+ay & (a+1)x+y & x+2y+z \end{pmatrix} ; x, y, z \in \mathbb{K} \right\}$$

$$A_3(a)_c = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax+y+2z & y+z & y \\ 2ax+(a+2)y+z & ax+y+z & z \end{pmatrix}; x,y,z \in \mathbb{K} \right\}$$

$$A_3(a)_{c^2} = \left\{ \begin{pmatrix} 2y+z & x+y & x \\ ax+2y+z & 2x+z & 2x+y \\ (a+2)y+z & (a+1)x+2z & x+y+z \end{pmatrix}; x,y,z \in \mathbb{K} \right\}$$

III. $\mathbb{Z}_3 \times \mathbb{Z}_3$-graduações, que são graduações isomorfas às graduações do tipo $A(X,Y)$, para $YX = \xi XY$, onde ξ é uma raiz cúbica primitiva da unidade e $X^3, Y^3 \in \mathbb{K}I_3$.

Dado esse pequeno resumo, dedico os últimos paragráfos do trabalho para comentar sobre a minha experiência pessoal com o tema.

Em 2018, comecei a trabalhar no programa de iniciação científica orientado pelo professor doutor Júlio César dos Reis. Me foi apresentado inicialmente um material com o título: "Matrizes: existem perguntas que ainda nao sabemos responder? Uma introdução às Algebras com Identidades Polinomiais", assim fui apresentado à uma nova área da álgebra que ia bem além do que o estudado em sala de aula. Nos primeiros meses senti uma certa dificuldade por se tratar de pesquisa matemática, pois o ambiente da pesquisa é diferente do ambiente "disciplinas acadêmicas", este segundo é bem estruturado o que possibilita um processo de aprendizado mais acelerado, porém mais limitado, a pesquisa expandiu meus horizontes.

Deixando o trabalho mais técnico de resolver exercícios em algumas horas e passando a pensar em alguns problemas durantes semanas, eu analisei o artigo Group Gradings of $M_2(\mathbb{K})$ e em seguida o artigo Group Gradings on $M_3(\mathbb{K})$. Por se tratar de artigo de 2007, algumas ferramentas ultilizadas pelos autores eram muito sofisticadas em relação ao conhecimento que eu tinha. Sob a orientação sempre próxima do professor Júlio, foi possível que eu aprendesse muitos conceitos que para mim eram novos, como, por exemplo, teoria de Galois elementar e teoria de Galois estendida, que foi uma ferramental crucial para o desenvolvimento desse trabalho.

Agradeço, novamente, ao professor Júlio por ter me apresentado esse mundo matemático novo em pesquisa acadêmica.

Referências Bibliográficas

[1] BATHURIN, Y. A., SEHGAL, S. K., ZAICIEV, M. V. Group gradings on associativem algebras. **J. Algebra**. 241(2):677–698, 2001.

[2] BOBOC, C. DASCALESCU, S. Group Gradings on $M_3(\mathbb{K})$. **Communications in Algebra**. 35:9, 2654-2670,2007.

[3] GONÇALVES, A. **Introdução à álgebra**; 6°. Rio de Janeiro: IMPA, 2017.

[4] HOFFMAN, K.; KUNZE, R. **Álgebra Linear**. Livros Técnicos e Cientícos Editora, Rio de Janeiro,1979.

[5] KHAZAL, R.; BOBOC, C.; DASCALESCU, S. Group Gradings of M2(K). **Bulletin of the Australian Mathematical Society**. 68, 285-293 (2003).

[6] KERSTEN, I., MICHALICEK, J. A characterization of Galois field extensions of degree 3. **Comm. Algebra**. 15:927–933, 1987.

[7] LANG, S. **Algebra: A graduate course**. 3°. Nova York: Springer Verlag, 2002.

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

[9] ROYDEN, H.L. **Real Analysis**. 3°. Califórnia: Macmillan, 1988.