UNIVERSIDADE FEDERAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA

FORMAS QUADRÁTICAS SOBRE CORPOS, ÁLGEBRAS COM DIVISÃO E ÁLGEBRAS DE CLIFFORD

Dissertação apresentada ao Departamento de Matemática da Universidade Federal de Pernambuco, como parte dos requisitos para obtenção do título de Mestre em Matemática.

ZAQUEU ALVES RAMOS
Orientador: Francesco Russo

Recife, 2008.

Ramos, Zaqueu Alves
Formas quadráticas sobre corpos, álgebras com divisão e álgebras de Clifford / Zaqueu Alves Ramos. – Recife: O Autor, 2008.
97 folhas : il.

Dissertação (mestrado) – Universidade Federal de Pernambuco. CCEN. Matemática, 2008.

Inclui bibliografia e apêndice.

1. Álgebra. Título.

512 CDD (22.ed.) MEI2008-04l

Tese submetida ao Corpo Docente do Programa de Pós-graduação do Departamento de Matemática da Universidade Federal de Pernambuco como parte dos requisitos necessários para a obtenção do Grau de Mestrado em Ciências.

Aprovado: _____

Francesco Russo, DMAT-UFPE
Orientador

_____

Aron Simis, DMAT-UFPE

_____

Jacqueline Fabiola ~~Rojas Arancibia~~, DM-UFPB

FORMAS QUADRÁTICAS SOBRE CORPOS, ÁLGEBRAS COM DIVISÃO E ÁLGEBRAS DE CLIFFORD

Por

Zaqueu Alves Ramos

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA
Cidade Universitária – Tels. (081) 2126 - 8414 – Fax: (081) 2126 - 8410
RECIFE – BRASIL

Fevereiro - 2008

AGRADECIMENTOS

A minha família por tudo que fazem para que eu possa realizar os meus objetivos.

A Mariana Cristina pelo carinho e companheirismo.

Aos professores Aron Simis e Jaqueline Rojas pela participação na banca examinadora e pelas sugestões e críticas responsáveis para a redação final do texto.

Ao CNPq pelo auxílio financeiro.

Aos amigos Adecarlos, Joilson Oliveira e Marcelo Fernandez pela convivência durante esses dois anos de mestrado.

Aos amigos sergipanos Bruno Luis, Bruna Dutra, Anderson Valença, Charlene Messias, Fábio Costa, Fábio Santos, Paulo Rabelo e Solange.

Aos amigos e funcionários do Dmat-UFPe.
Aos professores do DMA-UFS Alan Almeida e Natanael Oliveira.

E em especial, ao professor Francesco Russo, pela orientação, pelos ensinamentos e pelas inspiradoras aulas as quais tive o privilégio de presenciar.

RESUMO

Nesta dissertação tratamos alguns aspectos da teoria das formas quadráticas sobre um corpo, das álgebras com divisão e das álgebras centrais simples. Objetos importantes estudados são o anel de Witt, o grupo de Brauer, as álgebras de Clifford e o teorema de Wedderburn sobre a estrutura das álgebras centrais simples. Essas teorias são profundamente ligadas entre si e tem conexões com outras áreas como a teoria dos corpos, a geometria algébrica, a topologia algébrica, a teoria das representações e a física teórica. Matemáticos ilustres como Brauer, Clifford, Emmy Noether, Gauss, Hamilton, Hasse, Hurwitz e Wedderburn trabalharam nos temas detalhados nesta dissertação.

Palavras chave: Álgebras com divisão, grupo de Brauer, álgebras de Clifford, formas quadráticas.

ABSTRACT

In this dissertation we treat some aspects of the theory of quadratic forms over a field, algebras with division and simple central algebras. Important objects here studied are the Witt's ring, the Brauer's group, the Clifford's algebras and the Wedderburn's theorem over the structure of simple central algebras. These theories are deeply linked together and have connections with other areas like the theory of fields, the algebraic geometry, the algebraic topology and the theory of representations. Illustrious mathematicians as Brauer, Clifford, Emmy Noether, Gauss, Hamilton, Hasse, Hurwitz and Wedderburn worked in subjects that are detailed in this text.

Keywords: Algebras with division, Brauer's group, Clifford's algebras, Quadratic forms.

Conteúdo

Introdução

Os elementos que tratamos nessa dissertação são as formas quadráticas sobre corpos, as álgebras com divisão e as álgebras centrais simples. Nosso objetivo ao escrever esse texto é mostrar alguns aspectos e propriedades que mostram como esses estão relacionadas entre si.

No primeiro capítulo é feita a exposição de definições e resultados mínimos que dão suporte ao acompanhamento do resto do texto, seguindo a referência [**4**]. Também enunciamos os interessantes teoremas de Hurwitz e Bott-Milnor-Kervaire para as existências, respectivamente, de $\mathbb{R}$-álgebras de composição e de $\mathbb{R}$-álgebras com divisão de dimensão finita. Para o primeiro, incluímos uma demonstração que utiliza apenas ferramentas elementares de álgebra linear.

O capítulo seguinte é dedicado a um exemplo de álgebra central simples muito importante, a saber, a álgebra dos quatérnios generalizada. Esse exemplo já permite visualizar um pouco da ligação sugerida no primeiro parágrafo dessa introdução, através de um teorema que afirma o seguinte: duas álgebras de quatérnios são isomorfas se, e somente se, as formas quadráticas associadas a elas forem equivalentes.

No capítulo 3 apresentamos o anel de Witt e a descrição de algumas das suas propriedades algébricas mais importantes (por exemplo, noetherinidade) do ponto de vista aritmético e geométrico. Discutimos incialmente a construção de Grothendieck, que trata-se de estender um semi-anel comutativo a um anel comutativo, e em seguida especializamos essa construção ao caso do anel de Witt das classes de formas quadráticas regulares sobre um corpo.

No capítulo 4 voltamos a considerar a noção de álgebra central simples (definida no capítulo 2). Por meio do teorema de estrutura de Wedderburn fazemos a descrição desses objetos como anéis de matrizes sobre uma álgebra com divisão. Trataremos algumas propriedades dessas álgebras, chegando a definição do grupo de Brauer, e demonstraremos que a dimensão delas sobre o corpo base é necessariamente um quadrado. Em seguida incluímos a demonstração do importante teorema de Frobenius que é traduzido pelo isomorfismo $\mathrm{B}(\mathbb{R}) \simeq \mathbb{Z}_2$, onde $\mathrm{B}(\mathbb{R})$ significa o grupo de

Brauer do corpo $\mathbb{R}$. Finalmente, tratamos o caso de álgebras graduadas centrais simples e definimos o grupo de Brauer-Wall para tais estruturas.

No capítulo 5 estudamos a álgebra de Clifford associada a uma forma quadrática. Depois de alguns resultados preliminares, descrevemos as principais propriedades estruturais dessas álgebras, definindo os invariantes de Clifford, Witt e Hasse e explicando as ligações com as estruturas algébricas dos capítulos anteriores. Em seguida falamos dos teoremas de "periodicidade módulo 8", dos módulos de Clifford reais (análogos algébricos de teoremas de periodicidade em K-teoria). Por fim, aplicamos os resultados a teoria da composição de formas quadráticas, desenvolvida por Gauss, reobtendo como caso particular uma demonstração mais sofisticada do teorema de Hurwitz considerado no primeiro capítulo.

No capítulo 6 fazemos uma breve exposição a respeito das álgebras cíclicas. Essas álgebras são uma generalização da álgebra dos quatérnios e, como demonstraremos, são mais exemplos de álgebras centrais simples. Para algumas classes de corpos se mostra que elas são as únicas álgebras centrais simples (teorema de Brauer-Hasse-Noether). O estudo das álgebras cíclicas é estreitamente relacionado com a teoria de Galois. A própria terminologia é motivada pelo fato do corpo de decomposição dessas álgebras centrais simples ser uma extensão de Galois cíclica do corpo base. Um importante resultado que demonstramos nesse capítulo é o critério da norma de Wedderburn. Esse bonito resultado fornece condição suficiente para a obtenção de álgebras com divisão não comutativas sobre corpos infinitos.

CAPíTULO 1

Preliminares

Neste capítulo apresentaremos algumas definições e resultados básicos a respeito dos objetos principais de estudo dessa dissertação, a saber, as formas quadráticas sobre corpos e as álgebras com divisão. Alguns dos resultados serão apenas enunciados, em virtude de serem fatos já conhecidos em cursos de álgebra linear ou por serem de fácil dedução. Salvo menção contrária, em todo o texto, usaremos os símbolos F para representar um corpo de característica diferente de dois, F^* para o grupo multiplicativo dos elementos invertíveis de F e F^{*2} para o subgrupo de F^* correspondente aos quadrados de F.

1. Formas Quadráticas e Espaços Quadráticos

DEFINIÇÃO 1.1. Uma **forma quadrática** (n-ária) sobre um corpo F é um polinômio homogêneo do segundo grau em n variáveis com coeficientes em F.

Dada uma forma quadrática

$$f(X_1, \ldots, X_n) = \sum_{i,j}^{n} a_{ij} X_i X_j \in F[X_1, \ldots, X_n],$$

podemos apresentá-la matricialmente por

$$f(\mathbf{X}) = \mathbf{X}^t M_f \mathbf{X},$$

onde $M_f = (a'_{ij}) \in M_{n\times n}(F)$ com $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$ e $\mathbf{X} = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$.

A correspondência $f \mapsto M_f$ é uma função, de fato bijetora, do conjunto das formas quadráticas sobre F no conjunto das matrizes simétricas sobre F.

Dizemos que duas formas quadráticas n-árias f e g são equivalentes ($f \cong g$) se existir $C \in GL_n(F)$ tal que $f(\mathbf{X}) = g(C\mathbf{X})$. Claramente, $\cong$ define uma relação de equivalência no conjunto das formas quadráticas n-árias sobre F. Simbolizaremos a classe de equivalência de uma forma quadrática f nessa relação por (f).

OBSERVAÇÃO 1.2. $f \cong g \Leftrightarrow \exists\, C \in GL_n(F)\ : M_f = C^t M_g C$.

Sobre o F-espaço vetorial F^n uma forma quadrática n-ária f induz uma função

$$Q_f : F^n \longrightarrow F$$

definida por

$$Q_f(\mathbf{x}) = \mathbf{x}^t M_f \mathbf{x}$$

onde $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Essa Q_f é chamada de **função quadrática** associada a f.

Observação 1.3. A função quadrática Q_f determina unicamente a forma quadrática f (e não simplismente a classe de f módulo $\cong$). Com efeito, $Q_f = Q_g$ implica

$$(M_f)_{ii} = Q_f(\mathbf{e}_i) = Q_g(\mathbf{e}_i) = (M_g)_{ii}$$

e para $i \neq j$

$$Q_f(\mathbf{e}_i + \mathbf{e}_j) = (M_f)_{ii} + 2(M_f)_{ij} + (M_f)_{jj}$$
$$Q_g(\mathbf{e}_i + \mathbf{e}_j) = (M_g)_{ii} + 2(M_g)_{ij} + (M_g)_{jj}$$

ou seja,

$$(M_f)_{ij} = (M_g)_{ij} \quad \forall\, i, j \in \{1 \dots n\}.$$

Portanto, $M_f = M_g$.

Em virtude dessa observação, não faremos distinção entre formas quadráticas e aplicações quadráticas.

A aplicação Q_f apresenta as seguintes propriedades:

(1) $B_f : F^n \times F^n \to F$ dada por

$$B_f(\mathbf{x}, \mathbf{y}) = \frac{Q_f(\mathbf{x}+\mathbf{y}) - Q_f(\mathbf{x}) - Q_f(\mathbf{y})}{2}$$

é uma forma bilinear simétrica.

(2) $Q_f(\alpha\mathbf{x}) = \alpha^2 Q_f(\mathbf{x})$, $\forall\, \alpha \in F$ e $\forall\, \mathbf{x} \in F^n$.

Seja V um F-espaço vetorial de dimensão finita, e $B : V \times V \to F$ uma forma bilinear simétrica sobre V.

Definição 1.4. O par (V, B) é chamado de **espaço quadrático**.

Associado a um espaço quadrático (V, B) temos uma função $q = q_B : V \to F$ dada por

$$q(\mathbf{x}) = B(\mathbf{x}, \mathbf{x}).$$

Essa q é tal que

$$\begin{aligned} q(\mathbf{x}+\mathbf{y}) - q(\mathbf{x}) - q(\mathbf{y}) &= B(\mathbf{x}+\mathbf{y}, \mathbf{x}+\mathbf{y}) - B(\mathbf{x}, \mathbf{x}) - B(\mathbf{y}, \mathbf{y}) \\ &= B(\mathbf{x}, \mathbf{y}) + B(\mathbf{y}, \mathbf{x}) \\ &= 2B(\mathbf{x}, \mathbf{y}). \end{aligned} \tag{1}$$

e

$$q(\alpha \mathbf{x}) = \alpha^2 q(\mathbf{x})$$

$\forall\ \alpha \in F$ e $\forall\ \mathbf{x} \in V$. Estas propriedades da q são semelhantes às apresentadas por uma função quadrática.

A identidade (1) nos diz que q ou B pode ser obtida uma da outra (desde que se conheça uma das duas), em virtude disso também escreveremos (V, q) para representar o espaço quadrático (V, B).

Seja $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ uma base de V. Através dessa base, associamos a seguinte forma quadrática ao espaço quadrático (V, B)

$$\begin{aligned} f(X_1, \ldots, X_n) &= \sum_{i,j=1}^{n} B(\mathbf{e}_i, \mathbf{e}_j) X_i X_j \\ &= \mathbf{X}^t M_f \mathbf{X} \end{aligned}$$

com $(M_f)_{ij} = B(\mathbf{e}_i, \mathbf{e}_j)$.

Se identificarmos V com F^n via as coordenadas da base dada, então $q = q_B$ corresponde exatamente a função quadrática Q_f. Se ecolhermos outra base $\{\mathbf{e}'_1, \ldots, \mathbf{e}'_n\}$ para V, dado que

$$\mathbf{e}'_i = \sum_{j=1}^{n} c_{ji} \mathbf{e}_j$$

segue-se que a forma quadrática f' proveniente dessa nova base de V é tal que

$$\begin{aligned} (M_{f'})_{ij} &= B\left(\sum_k c_{ki} \mathbf{e}_k, \sum_l c_{lj} \mathbf{e}_l \right) \\ &= \sum_{k,l} c_{ki} B(\mathbf{e}_k, \mathbf{e}_l) c_{lj} \\ &= (C^t M_f C)_{ij} \end{aligned}$$

onde $C = (c_{kl})$. Assim, o espaço quadrático (V, B) determina unicamente uma classe de equivalência de formas quadráticas a qual denotaremos por (f_B).

Definição 1.5. Dois espaços quadráticos (V, B) e (V', B') são ditos **isométricos** ($(V, B) \cong (V', B')$) se existe um isomorfismo linear $\tau : V \to V'$ tal que

$$B'(\tau(\mathbf{x}), \tau(\mathbf{y})) = B(\mathbf{x}, \mathbf{y}) \text{ para cada } \mathbf{x}, \mathbf{y} \in V.$$

A relação de isometria entre espaços quadráticos é obviamente de equivalência. Simbolizaremos a classe de isometria de um espaço quadrático (V, B) por $[(V, B)]$.

Observação 1.6. $(V, B) \cong (V', B') \Leftrightarrow (f_B) = (f_{B'})$.

Essa observação nos diz que existe uma correspondência biunívoca entre as classes de equivalência das formas quadráticas n-árias e as classes de isometria dos espaços quadráticos n-dimensionais. Veremos essa correspondência como uma identificação.

Considere (V, B) um espaço quadrático e M uma matriz simétrica associada a uma das formas na classe de equivalência (f_B). Temos a

PROPOSIÇÃO 1.7. As seguintes afirmações são equivalentes:

(i) M é uma matriz não-singular;
(ii) $\mathbf{x} \mapsto B(\ , \mathbf{x})$ define um isomorfismo $V \to V^*$, onde V^* denota o espaço vetorial dual de V;
(iii) Para $\mathbf{x} \in V$, $B(\mathbf{x}, \mathbf{y}) = 0$ para cada $\mathbf{y} \in V$ implica $\mathbf{x} = \mathbf{0}$.

Se uma dessas afirmações (portanto todas) é verdadeira, então chamamos o espaço quadrático (V, B) de **regular** (ou não singular). Equivalentemente, diremos que q_B é uma forma quadrática não singular. Usaremos $M(F)$ para representar o conjunto de todas as classes de isometria de espaços quadráticos regulares.

Seja (V, B) um espaço quadrático e U um subespaço de V. Definimos o **conjunto ortogonal** de U por

$$U^{\perp} = \{\mathbf{x} \in V \mid B(\mathbf{x}, \mathbf{u}) = 0, \forall\ \mathbf{u} \in U\}$$

O conjunto ortogonal de V é também chamado de o **radical** de (V, B) e é denotado por $V^{\perp} = \mathrm{rad}V$.

OBSERVAÇÃO 1.8. (V, B) regular $\Leftrightarrow \mathrm{rad}V = \{\mathbf{0}\}$.

PROPOSIÇÃO 1.9. Seja (V, B) um espaço quadrático regular e U um subespaço de V. Então:

(i) $\dim U + \dim U^{\perp} = \dim V$;
(ii) $(U^{\perp})^{\perp} = U$.

2. Diagonalização de Formas Quadráticas

Os resutados desta seção nos asseguram a existência de representantes ideais para as classes de isometria dos espaços quadráticos sobre um corpo F.

DEFINIÇÃO 1.10. Seja f uma forma quadrática n-ária sobre F e $d \in F^*$. Diremos que f **representa** d se existirem $x_1, \ldots, x_n \in F$ tais que $f(x_1, \ldots, x_n) = d$.

O conjunto dos elementos de F^* que são representados por f será denotado por $D_F(f) = D(f)$.

OBSERVAÇÃO 1.11. Se f, g são duas formas quadráticas sobre F tais que $f \cong g$, então $D(f) = D(g)$. Por isso em um espaço quadrático (V, B) podemos definir $D(V) = D_F(q_B)$.

Introduzimos agora a noção de **soma ortogonal**. Se (V_1, B_1) e (V_2, B_2) são espaços quadráticos, definimos a soma ortogonal desses dois espaços como sendo o espaço quadrático (V, B) tal que $V = V_1 \oplus V_2$ e $B : V \times V \to F$ é a aplicação definida por

$$B((\mathbf{x}_1, \mathbf{x}_2), (\mathbf{y}_1, \mathbf{y}_2))) = B_1(\mathbf{x}_1, \mathbf{y}_1) + B_2(\mathbf{x}_2, \mathbf{y}_2).$$

B é de fato uma forma bilinear simétrica. Esse novo espaço (V, B) é denotado por $(V_1, B_1) \perp (V_2, B_2)$. Note que

$$\begin{aligned} q_B(\mathbf{x}_1, \mathbf{x}_2) &= B((\mathbf{x}_1, \mathbf{x}_2), (\mathbf{x}_1, \mathbf{x}_2)) \\ &= B_1(\mathbf{x}_1, \mathbf{x}_1) + B_2(\mathbf{x}_2, \mathbf{x}_2) \\ &= q_{B_1}(\mathbf{x}_1) + q_{B_2}(\mathbf{x}_2). \end{aligned}$$

OBSERVAÇÃO 1.12.

(1) (V, B) é regular $\Leftrightarrow$ (V_1, B_1) e (V_2, B_2) são espaços regulares.
(2) Sejam $(V_1, B_1) \cong (V_1', B_1')$, $(V_2, B_2) \cong (V_2', B_2')$, $(V, B) = (V_1, B_1) \perp (V_2, B_2)$ e $(V', B') = (V_1', B_1') \perp (V_2', B_2')$. Então $[(V, B)] = [(V', B')]$.

A partir da Observação 1.12(2) concluimos que $(M(F), \perp)$ é um monóide.

Para cada $d \in F$ escreveremos $\langle d \rangle$ para denotar a classe de isometria do espaço unidimensional correspondente a forma dX^2. Claramente $\langle d \rangle$ é regular se, e somente se, $d \in F^*$.

PROPOSIÇÃO 1.13. Seja (V, B) um espaço quadrático e $d \in F^*$. Então $d \in D(V)$ se, e somente se, existe outro espaço quadrático (V', B') tal que $[V] = \langle d \rangle \perp [V']$

COROLÁRIO 1.14. Se (V, B) é um espaço quadrático sobre F, então existem escalares $d_1, \ldots, d_n$ tais que $[V] = \langle d_1 \rangle \perp \ldots \perp \langle d_n \rangle$. (Em outras palavras, toda forma quadrática n-ária é equivalente a alguma forma diagonal $d_1X_1^2 + \ldots + d_nX_n^2$.)

Notação: No que segue, abreviaremos $\langle d_1 \rangle \perp \ldots \perp \langle d_n \rangle$ por $\langle d_1, \ldots, d_n \rangle$, e para $\langle d, \ldots, d \rangle$ usaremos $n\langle d \rangle$.

COROLÁRIO 1.15. Se (V, B) é um espaço quadrático (não necessariamente regular) e S é um subespaço regular, então:

(1) $V = S \perp S^\perp$
(2) Se T é um subespaço de V tal que $V = S \perp T$, então $T = S^\perp$.

COROLÁRIO 1.16. Seja (V, B) um espaço quadrático regular. Então um subespaço S é regular se, e somente se, existe $T \subseteq V$ tal que $V = S \perp T$.

Definiremos o determinante de uma forma quadrática regular f por

$$d(f) := \det(M_f) \cdot F^{*2} \in \frac{F^*}{F^{*2}}$$

Notemos que $f \cong g \Rightarrow d(f) = d(g)$. Sendo assim, diremos doravante que o determinante de um espaço quadrático (V, B), que denotaremos por $d(V)$, é o determinante da forma f_B.

3. Plano Hiperbólico e Espaços Hiperbólicos

No capítulo seguinte faremos a construção funtorial do anel de Witt, que é de muita importância quer seja no estudo da classificação das formas quadráticas, ou no das álgebras com divisão ou até mesmo na teoria dos corpos. Uma classe de isometria que se destacará nessa construção é a do plano hiperbólico, que passaremos a considerar nesta seção.

DEFINIÇÃO 1.17. Seja $\mathbf{v}$ um vetor não nulo em um espaço quadrático (V, B). Dizemos que $\mathbf{v}$ é um vetor **isotrópico** se $B(\mathbf{v}, \mathbf{v}) = 0$ e que $\mathbf{v}$ é **anisotrópico** caso contrário. O espaço quadrático (V, B) é dito **isotrópico** se ele contém um vetor isotrópico e caso contrário ele é dito **anisotrópico**. Finalmente, dizemos que (V, B) é **totalmente isotrópico** se todo vetor em V é isotrópico (isto é, $B \equiv 0$).

PROPOSIÇÃO 1.18. Seja (V, B) um espaço quadrático bidimensional. As seguintes sentenças são equivalentes:

(1) V é regular e isotrópico;
(2) V é regular, com $d(V) = -1 \cdot F^{*2}$;
(3) $[V] = \langle 1, -1 \rangle$;
(4) V corresponde a classe das formas quadráticas binárias X_1X_2.

A classe de isometria dos espaços quadráticos bidimensionais satisfazendo as condições do teorema acima é chamada de **plano hiperbólico** e o representaremos por $\mathcal{H}$. A soma ortogonal de planos hiperbólicos será chamado de **espaço hiperbólico**.

DEFINIÇÃO 1.19. Uma forma quadrática (ou espaço quadrático) é chamada **universal** se ela representa todos os elementos não nulos de F.

TEOREMA 1.20. Seja (V, B) um espaço quadrático regular. Então:

(1) Todo subespaço totalmente isotrópico $U \subseteq V$ de dimensão r positiva está contido em um subespaço hiperbólico $T \subseteq V$de dimensão $2r$;

(2) V é isotrópico se, e somente se, V contém um plano hiperbólico.
(3) V isotrópico $\Rightarrow V$ universal.

COROLÁRIO 1.21. (**Primeiro Teorema de Representação**). Seja q uma forma quadrática regular e $d \in F^*$. Então $d \in D(q)$ se, e somente se, $q \perp \langle -d \rangle$ é isotrópico.

COROLÁRIO 1.22. Sejam q_1, q_2 duas formas quadráticas regulares de dimensões positivas. Então $q := q_1 \perp q_2$ é isotrópico se, e somente se, $D(q_1) \cap D(q_2) \neq \emptyset$.

COROLÁRIO 1.23. Para um inteiro positivo r, as seguintes sentenças são equivalentes:

(1) Qualquer forma quadrática regular de dimensão r sobre F é universal.
(2) Qualquer forma quadrática de dimensão $r+1$ sobre F é isotrópica.

4. Teorema da Decomposição e Teorema do Cancelamento de Witt

TEOREMA 1.24. (**Decomposição de Witt**) Qualquer espaço quadrático (V, q) se decompõe como uma soma ortogonal

$$(V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a)$$

onde V_t é totalmente isotrópico, V_h é hiperbólico, e V_a é anisotrópico. Além disso, se

$$(V'_t, q'_t) \perp (V'_h, q'_h) \perp (V'_a, q'_a)$$

é uma outra decomposição como acima, então

$$(V_t, q_t) \simeq (V'_t, q'_t), \;\; (V_h, q_h) \simeq (V'_h, q'_h) \text{ e } (V_a, q_a) \simeq (V'_a, q'_a).$$

TEOREMA 1.25. (**Teorema do Cancelamento de Witt**) Se q, q_1, q_2 são formas quadráticas arbitrárias, então $q \perp q_1 \cong q \perp q_2 \Rightarrow q_1 \cong q_2$.

Um monóide M é dito de cancelamento se quaisquer que sejam $x, y, z \in M$

$$x + z = y + z \Rightarrow x = y.$$

O teorema do cancelamento de Witt nos diz que $(M(F), \perp)$ é um monóide de cancelamento.

DEFINIÇÃO 1.26. O inteiro m $(= \frac{1}{2}\dim V_h)$ unicamente determinado na decomposição de Witt é chamado de **índice de Witt do espaço quadrático** (V, q). A classe de isometria de V_a é chamada a parte anisotrópica de (V, q).

COROLÁRIO 1.27. Se (V, q) é regular, o índice de Witt de (V, q) é igual a dimensão de qualquer subespaço maximal totalmente isotrópico de V.

5. Teorema das Cadeias de Equivalência de Witt

A proposição seguinte nos diz que uma forma quadrática binária q regular, a menos de isometria, é completamente determinada pelo seu determinante e por um elemento em $D(q)$.

PROPOSIÇÃO 1.28. Suponhamos $\langle a, b\rangle$, $\langle a', b'\rangle$ regulares. Então $\langle a, b\rangle = \langle a', b'\rangle$ se, e somente se, $d(q) = d(q')$ e $\langle a, b\rangle \cap \langle a', b'\rangle \neq \emptyset$.

Introduzimos agora a noção de equivalência simples para formas diagonais. Seja $q = a_1X_1^2 + \ldots + a_nX_n^2$ e $q' = b_1X_1^2 + \ldots + b_nX_n^2$. Dizemos que q e q' são simplesmente equivalentes, se existem dois índices, i e j, tais que

(1) $\langle a_i, a_j\rangle = \langle b_i, b_j\rangle$.
(2) $a_k = b_k$ sempre que k é diferente de i e j.

Mais geralmente, dizemos que duas formas diagonais f e g são cadeia-equivalentes, se existe uma sequência de formas diagonais $f_0, f_1 \ldots, f_m$ tais que $f_0 = f$, $f_m = g$, e cada f_i é simplesmente equivalente a f_{i+1} $(0 \leq i \leq m-1)$. Cadeia equivalência é claramente uma relação de equivalência sobre todas as formas diagonais (de uma dimensão fixada); ela será denotada pelo símbolo $\approx$.

TEOREMA 1.29. Sejam f e g formas diagonais arbitrárias de mesma dimensão. Então

$$f \cong g \Leftrightarrow f \approx g$$

6. Produto de Kronecker de Espaços Quadráticos

Sejam (V_1, B_1, q_1) e (V_2, B_2, q_2) dois espaços quadráticos sobre F, de dimensões m e n respectivamente. Sejam V o produto tensorial de V_1 com V_2 e $B : V \times V \to F$ a única forma bilinear satisfazendo

$$B(\mathbf{v}_1 \otimes \mathbf{v}_2, \mathbf{v}_1' \otimes \mathbf{v}_2') = B_1(\mathbf{v}_1, \mathbf{v}_1')B_2(\mathbf{v}_2, \mathbf{v}_2') \qquad (\mathbf{v}_i, \mathbf{v}_i' \in V_i).$$

O par (V, B) é um novo espaço quadrático sobre F de dimensão $m \cdot n$, chamado o **produto de Kronecker** (ou *produto tensorial*) dos (V_i, B_i)'s. A função quadrática associada $q = q_B$ satisfaz

$$\begin{aligned} q(\mathbf{v}_1 \otimes \mathbf{v}_2) &= B(\mathbf{v}_1 \otimes \mathbf{v}_2, \mathbf{v}_1 \otimes \mathbf{v}_2) \\ &= B_1(\mathbf{v}_1, \mathbf{v}_1)B_2(\mathbf{v}_2, \mathbf{v}_2) \\ &= q_1(\mathbf{v}_1)q_2(\mathbf{v}_2). \end{aligned}$$

Denotamos q por $q_1 \otimes q_2$, ou simplesmente q_1q_2.

Escolhamos bases ordenadas, $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ para V_1 e $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ para V_2. Sejam $a_{ij} = B_1(\mathbf{e}_i, \mathbf{e}_j)$, $b_{kl} = B_2(\mathbf{f}_k, \mathbf{f}_l)$. Então $M = (a_{ij})$ e $N = (b_{kl})$ são as matrizes simétricas associadas respectivamente a q_1 e q_2 nas bases dadas. Agora considere a base ordenada de V dada por

$$\{\mathbf{e}_1 \otimes \mathbf{f}_1, \mathbf{e}_1 \otimes \mathbf{f}_2, \ldots, \mathbf{e}_1 \otimes \mathbf{f}_n, \ldots, \mathbf{e}_m \otimes \mathbf{f}_1, \ldots, \mathbf{e}_m \otimes \mathbf{f}_n\}.$$

Com respeito a essa base, a forma q é representada pela seguinte matriz simétrica

$$\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{12}b_{11} & a_{12}b_{12} & \cdots & \cdots \\ a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{12}b_{21} & a_{12}b_{22} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{21}b_{11} & a_{21}b_{12} & \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} = \begin{pmatrix} a_{11}N & a_{12}N & \cdots & a_{1m}N \\ a_{21}N & a_{22}N & \cdots & a_{2m}N \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}N & a_{m2}N & \cdots & a_{mm}N \end{pmatrix}$$

a qual é precisamente o *produto de Kronecker* das duas matrizes M, N. Em particular,

$\langle a \rangle \otimes \langle b \rangle \cong \langle ab \rangle$.

O produto de Kronecker entre formas quadráticas satisfaz as leis comutativa, associativa e distributiva como segue.

(1) $q_1 \otimes q_2 \cong q_2 \otimes q_1$.
(2) $(q_1 \otimes q_2) \otimes q_3 \cong q_1 \otimes (q_2 \otimes q_3)$.
(3) $q \otimes (q_1 \perp q_2) \cong (q \otimes q_1) \perp (q \otimes q_2)$.

OBSERVAÇÃO 1.30. Definamos $\otimes : M(F) \times M(F) \to M(F)$ por

$$[(V, B)] \otimes [(V', B')] = [(V, B) \otimes (V', B')].$$

Essa operação está bem definida.

Pelas observações 1.12, 1.30 e pelas propriedades do produto tensorial, segue que $(M(F), \perp, \otimes)$ tem estrutura de semi-anel comutativo.

Usando a lei distributiva, obtemos a seguinte regra para formar o produto.

$$\langle a_1, \ldots, a_m \rangle \otimes \langle b_1, \ldots, b_n \rangle = \langle a_1 b_1, \ldots, a_i b_j, \ldots, a_m b_n \rangle.$$

OBSERVAÇÃO 1.31. Se q é uma forma regular qualquer, então $[q] \otimes \mathcal{H} = (\dim q)\mathcal{H}$.

7. Álgebras com Divisão

Seja V um F-espaço vetorial e $* : V \times V \to V$ uma aplicação bilinear. As propriedades de $*$ como aplicação bilinear garantem que

$$\mathbf{v}_1 * (\alpha \mathbf{v}_2 + \beta \mathbf{v}_3) = \alpha(\mathbf{v}_1 * \mathbf{v}_2) + \beta(\mathbf{v}_1 * \mathbf{v}_3),$$

$$(\alpha\mathbf{v}_1 + \beta\mathbf{v}_2) * \mathbf{v}_3 = \alpha(\mathbf{v}_1 * \mathbf{v}_3) + \beta(\mathbf{v}_2 * \mathbf{v}_3)$$

e

$$(\alpha\mathbf{v}_1) * \mathbf{v}_2 = \mathbf{v}_1 * (\alpha\mathbf{v}_2) = \alpha(\mathbf{v}_1 * \mathbf{v}_2),$$

i.e., uma aplicação bilinear de $V \times V$ em V define uma **multiplicação sobre** V. Observamos que tal multiplicação não é nescessariamente comutativa nem associativa.

OBSERVAÇÃO 1.32. Se $S \subseteq V$ é subconjunto gerador do F-espaço vetorial V então a multiplicação $*$ é completamente determinada pela sua ação sobre os elementos do conjunto $S \times S$.

DEFINIÇÃO 1.33. (F**-álgebra**) Um espaço vetorial V sobre F com multiplicação $*$ se diz uma F**-álgebra**, que vamos indicar com $\mathcal{A} = (\mathrm{V}, *)$.

Se a multiplicação $*$ for associativa, respectivamente comutativa, a álgebra $\mathcal{A}$ se diz **associativa**, respectivamente **comutativa**. Se $\mathbf{v} * \mathbf{u} = -\mathbf{u} * \mathbf{v}$ para qualquer $\mathbf{v}, \mathbf{u} \in V$, a álgebra $\mathcal{A}$ se diz **anti-comutativa**.

Um elemento $\mathbf{e} \in V$ se diz **identidade** de $\mathcal{A}$ se $\mathbf{e} * \mathbf{v} = \mathbf{v} * \mathbf{e} = \mathbf{v}$ para cada $\mathbf{v} \in V$. Se a identidade existe, então é claramente única. Habitualmente identificaremos a subálgebra $F * \mathbf{e}$ de uma álgebra $\mathcal{A}$ com o corpo F (pelo isomorfismo $a \mapsto a * e$ de F em $F * \mathbf{e}$). Como podemos ver, uma álgebra $\mathcal{A}$ associativa e com identidade é de fato um anel (não necessariamente comutativo), daí podermos falar nessas situações de $\mathcal{A}$-módulos, ideais a esquerda, ideais a direita, ideais bilaterais, etc.

EXEMPLO 1.34. Seja $\mathcal{A}$ uma F-álgebra associativa com identidade. Seja M um $\mathcal{A}$-módulo. Denotaremos o conjunto das aplicações $\mathcal{A}$-lineares de M em M por $\mathrm{End}_{\mathcal{A}}(M)$. Restringindo a ação linear de $\mathcal{A}$ sobre $\mathrm{End}_{\mathcal{A}}(M)$ a F vemos que $(\mathrm{End}_{\mathcal{A}}(M), +, \circ)$ tem estrutura de F-álgebra, onde $\circ$ é a operação de composição entre os elementos de $\mathrm{End}_{\mathcal{A}}(M)$.

EXEMPLO 1.35. Seja $\mathcal{A}$ uma F-álgebra associativa com identidade. A restrição da ação linear de $\mathcal{A}$ sobre o $\mathcal{A}$-módulo das matrizes de ordem n com entradas em $\mathcal{A}$ $M_n(\mathcal{A})$ a F também faz de $(M_n(\mathcal{A}), +, \cdot)$ uma F-álgebra.

EXEMPLO 1.36. Se $\mathcal{A}_1 = (V_1, *_1)$ e $\mathcal{A}_2 = (V_2, *_2)$ são duas F-álgebras podemos formar uma nova F-álgebra $\mathcal{A}$ chamada o produto tensorial da álgebra $\mathcal{A}_1$ pela álgebra $\mathcal{A}_2$. Essa nova F-álgebra é dada por $\mathcal{A} = (V_1 \otimes V_2, *)$ onde $*$ está expresso no conjunto de geradores $\{\mathbf{a} \otimes \mathbf{b} \in V_1 \otimes V_2\}$ por

$$(\mathbf{a} \otimes \mathbf{b}) * (\mathbf{a}' \otimes \mathbf{b}') = \mathbf{a} *_1 \mathbf{a}' \otimes \mathbf{b} *_2 \mathbf{b}'.$$

O produto tensorial de duas álgebras $\mathcal{A}_1$, $\mathcal{A}_2$ é representado por $\mathcal{A}_1 \otimes \mathcal{A}_2$.

EXEMPLO 1.37. Denotemos o F-espaço vetorial $V \otimes \ldots \otimes V$ (r-fatores) por $T^r(V)$ e definamos $T^0(V) = F$ e $T^1(V) = V$. Consideremos agora o F-espaço vetorial $\bigoplus T^r(V)$ que consiste das sequências $(\mathbf{u}_0, \mathbf{u}_1, \ldots)$ com somente um número finito de termos não nulos. Diremos que o produto de $(\mathbf{u}_0, \mathbf{u}_1, \ldots)$ por $(\mathbf{v}_0, \mathbf{v}_1, \ldots)$ é o vetor $(\mathbf{w}_0, \mathbf{w}_1, \ldots)$ tal que

$$\mathbf{w}_p = \sum_{0 \leq r \leq p} \mathbf{u}_r \mathbf{v}_{p-r}.$$

A álgebra assim construida é chamada de **álgebra tensorial** do espaço vetorial V e será simbolizada por $T(V)$.

EXEMPLO 1.38. Dada uma F-álgebra $\mathcal{A}$ com multiplicação $*$, a sua **álgebra oposta**, que simbolizamos por $\mathcal{A}^{\text{op}}$, como conjunto coincide com $\mathcal{A}$ e tem multiplicação $*'$ definida por

$$\mathbf{u} *' \mathbf{v} = \mathbf{v} * \mathbf{u} \ \ \forall\, \mathbf{u}, \mathbf{v} \in \mathcal{A}.$$

Um elemento $\mathbf{u} \in V$ se diz **divisor de zero de** $\mathcal{A}$ se existir $\mathbf{v} \in V \setminus \{\mathbf{0}_V\}$ tal que $\mathbf{v} * \mathbf{u} = \mathbf{0}_V$ ou $\mathbf{u} * \mathbf{v} = \mathbf{0}_V$.

Um elemento $\mathbf{v} \in V$ se diz **nilpotente** se existir um inteiro $m \geq 1$ tal que $\mathbf{v}^m := \mathbf{v} * (\mathbf{v})^{m-1} = \mathbf{0}_V$. Se $\mathbf{v} \neq \mathbf{0}_V$ for um elemento nilpotente então ele é um divisor de zero. Em geral existem divisores de zero que não são nilpotentes.

Um subespaço vetorial U de V se diz **subálgebra de** $(V, *)$ se $\mathbf{u}_1 * \mathbf{u}_2 \in U$ para cada $\mathbf{u}_1, \mathbf{u}_2 \in U$.

Sejam $\mathcal{A} = (V, *)$ e $\mathcal{A}' = (V, *')$ duas F-álgebras. Um **homomorfismo de F-álgebras** $\varphi : \mathcal{A} \to \mathcal{A}'$ é uma aplicação F-linear $\varphi : V \to V'$ tal que $\varphi(\mathbf{v} * \mathbf{u}) = \varphi(\mathbf{v}) *' \varphi(\mathbf{u})$ para cada $\mathbf{v}, \mathbf{u} \in V$. Se φ é invertível dizemos então que φ é um **isomorfismo de F-álgebras**. Duas F-álgebras $\mathcal{A}$, $\mathcal{A}'$ são ditas **isomorfas** se existe um isomorfismo entre elas. (**Notação**: $\mathcal{A} \simeq \mathcal{A}'$).

Os exemplos a seguir podem ser conferidos sem dificuldades:

EXEMPLO 1.39. Se V é um F-espaço vetorial de $\dim V = n$ então $\text{End}_F(V) \simeq M_n(F)$.

EXEMPLO 1.40. $M_r(F) \otimes_F M_s(F) \simeq M_{rs}(F)$.

DEFINIÇÃO 1.41. A dimensão de uma álgebra $\mathcal{A} = (V, *)$ é igual a dimensão do espaço vetorial V ($\dim \mathcal{A} := \dim V$).

DEFINIÇÃO 1.42. Uma F-álgebra $\mathcal{A} = (V, *)$ se diz **associativa por potências** se, para cada $\mathbf{v} \in V$ e para cada m_1, m_2 inteiros temos

$$\mathbf{v}^{m_1} * \mathbf{v}^{m_2} = \mathbf{v}^{m_1 + m_2}. \tag{2}$$

Uma F-álgebra $\mathcal{A} = (V, *)$ se diz **alternante** se, para cada $\mathbf{v}, \mathbf{u} \in V$,

$$\mathbf{v} * (\mathbf{v} * \mathbf{u}) = (\mathbf{v} * \mathbf{v}) * \mathbf{u}, \quad (\mathbf{v} * \mathbf{u}) * \mathbf{u} = \mathbf{v} * (\mathbf{u} * \mathbf{u}). \tag{3}$$

Se as aplicações esquerdas e direitas de $*$ são isomorfismos (isto é, $\forall\ \mathbf{v} \in V \mathbf{x} \mapsto \mathbf{v} * \mathbf{x}$ e $\mathbf{x} \mapsto \mathbf{x}\mathbf{v}$ são isomorfismos de V em V), $\mathcal{A} = (V, *)$ se diz uma **álgebra com divisão**. Isso significa que para cado $\mathbf{v} \in V \setminus \{\mathbf{0}_V\}$ as equações

$$\mathbf{v} * \mathbf{x} = \mathbf{u}$$

e

$$\mathbf{x} * \mathbf{v} = \mathbf{w}$$

têm solução única quaisquer que sejam $\mathbf{u}, \mathbf{w} \in V$. Se $\dim \mathcal{A} < \infty$, a existência de uma solução ou a unicidade da solução automaticamente garante a outra condição. No caso de dimensão finita portanto a condição de ser uma álgebra com divisão pode ser exprimida com a condição de não ter divisores de zero, i.e., exigir que as aplicações esquerdas e direitas de $*$ sejam injetivas.

Uma propriedade importante das álgebras com divisão alternantes (e em particular das álgebras com divisão associativas) é a presença da identidade.

PROPOSIÇÃO 1.43. Seja $\mathcal{A}$ uma F-álgebra com divisão alternante. Então existe uma identidade em $\mathcal{A}$. Em particular, em toda F-álgebra com divisão associativa existe uma identidade.

DEMONSTRAÇÃO. Seja $\mathbf{v} \in V \setminus \{\mathbf{0}_V\}$. Existe $\mathbf{e} \in V$ tal que $\mathbf{e} * \mathbf{v} = \mathbf{v}$. Sendo $\mathbf{v} \neq 0_V$, $\mathbf{e} \neq \mathbf{0}_V$. De $\mathbf{e} * (\mathbf{e} * \mathbf{v}) = \mathbf{e} * \mathbf{v} = \mathbf{v}$ e do fato de $\mathcal{A}$ ser alternante, deduzimos $\mathbf{e}^2 * \mathbf{v} = \mathbf{e} * \mathbf{v}$, i.e. $(\mathbf{e}^2 - \mathbf{e}) * \mathbf{v} = \mathbf{0}_V$. Sendo $\mathbf{v} \neq \mathbf{0}_V$, temos $\mathbf{e}^2 = \mathbf{e}$. De $\mathbf{e} \neq \mathbf{0}_V$ e de

$$\mathbf{e} * (\mathbf{e} * \mathbf{u} - \mathbf{u}) = \mathbf{e} * (\mathbf{e} * \mathbf{u}) - \mathbf{e} * \mathbf{u} = \mathbf{e}^2 * \mathbf{u} - \mathbf{e} * \mathbf{u} = \mathbf{0}_V$$

deduzimos $\mathbf{e} * \mathbf{u} = \mathbf{u}$ para cada $\mathbf{u} \in V$. Similarmente se deduz que $\mathbf{u} * \mathbf{e} = \mathbf{u}$ para cada $\mathbf{u} \in V$. □

DEFINIÇÃO 1.44. (**F-álgebra quadrática**) Seja $\mathcal{A}$ uma F-álgebra com identidade $\mathbf{e} \in \mathcal{A}$. A álgebra $\mathcal{A}$ se diz **quadrática** se cada elemento $\mathbf{v} \in \mathcal{A}$ satisfaz uma equação quadrática do tipo

$$\mathbf{v}^2 = \alpha\mathbf{e} + \beta\mathbf{v} \tag{4}$$

com $\alpha, \beta \in F$.

EXEMPLO 1.45. Pelo teorema de Cayley-Hamilton, $M_2(F)$ é uma álgebra quadrática.

Em cada F-álgebra $\mathcal{A}$ associativa por potências e com identidade, temos um homomorfismo de F-álgebras, dito de **avaliação em v**,

$$\varphi_{\mathbf{v}} : F[\mathbf{x}] \to \mathcal{A},$$

definido como

$$\varphi_{\mathbf{v}}(f(\mathbf{x})) = a_0\mathbf{e} + a_1\mathbf{v} + \ldots + a_r\mathbf{v}^r \in \mathcal{A},$$

onde $f(\mathbf{x}) = \sum_{i=0}^{r} a_i\mathbf{x}^r$. Com essa definição podemos provar o seguinte fato interessante

PROPOSIÇÃO 1.46. Uma $\mathbb{R}$-álgebra alternante de dimensão finita e sem divisores de zero é quadrática.

DEMONSTRAÇÃO. Sejam $\mathbf{v} \in \mathcal{A}$ um elemento qualquer e $\varphi_{\mathbf{v}} : \mathbb{R}[\mathbf{x}] \to \mathcal{A}$ o homomorfismo de avaliação correspondente. O ideal $\ker(\varphi_{\mathbf{v}}) \subset \mathbb{R}[\mathbf{x}]$ é próprio porque $\dim(\mathcal{A}) < \infty$. Logo, é gerado por um polinômio mônico irredutível porque $\mathcal{A}$ não tem divisores de zero. Esse polinômio tem portanto grau menor ou igual a dois e anula $\mathbf{v}$, fornecendo uma equação do tipo (4). □

7.1. Álgebras de Composição. Quando olhamos para um espaço quadrático (V, B) tal que V aparece munido com uma multiplicação $*$, é natural perguntarmos sobre a compatibilidade dessa multiplicação com a forma bilinear B. Uma definição próxima desse questionamento é a seguinte.

DEFINIÇÃO 1.47. Sejam $\mathcal{A} = (V, *)$ uma $\mathbb{R}$-álgebra com divisão e $\langle\ ,\ \rangle$ um produto euclidiano sobre V com norma associada $\|\ \|$. Se

$$\| \mathbf{v} * \mathbf{u} \| = \| \mathbf{v} \| \cdot \| \mathbf{u} \| \tag{5}$$

para cada $\mathbf{v}, \mathbf{u} \in V$, a álgebra com divisão $\mathcal{A}$ se diz $\mathbb{R}$-**álgebra de composição** com respeito a $\langle\ ,\ \rangle$ (ou $\|\ \|$).

Duas $\mathbb{R}$-álgebras de composição $\mathcal{A} = (V, *, \langle\ ,\ \rangle)$ e $\mathcal{A}' = (V', *', \langle\ ,\ \rangle')$ se dizem isométricas se existir um isomorfismo de $\mathbb{R}$-álgebras $\varphi : V \to V'$ tal que

$$\langle \varphi(\mathbf{v}), \varphi(u) \rangle' = \langle \mathbf{v}, \mathbf{u} \rangle$$

para cada $\mathbf{v}, \mathbf{u} \in V$.

Outra pergunta natural é:

QUESTÃO 1.48. Para quais valores de $n \geq 1$ existem $\mathbb{R}$-álgebras de composição $\mathcal{A} = (V, *, \langle\ ,\ \rangle)$ de dimensão n?

Tentemos refazer essa pergunta de outra maneira. Para isso, suponhamos uma álgebra de composição $\mathcal{A}$ de dimensão $n \geq 1$ fixada e com $\mathcal{B} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ uma

base ortonormal de V com respeito ao produto euclidiano $\langle\ ,\ \rangle$. Ora, para cada $p, q = 1, \ldots, n$ existem $\gamma_{p,q}^i \in \mathbb{R}$ unicamente determinados tais que

$$\mathbf{e}_p * \mathbf{e}_q = \sum_{i=1}^{n} \gamma_{p,q}^i \mathbf{e}_i. \tag{6}$$

Sejam $\mathbf{u} = \sum_{i=1}^n u_i \mathbf{e}_i$ e $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{e}_i$. Pela bilinearidade da multiplicação temos

$$\begin{aligned} \mathbf{u} * \mathbf{v} &= \left(\sum_{p=1}^{n} u_p \mathbf{e}_p \right) * \left(\sum_{q=1}^{n} v_q \mathbf{e}_q \right) \\ &= \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q (e_p * e_q) \\ &= \sum_{i=1}^{n} \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q \gamma_{p,q}^i \mathbf{e}_i \\ &= \sum_{i=1}^{n} z_i \mathbf{e}_i \qquad (7) \end{aligned}$$

onde

$$z_i = \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q \gamma_{p,q}^i \in \mathbb{R} \tag{8}$$

são as cordenadas de $\mathbf{u} * \mathbf{v} \in V$ com respeito a base ortonormal $\mathcal{B}$.

Sendo assim, a questão 1.48 tornar-se equivalente a

QUESTÃO 1.49. Para quais valores de n existe uma identidade

$$(u_1^2 + \ldots + u_n^2)(v_1^2 + \ldots + v_n^2) = (z_1^2 + \ldots + z_n^2) \tag{9}$$

onde $u_1, \ldots, u_n$ e $v_1, \ldots, v_n$ são números reais arbitrários e

$$z_i = \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q \gamma_{p,q}^i \in \mathbb{R}?$$

A identidade (9) é chamada de **identidade sobre soma de quadrados**

OBSERVAÇÃO 1.50. Para cada $i = 1, \ldots, n$ podemos construir as **matrizes de multiplicação**:

$$C^i = \left[\gamma_{p,q}^i \right]$$

As matrizes C^i determinam completamente a multiplicação $*$ e temos

$$z_i = \begin{pmatrix} u_1 & \ldots & u_n \end{pmatrix} \cdot C^i \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Antes de respondermos à 1.49, vejamos alguns exemplos de $\mathbb{R}$-álgebras de composição:

EXEMPLO 1.51. Por razões triviais, $\mathbb{R}$ com a multiplicação usual é uma $\mathbb{R}$-álgebra de composição unidimensional.

EXEMPLO 1.52. Seja $\{\mathbf{e}_1, \mathbf{e}_2\}$ a base canônica de $\mathbb{R}^2$. Definamos uma multiplicação $*$ sobre $\mathbb{R}^2$ tal que $\mathbf{e}_1$ corresponda a identidade e $\mathbf{e}_2 * \mathbf{e}_2 = -\mathbf{e}_1$. Essa é uma $\mathbb{R}$-álgebra de composição isomorfa a álgebra $\mathbb{C}$ dos complexos.

EXEMPLO 1.53. Seja $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$ a base canônica de $\mathbb{R}^4$. Definamos $\mathbf{e}_1 = \mathbf{e}$ a identidade e

$*$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$
$\mathbf{e}_2$	$-\mathbf{e}_1$	$\mathbf{e}_4$	$-\mathbf{e}_3$
$\mathbf{e}_3$	$-\mathbf{e}_4$	$-\mathbf{e}_1$	$\mathbf{e}_2$
$\mathbf{e}_4$	$\mathbf{e}_3$	$-\mathbf{e}_2$	$-\mathbf{e}_1$

Nesse caso temos:

$$\begin{aligned} z_1 &= u_1v_1 - u_2v_2 - u_3v_3 - u_4v_4, \\ z_2 &= u_1v_2 + u_2v_1 + u_3v_4 - u_4v_3, \\ z_3 &= u_1v_3 - u_2v_4 + u_3v_1 + u_4v_2, \\ z_4 &= u_1v_4 + u_2v_3 - u_3v_2 + u_4v_1. \end{aligned}$$

que satisfazem a fórmula 9. Logo, essa é uma $\mathbb{R}$-álgebra de composição de dimensão 4. Essa $\mathbb{R}$-álgebra é chamada de álgebra dos quatérnios e a indicamos por $\mathbb{H}$ em homenagem Sir Rowan Hamilton. Podemos verificar, via a tabela de multiplicação acima, que $\mathbb{H}$ é associativa, com identidade e não comutativa.

EXEMPLO 1.54. Seja agora $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \mathbf{e}_5, \mathbf{e}_6, \mathbf{e}_7, \mathbf{e}_8\}$ a base canônica de $\mathbb{R}^8$. Definamos $\mathbf{e}_1 = \mathbf{e}$ a identidade e

$*$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$
$\mathbf{e}_2$	$-\mathbf{e}_1$	$\mathbf{e}_4$	$-\mathbf{e}_3$	$\mathbf{e}_6$	$-\mathbf{e}_5$	$-\mathbf{e}_8$	$\mathbf{e}_7$
$\mathbf{e}_3$	$-\mathbf{e}_4$	$-\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_7$	$\mathbf{e}_8$	$-\mathbf{e}_5$	$\mathbf{e}_6$
$\mathbf{e}_4$	$\mathbf{e}_3$	$-\mathbf{e}_2$	$-\mathbf{e}_1$	$\mathbf{e}_8$	$-\mathbf{e}_7$	$\mathbf{e}_6$	$-\mathbf{e}_5$
$\mathbf{e}_5$	$-\mathbf{e}_6$	$-\mathbf{e}_7$	$-\mathbf{e}_8$	$-\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$
$\mathbf{e}_6$	$\mathbf{e}_5$	$-\mathbf{e}_8$	$\mathbf{e}_7$	$-\mathbf{e}_2$	-$\mathbf{e}_1$	$-\mathbf{e}_4$	$\mathbf{e}_3$
$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_5$	$-\mathbf{e}_6$	$-\mathbf{e}_3$	$\mathbf{e}_4$	$-\mathbf{e}_1$	$-\mathbf{e}_2$
$\mathbf{e}_8$	$-\mathbf{e}_7$	$\mathbf{e}_6$	$\mathbf{e}_5$	$-\mathbf{e}_4$	$-\mathbf{e}_3$	$\mathbf{e}_2$	$-\mathbf{e}_1$

Daí temos

$$\begin{aligned}
z_1 &= u_1v_1 - u_2v_2 - u_3v_3 - u_4v_4 - u_5v_5 - u_6v_6 - u_7v_7 - u_8v_8,\\
z_2 &= u_1v_2 + u_2v_1 + u_3v_4 - u_4v_3 + u_5v_6 - u_6v_5 - u_7v_8 + u_8v_7,\\
z_3 &= u_1v_3 - u_2v_4 + u_3v_1 + u_4v_2 + u_5v_7 + u_6v_8 - u_7v_5 - u_8v_6,\\
z_4 &= u_1v_4 + u_2v_3 - u_3v_2 + u_4v_1 + u_5v_8 - u_6v_7 + u_7v_6 - u_8v_5,\\
z_5 &= u_1v_5 - u_2v_6 - u_3v_7 - u_4v_8 + u_5v_1 + u_6v_2 + u_7v_3 + u_8v_4,\\
z_6 &= u_1v_6 + u_2v_5 - u_3v_8 + u_4v_7 - u_5v_2 + u_6v_1 - u_7v_4 + u_8v_3,\\
z_7 &= u_1v_7 + u_2v_8 + u_3v_5 - u_4v_6 - u_5v_7 + u_6v_4 + u_7v_1 - u_8v_2,\\
z_8 &= u_1v_8 - u_2v_7 + u_3v_6 + u_4v_5 - u_5v_4 - u_6v_3 + u_7v_2 + u_8v_1.
\end{aligned}$$

Essa $\mathbb{R}$-álgebra é chamada de álgebra dos octônios e foi descoberta em 1845 por Arthur Cayley. Como vemos pela tabela ela possui identidade, não é comutativa ($\mathbf{e}_2 * \mathbf{e}_3 = \mathbf{e}_4 \neq \mathbf{e}_3 * \mathbf{e}_2 = -\mathbf{e}_4$) e não é associativa ($(\mathbf{e}_5 * \mathbf{e}_6) * \mathbf{e}_7 = -\mathbf{e}_8 \neq \mathbf{e}_5 * (\mathbf{e}_6 * \mathbf{e}_7) = \mathbf{e}_8$). Simbolizaremos-na por $\mathbb{O}$.

Finalmente, respondemos a 1.49 com o seguinte

TEOREMA 1.55. (**Hurwitz**) Existem álgebras de composição reais se, e somente se, $n = 1, 2, 4$ ou 8. Equivalentemente, temos identidade sobre soma de quadrados se, e somente se, $n = 1, 2, 4$ ou 8

Antes de fazermos sua demonstração, verifiquemos o seguinte

LEMA 1.56. Se $\{B_1, \ldots, B_{n-1}\}$ é um conjunto de matrizes anti-simétricas $n \times n$ tal que

$$B_i^2 = -I \quad 1 \leq i \leq n-1$$

e

$$B_iB_j = -B_jB_i$$

para cada $i \neq j$, então $n = 2, 4$ ou 8

DEMONSTRAÇÃO. Por hipótese, as matrizes B_i são anti-simétricas e invertíveis logo, n deve ser par. Consideremos o conjunto

$$\beta = \{B_{i_1}B_{i_2}\cdots B_{i_r} : 1 \leq i_1, \ldots, i_r \leq n-1 \text{ e } r \geq 1\}.$$

Pelas propriedades das B_i's os elementos desse conjunto são da forma

$$\pm B_1^{e_1}\cdots B_{n-1}^{e_{n-1}}, \;\; e_i = 0 \text{ ou } 1$$

que correspondem a 2^{n-1} produtos. Vejamos quais dessas matrizes são simétricas e quais são anti-simétricas. Para isso, consideremos

$$M = B_{i_1}B_{i_2}\cdots B_{i_r}, \quad r \leq n-1, \; i_1 < i_2 < \ldots < i_r. \tag{10}$$

Então, usando novamente as propriedades das B_i's, temos

$$M^t = (-1)^{r(r+1)/2} M.$$

Desse modo, M é simétrica se, e somente se, r ou $(r+1)$ é divisível por 4. Suponhamos que β não seja um conjunto linearmente independente. Então podemos escolher uma relação de dependência linear

$$\alpha_1 M_1 + \ldots + \alpha_k M_k = \mathbf{0} \tag{11}$$

tal que qualquer $\alpha_i \neq 0$ e qualquer subconjunto próprio de $\{M_1, \ldots, M_k\}$ é linearmente independente. Ora, dessa forma, ou todas estas M_i's são simétricas ou todas elas são anti-simétricas. Multiplicando (11) por $\alpha_1^{-1} M_1^{-1}$ podemos assumir essa relação da forma

$$I = \beta_1 M_1 + \ldots + \beta_{k-1} M_{k-1}. \tag{12}$$

Suponhamos que M_1 envolva o menor número r de fatores e que $r < n-1$. Se r não é divisível por 4, podemos escolher $j \neq i_1, \ldots, i_r$ e multiplicar (12) por B_j obtendo

$$B_j = \beta_1 M_1 B_j + \ldots + \beta_{k-1} M_{k-1} B_j \tag{13}$$

com B_j anti-simétrica e $M_1 B_j$ simétrica o que é um absurdo. Por outro lado, se r é divisível por 4, multiplicando ambos os lados por B_{i_1} temos $B_{i_1} M_1$ simétrica e B_{i_1} anti-simétrica, que também é um absurdo. Isso nos diz, a única relação do tipo (12) possível é

$$I = a B_1 \cdots B_{n-1} \tag{14}$$

(se em particular esta relação acontece, n deve ser divisível por 4). Deduzimos assim que o conjunto dos produtos com no máximo $\frac{1}{2}(n-2)$ fatores é linearmente independente. O número de tais matrizes é

$$1 + \binom{n-1}{1} + \binom{n-1}{2} + \ldots + \binom{n-1}{\frac{n-2}{2}} = 2^{n-2}.$$

Sendo assim, em todo caso temos

$$2^{n-2} \leq n^2$$

e daí que n =2, 4, 6 ou 8. Contudo, $n = 6$ não é possível pois nesse caso teríamos as $2^5 = 32$ matrizes de β linearmente independentes sendo que

$$\binom{5}{1} + \binom{5}{2} + 1 = 16$$

dessas matrizes antissimétricas. Mas isso é um absurdo, pois a dimensão do espaço das matrizes anti-simétricas de ordem 6 é igual a 15. Portanto, $n = 2, 4$ ou 8. □

Passemos agora a prova do Teorema 1.55

DEMONSTRAÇÃO. Podemos assumir $n > 1$. Para um $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{R}^n$ fixado vamos definir

$$\alpha_{i,j} = \sum_{p=1}^{n} \gamma_{p,j}^{i} v_p. \tag{15}$$

A identidade (9) pode ser escrita na forma

$$(u_1^2 + \ldots + u_n^2)(v_1^2 + \ldots + v_n^2) = \left(\sum_{j=1}^{n} \alpha_{1,j} u_j\right)^2 + \ldots + \left(\sum_{j=1}^{n} \alpha_{n,j} u_j\right)^2, \tag{16}$$

Fixado $\mathbf{v}$, (16) vale para cada $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{R}^n$. Tomando $\mathbf{u} = \mathbf{e}_j$, temos

$$\begin{aligned} v_1^2 + \ldots + v_n^2 &= \alpha_{1,1}^2 + \alpha_{2,1}^2 + \ldots + \alpha_{n,1}^2 \\ &\vdots \\ v_1^2 + \ldots + v_n^2 &= \alpha_{1,n}^2 + \alpha_{2,n}^2 + \ldots + \alpha_{n,n}^2. \end{aligned} \tag{17}$$

Cancelando em (16) os termos com v_i^2 por meio de (17), deduzimos que para cada $\mathbf{u} \in \mathbb{R}^n$ vale

$$0 = 2 \sum_{i=1}^{n} \sum_{j=1}^{n} (\alpha_{1,i}\alpha_{1,j} + \ldots + \alpha_{n,i}\alpha_{n,j}) u_i u_j. \tag{18}$$

Para $\mathbf{u} = \mathbf{e}_i + \mathbf{e}_j$, deduzimos

$$0 = 2(\alpha_{1,i}\alpha_{1,j} + \ldots + \alpha_{n,i}\alpha_{n,j}) \tag{19}$$

para cada $i, j = 1, \ldots, n$. Definindo

$$A = [\alpha_{i,j}]$$

podemos escrever as equações acima na forma compacta:

$$A^t \cdot A = \left(\sum_{i=1}^{n} v_i^2\right) \cdot I. \tag{20}$$

Pela definição de A, temos

$$A = v_1 A_1 + \ldots + v_n A_n$$

com $A_i \in M_n(\mathbb{R})$ independentes dos u_i e v_i.

A equação (20) pode ser reescrita como

$$(v_1 A_1^t + \ldots + v_n A_n^t) \cdot (v_1 A_1 + \ldots + v_n A_n) = \left(\sum_{i=1}^{n} v_i^2\right) \cdot I, \tag{21}$$

que implica

$$A_i^t \cdot A_i = I \ , \ A_i \cdot A_i^t = I \tag{22}$$

para cada $i = 1, \ldots, n$.

Agora definamos $B_i = A_n^t A_i$, $i = 1, \ldots, n-1$. Então reescrevemos (21) por

$$(v_1 B_1^t + \ldots + v_{n-1} B_{n-1}^t + v_n I)(v_1 B_1 + \ldots + v_{n-1} B_{n-1} + v_n I) = \left(\sum_{i=1}^{n} v_i^2 \right) I \tag{23}$$

Daí obtemos

$$B_i^t B_i = I, \quad 1 \leq i \leq n-1.$$

Cancelando esses termos, e considerando $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$ para $i \neq j$ temos

$$B_i^t + B_i = \mathbf{0}, \quad 1 \leq i \leq n-1$$

e

$$B_i^t B_j + B_j^t Bi = \mathbf{0}, \quad 1 \leq i, j \leq n-1, \;\; i \neq j.$$

Portanto, pelo Lema 1.56, $n = 2, 4$ ou 8. □

Retornaremos a essa questão das $\mathbb{R}$-álgebras de composição no capítulo 5 onde faremos a demonstração desse último teorema por meio de resultados menos elementares.

Ao contrário do Teorema de Hurwitz, o seguinte resultado, que claramente implica no primeiro, tem até agora somente demonstrações que utilizam técnicas sofisticadas de topologia algébrica.

TEOREMA 1.57. (**Bott-Milnor-Kervaire, 1958**) Existem $\mathbb{R}$-álgebras com divisão de dimensão $n \geq 1$ se, e somente se, $n = 1, 2, 4$ ou 8.

CAPíTULO 2

Álgebras dos Quatérnios e a Forma Norma

A álgebra que construiremos nesse capítulo é uma generalização imediata da $\mathbb{R}$-álgebra $\mathbb{H}$ vista no capítulo 1. Veremos que essa álgebra pode ser tornada naturalmente um espaço quadrático e, a partir daí, chegaremos a resultados que relacionam a questão da classificação de tais álgebras módulo isomorfismo com a teoria das classes de isometria dos espaços quadráticos sobre o corpo F.

1. Construção da Álgebra dos Quatérnios

Sejam $a, b \in F^*$. Definimos a álgebra de quatérnio $A = \left(\frac{a,b}{F}\right)$ como sendo a F-álgebra gerada pelos elementos $\mathbf{i}, \mathbf{j}$ com as seguintes relações definidoras

$$\mathbf{i}^2 = a, \quad \mathbf{j}^2 = b, \quad \mathbf{ij} = -\mathbf{ji}.$$

Para $\mathbf{k} := \mathbf{ij} \in A$, temos

$$\mathbf{k}^2 = (\mathbf{ij})(\mathbf{ij}) = -\mathbf{i}^2\mathbf{j}^2 = -ab \in F^*$$

e

$$\mathbf{ik} = -\mathbf{ki} = a\mathbf{j}, \quad \mathbf{kj} = -\mathbf{jk} = b\mathbf{i}.$$

Com estas relações vê-se a associatividade dos produtos envolvendo i,j. Logo, $\left(\frac{a,b}{F}\right)$ é associativa, com identidadee não comutativa. Notemos que no caso onde $F = \mathbb{R}$ e $a = b = -1$, $\left(\frac{-1,-1}{F}\right)$ é o anel de divisão $\mathbb{H}$.

Pelas regras de multiplicação acima, é claro que $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ é um conjunto gerador do F-espaço vetorial $A = \left(\frac{a,b}{F}\right)$.

Proposição 2.1. $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ forma uma F-base para $A = \left(\frac{a,b}{F}\right)$.

Demonstração. Fixemos α, β no fecho algébrico E de F tais que $\alpha^2 = -a$, $\beta^2 = b$ e consideremos as matrizes $\mathbf{i}_0 = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}$ e $\mathbf{j}_0 = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}$ em $M_2(E)$. Cálculos diretos mostram que

$$\mathbf{i}_0^2 = aI, \quad \mathbf{j}_0^2 = bI \text{ e } \mathbf{i}_0\mathbf{j}_0 = \begin{pmatrix} \alpha\beta & 0 \\ 0 & -\alpha\beta \end{pmatrix} = -\mathbf{j}_0\mathbf{i}_0.$$

Assim, existe um homomorfismo de F-álgebras

$$\varphi : \left(\frac{a,b}{F}\right) \to M_2(E)$$

com $\varphi(\mathbf{i}) = \mathbf{i}_0$ e $\varphi(\mathbf{j}) = \mathbf{j}_0$. Como $\{I, \mathbf{i}_0, \mathbf{j}_0, \mathbf{i}_0\mathbf{j}_0\}$ é linearmente independente sobre E, $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ é linearmente independente sobre F. □

Observação 2.2. Se $K|F$ é uma extensão de corpos, então $K \otimes_F \left(\frac{a,b}{F}\right) \simeq \left(\frac{a,b}{K}\right)$ (como K-álgebras).

De agora por diante, todas as F-álgebras consideradas nesta dissertação serão de dimensão finita, associativas e com identidade.

Os objetos que definiremos na sequência serão tratados com mais detalhes no capítulo 4.

Definição 2.3. Seja A uma F-álgebra e S um subconjunto de A. O **centralizador de** S é o conjunto

$$C_A(S) = \{a \in A : as = sa \ \ \forall s \in S\}.$$

Podemos verificar facilmente que $C_A(S)$ é uma subálgebra de A. Quando $S = A$ denotamos $C_A(A)$ por $Z(A)$ e damos a esse conjunto o nome de **centro da F-álgebra** A.

Definição 2.4. Uma F-álgebra A é chamada **F-central** (ou central sobre F) se $Z(A) = F$. A é chamada **simples** se A não tem ideais bilaterais além de (0) e A. Se A é uma F-álgebra central e simples dizemos então que A é **central simples**.

Denotaremos o conjunto de todas as F-álgebras centrais simples por $\mathrm{ACS}(F)$.

Proposição 2.5. Temos as seguintes propriedades:

(1) $\left(\frac{a,b}{F}\right) \simeq \left(\frac{ax^2,by^2}{F}\right)$ quaisquer que sejam $a, b, x, y \in F^*$.
(2) $\left(\frac{-1,1}{F}\right) \simeq M_2(F)$.
(3) $\left(\frac{a,b}{F}\right) \in \mathrm{ACS}(F)$.

Demonstração. (1) Consideremos $A = \left(\frac{a,b}{F}\right)$, com base $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ como na construção geral e $A' = \left(\frac{ax^2,by^2}{F}\right)$, com base $\{1, \mathbf{i}', \mathbf{j}', \mathbf{k}'\}$ tal que $\mathbf{i}'^2 = ax^2$, $\mathbf{j}'^2 = by^2$, etc. Consideremos os elementos $x\mathbf{i}$ e $y\mathbf{j}$ em A para os quais temos

$$(x\mathbf{i})^2 = x^2\mathbf{i}^2 = ax^2, \quad (y\mathbf{j})^2 = y^2\mathbf{j}^2 \ \text{ e } \ (\mathrm{x}\mathbf{i})(\mathrm{y}\mathbf{j}) = \mathrm{xy}(\mathbf{ij}) = -\mathrm{xy}(\mathbf{ji}) = (-\mathrm{y}\mathbf{j})(\mathrm{x}\mathbf{i}).$$

Assim, $\varphi : A' \to A$ induzida por $\mathbf{i}' \mapsto x\mathbf{i}$, $\mathbf{j}' \mapsto y\mathbf{j}$ fornece um isomorfismo de F-álgebras entre A' e A.

(2) Com $a = -1$ e $b = 1$ podemos escolher $\alpha = \beta = 1 \in F$ na prova de 2.1.

(3) Considere E ser o fecho algébrico de F. Pela observação 2.2 temos

$$E \otimes_F (\frac{a,b}{F}) \simeq \left(\frac{a,b}{E}\right).$$

(1) e (2) implicam que $\left(\frac{a,b}{F}\right) \simeq M_2(E)$. Como o centro de $M_2(E)$ é E, segue que o centro de $\left(\frac{a,b}{F}\right)$ é F. Como $M_2(E)$ é E-álgebra simples, segue que $\left(\frac{a,b}{F}\right)$ é F-álgebra simples. □

DEFINIÇÃO 2.6. Um quatérnio $\mathbf{v} = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \in A$ é chamado **quatérnio puro** se $\alpha = 0$. O F-espaço dos quatérnios puro será denotado por A_0.

PROPOSIÇÃO 2.7. Seja $0 \neq \mathbf{v} \in A$. Então $\mathbf{v} \in A_0$ se, e somente se, $\mathbf{v} \notin F$ e $\mathbf{v}^2 \in F$.

DEMONSTRAÇÃO. Em geral, se $\mathbf{v} = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \in A$, então

$$(*) \quad \mathbf{v}^2 = (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2\alpha(\beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k})$$

Assim, se $\mathbf{v}$ é quatérnio puro temos

$$\mathbf{v}^2 = (a\beta^2 + b\gamma^2 - ab\delta^2) \in F.$$

Reciprocamente, se $\mathbf{v} \notin F$ e $\mathbf{v}^2 \in F$, então a equação $(*)$ implica que $\alpha = 0$, isto é, $\mathbf{v}$ é quatérnio puro.

□

Essa proposição mostra que a noção de "puridade"é independente da escolha da base $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$.

COROLÁRIO 2.8. Se $A = \left(\frac{a,b}{F}\right)$, $A' = \left(\frac{a',b'}{F}\right)$ e $\varphi : A \to A'$ é um isomorfismo de F-álgebras, então $\varphi(A_0) = A'_0$

Estudaremos agora com mais detalhes o anel de divisão dos quatérnios $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. A $\mathbb{R}$-subálgebra $\mathbb{R} + \mathbb{R}\mathbf{i}$ é claramente isomorfa ao corpo dos complexos, e desse modo podemos escrever $\mathbb{C} = \mathbb{R} + \mathbb{R}\mathbf{i} \subset \mathbb{H}$. Note que $\mathbb{H}$ não é uma $\mathbb{C}$-álgebra, mas ela é um $\mathbb{C}$-espaço vetorial, com $\mathbb{C}$-base $\{1, j\}$. De fato, qualquer quatérnio real $\mathbf{v} = x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$ pode ser escrito como

$$(x + y\mathbf{i}) + (z\mathbf{j} - w\mathbf{ji}) = \alpha + \mathbf{j}\beta$$

onde $\alpha = x + y\mathbf{i} \in \mathbb{C}$ e $\beta = z - w\mathbf{i} \in \mathbb{C}$. Temos uma "representação regular a esquerda"de $\mathbb{H}$, construída como segue. Para $\mathbf{v} \in \mathbb{H}$, denotemos por $L_\mathbf{v}$ a multiplicação a esquerda por $\mathbf{v}$ (que é $L_\mathbf{v}(\mathbf{q}) = \mathbf{vq}$). Graças a lei associativa, $L_\mathbf{v}$ é um endomorfismo do $\mathbb{C}$-espaço vetorial $\mathbb{H}$, operando pela esquerda. Como $L_{\mathbf{vv}'} = L_\mathbf{v} \circ L_{\mathbf{v}'}$, então

L define um homomorfismo de $\mathbb{R}$-álgebras

$$L : \mathbb{H} \to \mathrm{End}_{\mathbb{C}}(\mathbb{H}) \simeq M_2(\mathbb{C}).$$

Consideremos calculados $L_{\mathbf{i}}, L_{\mathbf{j}}, L_{\mathbf{k}}$ em forma matricial (com respeito a $\mathbb{C}$-base $\{1, j\}$ em $\mathbb{H}$). Por exemplo, $\mathbf{i}.1 = \mathbf{i}$ e $\mathbf{ij} = -\mathbf{ji} = \mathbf{j}(-\mathbf{i})$, e assim temos

$$L_{\mathbf{i}} = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix} \in M_2(\mathbb{C})$$

e semelhantemente

$$L_{\mathbf{j}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad L_{\mathbf{k}} = \begin{pmatrix} 0 & -\mathbf{i} \\ -\mathbf{i} & 0 \end{pmatrix}.$$

Mais geralmente, se $x, y \in \mathbb{R}$, temos

$$L_{x+y\mathbf{i}} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix} = \begin{pmatrix} x + y\mathbf{i} & 0 \\ 0 & \overline{x + y\mathbf{i}} \end{pmatrix}.$$

Assim, para um quatérnio geral $\mathbf{v} = \alpha + \mathbf{j}\beta$ (onde $\alpha, \beta \in \mathbb{C}$) temos

$$L_{\mathbf{v}} = L_\alpha + L_{\mathbf{j}} L_\beta = \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \beta & 0 \\ 0 & \overline{\beta} \end{pmatrix} = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}.$$

Ora, L é uma representação fiel da $\mathbb{R}$-álgebra $\mathbb{H}$, uma vez que

$$L_{\mathbf{v}} = 0 \Rightarrow L_{\mathbf{v}}(1) = 0 \Rightarrow \mathbf{v} = \mathbf{v}.1 = 0.$$

Consequentemente, $\mathbb{H}$ é isomorfo à subálgebra real de $M_2(\mathbb{C})$ consistindo de todas as matrizes da forma $\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}$, onde $\alpha, \beta \in \mathbb{C}$.

Corolário 2.9. O grupo dos quatérnios unitários

$$U_0 = \{x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k} \mid x^2 + y^2 + z^2 + w^2 = 1\}$$

é isomorfo ao grupo especial unitário $SU(2)$.

Demonstração. Pela representação fiel L acima, o grupo U_0 corresponde isomorficamente à

$$\{\sigma = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} : \alpha,\ \beta \in \mathbb{C}, ; \det \sigma = \alpha\overline{\alpha} + \beta\overline{\beta} = 1\}$$

o qual é precisamente o $SU(2)$.

□

Definição 2.10. Para cada $\mathbf{v} = x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k} \in \mathbb{H}$ o **conjugado** de $\mathbf{v}$ é definido como sendo o quatérnio $\overline{\mathbf{v}} = x - y\mathbf{i} - z\mathbf{j} - w\mathbf{k}$.

Se expressarmos $\mathbf{v}$ em termos da $\mathbb{C}$-base $\{1, \mathbf{j}\}$ temos $\mathbf{v} = \alpha + \mathbf{j}\beta$ onde $\alpha = x + y\mathbf{i} \in \mathbb{C}$ e $\beta = z - w\mathbf{i}$. Desse modo, podemos reescrever $\overline{\mathbf{v}}$ por

$$\overline{\alpha + \mathbf{j}\beta} = x - y\mathbf{i} - z\mathbf{j} + w\mathbf{ji} = \overline{\alpha} - j\beta,$$

onde $\overline{\alpha}$ significa o conjugado complexo de α.

No modelo matricial $L(\mathbb{H})$,

$$\alpha + \mathbf{j}\beta \longleftrightarrow \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}$$

e

$$\overline{\alpha} - \mathbf{j}\beta \longleftrightarrow \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix}.$$

Assim, conjugação em $\mathbb{H}$ corresponde precisamente a "transposta conjugada"em $M_2(\mathbb{C})$. Em particular,

$$\mathbf{v} \in \mathbb{H} \text{ puro} \Leftrightarrow \overline{\mathbf{v}} = -\mathbf{v} \Leftrightarrow \mathrm{L}_{\mathbf{v}} \text{ anti} - \text{hermitiana}.$$

Assim, o espaço tridimensional dos quatérnios puro é representado por matrizes anti-hermitianas no modelo $L(\mathbb{H})$. Por outro lado, as matrizes hermitianas em $L(\mathbb{H})$ são justamente as matrizes escalares sobre $\mathbb{R}$, e estas correspondem aos escalares em $\mathbb{R} \subset \mathbb{H}$.

2. Álgebra dos Quatérnios como Espaços Quadráticos

Considere a álgebra de quatérnio $A = \left(\frac{a,b}{F}\right)$ com base usual $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ $(a, b \in F^*)$. Desejamos tornar A um espaço quadrático.

Para qualquer quatérnio $\mathbf{x} = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$ defina o conjugado de $\mathbf{x}$ como sendo $\overline{\mathbf{x}} = \alpha - (\beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k})$. Cálculos diretos mostram que

$$\overline{\mathbf{x} + \mathbf{y}} = \overline{\mathbf{x}} + \overline{\mathbf{y}}, \quad \overline{\mathbf{x}\mathbf{y}} = \overline{\mathbf{y}}\,\overline{\mathbf{x}}, \quad \overline{\overline{\mathbf{x}}} = \mathbf{x}$$

e

$$\overline{r\mathbf{x}} = r\overline{\mathbf{x}} \quad (r \in F).$$

Definição 2.11. A função $\mathbf{x} \mapsto \overline{\mathbf{x}}$ é chamada a **involução barra** sobre A. Para $\mathbf{x} \in A$ como acima, definamos $N\mathbf{x} = \mathbf{x}\overline{\mathbf{x}}$ a **norma de** $\mathbf{x}$ e $T\mathbf{x} = \overline{\mathbf{x}} + \mathbf{x}$ o traço de $\mathbf{x}$.

Notemos que

$$\overline{T\mathbf{x}} = \overline{\mathbf{x}} + \mathbf{x} = T\mathbf{x} \Rightarrow T\mathbf{x} \in F$$

e

$$\overline{N\mathbf{x}} = \overline{\overline{\mathbf{x}}\mathbf{x}} = N\mathbf{x} \Rightarrow N\mathbf{x} \in F.$$

Definamos

$$B(\mathbf{x}, \mathbf{y}) := \frac{(\mathbf{x}\overline{\mathbf{y}} + \mathbf{y}\overline{\mathbf{x}})}{2} = \frac{T(\mathbf{x}\overline{\mathbf{y}})}{2} \in F.$$

B é claramente uma forma bilinear simétrica sobre F. Assim, (A, B) é um espaço quadrático sobre F. A forma quadrática associada com essa forma bilinear envia

$$\mathbf{x} \mapsto B(\mathbf{x}, \mathbf{x}) = \frac{T(\mathbf{x}\overline{\mathbf{x}})}{2} = 2 \cdot \frac{\mathbf{x}\overline{\mathbf{x}}}{2} = N\mathbf{x}$$

logo, N é uma forma quadrática sobre F.

Sejam $\mathbf{x}, \mathbf{y} \in A_0$. Notemos que

$$B(\mathbf{x}, \mathbf{y}) = \frac{(\mathbf{x}\overline{\mathbf{y}} + \mathbf{y}\overline{\mathbf{x}})}{2} = -\frac{(\mathbf{x}\mathbf{y} + \mathbf{y}\mathbf{x})}{2}.$$

Consequentemente, $\mathbf{x}, \mathbf{y}$ são ortogonais no espaço (A_0, B) se, e somente se, $\mathbf{x}, \mathbf{y}$ são anticomutativos em A_0. Em particular, $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$ formam uma base ortogonal para o subespaço quadrático $A_0 \subseteq A$. Além disso, se $\mathbf{x}$ é quatérnio puro, então

$$B(\mathbf{x}, 1) = \frac{T(\mathbf{x})}{2} = 0,$$

assim F é ortogonal ao subespaço A_0.

Corolário 2.12. O espaço quadrático (A, B) tem base ortogonal $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Ele é regular e isométrico a

$$\langle 1, -a, -b, ab\rangle \cong \langle 1, -a\rangle \otimes \langle 1, -b\rangle.$$

Notemos que $\langle 1, -a, -b, ab\rangle$ são precisamente formas quadráticas quadridimensionais q sobre F tais que $d(q) = 1$ e $1 \in D_F(q)$.

Corolário 2.13. Se $x = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \in A$, então $N\mathbf{x} = \alpha^2 - \beta^2 a - \gamma^2 b + \delta^2 ab$.

Proposição 2.14. Para cada $\mathbf{x}, \mathbf{y} \in A$ temos:

(1) $N(\mathbf{x}\mathbf{y}) = N\mathbf{x} \cdot N\mathbf{y}$

(2) $\mathbf{x} \in A$ é invertível $\Leftrightarrow N\mathbf{x} \neq 0$ ($\Leftrightarrow \mathbf{x}$ é anisotrópico em (A, B)).

Demonstração. (1) é consequência da conta

$$N(\mathbf{x}\mathbf{y}) = \mathbf{x}\mathbf{y}\overline{\mathbf{x}\mathbf{y}} = \mathbf{x}(\mathbf{y}\overline{\mathbf{y}})\overline{\mathbf{x}} = (\mathbf{x}\overline{\mathbf{x}})(\mathbf{y}\overline{\mathbf{y}}) = N\mathbf{x} \cdot N\mathbf{y}$$

Para (2), se x^{-1} existe, então

$$N\mathbf{x} \cdot N(\mathbf{x}^{-1}) = N(\mathbf{x}\mathbf{x}^{-1}) = N(1) = 1$$

e dai temos $N(\mathbf{x}) \neq 0$. Reciprocamente, se $N\mathbf{x} \neq 0$, a equação

$$\mathbf{x} \cdot \overline{\mathbf{x}} = N(\mathbf{x}) \cdot 1$$

implica que $\mathbf{x}^{-1}$ existe e é dado por $\overline{\mathbf{x}}/N\mathbf{x} \in A$. □

Chegamos finalmente ao resultado que mostra a equivalência entre a questão da classificação das álgebras $\left(\frac{a,b}{F}\right)$ módulo isomorfismo com a das classes de isometria dos espaços quadráticos binários sobre F.

Teorema 2.15. Para $A = \left(\frac{a,b}{F}\right)$ e $A' = \left(\frac{a',b'}{F}\right)$ as seguintes safirmações são equivalentes:

(1) A e A' são isomorfos como F-álgebras.

(2) A e A' são isométricos como espaços quadráticos.
(3) A_0 e A'_0 são isométricos como espaços quadráticos.

DEMONSTRAÇÃO. A equivalência (2) $\Leftrightarrow$ (3) é clara pelo teorema do Cancelamento de Witt. Provaremos agora (1) $\Rightarrow$ (2). Para isso, suponha $\varphi : A \to A'$ um isomorfismo de álgebras. Então o Corolário 2.8 implica que $\varphi(A_0) = \varphi(A'_0)$. Se $\mathbf{x} = \alpha + \mathbf{x}_0$, onde $\alpha \in F$ e $\mathbf{x}_0 \in A_0$, então $\overline{\mathbf{x}} = \alpha - \mathbf{x}_0$ e desse modo $\varphi(\mathbf{x}) = \alpha - \varphi(\mathbf{x}_0)$ e $\varphi(\overline{\mathbf{x}}) = \alpha - \varphi(\mathbf{x}_0)$. Como $\varphi(\mathbf{x}_0) \in A'_0$ temos $\overline{\varphi(\mathbf{x})} = \varphi(\overline{\mathbf{x}})$. Logo,

$$N(\varphi(\mathbf{x})) = \varphi(\mathbf{x}) \cdot \overline{\varphi(\mathbf{x})} = \varphi(\mathbf{x}) \cdot \varphi(\overline{\mathbf{x}}) = \varphi(\mathbf{x}\overline{\mathbf{x}}) = \varphi(N\mathbf{x}) = N\mathbf{x},$$

e assim φ é uma isometria de A em A'.

Finalmente, demonstraremos que (3) $\Rightarrow$ (1). Seja $\sigma : A_0 \to A'_0$ uma isometria. Então

$$N(\sigma(\mathbf{i})) = N(\mathbf{i}) = -a \text{ e } N(\sigma(\mathbf{i})) = \sigma(\mathbf{i})\overline{\sigma(\mathbf{i})} = -\sigma(\mathbf{i})^{2.}$$

Logo, $\sigma(\mathbf{i})^2 = a$, e analogamente, $\sigma(\mathbf{j})^2 = b$. Enfim,

$$\mathbf{i} \text{ ortogonal a } \mathbf{j} \Rightarrow \sigma(\mathbf{i}) \text{ ortogonal a } \sigma(\mathbf{j}) \Rightarrow \sigma(\mathbf{i})\sigma(\mathbf{j}) = -\sigma(\mathbf{j})\sigma(\mathbf{i}) \in A'.$$

Tudo isso implica que $A' \simeq \left(\frac{a,b}{F}\right) = A$, provando (1). □

TEOREMA 2.16. Para $A = \left(\frac{a,b}{F}\right)$ as seguintes afirmações são equivalentes:

(1) $A \simeq \left(\frac{1,-1}{F}\right)$ $(\simeq M_2(F))$
(2) A não é uma álgebra com divisão.
(3) A é isotrópico como espaço quadrático.
(4) A é hiperbólico como espaço quadrático.
(5) A_0 é isotrópico como espaço quadrático.
(6) A forma binária $\langle a, b\rangle$ representa 1.
(7) $a \in N_{E|F}(E)$, onde $E = F(\sqrt{b})$ e $N_{E|F}$ é a norma do corpo.

DEMONSTRAÇÃO. Como a forma norma de $\left(\frac{1,-1}{F}\right)$ é hiperbólica, as equivalências entre (1), (4) e (6) seguem do Teorema 2.15. Essas afirmações também são equivalemtes a (3) pois A tem determinante 1. Também temos claramente (4) $\Rightarrow$ (5) $\Rightarrow$ (3) bem como (1) $\Rightarrow$ (2) $\Rightarrow$ (3), vide Proposição 2.14(2). Isso mostra a equivalência entre (1) e (6).

Finalmente, provaremos (6) $\Leftrightarrow$ (7). Podemos assumir que $b \notin F^{*2}$ (por outro lado a equivalência é óbvia). Considere E a extensão quadrática $F(\sqrt{b})$. Como $N_{E|F}(x + y\sqrt{b}) = x^2 - by^2$ (para $x, y \in F$), a forma norma de $E|F$ é $\langle 1, -b\rangle$. Daí, temos a equivalência. □

DEFINIÇÃO 2.17. Uma extensão de corpos $K|F$ tal que $A \otimes_F K$ é isomorfa a $M_n(K)$, para alguma n conveniente, é chamado de **corpo de decomposição**. Também usamos a terminologia A **se decompõe** sobre K. No caso em que $A \simeq M_n(F)$ para algum n dizemos simplismente que A se **decompõe**.

COROLÁRIO 2.18. Seja $a \in F^*$. Então:

(1) $\left(\frac{1,a}{F}\right)$ e $\left(\frac{a,-a}{F}\right)$ ambas se decompõe.
(2) Se $a \neq 1$, então $\left(\frac{a,1-a}{F}\right)$ se decompõe.
(3) $\left(\frac{a,b}{F}\right)$ se decompõe se, e somente se, a é uma soma de dois quadrados em F.

DEMONSTRAÇÃO. As formas binárias $\langle 1, a\rangle$, $\langle a, -a\rangle$ ($\simeq \mathcal{H}$), e $\langle a, 1-a\rangle$ (nos casos $a \neq 0, 1$) representam 1. Assim, (1) e (2) seguem do critério (7) do Teorema 2.16. (3) também se deduz similarmente, bastando para isso observar as equivalências

$$1 \in D(\langle -1, a\rangle) \Leftrightarrow a \in D(\langle 1, 1\rangle) \Leftrightarrow a \text{ e uma soma de quadrados em } F.$$

□

COROLÁRIO 2.19. Se F é um corpo finito ou $F = k(t)$ onde k é um corpo algebricamente fechado, então $\left(\frac{a,b}{F}\right) \simeq M_2(F)$ quaisquer que sejam $a, b \in F^*$.

DEMONSTRAÇÃO. Por 3.16 (respectivamente 3.19) toda forma binária é universal. A conlusão segue então de 2.16(7). □

COROLÁRIO 2.20. (**Classificação das formas binárias**) As formas binárias $q = \langle a, b\rangle$ e $q' = \langle a', b'\rangle$ são isométricos se, e somente se, $d(q) = d(q')$ e $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a',b'}{F}\right)$.

DEMONSTRAÇÃO. ($\Rightarrow$) $q \cong q' \Rightarrow d(q) = d(q') \Rightarrow ab = a'b' \in F^*/F^{*2} \Rightarrow \langle 1, -a, -b, ab\rangle \simeq \langle 1, -a', -b', a'b'\rangle \Rightarrow \left(\frac{a,b}{F}\right)$ e $\left(\frac{a',b'}{F}\right)$ têm formas norma isométricas $\Rightarrow \left(\frac{a,b}{F}\right) \simeq \left(\frac{a',b'}{F}\right)$.
($\Leftarrow$) $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a',b'}{F}\right) \Rightarrow \langle 1, -a, -b, ab\rangle \simeq \langle 1, -a', -b', a'b'\rangle$. Como também $\langle ab\rangle \simeq \langle a'b'\rangle$ o Teorema do Cancelamento de Witt produz $\langle -a, -b\rangle \simeq \langle -a', -b'\rangle$. Portanto, $q \cong q'$. □

TEOREMA 2.21. (**Linearidade**) Quaisquer que sejam $a, b, c \in F^*$ temos:

$$\left(\frac{a,b}{F}\right) \otimes \left(\frac{a,c}{F}\right) \simeq \left(\frac{a,bc}{F}\right) \otimes \left(\frac{c,-a^2c}{F}\right) \simeq \left(\frac{a,bc}{F}\right) \otimes M_2(F).$$

DEMONSTRAÇÃO. Sejam $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ e $\{1, \mathbf{i}', \mathbf{j}', \mathbf{k}'\}$ as bases canônicas de $B = \left(\frac{a,b}{F}\right)$ e $C = \left(\frac{a,c}{F}\right)$ respectivamente. Considere o seguinte subespaço

$$\begin{aligned} X &= F \cdot (1 \otimes 1) + F \cdot (\mathbf{i} \otimes 1) + F \cdot (\mathbf{j} \otimes \mathbf{j}') + F \cdot (\mathbf{k} \otimes \mathbf{j}') \\ &= F \cdot 1 + F \cdot I + F \cdot J + F \cdot (IJ), \end{aligned}$$

onde $I = \mathbf{i} \otimes 1$, $J = \mathbf{j} \otimes \mathbf{j}'$ (com $IJ = \mathbf{k} \otimes \mathbf{j}'$). X é uma subálgebra quadridimensional de $B \otimes C$. De fato temos

$$I^2 = \mathbf{i}^2 \otimes 1 = a, \quad J^2 = \mathbf{j}^2 \otimes \mathbf{j}'^2 = bc, \quad -IJ = -\mathbf{ij} \otimes \mathbf{j}' = \mathbf{ji} \otimes \mathbf{j}' = JI.$$

Assim, a subálgebra X é uma cópia da álgebra de quatérnios $\left(\frac{a,bc}{F}\right)$. De maneira semelhante, considere a outra subálgebra

$$\begin{aligned} Y &= F \cdot (1 \otimes 1) + F \cdot (1 \otimes \mathbf{j}') + F \cdot (\mathbf{i} \otimes \mathbf{k}') + F \cdot (-c\mathbf{i} \otimes \mathbf{i}') \\ &= F \cdot 1 + F \cdot I' + F \cdot J' + F \cdot (I'J') \end{aligned}$$

Desse modo, Y é uma cópia da álgebra de quatérnio $\left(\frac{c,-a^2c}{F}\right)$. Por 3.11 (1) e 2.18 (1), essa álgebra é isomorfa a $M_2(F)$. Agora completamos a prova do teorema mostrando que $B \otimes C \simeq X \otimes Y$. Primeiro, por inspeção direta, o conjunto $\{I, J\}$ comuta elemento com elemento do conjunto $\{I', J'\}$. Assim, elementos de X comutam com elementos de Y. Segundo, podemos verificar facilmente que as subálgebras X e Y geram a álgebra $B \otimes C$. Dsses dois fatos segue que

$$B \otimes C \simeq X \otimes Y \simeq \left(\frac{a, bc}{F}\right) \otimes M_2(F).$$

□

CAPíTULO 3

Introdução aos Anéis de Witt

1. Definição de $\widehat{W}(F)$ e $W(F)$

O fato de um monóide M ser de cancelamento implica que a relação $\sim$, sobre $M \times M$, definida por:

$$(x, y) \sim (x', y') \Leftrightarrow x + y' = x' + y.$$

é de equivalência. Denotaremos

$$\text{Groth}(M) = \frac{(M \times M)}{\sim}$$

e definiremos

$$+ : \text{Groth}(M) \times \text{Groth}(M) \to \text{Groth}(M)$$

dada por

$$(x, y) + (x', y') = (x + x', y + y').$$

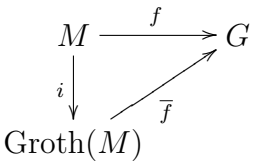
Essa operação + está bem definida e vale o seguinte resultado.

PROPOSIÇÃO 3.1. $(\text{Groth}(M), +)$ é um grupo abeliano e:

(1) A aplicação $\imath : M \to \text{Groth}(M)$ definida por

$$i(x) = (x, 0)$$

é um homomorfismo injetor de monóides tal que para quaisquer grupo abeliano G e $f : M \to G$ homomorfismo de monóides existe um único homomorfismo de grupos $\overline{f} : \text{Groth}(M) \to G$ com a propriedade de que o diagrama



é comutativo.

(2) O par $(\text{Groth}(M), i)$ é único com a propriedade acima.

DEMONSTRAÇÃO. Cálculos diretos nos mostram que as classes (x, y) e (y, x) são uma inversa da outra. Logo, $(\text{Groth}(M), +)$ é de fato um grupo abeliano. Que i é um homomorfismo injetor é trivial. Veremos essa aplicacão como uma inclusão $M \subseteq \text{Groth}(M)$. Dessa maneira, em particular, $\text{Groth}(M)$ é um grupo aditivo gerado por M. Com isso, obtemos $\overline{f}$ pela regra

$$\overline{f}(x, y) = f(x) - f(y).$$

Daí segue a afirmação (1). A asserção (2) segue de argumentos tradicionais de propriedade universal . □

É comum o abuso de notação segundo o qual o homomorfismo $\overline{f}$ é representado por f. Se M tem uma multiplicação que lhe dá a estrutura de semi anel então

$$(x, y) \cdot (x', y') = (xx' + yy', yx' + xy')$$

induz uma multiplicação sobre $\text{Groth}(M)$ que faz dele um anel comutativo.

A construção acima que estende um monóide de cancelamanto com multiplicação a um anel comutativo é chamado de **construção de Grothendieck**.

Consideremos agora o conjunto $M(F)$ de todas as classes de isometrias de formas quadráticas regulares sobre F. As operações binárias $\perp$ e $\otimes$ dão a $M(F)$ apenas estrutura de semi-anel comutativo, uma vez que os elementos não nulos de $M(F)$ não possuem inverso aditivo. Aplicando então a construção de Grothendieck a $M(F)$ temos

DEFINIÇÃO 3.2. O **anel de Witt-Grothendieck** das formas quadráticas sobre o corpo F é o anel $\widehat{W}(F) = \text{Groth}(M(F))$.

Todo elemento de $\widehat{W}(F)$ tem a expressão formal $q_1 - q_2$, onde q_1, q_2 são formas quadráticas regulares, ou classes de isometrias de tais formas. Depois que observamos que $M(F) \subseteq \widehat{W}(F)$, as duas sentenças $q_1 = q_2 \in \widehat{W}(F)$ e $q_1 \cong q_2$ são sinônimas.

Agora consideremos a função dimensão

$$\dim : M(F) \to \mathbb{Z}$$

a qual é um homomorfismo de semianéis. Esse homomorfismo se estende unicamente (via propriedade universal) a um homomorfismo de anéis $\dim : \widehat{W}(F) \to \mathbb{Z}$, por

$$\dim (q_1 - q_2) = \dim (q_2) - \dim (q_2).$$

O núcleo desse homomorfismo de anéis, denotado por $\widehat{I}F$, é chamado o **ideal fundamental** de $\widehat{W}(F)$. Temos claramente $\widehat{W}(F)/\widehat{I}F \cong \mathbb{Z}$.

PROPOSIÇÃO 3.3. $\widehat{I}F$ é aditivamente gerado pelas expressões $\langle a \rangle - \langle 1 \rangle$, $a \in F^*$.

DEMONSTRAÇÃO. Seja $z \in \widehat{I}F$, então $z = q_1 - q_2$, onde $\dim q_1 = \dim q_2 = n$. Escrevamos então $q_1 = \langle a_1, \ldots, a_n \rangle$, $q_2 = \langle b_1, \ldots, b_n \rangle$. Assim,

$$z = \sum_i (\langle a_i \rangle - \langle b_i \rangle) = \sum_i (\langle a_i \rangle - \langle 1 \rangle) - \sum_i (\langle b_i \rangle - \langle 1 \rangle).$$

□

Denotemos por $\mathbb{Z} \cdot \mathcal{H}$ o conjunto de todos os espaços hiperbólicos e seus "inversos aditivos". Esse subconjunto constitui um ideal de $\widehat{W}(F)$.

DEFINIÇÃO 3.4. O anel

$$W(F) = \frac{\widehat{W}(F)}{\mathbb{Z} \cdot \mathcal{H}}$$

é chamado o **anel de Witt** de F.

Em $W(F)$ cada elemento é representado por uma forma quadrática, uma vez que $-\langle a \rangle = \langle -a \rangle$ qualquer que seja $a \in F^*$. A proposição a seguir contém um refinamento desse resultado.

PROPOSIÇÃO 3.5. Temos as seguintes propriedades:

(1) Os elementos de $W(F)$ estão em correspondência biunívoca com as classes de isometrias de todas as formas anisotrópicas.
(2) Duas formas q, q' representam o mesmo elemento em $W(F)$ se, e somente se, $q_a \cong q'_a$. (Nesse caso q e q' são ditas "Witt semelhantes").
(3) Se $\dim(q) = \dim(q')$, então q e q' representam o mesmo elemento em $W(F)$ se, e somente se, $q \cong q'$.

DEMONSTRAÇÃO. (1) Como cada elemento em $W(F)$ é representado por uma forma q, escrevamos a decomposição de Witt de q, digamos $q = q_h \perp q_a$. Então q e q_a representam o mesmo elemento em $W(F)$. Desse modo, todo elemento de $W(F)$ é representado por uma forma anisotrópica. Agora, suponhamos q, q' formas anisotrópicas que representam um mesmo elemento em $W(F)$. Então, $q = q' + m\mathcal{H} \in \widehat{W}(F)$ para algum inteiro m. Assim, $q \cong q' \perp m\mathcal{H}$, o que implica $m = 0$. Portanto $q \cong q'$. As propriedades (2) e (3) são consequência imediata de (1). □

A imagem do ideal $\widehat{I}F$ sobre a projeção natural $\widehat{W}(F) \to W(F)$ será denotada por IF. Esse ideal é chamado de **ideal fundamental** de $W(F)$.

OBSERVAÇÃO 3.6. Como $\dim \mathcal{H} = 2$ temos, $\mathbb{Z} \cdot \mathcal{H} \cap \widehat{I}F = \{0\}$. Assim, a projeção natural induz um isomorfismo $\widehat{I}F \simeq IF$

PROPOSIÇÃO 3.7. Uma forma q representa um elemento em $IF \subseteq W(F)$ se, e somente se, $\dim(q)$ é par.

DEMONSTRAÇÃO. **se**) É suficiente provarmos para uma forma binária q, digamos, $q = \langle a, b\rangle$. Então q é a imagem de $\langle a\rangle - \langle -b\rangle \in \widehat{I}F$ através da projeção natural. Por definição, isto nos diz que $q \in IF \subseteq W(F)$.
somente se) Se q representa um elemento em IF, então existe uma equação $q = q_1 - q_2 + m\mathcal{H} \in \widehat{W}(F)$, onde $m \in \mathbb{Z}$ e $\dim q_1 = \dim q_2$. Aplicando a função "dim ", temos que $\dim q = 2m$. □

O epimorfismo de anéis

$$\dim : \widehat{W}(F) \to \mathbb{Z}$$

induz um outro epimorfismo

$$W(F) \to \frac{\mathbb{Z}}{2\mathbb{Z}},$$

o qual denotamos por $\dim_0$. Pela proposição acima, $\ker(\dim_0) = IF$, assim obtemos:

COROLÁRIO 3.8. $\dim_0$ define um isomorfismo

$$\frac{W(F)}{IF} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

2. Grupo das Classes de Quadrados

Considere a aplicação determinante $d : M(F) \to F^*/F^{*2}$ definida no capítulo 1. Verifica-se que d é um homomorfismo de monóides pois, como vimos

$$d(q_1 \perp q_2) = d(q_1)d(q_2), \forall\ q_1, q_2 \in M(F).$$

Também vimos que essa aplicação é um invariante no conjunto das classes de uma forma q.

Via propriedade universal, podemos estender esse homomorfismo a um homomorfismo d do grupo aditivo $\widehat{W}(F)$ no grupo F^*/F^{*2}. Entretanto, d não pode ser fatorado através de $W(F)$ uma vez que $d(\mathcal{H}) = -1 \cdot F^{*2}$. Para remediar isso podemos definir o sinal determinante de q por

$$d_\pm(q) = (-1)^{n(n-1)/2} d(q) \in \frac{F^*}{F^{*2}}.$$

mas como vemos facilmente, $d_\pm$ não satisfaz $d_\pm(q \perp q') = d_\pm(q).d_\pm(q')$.

A saída então para obtermos um homomorfismo apartir de d que se fatore através de $W(F)$ e que continue sendo um invariante na classe de uma forma q é a seguinte:

Definamos

$$Q(F) = \mathbb{Z}_2 \times (F^*/F^{*2})$$

e introduzamos a operação binária

$$(e,d).(e',d') = (e+e', (-1)^{ee'}dd').$$

Essa operação satisfaz as propriedades comutativa e associativa, e $(0,1)$ atua como elemento identidade. O inverso de (e,d) é $(e,(-1)^e d)$, pois

$$(e,d)(e,(-1)^e d) = (e+e,(-1)^{ee}(-1)^e dd) = (0,1).$$

Portanto, $Q(F)$ é de fato um grupo.

Observação 3.9. A inclusão $d \mapsto (0,d)$ identifica F^*/F^{*2} com um subgrupo de índice dois em $Q(F)$.

Temos a seguinte

Proposição 3.10. $(\dim_0, d_\pm)$ define um epimorfismo de monóides de $M(F)$ em $Q(F)$. Isso se estende para um epimorfismo de grupos $\widehat{W}(F) \to Q(F)$ o qual induz um isomorfismo de grupos

$$f : \frac{W(F)}{I^2F} \simeq Q(F).$$

Demonstração. A função em questão leva uma forma q em

$$(\dim_0 q, d_\pm(q)) \in Q(F)$$

(observemos que $\dim_0 q$ é $\dim(q)$ tomado módulo 2). Sejam então q e q' formas quadráticas de dimensões n e n', respectivamente, temos

$$\begin{aligned}
(\dim_0, d_\pm)(q).(\dim_0, d_\pm)(q') &= (n,(-1)^{n(n-1)/2}d(q))(n',(-1)^{n'(n'-1)/2}d(q')) \\
&= (n+n', (-1)^{nn'}(-1)^{[n(n-1)+n'(n'-1)]/2}.d(q)d(q')) \\
&= (n+n', (-1)^{(n+n')(n+n'-1)/2}.d(q \perp q')) \\
&= (\dim_0, d_\pm)(q \perp q')
\end{aligned}$$

Isso prova que $(\dim_0, d_\pm)$ é um homomorfismo.

Pela propriedade universal de $\widehat{W}(F)$, a função $(\dim_0, d_\pm)$ se estende unicamente a um epimorfismo de grupos de $\widehat{W}(F)$ em $Q(F)$ e é tal que

$$(\dim_0, d_\pm)(\mathcal{H}) = (0, (-1)\cdot d(\mathcal{H})) = (0,1)$$

e dai que de fato ele induz um epimorfismo $W(F) \to Q(F)$. Notemos pela Proposição 3.3 que IF é aditivamente gerado pelas formas binárias $\langle 1,a\rangle$, de onde segue que I^2F é aditivamente gerado pelas formas quadridimesionais $\langle 1,a\rangle \otimes \langle 1,b\rangle \cong \langle 1,a,b,ab\rangle$. Logo,

$$(\dim_0, d_\pm)(\langle 1,a,b,ab\rangle) = (0,(-1)^0.a.b.ab.F^{*2}) = (0,1)$$

assim, obtemos um epimorfismo $f : W(F)/I^2F \to Q(F)$. Para mostrar que f é isomorfismo considere $g : Q(f) \to W(F)/I^2F$ dada por

$$g(0,a) = \langle 1, -a\rangle (\text{mod } I^2F), \quad g(1,a) = \langle a\rangle (\text{mod } I^2F)$$

os seguinttes cálculos

$$\begin{aligned}
g[(0,a)(0,b)] &= g(0,ab) \\
&= \langle 1, -ab\rangle \\
&\equiv \langle 1, -a, 1, -b\rangle \\
&\equiv g(0,a) + g(0,b) (\text{mod } I^2F) \\
g[(1,a)(1,b)] &= g(0,-ab) \\
&= \langle 1, ab\rangle \\
&\equiv \langle a, b\rangle \\
&\equiv g(1,a) + g(1,b) (\text{mod } I^2F) \\
g[(0,a)(1,b)] &= g(1,ab) \\
&= \langle ab\rangle \\
&\equiv \langle 1, -a, b\rangle \\
&\equiv g(0,a) + g(1,b) (\text{mod } I^2F)
\end{aligned}$$

nos dizem que g é um homomorfismo. Fazendo $f \circ g$ obtemos a identidade de $Q(F)$. Por outro lado, $g(1,a) \equiv \langle a\rangle (\text{mod } I^2F)$, ou seja, g é sobrejetora. Assim segue-se que f e g são isomorfismos um inverso do outro. □

Corolário 3.11. (**Pfister**) I^2F consiste das classes de formas q de dimensão par para as quais $d(q) = (-1)^{n(n-1)/2}$ (onde $n = \dim(q)$)

Corolário 3.12. (**Pfister**) A restrição de f induz um isomorfismo de IF/I^2F em F^*/F^{*2}.

Corolário 3.13. As seguintes afirmações são equivalentes

(1) $\widehat{W}(F)$ é um anel noetheriano;
(2) $W(F)$ é um anel noetheriano;
(3) F^*/F^{*2} é um grupo finito.

Demonstração. (1) ⇒ (2) é consequência do resultado mais geral segundo o qual o quociente de um anéis noetherianos ainda é um anel noetheriano.
(2) ⇒ (3). Como $W(F)$ é noetheriano então IF é $W(F)$-módulo finitamente gerado.

Desse modo, IF/I^2F é um $W(F)/IF$-módulo finitamente gerado. Mas

$$\frac{W(F)}{IF} \simeq \mathbb{Z}_2,$$

logo IF/I^2F é finito. Segue-se então do Corolário 3.12 que F^*/F^{*2} é finito.

(3) $\Rightarrow$ (1) Por 2, $\widehat{W}(F)$ é aditivamente gerado por $\langle a\rangle$, $a \in F^*/F^{*2}$. Assim, (3) implica que $\widehat{W}(F)$ é um gupo abeliano finitamente gerado. Como anel, $\widehat{W}(F)$ é então noetheriano. □

Proposição 3.14. F é quadraticamente fechado se, e somente se,

$$\dim : \widehat{W}(F) \to \mathbb{Z}$$

é um isomorfismo de anéis.

Demonstração. Se F é quadraticamente fechado, então $\langle a\rangle \simeq \langle 1\rangle$, e $q \cong \dim q\langle 1\rangle$ para toda forma q. Desse modo, "dim" é um isomorfismo. Reciprocamente, se "dim" é um isomorfismo, então $\langle a\rangle \cong \langle 1\rangle$ para todo a ($\neq 0$), logo $a \in F$ é um quadrado. □

Proposição 3.15. Seja $F = \mathbb{R}$. Então:

(1) Existem exatamente duas formas anisotrópicas para cada dimensão. Para $n > 0$, elas são $n\langle 1\rangle$ e $n\langle -1\rangle$
(2) $W(F) \simeq \mathbb{Z}$.
(2) (**Lei da inércia de Silvester**) Duas formas sobre F são equivalentes se, e somente se, elas tem a mesma dimensão e a mesma assinatura (esse termo será definido na demonstração).
(4) $\widehat{W}(F) \simeq \mathbb{Z} \oplus \mathbb{Z}$. Como anel, $\widehat{W}(F)$ é isomorfo ao anel de grupos $\mathbb{Z}[G]$ de um grupo de dois elementos.

Demonstração. Temos aqui $F^*/F^{*2} = \{1, -1\}$. Se uma forma anisotrópica, em sua diagonalização tem coeficientes com sinais diferentes. Assim, (1) é óbvio. Como os elementos de $W(F)$ estão em correspondência biunívoca com as formas anisotrópicas, (2) segue imediatamente de (1).

Antes de provarmos (3) definamos inicialmente o termo assinatura. Obviamente na diagonalização de uma forma q o número de coeficientes positivos (do mesmo modo o número de coeficientes negativos) é unicamente determinado. De fato, suponha $r\langle 1\rangle \perp (n-r)\langle -1\rangle$ e $s\langle 1\rangle \perp (n-s)\langle -1\rangle$ duas diagonalizações de q ($\dim q = n$), onde $s \geq r$. Passando ao anel de Witt $W(F)$, temos a equação

$$r\langle 1\rangle - (n-r)\langle -1\rangle = s\langle 1\rangle - (n-s)\langle -1\rangle \in W(F)$$

a qual implica que $2r\langle 1\rangle = 2s\langle 1\rangle \in W(F)$. Por (2), segue que $r = s$. Assim, devemos ter $n_+ = r$ (números de termos positivos), e $n_- = n-r$ (número de termos negativos). A assinatura de q é então definida como sendo o número

$$n_+ - n_- = 2 \cdot n_+ - n.$$

Logo, duas formas são equivalentes se, e somente se, elas tem a mesma dimensão e mesma assinatura.

Para provar (4), é suficiente mostrarmos que $\langle 1\rangle$ e $\langle -1\rangle$ formam uma $\mathbb{Z}$-base livre de $\widehat{W}(F)$. Claramente eles geram $\widehat{W}(F)$. Para mostrar que são linearmente independentes, considere

$$a\langle 1\rangle + b\langle -1\rangle = 0,$$

onde $a, b \in \mathbb{Z}$. Passando para $W(F)$, vemos que $a = b$. Mas então claramente $a = b = 0$ como desejado. □

Proposição 3.16. Seja $F = \mathbb{F}_q$, e $F^*/F^{*2} = \{1, s\}$. Então:

(1) s é uma soma de dois quadrados, e
(2) toda forma binária é universal.

Demonstração. Para provar (1) dividiremos a argumentação em dois casos

(A) $-1 \in F^{*2}$. Então $\langle 1, 1\rangle \cong \langle 1, -1\rangle = \mathcal{H}$ e em particular, $\langle 1, 1\rangle$ é universal por 3.

(B) $-1 \notin F^{*2}$. Os conjuntos F^{*2} e $1 + F^{*2}$ são subconjuntos de F com a mesma cardinalidade. Eles não são iguais pois $1 \in F^{*2}$ mas $1 \notin 1 + F^{*2}$. Assim, existe um elemento da forma $1 = z^2$ que não está em $1 + F^{*2}$. Mas $1 + z^2 \neq 0$. Assim, podemos considerar $s = 1 + z^2$, o que prova (1).

Provemos agora que (1) $\Rightarrow$ (2). Como 1 e s são as únicas classes de quadrados então existe no máximo três formas binárias (regulares) não equivalentes, digamos

$$f_1 = \langle 1, 1\rangle, \quad f_2 = \langle s, s\rangle \quad f_3 = \langle 1, s\rangle.$$

Claramente, $D(f_3) = F^*$, e por (1), $D(f_1) = D(f_2) = F^*$. Isso prova (2) □

Teorema 3.17. Assuma que toda forma binária sobre o corpo F é universal. Então:

(1) duas formas quadráticas são isométricas se, e somente se, elas tem a mesma dimensão e o mesmo determinante.
(2) $\widehat{I}^2F \simeq I^2F = \mathbf{0}$ e $\widehat{I}F \simeq IF \simeq F^*/F^{*2}$.
(3) $W(F) \simeq Q(F)$ como anéis, e $\widehat{W}(F) = \mathbb{Z} \oplus \widehat{I}F$ com multiplicação trivial sobre $\widehat{I}F$.

DEMONSTRAÇÃO. Como por hipótese qualquer forma binária $\langle a_1, a_2\rangle$ representa 1, temos $\langle a_1, a_2\rangle \cong \langle 1, a_1 \cdot a_2\rangle$. Por indução, uma forma regular arbitrária $q = \langle a_1, \ldots, a_n\rangle$ é equivalente a $\langle 1, \ldots, 1, d(q)\rangle$ e isso prova (1). Por 3.3, $\widehat{I}^2F$ é aditivamente gerado por

$$(\langle a_1\rangle - \langle 1\rangle)(\langle a_2\rangle - \langle 1\rangle) = \langle a_1a_2\rangle + \langle 1\rangle - \langle a_1\rangle - \langle a_2\rangle = 0.$$

Logo, $\widehat{I}^2F = 0$, provando assim a primeira parte de (2). Segue-se que

$$\widehat{I}F \simeq IF \simeq \frac{IF}{I^2F} \simeq \frac{F^*}{F^{*2}},$$

por 2.18. Finalmente, o isomorfismo $W(F) \simeq Q(F)$ em (3) segue da Proposição 3.10 e a descrição de $\widehat{W}(F)$ segue da sequência exata curta

$$0 \to \widehat{I}F \to \widehat{W}F \to \mathbb{Z} \to 0.$$

□

LEMA 3.18. Sobre qualquer corpo F, qualquer forma quadrática $q = \langle 1, a\rangle$ é tal que $D(q)$ é um subgrupo de F^*.

DEMONSTRAÇÃO. Consideremos a álgebra $K = F[x]/(x^2 + a)$, a qual tem uma F-base $\{1, \theta\}$ onde $\theta^2 = -a$. Com respeito a essa base, multiplicação por $x + y\theta$ sobre K tem matriz $M = \begin{pmatrix} x & -ay \\ y & x \end{pmatrix}$. Assim,

$$N_{K|F}(x + y\theta) = x^2 + ay^2 = \det M.$$

Como a norma é multiplicativa, temos o resultado.

□

PROPOSIÇÃO 3.19. Seja $F = k(t)$, onde k é um corpo algebricamente fechado. Então qualquer forma quadrática binária q sobre F é universal.

DEMONSTRAÇÃO. Podemos assumir que $q = \langle 1, f\rangle$, onde $f \in F^*$. É fácil ver que o $\mathbb{F}_2$-espaço F^*/F^{*2} tem uma base $\{(t-b)F^{*2} \mid b \in k\}$. Dessa maneira, pelo Lema 3.18 é suficiente provar que $t - b \in D(q)$ para qualquer $b \in k$. Depois de uma mudança de variáveis podemos reduzir a mostrar que $t \in D(q)$, ou equivalentemente, que $\langle 1, -t, f\rangle$ é isotrópico. Mais uma aplicão do mesmo truque permite assumir que $f = t - c$. Para um tal f, a isotropia da forma $\langle 1, -t, f\rangle$ segue da equação $(\sqrt{c})^2 - t + f = 0$. □

CAPíTULO 4

O Grupo de Brauer-Wall

Faremos nesse capítulo a construção de dois funtores, ambos da categoria dos corpos de característica diferente de dois na categoria dos grupos abelianos. Um resultado que será central no estudo que segue é o Teorema de Wedderburn. Vejamos o que esse teorema nos diz.

TEOREMA 4.1. (**Teorema de Wedderburn**) Seja $A \in \mathrm{ACS}(F)$. Então existem um inteiro $n \geq 1$ e uma álgebra com divisão $D \in \mathrm{ACS}(F)$ tais que

$$A \simeq M_n(D).$$

Além disso, n é unicamente determinado e D é único a menos de isomorfismo.

Uma demonstração desse importante resultado encontra-se no Apêndice A. Chamaremos a álgebra D, unicamente determinada pelo Teorema de Wedderburn, de **álgebra básica** da álgebra A.

1. Álgebras Centrais Simples

PROPOSIÇÃO 4.2. $A, B \in \mathrm{ACS}(F) \Rightarrow A \otimes B \in \mathrm{ACS}(F)$.

Essa proposição é um caso particular da Proposição 4.37. Por esse motivo não incluiremos sua demonstração aqui.

PROPOSIÇÃO 4.3. Se $D \in \mathrm{ACS}(F)$ é uma álgebra com divisão então $M_n(D) \in \mathrm{ACS}(F)$.

DEMONSTRAÇÃO. Da Proposição A.5 temos

$$M_n(D) \simeq F \otimes M_n(F).$$

Desse modo, pela proposição anterior, é suficiente provarmos que $M_n(F) \in \mathrm{ACS}(F)$. Para isso, consideremos as matrizes $\mathbf{e}_{ij}$ que assumem valor um na entrada (i, j) e zero nas demais. Como sabemos, o conjunto de todas essas matrizes formam uma base do F-espaço vetorial $M_n(F)$. Seja $\sum_{1 \leq \lambda, \mu \leq n} \alpha_{\lambda\mu} \mathbf{e}_{\lambda\mu}$ um elemento típico de $Z(M_n(F))$. Então,

$$\mathbf{e}_{ij} \left(\sum_{1 \leq \lambda, \mu \leq n} \alpha_{\lambda\mu} \mathbf{e}_{\lambda\mu} \right) = \sum_{\mu=1}^{n} \alpha_{j\mu} \mathbf{e}_{i\mu},$$

e

$$\left(\sum_{1\leq\lambda,\mu\leq n}\alpha_{\lambda\mu}\mathbf{e}_{\lambda\mu}\right)\mathbf{e}_{ij}=\sum_{\lambda=1}^{n}\alpha_{\lambda i}\mathbf{e}_{\lambda j},$$

logo

$$\sum_{\mu=1}^{n}\alpha_{j\mu}\mathbf{e}_{i\mu}=\sum_{\lambda=1}^{n}\alpha_{\lambda i}\mathbf{e}_{\lambda j}.$$

comparando os coeficientes temos $\alpha_{j\mu}=0$ sempre que $\mu\neq j$ e $\alpha_{jj}=\alpha_{ii}$. Assim, de fato $Z(M_n(F))=F\cdot I_n$. Resta-nos demonstrar que $M_n(F)$ é simples. Suponhamos então $\mathfrak{a}$ um ideal bilateral de $M_n(F)$ não nulo. Digamos que $\sum_{1\leq\lambda,\mu\leq n}\alpha_{\lambda\mu}\mathbf{e}_{\lambda\mu}\in\mathfrak{a}$ com $\alpha_{ij}\neq 0$. Então

$$\alpha_{ij}^{-1}\mathbf{e}_{pi}(\sum_{\lambda,\mu}\alpha_{\lambda\mu}\mathbf{e}_{\lambda\mu})\mathbf{e}_{jp}=\mathbf{e}_{pp}$$

está em $\mathfrak{a}$ para $1\leq p\leq n$. Portanto, a identidade $\mathbf{e}_{11}+\ldots+\mathbf{e}_{nn}$ está em $\mathfrak{a}$. □

Proposição 4.4. Seja $A\in\mathrm{ACS}(F)$. Então $A^{\mathrm{op}}\in\mathrm{ACS}(F)$ e $A\otimes_F A^{\mathrm{op}}\simeq M_n(D)$, onde $n=\dim_F(A)$.

Uma consequência do Teorema de Wedderburn é a seguinte

Proposição 4.5. Sejam $A,B\in\mathrm{ACS}(F)$. As seguintes afirmações são equivalentes:

(1) As álgebras básicas de A e B são isomorfas.
(2) Existe uma álgebra com divisão $D\in\mathrm{ACS}(F)$ e inteiros positivos m e n tais que $A\simeq M_m(D)$ e $B\simeq M_n(D)$.
(3) Existem inteiros positivos r e s tais que $A\otimes M_r(F)\simeq B\otimes M_s(F)$.

Esse resultado nos sugere a seguinte definição

Definição 4.6. Dizemos que $A,B\in\mathrm{ACS}(F)$ são **semelhantes** (e denotamos $A\sim B$) se satisfazem as condições equivalentes do Corolário 4.5.

Claramente, pela Proposição 4.5(1), $\sim$ é uma relação de equivalência sobre $\mathrm{ACS}(F)$. Denotaremos a classe de $A\in\mathfrak{G}(F)$ por $[A]$ e $\mathrm{ACS}(F)/\sim$ por $B(F)$. Definamos

$$\cdot : B(F)\times B(F)\to B(F)$$

por

$$[A]\cdot[B]=[A\otimes B].$$

Essa operação está bem definida e vale o seguinte resultado.

Proposição 4.7. $(B(F),\cdot)$ é um grupo abeliano com identidade $[F]$ e operação inversa $[A]^{-1}=[A^{\mathrm{op}}]$.

Demonstração. Primeiro verificaremos que o produto está bem definido. Pela Proposição 4.2, se $A, B \in \mathrm{ACS}(F)$ então $A \otimes B$ também pertence a $\mathrm{ACS}(F)$. Além disso, $A \sim A'$ e $B \sim B'$ implicam as existências de $M_r(F)$, $M_s(F)$, $M_k(F)$ e $M_l(F)$ tais que $A \otimes M_r(F) \simeq A' \otimes M_s(F)$, $B \otimes M_k(F) \simeq B' \otimes M_l(F)$ e dai

$$\begin{aligned} A \otimes B \otimes M_{rk}(F) &\simeq (A \otimes M_r(F)) \otimes (B \otimes M_k(F)) \\ &\simeq (A' \otimes M_s(F)) \otimes (B' \otimes M_l(F)) \\ &\simeq A' \otimes B' \otimes M_{sl}(F). \end{aligned}$$

A associatividade e a comutatividade de $\otimes$ são transportadas para esse produto; $A \otimes F \simeq A$ implica que $[F] = 1$. Finalmente, da Proposição 4.4 temos $A \otimes_F A^{\mathrm{op}} \simeq M_n(F) \sim F$. □

Definição 4.8. $B(F)$ é chamado o **grupo de Brauer do corpo** F.

Proposição 4.9. Se $A \in \mathrm{ACS}(F)$ e B é uma subálgebra simples de A então:

(1) $C_A(B)$ é simples;
(2) $B = C_A(C_A(B))$;
(3) $\dim A = \dim B \cdot \dim C_A(B)$.

Corolário 4.10. Se $B \subseteq A$ e $A, B \in \mathrm{ACS}(F)$ então $C_A(B) \in \mathrm{ACS}(F)$ e $B \otimes C_A(B) \simeq A$.

Proposição 4.11. Temos as seguintes propriedades:

(1) Se $A, B \in \mathrm{ACS}(F)$, então $A \simeq B$ se, e somente se, $[A] = [B]$ em $B(F)$ e $\dim A = \dim B$.
(2) Toda classe em $B(F)$ é representada por uma álgebra com divisão que é unica a menos de isomorfismos.

Demonstração. (1) Se $[A] = [B]$ então $A \simeq M_n(D)$ e $B \simeq M_m(D)$; $\dim A = \dim B$ implica $m = n$ e daí temos $A \simeq B$. Reciprocamente, $A \simeq B$ implica $A \simeq B \simeq M_n(D)$ e dai, $[A] = [B]$ e $\dim A = \dim B$.
(2) Consequência imediata do Teorema de Wedderburn. □

Corolário 4.12. Se F é um corpo algebricamente fechado então $B(F) = \{1\}$

Demonstração. É suficiente provarmos que F é a única F-álgebra com divisão. Consideremos então D uma F-álgebra com divisão de dimensão n e $\mathbf{x} \in D$ um elemento não nulo. O conjunto $\{1, \mathbf{x}, \ldots, \mathbf{x}^n\}$ é linearmente dependente. Logo, podemos escolher $\varphi(t) \in F[t]$ polinômio minimal que anula $\mathbf{x}$. Como F é algebricamente fechado temos que $\varphi(t) = t - a \in F[t]$. Portanto, $\mathbf{x} \in F$. □

Observação 4.13. Uma outra tradução desse teorema é que F algebricamente fechado implica que toda álgebra central simples sobre F é isomorfa a $M_n(F)$ para algum $n \geq 1$.

Vale apena mencionar aqui também o **Teorema de Tsen**, segundo o qual o grupo de Brauer do corpo de funções racionais de uma curva algébrica irredutível sobre um corpo algebricamente fechado é trivial. Para a demonstração desse resultado consultar [**10**]. Outra classe de corpos que apresentam grupo de Brauer trivial é a dos corpos finitos. Vejamos essa afirmação através do seguinte

Teorema 4.14. (**Pequeno Teorema de Wedderburn**) Seja D uma álgebra com divisão sobre um corpo finito F. Então D é um corpo.

Demonstração. Uma observação óbvia é que o centro de uma álgebra com divisão é um corpo. Sendo assim, definamos $n = \dim_{Z(D)} D$. Digamos que $|Z(D) = q|$ (uma potência de primo ≥ 2). Temos a seguinte equação de classes para o grupo D^*

$$|D^*| = q^n - 1 = q - 1 + \sum_{C(a) \neq D^*} [D^* : C(a)]$$

onde a varia sobre o conjunto (não vazio) dos representantes das classes de conjugação de D^*. Escrevamos $r = r(a) = \dim_{Z(D)} C(a)$. Então $1 \leq r \leq n$ e $r|n$. Reescrevendo a equação das classes temos

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^r - 1}. \tag{24}$$

Como $r|n$, temos a seguinte fatoração em $\mathbb{Z}[x]$

$$x^n - 1 = \Phi_n(x)(x^r - 1)h(x) \quad (h(x) \in \mathbb{Z}[x])$$

onde $\Phi_n(x)$ é o n-ésimo polinômio ciclotômico. Essa equação implica que cada $(q^n - 1)/(q^r - 1)$ é um inteiro divisível por $\Phi_n(q)$. De (24) segue que $\Phi_n(q)|(q-1)$. Em particular,

$$q - 1 \geq |\Phi_n(q)| = \prod |q - \zeta|,$$

onde ζ varia sobre todas as n-ésimas raízes da unidade. Se $n > 1$ e $q \geq 2$ temos um absurdo pois nesse caso $|q - \zeta| > q - 1 \geq 1$ para cada ζ. Portanto, $D = Z(D)$. □

Finalizaremos essa seção com alguns resultados que indicam a possibilidade de atacar o problema da classificação das álgebras centrais simples por meio de métodos da teoria de Galois.

Teorema 4.15. Seja A uma F-álgebra de dimensão finita. Então A é uma álgebra central simples se, e somente se, existe um extensão de corpos $K|F$ finita tal que A se decompõe sobre K.

Antes de provar esse teorema discutiremos o seguinte lema:

LEMA 4.16. Sejam A uma F-álgebra de dimensão finita e $K|F$ uma extensão de corpo finita. Então $A \in \mathrm{ACS}(F)$ se, e somente se, $A \otimes_F K \in \mathrm{ACS}(K)$

DEMONSTRAÇÃO. Se $\mathfrak{a}$ é um ideal bilateral não trivial de A então $\mathfrak{a} \otimes_F K$ também é um ideal bilateral de $A \otimes_F K$. Da mesma maneira, se A não é central então $A \otimes_F K$ também não é central. Portanto, $A \otimes_F K \in \mathrm{ACS}(K)$ implica $A \in \mathrm{ACS}(F)$.

Para provarmos a recíproca é suficiente verificar o caso onde $A = D \in \mathrm{ACS}(F)$ é uma álgebra com divisão. Sobre essa hipótese, se $w_1, \ldots, w_n$ é uma F-base de K então $1 \otimes w_1, \ldots, 1 \otimes w_n$ é uma D-base de $D \otimes_F K$ como um espaço vetorial esquerdo. Dado um elemento $\mathbf{x} = \sum_{i=1}^n \alpha_i (1 \otimes w_i) \in Z(D \otimes_F K)$, para cada $\mathbf{d} \in D$ não nulo a relação $\mathbf{x} = (\mathbf{d}^{-1} \otimes 1)\mathbf{x}(\mathbf{d} \otimes 1) = \sum_{i=1}^n (\mathbf{d}^{-1}\alpha_i \mathbf{d})(1 \otimes w_i)$ implica $\mathbf{d}^{-1}\alpha_i \mathbf{d} = \alpha_i$. Como D é central sobre F, os $\alpha_i \in F$, assim $D \otimes_F K$ é central sobre K. Agora, se $\mathfrak{b}$ é um ideal bilateral não nulo de $D \otimes_F K$ gerado por $\mathbf{z}_1, \ldots, \mathbf{z}_r$, podemos assumir os $\mathbf{z}_i$ D-linearmente independentes e estende-los a uma D-base de $D \otimes_F K$ pela adjunção de alguns dos elementos $1 \otimes w_i$, digamos, $1 \otimes w_{r+1}, \ldots, 1 \otimes w_n$. Assim, para $1 \leq i \leq r$ podemos escrever

$$1 \otimes w_i = \sum_{j=r+1}^{n} \alpha_{ij}(1 \otimes w_j) + \mathbf{y}_i$$

onde $\mathbf{y}_i$ é uma combinação D-linear dos $\mathbf{z}_i$. Aqui $\mathbf{y}_1, \ldots, \mathbf{y}_r$ são linearmente independentes (porque assim são $1 \otimes w_1, \ldots, w_r$), e por isso formam uma D-base de $\mathfrak{b}$. Como $\mathfrak{b}$ é um ideal bilateral, para algum $\mathbf{d} \in D$ devemos ter $\mathbf{d}^{-1}\mathbf{y}_i\mathbf{d} \in \mathfrak{b}$ para $1 \leq i \leq r$ e desse modo existem $\beta_{il} \in D$ com $\mathbf{d}^{-1}\mathbf{y}_i\mathbf{d} = \sum \beta_{il}\mathbf{y}_l$. Podemos escrever essa relação como

$$(1 \otimes w_i) - \sum_{j=r+1}^{n} (\mathbf{d}^{-1}\alpha_{ij}\mathbf{d})(1 \otimes w_j) = \sum_{l=1}^{r} \beta_{il}(1 \otimes w_l) - \sum_{l=1}^{r} \beta_{il} \sum_{j=r+1}^{n} \alpha_{lj}(1 \otimes w_j),$$

pela qual, usando a independência dos $1 \otimes w_j$ tem-se $\beta_{ii} = 1$, $\beta_{il} = 0$ para $l \neq i$ e $\mathbf{d}^{-1}\alpha_{ij}\mathbf{d} = \alpha_{ij}$, i.e, $\alpha_{ij} \in F$. Isso significa que $\mathfrak{b}$ pode ser gerada por elementos de K (vista como uma F-subálgebra de $D \otimes_F K$ via a imersão $w \mapsto 1 \otimes w$). Como K é um corpo, devemos ter $\mathfrak{a} \cap K = K$, e daí $\mathfrak{b} = D \otimes_F K$. □

Passemos agora a demonstração de 4.15.

DEMONSTRAÇÃO. A suficiência segue do lema acima e da Proposição 4.3. Para a necessidade, notemos primeiro que denotando por $\overline{F}$ o fecho algébrico de F o lema acima com a Observação 4.13 implica que $A \otimes_F \overline{F} \simeq M_n(\overline{F})$ para algum $n \geq 1$. Agora observemos que toda extensão de corpo finita K de F está contida em $\overline{F}$. A inclusão induz uma função injetiva $A \otimes_F K \to A \otimes_F \overline{F}$ e $A \otimes_F \overline{F}$ aparece como união dos $A \otimes_F K$.

Desse modo, para uma extensão finita $K|F$ suficientemente grande contida em $\overline{F}$ a álgebra $A \otimes_F K$ contém os elementos $\mathbf{e}_1, \ldots, \mathbf{e}_{n^2}$ correspondente a base canônica de $M_n(F)$, via o isomorfismo $A \otimes_F M_n(\overline{F})$, e além disso os elementos a_{ij} que ocorrem nas relações $\mathbf{e}_i\mathbf{e}_j = \sum a_{ij}\mathbf{e}_1$ e definem a multiplicação também estão contidos em K. A aplicação que envia os $\mathbf{e}_i$ nos elementos da base canônica de $M_n(K)$ induz então um K-isomorfismo $A \otimes_F K \simeq M_n(K)$. □

Corolário 4.17. Se $A \in \mathrm{ACS}(F)$ então sua dimensão sobre F é um quadrado. O inteiro $\sqrt{\dim\, {}_FA}$ é chamado o **grau** de A.

A proposição a seguir informa que a extensão da Proposição 4.15 pode ser suposta separável.

Proposição 4.18. (**Noether-Köthe**) Toda F-álgebra central simples se decompõe sobre alguma extensão $K|F$ separável sobre F.

Demonstração. Consultar [**9**].

□

Corolário 4.19. Uma F-álgebra de dimensão finita A é central simples se, e somente se, existe um inteiro $n > 0$ e uma extensão galoisiana finita $K|F$ tal que $A \otimes_F K$ é isomorfo ao anel de matrizes $M_n(K)$.

Demonstração. Consequência do Teorema 4.15, Proposição 4.18 e do fato da teoria de Galois segundo o qual toda extensão de corpo finita e separável é pode ser imersa em uma extensão Galoisiana.

□

Proposição 4.20. Seja $A \in \mathfrak{C}(F)$ contendo uma F-subálgebra comutativa K a qual é uma extensão galoisiana finita de F de grau n. Então K é um corpo spliting de A.

Demonstração. Vide [**9**]. □

2. O Grupo $B(\mathbb{R})$

Definição 4.21. (**Tripla Hamiltoniana**) Seja $\mathcal{A}$ uma $\mathbb{R}$-álgebra com identidade $\mathbf{e}$. Três elementos $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{A}$ formam um **tripla Hamiltoniana** se verificam as nove condições de Hamilton

$*$	$\mathbf{u}$	$\mathbf{v}$	$\mathbf{w}$
$\mathbf{u}$	$-\mathbf{e}$	$\mathbf{w}$	$-\mathbf{v}$
$\mathbf{v}$	$-\mathbf{w}$	$-\mathbf{e}$	$\mathbf{u}$
$\mathbf{w}$	$\mathbf{v}$	$-\mathbf{u}$	$-\mathbf{e}$

Isso significa que idenficando $\mathbf{e}$, $\mathbf{u}$, $\mathbf{v}$ e $\mathbf{w}$ com os elementos $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$ e $\mathbf{e}_4$ de $\mathbb{H}$, respectivamente, temos um isomorfismo entre a subálgebra de $\mathcal{A}$ gerada por $<\mathbf{e}, \mathbf{u}, \mathbf{v}, \mathbf{w}>$ e $\mathbb{H}$, como vamos provar abaixo em 4.22.

Seja

$$\text{Im}(\mathcal{A}) = \{\mathbf{v} \in \mathcal{A} \ : \ \mathbf{v}^2 \in <\mathbf{e}> \text{ e } \mathbf{v} \notin <\mathbf{e}> \setminus \mathbf{0}\}. \tag{25}$$

O conjunto $\text{Im}(\mathcal{A})$ se diz **parte imaginária de** $\mathcal{A}$. Claramente

$$<\mathbf{e}> \cap \text{Im}(\mathcal{A}) = \{\mathbf{0}\}$$

e se $\mathbf{v} \in \text{Im}(\mathcal{A})$, então $\alpha\mathbf{v} \in \text{Im}(\mathcal{A})$ para cada $\alpha \in \mathbb{R}$. A terminologia é baseada na observação que no caso $\mathcal{A} = \mathbb{C}$ ou $\mathbb{H}$, existe um espaço de vetores **imaginários**, no sentido que se $\mathbf{v} \notin <\mathbf{e}>$, então $\mathbf{v}^2 \in <\mathbf{e}> = \mathbb{R}$. Observamos os seguintes resultados;

Proposição 4.22. Seja $\mathcal{A}$ uma $\mathbb{R}$-álgebra com identidade $\mathbf{e}$.

(1) Se $\mathbf{v}, \mathbf{u} \in \text{Im}(\mathcal{A})$ são linearmente independentes, então $\mathbf{e}, \mathbf{v}$ e $\mathbf{u}$ são linearmente independentes.

(2) se $\mathbf{v}, \mathbf{u}, \mathbf{v} + \mathbf{u} \in \text{Im}(\mathcal{A})$, então

$$\mathbf{u} * \mathbf{v} + \mathbf{v} * \mathbf{u} \in <\mathbf{e}>; \tag{26}$$

(3) Se $\mathcal{A}$ não tem divisores de zero, para cada elemento $\mathbf{v} \in \text{Im}(\mathcal{A})$ temos $\mathbf{v}^2 = -\omega\mathbf{e}$ com $\omega > 0$. Em particular se $\text{Im}(\mathcal{A}) \neq \emptyset$, existe $\mathbf{u} \in \text{Im}(\mathcal{A})$ tal que $\mathbf{u}^2 = -\mathbf{e}$.

(4) se $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{A}$ é uma tripla Hamiltoniana, então o homomorfismo de $\mathbb{R}$-álgebras

$$\varphi : \mathbb{H} \to \mathcal{A}$$

definido por $\varphi(\mathbf{e}_1) = \mathbf{e}$, $\varphi(\mathbf{e}_2) = \mathbf{u}$, $\varphi(\mathbf{e}_3) = \mathbf{v}$, $\varphi(\mathbf{e}_4) = \mathbf{w}$ é injetor e o subespaço $<\mathbf{u}, \mathbf{v}, \mathbf{w}>$ está contido em $\text{Im}(\mathcal{A})$.

Demonstração. Suponhamos que $\mathbf{v} = \alpha\mathbf{e} + \beta\mathbf{u}$. Teremos

$$2\alpha\beta\mathbf{u} = \mathbf{v}^2 - \alpha^2\mathbf{e} - \beta^2\mathbf{u}^2 \in <\mathbf{e}>$$

e portanto $\alpha\beta = 0$, pela definição de elementos puramente imaginários. Pela hipótese, $\alpha \neq 0$ porque $\mathbf{v}$ e $\mathbf{u}$ são linearmente independentes. A condição $\beta = 0$ implicaria $\mathbf{v} \notin \text{Im}(\mathcal{A})$. Portanto (1) está provada. A segunda parte segue observando-se que

$$\mathbf{u} * \mathbf{v} + \mathbf{v} * \mathbf{u} = (\mathbf{u} + \mathbf{v})^2 - \mathbf{u}^2 - \mathbf{v}^2 \in <\mathbf{e}> .$$

Seja $\mathbf{v} \in \text{Im}(\mathcal{A})$. Por definição $\mathbf{v}^2 = \alpha\mathbf{e}$ com $\alpha \in \mathbb{R}$. Se $\alpha \geq 0$, $\alpha = \beta^2$, $\beta \in \mathbb{R}$ e teremos

$$(\mathbf{v} - \beta\mathbf{e}) * (\mathbf{v} + \beta\mathbf{e}) = \mathbf{v}^2 - \alpha\mathbf{e} = \mathbf{0}.$$

Disso segue $\mathbf{v} = \beta\mathbf{e}$ ou $\mathbf{v} = -\beta\mathbf{e}$ e $\mathbf{v}$ não pertenceria a $\mathrm{Im}(\mathcal{A})$. Seja $\alpha = -\omega$ com $\omega > 0$ e $\omega = \gamma^2$. O elemento $\mathbf{u} = \gamma^{-1}\mathbf{v}$ é tal que $\mathbf{u}^2 = -\mathbf{e}$.

Pela definição de tripla Hamiltoniana, φ é um homomorfismo de $\mathbb{R}$-álgebras. A injetividade de φ é equivalente a mostrar que $\mathbf{e}, \mathbf{u}, \mathbf{v}$ e $\mathbf{w}$ são linearmente independentes em $\mathcal{A}$. Os vetores $\mathbf{u}$ e $\mathbf{v}$ são linearmente independetes porque se $\mathbf{v} \in < \mathbf{u} >$, teremos $\mathbf{w} = \mathbf{u} * \mathbf{v} = \mathbf{v} * \mathbf{u} = -\mathbf{w}$ e portanto $\mathbf{w} = \mathbf{0}$, contradizendo $\mathbf{w}^2 = -\mathbf{e} \neq \mathbf{0}$. A primeira parte mostra que $\mathbf{e}, \mathbf{u}$ e $\mathbf{v}$ são linearmente independentes. Se $\mathbf{w} \in < \mathbf{e}, \mathbf{u}, \mathbf{v} >$, existiriam únicos $\alpha, \beta, \gamma \in \mathbb{R}$ tais que

$$\mathbf{w} = \alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{e}.$$

Multiplicando essa relação por $\mathbf{u}$, teremos

$$-\mathbf{v} = -\alpha\mathbf{e} + \beta\mathbf{w} + \gamma\mathbf{u},$$

que implicaria, pela unicidade das constantes, $\beta^2 = -1$. Essa contradição prova a asserção, enquanto uma conta direta prova que $(\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w})^2 \in < \mathbf{e} >$. □

A noção de tripla de Hamilton deve a sua importância ao seguinte resultado de existência.

Proposição 4.23. Seja $\mathcal{A}$ uma $\mathbb{R}$-álgebra alternante sem divisores de zero e com identidade $\mathbf{e}$. Seja $U \subseteq \mathrm{Im}(\mathcal{A})$ um subespaço de dimensão dois de $\mathcal{A}$. Para cada elemento $\mathbf{u} \in U$ tal que $\mathbf{u}^2 = -\mathbf{e}$, existe $\mathbf{v} \in U$ tal que $\mathbf{u}, \mathbf{v}$ e $\mathbf{u} * \mathbf{v}$ formam uma tripla Hamiltoniana em $\mathcal{A}$.

Demonstração. A Proposição 4.22 garante a existência de $\mathbf{v}' \in U$ tal que $\mathbf{u} * \mathbf{v} + \mathbf{v} * \mathbf{u} = \beta\mathbf{e}$. Seja $\mathbf{v} = \mathbf{v}' + \delta\mathbf{u}$ com $\delta = -\beta(2\alpha)^{-1}$, onde $\mathbf{u}^2 = \alpha\mathbf{e}$. Se verifica facilmente que $\mathbf{u} * \mathbf{v} = -\mathbf{v} * \mathbf{u}$. Mostramos que se $\mathbf{w} = \mathbf{u} * \mathbf{v}$, então $\mathbf{w}^2 = -\mathbf{e}$. De $\mathbf{v} * \mathbf{w}^2 = (\mathbf{v} * \mathbf{w}) * \mathbf{w} = \mathbf{u} * \mathbf{w} = -\mathbf{v}$, deduzimos $\mathbf{v}(\mathbf{w}^2 + \mathbf{e}) = \mathbf{0}$ e portanto $\mathbf{w}^2 = -\mathbf{e}$ porque $\mathcal{A}$ não tem divisores de zero. □

O seguinte resultado de Frobenius mostra a importância da noção de elemento imaginário.

Teorema 4.24. (**Lema de Frobenius**) Seja $\mathcal{A}$ uma $\mathbb{R}$-álgebra quadrática. Então $\mathrm{Im}(\mathcal{A})$ é um subespaço vetorial de $\mathcal{A}$ e

$$\mathcal{A} = < \mathbf{e} > \oplus \mathrm{Im}(\mathcal{A}).$$

Demonstração. Sejam $\mathbf{u}, \mathbf{v} \in \mathrm{Im}(\mathcal{A})$. É suficiente mostrar que $\mathbf{u} + \mathbf{v} \in \mathrm{Im}(\mathcal{A})$ porque $\alpha\mathbf{u} \in \mathrm{Im}(\mathcal{A})$ para cada $\mathbf{u} \in \mathrm{Im}(\mathcal{A})$ e para cada $\alpha \in \mathbb{R}$. Se $\mathbf{u}$ e $\mathbf{v}$ são linearmente

dependentes, teremos $\mathbf{v} = \alpha\mathbf{u}$ e $\mathbf{u}+\mathbf{v} = (1+\alpha)\mathbf{u} \in \mathrm{Im}(\mathcal{A})$. Sejam $\mathbf{u}$ e $\mathbf{v}$ linearmente independentes. Sendo $\mathcal{A}$ quadrática,

$$(\mathbf{u}+\mathbf{v})^2 = \alpha_1\mathbf{e} + \beta_1(\mathbf{u}+\mathbf{v}), \;\; (\mathbf{u}-\mathbf{v})^2 = \alpha_2\mathbf{e} + \beta_2(\mathbf{u}-\mathbf{v}).$$

Isso implica

$$(\beta_1+\beta_2)\mathbf{u} + (\beta_1-\beta_2)\mathbf{v} = 2\mathbf{u}^2 + 2\mathbf{v}^2 - (\alpha_1+\alpha_2)\mathbf{e} \in <\mathbf{e}> .$$

A Proposição 4.22 garante que $\beta_1+\beta_2 = \beta_1-\beta_2 = 0$, i.e. $\beta_1 = \beta_2 = 0$ e $(\mathbf{u}+\mathbf{v})^2 = \alpha_1\mathbf{e}$. Pela Proposição 4.22 $\mathbf{u}+\mathbf{v} \notin <\mathbf{e}>$ e portanto $\mathbf{u}+\mathbf{v} \in \mathrm{Im}(\mathcal{A})$.

Seja $\mathbf{v} \in \mathcal{A} \setminus \mathrm{Im}(\mathcal{A})$. Por hipótese $\mathbf{v}^2 = \alpha\mathbf{e} + \beta\mathbf{v}$ e portanto $(\mathbf{v} - \beta/2\mathbf{e})^2 = (\alpha + \beta^2/4)\mathbf{e}$. O fato que $\mathbf{v} - \beta\mathbf{e} \notin <\mathbf{e}>$ implica que $\mathbf{v} - \beta\mathbf{e} \in \mathrm{Im}(\mathcal{A})$, i.e. $\mathcal{A} = <\mathbf{e}> + \mathrm{Im}(\mathcal{A})$ e portanto $\mathcal{A} = <\mathbf{e}> \oplus \mathrm{Im}(\mathcal{A})$. □

Podemos finalmente provar o seguinte interessante resultado.

Teorema 4.25. (**Frobenius, 1877**) Seja $\mathcal{A} \neq \mathbf{0}$ uma $\mathbb{R}$-álgebra associativa, quadrática e sem divisores de zero. Então a menos de isomorfismos $\mathcal{A}$ é uma das seguintes $\mathbb{R}$-álgebras: $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$.

Em particular uma $\mathbb{R}$-álgebra com divisão associativa de dimensão finita é isomorfa a uma das $\mathbb{R}$-álgebras acima.

Demonstração. Seja $n = \dim(\mathcal{A}) \geq 1$. Se $n = 1$, é imediato deduzir que o homomorfismo $\varphi : \mathcal{A} \to \mathbb{R}$ definido por $\varphi(\mathbf{e}) = 1$ é um isomorfismo de $\mathbb{R}$-álgebras. Seja $n = 2$. Pelo Lema de Frobenius temos $\mathrm{Im}(\mathcal{A}) \neq \emptyset$ e portanto existe $\mathbf{u} \in \mathcal{A}$ tal que $\mathbf{u}^2 = -\mathbf{e}$. Seja $\varphi : \mathbb{C} \to \mathcal{A}$ definido por $\varphi(1) = \mathbf{e}$ e $\varphi(i) = \mathbf{u}$. O homorfismo de $\mathbb{R}$-espaços vetoriais é um homomorfismo de álgebras que é injetor porque $\mathbf{e}$ e $\mathbf{u}$ são linearmente independentes. Sendo $n = 2$, φ é um isomorfismo e estamos no caso 2).

Seja $n \geq 3$. Sendo que $\dim(\mathrm{Im}(\mathcal{A})) \geq 2$, $\mathcal{A}$ contém uma tripla Hamiltoniana $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathrm{Im}(\mathcal{A})$ e uma subálgebra isomorfa a $\mathbb{H}$, vide Proposição 4.22 e . Seja $\mathbf{x} \in \mathrm{Im}(\mathcal{A})$ qualquer. Pela Proposição 4.22 existem $\alpha, \beta, \gamma \in \mathbb{R}$ tais que

$$\mathbf{x}*\mathbf{u} + \mathbf{u}*\mathbf{x} = \alpha\mathbf{e}\,,\; \mathbf{x}*\mathbf{v} + \mathbf{v}*\mathbf{x} = \beta\mathbf{e}\,,\; \mathbf{x}*\mathbf{w} + \mathbf{w}*\mathbf{x} = \gamma\mathbf{e}. \tag{27}$$

Multiplicando a direita a primeira equação por $\mathbf{v}$ e multiplicando a esquerda a segunda equação por $\mathbf{u}$, deduzimos

$$\mathbf{x}*\mathbf{w} + (\mathbf{u}*\mathbf{x})*\mathbf{v} = \alpha\mathbf{v}\,,\; \mathbf{u}*(\mathbf{x}*\mathbf{v}) + \mathbf{w}*\mathbf{x} = \beta\mathbf{u}$$

e portanto

$$\mathbf{x}*\mathbf{w} - \mathbf{w}*\mathbf{x} = \alpha\mathbf{v} - \beta\mathbf{u}$$

pela associatividade de $\mathcal{A}$. A última equação combinada com a terceira em (27) fornece

$$2\mathbf{x} * \mathbf{w} \in < \mathbf{e}, \mathbf{u}, \mathbf{v} >$$

e enfim $-2\mathbf{x} = \mathbf{x} * \mathbf{w}^2 \in < \mathbf{u}, \mathbf{v}, \mathbf{w} >$, i.e. $\mathrm{Im}(\mathcal{A}) = < \mathbf{u}, \mathbf{v}, \mathbf{w} >$ e $\mathcal{A} \simeq \mathbb{H}$. □

Corolário 4.26. $B(\mathbb{R}) \simeq \mathbb{Z}_2$.

Demonstração. Do teorema anterior segue que as únicas álgebras com divisão centrais simples são $\mathbb{R}$ e $\mathbb{H}$. Também temos $[\mathbb{R}] \neq [\mathbb{H}]$. Assim, o número de elementos de $B(\mathbb{R})$ é igual a dois. Daí segue o isomorfismo

$$B(\mathbb{R}) \simeq \mathbb{Z}_2.$$

□

Uma observação que decorre do Teorema da Linearidade e do Corolário 2.18 do capítulo 3 é que cada álgebra de quatérnio com divisão representa um elemento em $B(F)$ de ordem 2, como é o caso de $\mathbb{H}$ na proposição acima.

3. Álgebras Graduadas

Definição 4.27. Dizemos que uma álgebra A de dimensão finita é uma F-álgebra $\mathbb{Z}_2$-**graduada** se existem $A_0,\ A_1 \subseteq A$ tais que:

(1) $A = A_0 \oplus A_1$;
(2) $F = F \cdot 1 \subseteq A_0$
(3) $A_i A_j \subseteq A_{i+j}$ (onde os subescritos são tomados módulo 2).

A decomposição $A = A_0 \oplus A_1$ com as propriedades da definição acima é dita uma $\mathbb{Z}_2$-graduação da álgebra A.

Nesse texto consideraremos apenas álgebras $\mathbb{Z}_2$-graduadas. Por esse motivo, iremos nos referir a elas apenas por álgebras graduadas.

Os elementos de $h(A) = A_0 \cup A_1$ são chamados de elementos **homogêneos**. Para cada $a \in h(A)$ escrevemos $\partial(a) = i$ se $a \in A_i$ $(i = 0, 1)$. Em $\mathbf{0}$, a "função grau" ∂ não está bem definida porém, esse fato não trará nenhum transtorno.

Exemplo 4.28. Seja A uma álgebra graduada. Definimos a **álgebra oposta graduada** de A como sendo a álgebra graduada A^* que como conjunto coincide com A, possui graduação dada por

$$(A^*)_0 = \{\mathbf{a} \ : \ \mathbf{a} \in A_0\} \ \ (A^*)_1 = \{\mathbf{a} \ : \ \mathbf{a} \in A_1\}$$

e multiplicação induzida por

$$\mathbf{a} \cdot \mathbf{b} := (-1)^{\partial \mathbf{a} \partial \mathbf{b}} (\mathbf{ba}).$$

EXEMPLO 4.29. Sejam $F^n = V_0 \oplus V_1$ $A = M_n(F)$ e

$$A_i = \{B \in M_n(F) \mid B\mathbf{x} \in V_{i+j}\ \forall \mathbf{x}\ \in V_j, \}.$$

A decomposição $A = A_0 \oplus A_1$ é uma graduação da álgebra A. Se $V_0 =< \mathbf{e}_1 > \oplus < \mathbf{e}_3 > \oplus \ldots$ e $V_1 =< \mathbf{e}_2 > \oplus < \mathbf{e}_4 > \oplus \ldots$ denotaremos A com essa graduação por $\widehat{M}_n(F)$.

EXEMPLO 4.30. Consideremos a extensão quadrática $A = F(\sqrt{a})$. Podemos fazer A uma F-álgebra graduada declarando $A_0 = F$ e $A_1 = F \cdot \sqrt{a}$. Para ilustrar o uso dessa graduação usamos a notação $A = F\langle\sqrt{a}\rangle$. Analogamente, para a álgebra $B = F \oplus Fe$ sujeita as relações $e^2 = 1$ e $\partial(e) = 1$ também utilizaremos a notação $B = F\langle\sqrt{1}\rangle$.

EXEMPLO 4.31. A álgebra dos quatérnios $C = \left(\frac{a,b}{F}\right)$ possui uma graduação dada pela decomposição $C = C_0 \oplus C_1$, onde

$$C_0 = F \oplus F \cdot \mathbf{k}$$

e

$$C_1 = F\mathbf{i} \oplus F\mathbf{j}.$$

A álgebra dos quatérnios com essa graduação será denotada por $C = \left\langle \frac{a,b}{F} \right\rangle$.

EXEMPLO 4.32. Sejam A, B duas álgebras graduadas. Podemos induzir uma multiplicação sobre $A \otimes B$ através de

$$(\mathbf{a} \otimes \mathbf{b})(\mathbf{a}' \otimes \mathbf{b}') = (-1)^{\partial\mathbf{b}\partial\mathbf{a}} \cdot \mathbf{a}\mathbf{a}' \otimes \mathbf{b}\mathbf{b}'.$$

Mediante esse produto, a decomposição

$$A \otimes B = \left(\sum_{j+k \equiv 0 (\mathrm{mod} 2)} A_j \otimes B_k \right) \oplus \left(\sum_{j+k \equiv 1 (\mathrm{mod} 2)} A_j \otimes B_k \right)$$

fornece uma graduação à álgebra $A \otimes B$. Denotaremos a álgebra graduada assim obtida por $A\widehat{\otimes}B$ e a chamaremos de **produto tensorial graduado**.

Diremos que um subespaço $S \subseteq A$ é graduado se ele é a soma direta das interseções $S_i = S \cap A_i$. Escreveremos $h(S) := S \cap h(A)$. As noções de subálgebra graduada, ideal laterais graduados, etc, tem significados óbvios.

DEFINIÇÃO 4.33. Seja $S \subseteq A$ um subespaço graduado. O **centralizador graduado de** S é o subespaço graduado $\widehat{C}_A(S)$ tal que

$$\mathbf{c} \in h(C) \Leftrightarrow \mathbf{cs} = (-1)^{\partial\mathbf{c}\partial\mathbf{s}}\mathbf{sc} \quad \forall \mathbf{s} \in h(S).$$

No caso particular $S = A$ denotaremos $C_A(S)$ por $\widehat{Z}(A)$ e o chamaremos de **centro graduado**.

Observação 4.34. Para um subespaço graduado de uma F-álgebra graduada A temos:

(1) $\widehat{C}_A(S)$ é uma subálgebra graduada.
(2) $S \cap A_1 = \{\mathbf{0}\} \Rightarrow \widehat{C}_A(S) = C_A(S)$.

Definição 4.35. Uma F-álgebra graduada A é dita **graduada central** se $\widehat{Z}(A) = F \cdot 1$. Quando os únicos ideais bilaterais graduados de A são os triviais dizemos que A é uma **álgebra graduada simples**. Finalmente, se A é álgebra graduada central e álgebra graduada simples dizemos nesse caso que ela é uma **álgebra graduada central simples**.

O conjunto das álgebras graduadas centrais simples sobre um corpo F será representado por AGCS(F).

É imediato observar que 4.29, 4.30 e 4.31 são exemplos de álgebras graduadas centrais simples. No Exemplo 4.28, $A \in \text{AGCS}(F)$ implica $A^* \in \text{AGCS}(F)$.

Observação 4.36. A decomposição dada a $A \otimes B$ no exemplo 4.32 também fornece uma graduação a $A \otimes B$ munido da multiplicação usual. Entretanto, apesar dos cálculos serem mais fáceis, nessa situação não é verdade que o produto de duas álgebras graduadas centrais simples também seja uma álgebra graduada central simples.

Dizemos que uma álgebra graduada é **concentrada no grau** 0 se $A_1 = \{\mathbf{0}\}$. Qualquer álgebra B está associada a uma álgebra graduada (B) tal que $(B)_0 = B$ e $(B)_1 = \{\mathbf{0}\}$. Obviamente, se A é uma álgebra concentrada no 0 então $Z(A) = \widehat{Z}(A)$ e as noções de álgebra graduada central, álgebra graduada simples, álgebra graduada central simples coincidem, respectivamente, com as noções de álgebra central, álgebra simples e álgebra central simples.

Teorema 4.37. Sejam A, B álgebras graduadas e $A' \subseteq A$, $B' \subseteq B$ subálgebras graduadas, então:

(1) $\widehat{C}_{A\widehat{\otimes}B}(A'\widehat{\otimes}B') = \widehat{C}_A(A')\widehat{\otimes}\widehat{C}_B(B')$
(2) Se $A \in \text{AGCS}(F)$ e B é álgebra graduada simples então $A\widehat{\otimes}B$ álgebra graduada simples.

Demonstração. (1) A inclusão " $\supseteq$ " segue de cálculos rotineiros. Para estabelecer a inclusão contrária, consideremos $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ uma base homogênea de B. Dado um elemento homogêneo $\mathbf{e} \in \widehat{C}_{A\widehat{\otimes}B}(A'\widehat{\otimes}B')$, escreveremos

$$\mathbf{e} = \sum_{i=1}^{n} \mathbf{a}_i \otimes \mathbf{b}_i$$

onde $\mathbf{a}_i \in h(A)$. Temos

$$\partial(\mathbf{a}_i) + \partial(\mathbf{b}_i) \equiv \partial(\mathbf{e})(\text{mod}2)$$

para cada i.

Para qualquer $\mathbf{a}' \in h(A')$, a definição de $\widehat{C}_{A\widehat{\otimes}B}(A'\widehat{\otimes}B')$ nos fornece a equação

$$(\mathbf{a}' \otimes 1)\mathbf{e} = (-1)^{\partial(\mathbf{e})\partial(\mathbf{a}')}\mathbf{e}(\mathbf{a}' \otimes 1)$$

e isso implica que

$$(-1)^{\partial(\mathbf{e})\partial(\mathbf{a}')}\sum_{i=1}^{n}(-1)^{\partial(\mathbf{a}')\partial(\mathbf{b}_i)}\mathbf{a}_i\mathbf{a}' \otimes \mathbf{b}_i = \sum_{i=1}^{n}(-1)^{\partial(\mathbf{a}')\partial(\mathbf{a}_i)}\mathbf{a}'\mathbf{a}_i \otimes \mathbf{b}_i.$$

Consequentemente,

$$\mathbf{a}'\mathbf{a}_i = (-1)^{\partial(\mathbf{a}')\partial(\mathbf{a}_i)}\mathbf{a}_i\mathbf{a}'$$

e isso significa que $\mathbf{a}_i \in \widehat{C}_A(A')$ para todo i. Em particular, $\mathbf{e} \in \widehat{C}_A(A')\widehat{\otimes}B$. Agora considere $\mathbf{c}_1, \ldots, \mathbf{c}_r$ uma base homogênea de $\widehat{C}_A(A')$. Expressando $\mathbf{e}$ como

$$\mathbf{e} = \sum_{j=1}^{r} \mathbf{c}_j \otimes \mathbf{d}_j$$

onde $\mathbf{d}_j \in h(B)$. Usando a equação

$$(1 \otimes \mathbf{b}')\mathbf{e} = (-1)^{\partial(\mathbf{e})\partial(\mathbf{b}')}\mathbf{e}(1 \otimes \mathbf{b}')$$

com $\mathbf{b}' \in B$ e repetindo os cálculos acima, temos $\mathbf{d}_j \in \widehat{C}_B(B')$. Assim, $\mathbf{e} \in \widehat{C}_A(A')\widehat{\otimes}\widehat{C}_B(B')$ como queríamos.

(2) Consideremos $I \neq \mathbf{0}$ um ideal graduado em $A\widehat{\otimes}B$. Cada elemento homogêneo $\mathbf{z} \in I$ pode ser escrito na forma

$$\mathbf{z} = \sum_{i=1}^{r} \mathbf{a}_i \otimes \mathbf{b}_i \text{ onde } \mathbf{a}_i \in h(A) \text{ e } \mathbf{b}_i \in h(B).$$

De todos os elementos homogeneos de I escolhamos $\mathbf{z}$ que tenha escrita como acima com r mínimo. Como $\mathbf{z}$ tem grau fixado, temos:

$$\partial(\mathbf{a}_i) + \partial(b_i) \equiv \partial(z)(\text{mod}2). \tag{28}$$

Nossa observação agora é que os $\mathbf{a}_i's$ (e analogamente os $\mathbf{b}_i's$) são linearmente independentes. Suponhamos o contrário. Então, renumerando se nescessário, teríamos $\mathbf{a}_1 = \sum_{i=2}^{r} \alpha_i\mathbf{a}_i$, implicando que $\mathbf{a}_1, \ldots, \mathbf{a}_r$ tem o mesmo grau. Reescrevamos $\mathbf{z}$ por

$$\mathbf{z} = \sum_{i=2}^{r} \mathbf{a}_i \otimes (\alpha\mathbf{b}_1 + \mathbf{b}_i).$$

O fato dos $\mathbf{a}_i's$ terem o mesmo grau e as equações (28) implicam que os $\mathbf{b}_i's$ também tem os mesmo grau logo, $\alpha_i\mathbf{b}_1 + \mathbf{b}_i$ são todos homogêneos, o que contradiz a escolha

do r. O conjunto

$$C = \left\{ \sum_j \mathbf{c}_j \mathbf{a}_1 \mathbf{d}_j;\ \mathbf{c}_j, \mathbf{d}_j \in A \right\}$$

é um ideal graduado de A, logo $C = A$. Assim, deve existir uma equação

$$\sum_j \mathbf{c}_j \mathbf{a}_1 \mathbf{d}_j = 1 \quad \mathbf{c}_j, \mathbf{d}_j \in h(A).$$

Consideremos

$$\mathbf{c}_j \mathbf{z} \mathbf{d}_j = \sum_{i=1}^{r} (-1)^{\partial(\mathbf{b}_i)\partial(\mathbf{d}_j)} \mathbf{c}_j \mathbf{a}_i \mathbf{d}_j \otimes \mathbf{b}_i.$$

Somando em j e multiplicando o resultado por $(-1)^{\partial(\mathbf{b}_1)\partial(\mathbf{d}_j)}$ obtemos

$$\mathbf{z}_1 = i \otimes \mathbf{b}_1 + \sum_{i=2}^{r} \mathbf{a}'_i \otimes \mathbf{b}_i$$

onde $\mathbf{a}_i = \sum_j \pm \mathbf{c}_j \mathbf{a}_i \mathbf{d}_j$. Como $\partial(\mathbf{c}_j) + \partial(\mathbf{d}_j) \equiv \partial(\mathbf{a}_1) (\mathrm{mod} 2)$ independente do j, temos que cada $\mathbf{a}'_i$ é homogêneo. Além disso, $\mathbf{z}_1$ é diferente de zero pois os $\mathbf{b}'_i s$ são linearmente independentes. Passamos de $\mathbf{z}$ para um elemento $\mathbf{z}_1$ com as mesmas propriedades. Agora fazendo o mesmo procedimento para $\mathbf{b}_1$ podemos encontrar $\mathbf{z}'$ com as mesmas propriedades de $\mathbf{z}$ tal que

$$\mathbf{z}' = 1 \otimes 1 + \sum \mathbf{a}'_i \otimes \mathbf{b}'_i \quad (\mathbf{a}_i \in h(A), \mathbf{b}_i \in h(B).$$

Fazendo a consideração do grau temos $\partial(\mathbf{a}'_i) \equiv \mathbf{b}'_i (\mathrm{mod} 2)$. Para qualquer elemento $\mathbf{a} \in h(A)$ calculemos $\mathbf{a}\mathbf{z}' - \mathbf{z}'\mathbf{a} \in I \cap h(A \widehat{\otimes} B)$. O resultado é

$$\sum (\mathbf{a}\mathbf{a}'_i) - (-1)^{\partial(\mathbf{b}'_i)\partial(\mathbf{a})} \mathbf{a}'_i \mathbf{a} \otimes \mathbf{b}'_i.$$

Pela escolha de r, concluímos que $\mathbf{a}\mathbf{a}'_i = (-1)^{\partial(\mathbf{a}'_i)\partial(\mathbf{a})} \mathbf{a}'_i \mathbf{a}$, i.e, $\mathbf{a}_i \in \widehat{Z}(A)$. Como A é álgebra graduada central, $\mathbf{a}'_i \in F$. Mas $\{1, \mathbf{a}'_2, \ldots, \mathbf{a}'_r\}$ é linearmente independente. Assim devemos ter $r = 1$, i.e., $1 \in I$. □

Teorema 4.38. Sejam A, B álgebras graduadas. Suponha que exista um elemento $\mathbf{z} \in Z(A_0)$ tal que $\mathbf{z}^2 = 1$ e $\mathbf{z}\mathbf{a}_1 = -\mathbf{a}_1\mathbf{z}$ para cada $\mathbf{a}_1 \in A_1$. Então existe um isomorfismo de álgebras graduadas

$$A \widehat{\otimes} B \simeq A \otimes B.$$

Demonstração. Consideremos a seguinte subálgebra

$$B' = 1 \widehat{\otimes} B_0 + z \widehat{\otimes} B_1 \subseteq A \widehat{\otimes} B.$$

Ora B' e $A = A \widehat{\otimes} 1$ comutam elemento com elemento, pois

$$(\mathbf{z} \widehat{\otimes} \mathbf{b}_1)(\mathbf{a}_1 \widehat{\otimes} 1) = -\mathbf{z}\mathbf{a}_1 \widehat{\otimes} \mathbf{b}_1 = (\mathbf{a}_1 \widehat{\otimes} 1)(\mathbf{z} \widehat{\otimes} \mathbf{b}_1),$$

para cada $\mathbf{a}_1 \in A$ e $\mathbf{b}_1 \in B_1$. Logo, B' e A geram $A\widehat{\otimes}B$ como uma álgebra. Assim, existe um isomorfismo de álgebras graduadas

$$A \otimes B' \simeq A\widehat{\otimes}B.$$

Finalmente, a regra

$$\mathbf{b}_0 + \mathbf{b}_1 \mapsto 1 \otimes \mathbf{b}_0 + \mathbf{z} \otimes \mathbf{b}_1 \quad (\mathbf{b}_i \in B_i)$$

claramente define um isomorfismo da álgebra graduada B em B'. Portanto, obtemos

$$A\widehat{\otimes}B \simeq A \otimes B.$$

□

Corolário 4.39. Sejam B, C álgebras graduadas onde $C_1 = \mathbf{0}$. Então existe um isomorfismo de álgebras graduadas

$$\widehat{M}_r(C)\widehat{\otimes}B \simeq \widehat{M}_r(C) \otimes B$$

Corolário 4.40. Para qualquer álgebra graduada B, existem isomorfismos de álgebras graduadas

$$\widehat{M}_r(F)\widehat{\otimes}B \simeq \widehat{M}_r(F) \otimes B \simeq \widehat{M}_r(B)$$

Corolário 4.41. $\widehat{M}_r(F)\widehat{\otimes}\widehat{M}_s(C) \simeq \widehat{M}_r(F) \otimes \widehat{M}_s(C) \simeq \widehat{M}_{rs}(C)$ para cada álgebra graduada C.

Teorema 4.42. Sejam A, B álgebras graduadas. Suponha que existe um elemento $\mathbf{z} \in A_1 \cap Z(A)$ tal que $\mathbf{z}^2 = -1$. Então existe um isomorfismo (de álgebras não graduadas)

$$(A\widehat{\otimes}B)_0 \simeq A_0 \otimes B.$$

Demonstração. Definamos

$$B' = B_0 \oplus \mathbf{z}B_1 \subseteq (A\widehat{\otimes}B)_0.$$

B' e A_0 comutam elemento com elemento, e eles geram $(A\widehat{\otimes}B)_0$ como álgebra. Desse modo, $A_0\widehat{\otimes}B' \simeq (A\widehat{\otimes}B)_0$. A regra

$$\mathbf{b}_0 + \mathbf{b}_1 \mapsto \mathbf{b}_0 + \mathbf{z}\mathbf{b}_1$$

é um isomorfismo de álgebras de B em B', pois

$$(\mathbf{z} \otimes \mathbf{b}_1)(\mathbf{z} \otimes \mathbf{c}_1) = -\mathbf{z}^2 \otimes \mathbf{b}_1\mathbf{c}_1 = 1 \otimes \mathbf{b}_1\mathbf{c}_1$$

para $\mathbf{b}_1, \mathbf{c}_1 \in B_1$. Consequentemente, $A_0 \otimes B \simeq (A\widehat{\otimes}B)_0$. □

4. Estrutura das Álgebras Graduadas Centrais Simples

PROPOSIÇÃO 4.43. Seja A uma álgebra graduada simples, com $A_1 \neq \{0\}$. Então $A_1^2 = A_0$. Se $I \neq \{0\}$ é ideal bilateral qualquer de A_0, então $I + A_1IA_1 = A_0$ e $A_1I + IA_1 = A_1$.

DEMONSTRAÇÃO. $A_1^2 = A_0$ segue dos fatos que $A_1^2 \subseteq A_0$ e $A_1^2 \oplus A_1$ é um ideal bilateral de A.

Agora considere o subespaço graduado

$$J = (I + A_1IA_1) \oplus (A_1I + IA_1).$$

Checa-se facilmente que J é um ideal bilateral de A. Como $J \neq \{0\}$, devemos ter $J_0 = A_0$ e $J_1 = A_1$ como desejávamos. □

PROPOSIÇÃO 4.44. Seja A uma álgebra graduada simples, com $A_1 \neq 0$. Seja J um ideal próprio em A (não necessariamente graduado). Então, as projeções $\pi_i : J \to A_i$ $(i = 0, 1)$ são isomorfismos.

DEMONSTRAÇÃO. O conjunto $I = J \cap A_0$ é um ideal em A_0. Pela Proposição 4.43, devemos ter $I = \{0\}$, e por outro lado J deve conter $I + A_1IA_1 \ni 1$. Também $I' = \pi_0(j)$ é um ideal de A_0 e não nulo pois J pode não ser, possivelmente, um subespaço graduado. Assim, 4.43 implica $A_1I'A_1 + I' = A_0$. Mas, claramnete, $A_1I'A_1 \subseteq I'$, e daí obtemos $I' = A_0$. Estabelecemos assim a injetividade de $\pi_1 : J \to A_1$ e a sobrejetividade de $\pi_0 : J \to A_0$. Mas

$$J \cap A_1 = A_0 \cdot (J \cap A_1) = A_1 \cdot A_1 \cdot (J \cap A_1) \subseteq A_1 \cdot (J \cap A_0) = \{0\}$$

logo, $\pi_1 : J \to A_1$ é sobrejetiva. □

PROPOSIÇÃO 4.45. Seja A uma álgebra graduada simples. Suponha que A não é simples como uma álgebra não graduada. Então A_0 é uma álgebra simples e $A_1 = A_0 \cdot \mathbf{u}$, onde $\mathbf{u} \in Z(A) \cap A_1$ e $\mathbf{u}^2 = 1$.

DEMONSTRAÇÃO. Escolha qualquer ideal próprio J em A (o qual existe por hipóteses). Temos automaticamente $A_1 \neq \{0\}$ e assim as duas proposições prévias se aplicam. Como $\pi_0 : J \to A_0$ é um isomorfismo, J contém um único elemento da forma $1 + \mathbf{u}$ $(\mathbf{u} \in A_1)$. Mas J também contém $\mathbf{u}(1 + \mathbf{u}) = \mathbf{u}^2 + \mathbf{u}$, daí devemos ter $\mathbf{u}^2 = 1$. Claramente, temos que $\mathbf{u} \in Z(A)$. Para $\mathbf{z} \in A_0$, J contém ambos

$$\mathbf{z}(1 + \mathbf{u} = \mathbf{z} + \mathbf{zu}); \text{e } (1 + \mathbf{u})\mathbf{z} = \mathbf{z} + \mathbf{uz}.$$

Aplicando o isomorfismo π_0, temos $\mathbf{zu} = \mathbf{uz}$. Analogamente, $\mathbf{u}$ comuta elemento com elemento de A_1, assim, realmente $\mathbf{u} \in Z(A)$. Também, para $\mathbf{x} \in A_1$, temos

$\mathbf{x} = \mathbf{x}\mathbf{u}^2 \in A_0\mathbf{u}$ daí, $A_1 = A_0\mathbf{u}$. Enfim, mostraremos que A_0 é simples. Consideremos $I \neq \{0\}$ ser um ideal bilateral de A_0. Então,

$$A_1 I A_1 = A_0\mathbf{u} I A_0\mathbf{u} = A_0\mathbf{u} I\mathbf{u} = A_0 I\mathbf{u}^2 = A_0 I = I.$$

Pelo Teorema 4.43, concluímos que $I = A_0$. □

Teorema 4.46. Seja $A \in \mathrm{AGCS}(F)$ com $A_1 \neq \mathbf{0}$ e $Z(A) = F \oplus Z_1$, onde $Z_1 \subseteq A_1$. Então:

(1) $Z_1 = \{0\}$ se, e somente se, $A \in \mathrm{ACS}(F)$.
(2) $Z_1 \neq \{0\}$ se, e somente se, $A_0 \in \mathrm{ACS}(F)$.

Demonstração. (1) se $Z_1 = \{0\}$, a proposição prescedente implica que A deve ser simples, e desse modo $A \in \mathrm{ACS}(F)$. A recíproca é trivial.

(2) Supondo $Z_1 \neq \{0\}$, claramente existe um $\mathbf{z}_1 \in Z_1$ tal que $\mathbf{z}_1^2 \neq \mathbf{0}$. De fato, se existir $\mathbf{z}_1 \in Z_1$ tal que $\mathbf{z}_1^2 = 0$, então $Z(A)$ certamente não é uma corpo, e desse modo A não é uma álgebra simples (como álgebras não graduadas). Nesse caso, pela Proposição 4.45, existe $\mathbf{u} \in Z_1$ satisfazendo $\mathbf{u}^2 = 1$. Assim, realmente existe $\mathbf{z}_1$ tal que $\mathbf{z}_1^2 = a \in F^*$. Como $A_1 = A_a\mathbf{u} = A_1\mathbf{z}_1^2 \subseteq A_0 Z_1$, temos $A_1 = A_0 Z_1$. Isso implica claramente que

$$Z(A_0) \subseteq Z(A) \cap A_0 = F,$$

e dai segue que A_0 é central sobre F. Reciprocamente, suponhamos $A_0 \in \mathrm{ACS}(F)$. Assumamos que $Z_1 = 0$. Então $A \in \mathrm{ACS}(F)$ por (1). Usando o Corolário 4.10 sabemos que $C_A(A_0) \in \mathrm{ACS}(F)$ e $A \simeq A_0 \otimes C_A(A_0)$ como álgebras não graduadas. Isso força $C_1 \neq \mathbf{0}$ e daí 4.43 fornece $C_1^2 \neq \mathbf{0}$. assim, existem $\mathbf{uv} \in C_1$ com $\mathbf{0} \neq \mathbf{uv} \in C_0 = F$. Temos

$$C_1 = C_1 \cdot 1 = C_1\mathbf{uv} \subseteq C_0\mathbf{v} \subseteq F\mathbf{v},$$

ou seja, $C = F \oplus F\mathbf{v}$. Isso implica que C é comutativa, contradizendo o fato de que $C \in \mathrm{ACS}(F)$. □

Definição 4.47. Seja $A \in \mathrm{AGCS}(F)$ e $Z(A) = F \oplus Z_1$ ($Z_1 \subseteq A_1$.) Se $Z_1 = \{0\}$ dizemos que A é de **tipo par** e se $Z_1 \neq \mathbf{0}$ dizemos que A é de **tipo ímpar**.

Para cada $A \in \mathrm{AGCS}(F)$ definimos

$$\mathrm{type}(A) = \begin{cases} 0 \text{ se } A \text{ e de tipo par} \\ 1 \text{ se } A \text{ e tipo impar} \end{cases}$$

As demonstrações dos dois resultados a seguir serão omitidas por serem muito técnicas. Para tanto, pode-se recorrer a [**4**].

Teorema 4.48. Se $A \in \mathrm{AGCS}(F)$ é do tipo ímpar, então:

(1) $Z(A) = C_A(A_0) = F \oplus F\mathbf{z}$, onde $\mathbf{z} \in Z_1$ e $\mathbf{z}^2 = a \in F^*$. A classe de quadrados de a não depende da escolha de $\mathbf{z} \in Z_1 \setminus \{\mathbf{0}\}$, e $Z(A) \simeq F(\sqrt{a})$ como álgebras graduadas.
(2) Existem os isomorfismos de álgebras graduadas

$$A \simeq (A_0)\widehat{\otimes}F(\sqrt{a}) \otimes F\langle\sqrt{a}\rangle$$

(3) Se $a \notin F^{*2}$, então $A \in \mathrm{ACS}(Z(A))$. Se $a \in F^{*2}$, então $Z(A) \simeq F \times F$ e $A \simeq A_0 \times A_0$.

Teorema 4.49. Seja $A \in \mathrm{AGCS}(F)$ de tipo par com $A_1 \neq \{0\}$. Suponha A isomorfo, como álgebra não graduada, a $M_n(D)$, onde D é uma algébra com divisão central. Então:

(1) $Z(A_0) = C_A(A_0)$, e existe $\mathbf{z} \in Z(A_0)$ tal que $Z(A_0) = F \oplus F\mathbf{z}$ e $\mathbf{z}^2 = a \in F^*$. O elemento $\mathbf{z}$ é determinado a menos de um escalar por essas propriedades e desse modo a classe de quadrados de a é unicamente determinada.
(2) Suponha $a \in F^{*2}$. Então $Z(A_0) \simeq F \times F$, e existe um F-espaço vetorial graduado $V = V_0 \oplus V_1$, tal que $A \simeq \mathrm{End}V\widehat{\otimes}D$ como álgebras graduadas. Além disso, $A_0 \simeq M_r(D) \times M_s(D)$ onde $r = \dim V_0$ e $s = \dim V_1$.
(3) Se $a \notin F^{*2}$ e o corpo $Z(A_0) \simeq F(\sqrt{a})$ pode ser imerso em D então existe uma graduação sobre D tal que

$$A \simeq \widetilde{M}_n(D).$$

Nesse caso, $A_0 \simeq M_n(D) \in \mathrm{ACS}(Z(A_0))$.
(4) Suponhamos que $a \notin F^{*2}$ e que o corpo $Z(A_0) \simeq F(\sqrt{a})$ não pode ser imerso em D. Então $n = 2m$, e

$$A \simeq (M_m(D))\widehat{\otimes}\left\langle \frac{-a, 1}{F} \right\rangle$$

como álgebras graduadas. Nesse caso, $A_0 \simeq M_m(D)\otimes F(\sqrt{a}) \in \mathrm{ACS}(Z(A_0))$.

Definição 4.50. Seja $A \in \mathrm{AGCS}(F)$. Se $\mathrm{type}(A) = 1$ e $\mathbf{z}_A \in A$ é o elemento $\mathbf{z}$ determinado em 4.48 escreveremos $\delta(A) =$ classe de $\mathbf{z}_A^2$ em F^*/F^{*2}. Se $\mathrm{type}(A) = 0$, $A_1 \neq \mathbf{0}$ e $\mathbf{z}_A$ denota o elemento determinado por 4.49 escreveremos $\delta(A) =$ classe de $\mathbf{z}_A^2$ em F^*/F^{*2}. Se $A_1 = \mathbf{0}$, consideramos $\mathbf{z}_A = 1$, e escrevemos $\delta(A) = 1 \in F^*/F^{*2}$. A classe $\delta(A)$ é chamada de o **invariante quadrático de A**

5. O Grupo de Brauer-Wall

Sejam $A, B \in \mathrm{AGCS}(F)$. Diremos que A e B são semelhantes se existirem r, s inteiros positivos tais que:

$$A\widehat{\otimes}M_r(F) \simeq B\widehat{\otimes}M_s(F)$$

onde $M_r(F)$ e $M_s(F)$ são graduadas como no exemplo 4.29.

Podemos facilmente constatar que semelhança em $\mathrm{AGCS}(F)$ define uma relação de equivalência. Denotaremos a classe de equivalência de um elemento $A \in \mathrm{AGCS}(F)$ por $\langle A\rangle$ e o conjunto das classes por $BW(F)$. A operação

$$\cdot : (\langle A\rangle, \langle B\rangle) \mapsto \langle A\rangle \cdot \langle B\rangle = \langle A\widehat{\otimes}B\rangle$$

está bem definida e temos a seguinte

Proposição 4.51. $(BW(F), \cdot)$ é um grupo abeliano.

Demonstração. Seja $\theta : A\widehat{\otimes}A^* \to \mathrm{End}(A)$ a aplicação F-linear induzida por

$$\theta(\mathbf{a}\otimes\mathbf{b})(\mathbf{e}) = (-1)^{\partial\mathbf{b}\partial\mathbf{e}}\mathbf{aeb},$$

onde $\mathbf{a}, \mathbf{b}, \mathbf{e} \in h(A)$. Claramente, θ preserva graduação. Checaremos assim a multiplicabilidade de θ. Para tanto, é suficiente verificarmos sobre elementos homogêneos:

$$\begin{aligned}
\theta((\mathbf{a}\otimes\mathbf{b})(\mathbf{c}\otimes\mathbf{d}))(\mathbf{e}) &= \theta((-1)^{\partial\mathbf{b}\partial\mathbf{c}}\cdot(-1)^{\partial\mathbf{b}\partial\mathbf{d}}\mathbf{ac}\otimes\mathbf{b}\cdot\mathbf{d})(\mathbf{e}) \\
&= (-1)^{\partial\mathbf{b}(\partial\mathbf{c}+\partial\mathbf{d})}\cdot(-1)^{\partial\mathbf{e}(\partial\mathbf{d}+\partial\mathbf{b})}\mathbf{acedb} \\
&= (-1)^{(\partial\mathbf{c}+\partial\mathbf{e}+\partial\mathbf{d})\partial\mathbf{b}}\cdot(-1)^{\partial\mathbf{d}\partial\mathbf{e}}\mathbf{acedb} \\
&= \theta(\mathbf{a}\otimes\mathbf{b})((-1)^{\partial\mathbf{d}\partial\mathbf{e}}\mathbf{ced}) \\
&= [\theta(\mathbf{a}\otimes\mathbf{b})\theta(\mathbf{c}\otimes\mathbf{d})](\mathbf{e}).
\end{aligned}$$

Como $A\widehat{\otimes}A^* \in \mathrm{AGCS}(F)$, o ideal graduado $\ker\theta$ é nulo. Consequentemente, θ é um isomorfismo. As conclusões seguem imediatamente desse isomorfismo.

□

O grupo dessa proposição é chamado de **grupo de Brauer-Wall do corpo** F e é denotado por $BW(F)$.

Proposição 4.52. A aplicação $i : B(F) \to BW(F)$ definida por

$$i([A]) = \langle (A)\rangle$$

é um homomorfismo injetivo de grupos.

DEMONSTRAÇÃO. Que i é um homomorfismo é evidente, assim, resta-nos demonstrar a injetividade de i. Para isso, temos que

$$i([A]) = i([B])$$

implica a existência de r, s inteiros positivos tais que

$$(A)\widehat{\otimes}\widehat{M_r}(F) \simeq (B)\widehat{\otimes}\widehat{M_s}(F).$$

Mas $(A)\widehat{\otimes}\widehat{M_r}(F)$ é idêntico a $A \otimes M_r(F)$ e do mesmo modo $(B)\widehat{\otimes}\widehat{M_s}(F)$. Dessa maneira,

$$A \otimes M_r(F) \simeq B \otimes M_s(F),$$

i.e., $[A] = [B]$. □

PROPOSIÇÃO 4.53. A regra $j : \langle A\rangle \mapsto (\text{type}(A), \delta(A)) \in Q(F)$ está bem definida e é um homomorfismo do grupo $BW(F)$ no grupo $Q(F)$.

TEOREMA 4.54. Temos a sequência exata

$$0 \longrightarrow B(F) \xrightarrow{i} BW(F) \xrightarrow{j} Q(F) \longrightarrow 0\ .$$

DEMONSTRAÇÃO. Se $B \in \text{ACS}(F)$ então $\text{type}((B)) = 0$ e seu invariante quadrático é 1. isso mostra que $j \circ i = \mathbf{0}$. Para mostrar a sobrejetividade de j, é suficiente mostrar que todo elemento da forma $(1, a)$ pertence a $\text{Im}(j)$, uma vez que $(1, -a)(1, 1) = (0, a)$. Consideremos então $A = F\langle a\rangle \in \text{AGCS}(F)$, temos precisamente $j(\langle A\rangle) = (1, a)$. Logo, j é sobrejetiva. □

CAPíTULO 5

Álgebras de Clifford

Em toda essa seção (V, q) denotará um espaço quadrático.

DEFINIÇÃO 5.1. Uma F-álgebra A contendo (V, q) como um subespaço é dita **compatível** com q se $\mathbf{x}^2 = q(\mathbf{x}) \cdot 1 \in A$ qualquer que seja $\mathbf{x} \in V$.

Se a regra q é clara pelo contexto diremos simplesmente que A é compatível com V. Também identificaremos $F \cdot 1$ com F e dessa maneira a equação acima se escreverá como $\mathbf{x}^2 = q(\mathbf{x})$. Se B é a forma bilinear associada a q temos

$$2B(\mathbf{x}, \mathbf{y}) = \mathbf{xy} + \mathbf{yx}, \quad \forall\, \mathbf{x}, \mathbf{y} \in V.$$

Em particular, $\mathbf{x}$ e $\mathbf{y}$ são ortogonais se, e somente se, são anticomutativos.

LEMA 5.2. Para uma F-álgebra como acima e $\mathbf{x} \in V \setminus \{\mathbf{0}\}$, $\mathbf{x}$ é invertível se, e somente se, $\mathbf{x}$ é um vetor anisotrópico em V.

DEMONSTRAÇÃO. Se $\mathbf{x}$ é anisotrópico, a equação $\mathbf{x}^2 = q(\mathbf{x})$ implica que $\mathbf{x}/q(\mathbf{x})$ é o inverso de $\mathbf{x}$. Reciprocamente, se existe $\mathbf{y} \in A$ tal que $\mathbf{x} \cdot \mathbf{y} = 1$ então $q(\mathbf{x}) \cdot \mathbf{y} = \mathbf{x} \cdot \mathbf{x} \cdot \mathbf{y} = \mathbf{x}$ e claramente; $\mathbf{x} \neq 0 \Rightarrow q(\mathbf{x}) \neq 0$. □

LEMA 5.3. Considere A uma F-álgebra como acima, e $\mathbf{u} \in A$ um vetor anisotrópico. Então, o hiperplano de reflexão $\tau_{\mathbf{u}}$ sobre V associado a $\mathbf{u}$ é igual a -1 vezes a conjugação por $\mathbf{u}$ sobre V na álgebra A.

DEFINIÇÃO 5.4. Uma F-álgebra $C \supseteq V$ compatível com q é dita ser uma **álgebra de Clifford** de (V, q) se ela tem a seguinte propriedade universal: dado qualquer F-álgebra $A \supseteq V$ compatível com q, existe um único homomorfismo de F-álgebras $\varphi : C \to A$ tal que $\varphi(\mathbf{x}) = \mathbf{x}$ qualquer que seja $\mathbf{x} \in V$.

TEOREMA 5.5. Seja (V, q) um espaço quadrático. Então existe uma álgebra de Clifford C de (V, q). Além disso, se C' é uma outra álgebra de Clifford de (V, q) então existe um único isomorfismo de álgebras $\psi : C \to C'$ o qual é a identidade sobre V (ou seja, a álgebra de Clifford de um espaço quadrático é única a menos de um isomorfismo).

DEMONSTRAÇÃO. Denotemos por $T(V)$ a álgebra tensorial de V e por $I(q)$ o ideal bilateral de $T(V)$ gerado pelos elementos da forma $\mathbf{x}\otimes\mathbf{x}-q(\mathbf{x}).1$. Seja $C = T(V)/I(q)$. Então a aplicação

$$\Pi : V \to C$$

que envia cada elemento de V em sua classe é injetiva, assim podemos identificar V com $\Pi(V)$. Claramente, V é um conjunto gerador da álgebra C e desse fato segue a propriedade universal.

Agora suponhamos C' uma outra álgebra de Clifford de (V, q). Então existem únicos homomorfismos de álgebras $\varphi : C \to C'$ e $\varphi' : C' \to C$ tais que

$$\varphi(\mathbf{x}) = \varphi'(\mathbf{x}) = \mathbf{x} \ \ \forall \mathbf{x} \in V.$$

Ora, $\varphi' \circ \varphi(\mathbf{x}) = \mathbf{x}, \quad \forall \mathbf{x} \in V$. Portanto, da propriedade universal de C temos $\varphi' \circ \varphi = \mathbb{I}_C$. □

Denotaremos a álgebra C acima por $C(V, q)$ e as imagens pela aplicação quociente de $\bigoplus_{i \text{ par}} T^i(V)$ e $\bigoplus_{i \text{ impar}} T^i(V)$ denotaremos, respectivamente, por $C_0(V, q)$ e $C_1(V, q)$.

Com essas notações temos a seguinte

OBSERVAÇÃO 5.6. $C(V, q) = C_0(V, q) \oplus C_1(V, q)$ é uma graduação.

EXEMPLO 5.7. Considere o espaço quadrático unidimensional $V =< a >$. Seja $\{\mathbf{x}\}$ uma base de V. Nesse caso podemos identificar a álgebra tensorial $T(V)$ com o anel de polinômios $F[t]$ e temos

$$C(V, q) = \frac{F[t]}{t^2 - a}$$

EXEMPLO 5.8. Seja (V, q) um espaço quadrático bidimensional com diagonalização $< a, b >$ $(a, b \in F^*)$ relativa a base ortogonal $\{\mathbf{x}, \mathbf{y}\}$. Seja $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ a base usual da álgebra de quatérnio $A = \left\langle \frac{a,b}{F} \right\rangle$. A aplicação linear

$$T : V \to A$$

tal que $\mathbf{x} \mapsto \mathbf{i}$ e $\mathbf{y} \mapsto \mathbf{j}$ nos dá uma imersão que permite identificarmos V com um subespaço de A. Com essa identificação temos:

$$(\alpha\mathbf{x} + \beta\mathbf{y})^2 = (\alpha\mathbf{i} + \beta\mathbf{j})^2 = \alpha^2 a + \beta^2 b = q(\alpha\mathbf{x} + \beta\mathbf{y})$$

e do fato que V é um gerador de A segue que

$$C(V, q) \simeq A.$$

EXEMPLO 5.9. Pelo exemplo acima, $C(\mathcal{H}) \simeq \left\langle \frac{-1,-1}{F} \right\rangle$. Da prova de 3.11 temos a existência de um isomorfismo $\varphi : \left(\frac{-1,-1}{F}\right) \simeq M_2(F)$ com

$$\varphi(\mathbf{i}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \varphi(\mathbf{j}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \varphi(\mathbf{k}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Sobre esse isomorfismo φ, $F \oplus F \cdot \mathbf{k}$ corresponde às matrizes da forma $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ e $F \oplus F \cdot \mathbf{j}$ à $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$. Assim, φ é um isomorfismo de álgebras graduadas $C(\mathcal{H}) \simeq \widehat{M_2}(F)$

PROPOSIÇÃO 5.10. Se (V, q), (V', q') são espaços quadráticos, existe uma sobrejeção

$$f : C(V \perp V', q \perp q') \to C(V, q) \otimes C(V', q')$$

na categoria das álgebras graduadas.

DEMONSTRAÇÃO. A regra $\xi(\mathbf{x}, \mathbf{x}') = \mathbf{x} \otimes 1 + 1 \otimes \mathbf{x}'$ ($\mathbf{x} \in V$, $\mathbf{x}' \in V'$) claramente define uma injeção de $V \perp V'$ em $C(V)\widehat{\otimes}C(V')$. Temos,

$$\begin{aligned} (\mathbf{x} \otimes 1 + 1 \otimes \mathbf{x}')^2 &= \mathbf{x}^2 \otimes 1 + 1 \otimes \mathbf{x}'^2 + (\mathbf{x} \otimes 1)(1 \otimes \mathbf{x}') + (1 \otimes \mathbf{x}')(\mathbf{x} \otimes 1) \\ &= q(\mathbf{x}) + q'(\mathbf{x}') + \mathbf{x} \otimes \mathbf{x}' + (-1) \cdot \mathbf{x} \otimes \mathbf{x}' \\ &= (q \perp q')(\mathbf{x}, \mathbf{x}'). \end{aligned}$$

Pela propriedade universal das álgebras de Clifford, temos um único homomorfismo de álgebras

$$f : C(V \perp V') \to C(V)\widehat{\otimes}C(V')$$

que coincide com ξ sobre $V \perp V'$. Resta somente mostrar a sobrejetividade de f. Como uma F-álgebra, $C(V)\widehat{\otimes}C(V')$ é gerada pelos elementos da forma $\mathbf{x} \otimes 1$ e $1 \otimes \mathbf{x}'$. Como todos esses elementos estão na imagem de f, concluímos que f é sobrejetiva. □

PROPOSIÇÃO 5.11. Seja (V, q) um espaço quadrático n-dimensional com base ortogonal $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$. Então $\beta = \{\mathbf{x}_1^{e_1} \cdots \mathbf{x}_n^{e_n};\ e_i = 0 \text{ ou } 1\}$ é uma base de $C(V, q)$. (Em particular, $\dim C(V, q) = 2^n$).

DEMONSTRAÇÃO. De $\mathbf{x}_i\mathbf{x}_j = -\mathbf{x}_j\mathbf{x}_i$ e $\mathbf{x}^2 = q(\mathbf{x})$ segue que $C(V, q)$ é um F-espaço vetorial gerado pelo conjunto β logo, $\dim C(V, q) \leq 2^n$.

Mostraremos agora $\dim C(V, q) \geq 2^n$. Para isso, utilizaremos indução sobre n. Para $n = 1$ segue do Exemplo 5.7. Para $n > 1$ considere uma decomposição ortogonal $V = U \perp U'$, onde $\dim U' = 1$. Da Proposição 5.10 segue que

$$\dim C(V, q) \geq \dim C(U, q|_U) \cdot \dim C(U', q|_{U'}) \geq 2^{n-1} \cdot 2 = 2^n.$$

Portanto, de fato β é uma F-base do espaço vetorial $C(V,q)$. □

Uma consequência imediata dessa proposição é que o homomorfismo f do teorema 5.10 é um isomorfismo.

COROLÁRIO 5.12. $C(m\mathcal{H}) \simeq \widehat{M}_{2^m}(F)$. Em particular, $\langle C(m\mathcal{H})\rangle = 0 \in BW(F)$

DEMONSTRAÇÃO. Consequência de 5.10, 5.9 e 4.41. □

TEOREMA 5.13. Seja (V,q) um espaço quadrático. Então $C(V,q) \in \mathrm{AGCS}(F)$.

DEMONSTRAÇÃO. De 4.30 e 5.7 segue que a álgebra de Clifford de um F-espaço quadrático unidimensional pertence a $\mathrm{AGCS}(F)$. A conclusão segue do fato de que o produto tensorial de elementos de $\mathrm{AGCS}(F)$ ainda é um elemento de $\mathrm{AGCS}(F)$ e de 5.10. □

Vejamos as traduções de 4.48 e 4.49 no caso das álgebras de Clifford.

TEOREMA 5.14. Suponhamos $\dim V$ ímpar e $\delta = d_{\pm}$. Então:

(1) $C_0(V) \in \mathrm{ACS}(F)$ e $C(V) \simeq (C_0(V))_0 \widehat{\oplus} F\langle\sqrt{\delta}\rangle$
(2) Se $\delta \notin F^{*2}$ então $Z(C(V)) \simeq F(\sqrt{\delta})$ e $C(V) \in \mathrm{ACS}(F(\sqrt{\delta}))$.
(3) Se $\delta \in F^{*2}$ então $Z(C(V)) \simeq F \times F$ e $C(V) \simeq C_0(V) \times C_0(V)$.

TEOREMA 5.15. Suponhamos $\dim V$ par e $\delta = d_{\pm}$. Então:

(1) $C(V) \in \mathrm{ACS}(F)$
(2) Se $\delta \notin F^{*2}$ então $Z(C_0(V)) \simeq F(\sqrt{\delta})$ e $C_0(V) \in \mathrm{ACS}(F(\sqrt{\delta}))$.
(3) Se $\delta \in F^{*2}$ então $Z(C_0(V)) \simeq F \times F$. Se $C(V) \simeq M_n(D)$, onde $D \in \mathrm{ACS}(F)$, então $C(V) \simeq \widehat{M}_n(D)$ como álgebras graduadas.

TEOREMA 5.16. Seja (V,q) um espaço quadrático. Então,

$$\mathrm{type\ C(V,q)} \equiv \dim V (\mathrm{mod}\ 2).$$

DEMONSTRAÇÃO. Sejam $n = \dim V$ e $\mathbf{e}_1, \ldots, \mathbf{e}_n$ uma base ortonormal de V. Definamos $\mathbf{z} = \mathbf{e}_1 \cdots \mathbf{e}_n \in C(V)$ e escrevamos $Z(C(V)) = F \oplus Z_1$.
Caso 1. n é impar. Como $\mathbf{e}_i\mathbf{e}_j = -\mathbf{e}_j\mathbf{e}_i$ para $i \neq j$, claramente $\mathbf{z}$ comuta com todos os $\mathbf{e}_i$ e desse modo $\mathbf{z} \in Z_1$. Isso implica que $Z_1 \neq \mathbf{0}$, ou seja, $C(V)$ é do tipo ímpar.
Caso 2. n é par. Claramente, $\mathbf{e}_i\mathbf{z} = -\mathbf{z}\mathbf{e}_i$ para todo i, e desse modo $\mathbf{e}_i\mathbf{e}_j\mathbf{z} = \mathbf{z}\mathbf{e}_i\mathbf{e}_j$ para todos i, j. Em particular, $\mathbf{z} \in Z(C_0(V))$ e assim $C_0(V)$ não é uma F-álgebra graduada central. Por 4.46(2) deduzimos que $Z_1 = \mathbf{0}$, i.e., $C(V)$ é do tipo par.

□

TEOREMA 5.17. $\delta(C(V,q)) = d_{\pm}(V) \in \frac{F^*}{F^{*2}}$.

TEOREMA 5.18. Seja A uma álgebra graduada que tem um elemento $\mathbf{z} \in A_1 \cap Z(A)$ tal que $\mathbf{z}^2 = \delta \in F^*$. Então para qualquer espaço quadrático (V, q) existe um isomorfismo de álgebra

$$(A\widehat{\otimes}C(V))_0 \simeq A_0 \otimes C(-\delta \cdot q).$$

DEMONSTRAÇÃO. Seja B a subálgebra graduada

$$C_0(q) \oplus \mathbf{z} \cdot C_1(q) \subseteq (A_0\widehat{\otimes}C(q))_0.$$

Claramente, B comuta elemento com elemento de $A_0 = A_0 \otimes 1$, e desse modo B e A_0 geram $(A\widehat{\otimes}C(q))_0$. Se $\mathbf{v} \in V$, o quadrado de $\mathbf{zv} = \mathbf{z} \otimes \mathbf{v} \in B$ é $-\mathbf{z}^2 \otimes \mathbf{v}^2 = -\delta \cdot q(\mathbf{v})$. Assim, a regra $\mathbf{v} \mapsto \mathbf{zv} \in B$ induz um isomorfismo de álgebras $C(-\delta \cdot q) \simeq B$. □

COROLÁRIO 5.19. Para qualquer forma q e qualquer $d \in F^*$ existe um isomorfismo de álgebras $C_0(\langle -d\rangle \perp q) \simeq C(d \cdot q)$.

COROLÁRIO 5.20. Para qualquer forma q e qualquer $a \in F^*$ existe um isomorfismo de álgebras

$$C_0(a \cdot q) \simeq C_0(q).$$

1. Os Invariantes de Clifford, Witt e Hasse

A propriedade

$$C((V, q) \perp (V', q')) \simeq C(V, q)\widehat{\otimes}C(V', q')$$

implica que a aplicação

$$(V, q) \mapsto \langle C(V, q)\rangle \in BW(F)$$

é um homomorfismo do monóide $M(F)$ no grupo $BW(F)$. Este, por sua vez, pode ser estendido, via propriedade universal, a um homomorfismo de grupos

$$\Gamma : \widehat{W}(F) \to BW(F)$$

Como $\langle C(m\mathbb{H})\rangle$ é a identidade em $BW(F)$ podemos fatorar Γ através de $W(F)$. Também denotaremos o homomorfismo induzido de $W(F)$ em $BW(F)$ por Γ, e o chamaremos de **invariante de Clifford**.

Na Proposição 3.10 mostramos que $f : W(F)/I^2F \to Q(F)$ definido por

$$f(V, q) = (\dim V(\mathrm{mod}2), d_{\pm}(V, q))$$

é um homomorfismo. Usando 5.16 e 5.17 e 4.54, vemos que o invariante de Clifford induz um homomorfismo γ de I^2F no grupo de Brauer $B(F)$. Assim, temos o diagrama

comutativo:

$$(*) \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & I^2F & \longrightarrow & W(F) & \longrightarrow & \frac{W(F)}{I^2(F)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \Gamma} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & B(F) & \xrightarrow{i} & BW(F) & \xrightarrow{j} & Q(F) & \longrightarrow & 0 \end{array}$$

LEMA 5.21. Para qualquer $a, b, c \in F^*$ temos

$$\gamma(\langle a, b, c, abc\rangle) = \left(\frac{-ab, -ac}{F}\right) \in B(F).$$

DEMONSTRAÇÃO. É suficiente calcularmos $\Gamma(\langle a, b, c, abc\rangle)$. Dessa maneira, trabalharemos na categoria das álgebras graduadas. Por 5.19,

$$C_0(\langle a, b, c\rangle) \simeq C(\langle -ab, -ac\rangle) \simeq \left(\frac{-ab, -ac}{F}\right),$$

como álgebras não graduadas. Assim, por 5.14(1) temos um isomorfismo de álgebras graduadas

$$C(\langle a, b, c\rangle) \simeq \left(\frac{-ab, -ac}{F}\right) \widehat{\otimes} C(\langle -abc\rangle),$$

onde o primeiro fator é visto como uma álgebra graduada concentrada no grau zero. Usando 5.10, e a lei associativa obtemos

$$C(\langle a, b, c, abc\rangle) \simeq \left(\frac{-ab, -ac}{F}\right) \widehat{\otimes} C(\langle -abc, abc\rangle).$$

Por 5.12 concluimos que $\Gamma(\langle a, b, c, abc\rangle)$ é precisamente $i\left(\frac{-ab,-ac}{F}\right)$. □

COROLÁRIO 5.22. $\gamma(\langle 1, -a\rangle \otimes \langle 1, -b\rangle) = \left(\frac{a,b}{F}\right)$

Na sequência, o símbolo Quat(F) será utilizado para representar o subgrupo de $B(F)$ gerado pelas classes de todas as álgebras de quatérnios.

COROLÁRIO 5.23. $\gamma(I^3(F)) = \{1\}$ e $\gamma(I^2F) = \text{Quat(F)}$.

DEMONSTRAÇÃO. Recordemos que IF é aditivamente gerado por $\langle 1, -a\rangle$ $(a \in F^*)$. Desse modo, I^2F é aditivamente gerado por $\langle 1, -a\rangle \otimes \langle 1, -b\rangle$ $(a, b \in F^*)$. A segunda conclusão segue assim do corolário acima. Também temos que I^3F é aditivamente gerado por

$$\varphi = \langle 1, -a\rangle \otimes \langle 1, -b\rangle \otimes \langle 1, -c\rangle = \langle 1, -a, -b, ab\rangle - \langle c, -ca, -cb, cab\rangle \in W(F)$$

Por 5.21

$$\gamma(\langle c, -ca, -cb, cab\rangle) = \left(\frac{c^2a, c^{2b}}{F}\right) = \left(\frac{a, b}{F}\right) = \gamma(\langle 1, -a, -b, ab\rangle).$$

Portanto, $\gamma(\varphi) = 1$

□

Corolário 5.24. Seja $f = \langle 1, -a\rangle \otimes \langle 1, -b\rangle$ e $g = \langle 1, -c\rangle \otimes \langle 1, -d\rangle$. Se $f \equiv g \pmod{I^3F}$, então $f \cong g$.

Uma consequência do Corolário 5.22 é que o diagrama (*) pode ser reescrito como

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{I^2F}{I^3F} & \longrightarrow & \frac{W(F)}{I^3F} & \longrightarrow & \frac{W(F)}{I^3(F)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \overline{\gamma}} & & \downarrow{\scriptstyle \overline{\Gamma}} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & B(F) & \xrightarrow{i} & BW(F) & \xrightarrow{j} & Q(F) & \longrightarrow & 0 \end{array}$$

onde $\overline{\gamma}$ e $\overline{\Gamma}$ são homomorfismos induzidos por γ e Γ.

Se $F = \mathbb{R}$, então $\overline{\Gamma}$ é um isomorfismo e

$$BW(\mathbb{R}) \simeq \frac{\mathbb{Z}}{8\mathbb{Z}}.$$

Esses resultados seguem dos fatos:

$$W(\mathbb{R}) \simeq \mathbb{Z},$$

$$\frac{I^2\mathbb{R}}{I^3\mathbb{R}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \simeq B(\mathbb{R})$$

e que γ envia $\langle 1, 1, 1, 1\rangle$ no gerador $\left(\frac{-1,-1}{\mathbb{R}}\right) \in B(\mathbb{R})$.

Na demonstração do Teorema 4.54 obtemos $t : Q(F) \to BW(F)$ dada por

$$t(1, a) = \langle C(\langle a\rangle)\rangle, \;\; t(0, a) = \langle C(\langle -a, 1\rangle)\rangle \;\; \forall a \in F^*$$

com as seguintes propriedades:

$$j \circ t = \mathbb{I}_{Q(F)} \;\text{ e } t(0, 1) = 1 \in BW(F).$$

Através dessa aplicação, cada elemento b de $BW(F)$ pode ser escrito unicamente na forma

$$b = a \cdot t(e, d),$$

onde $a \in B(F)$. A partir da t também podemos considerar $\Delta : Q(F) \times Q(F) \to B(F)$ dada por $\Delta(x, y) = t(x)t(y)t(xy)^{-1}$. Se definirmos em $B(F) \times Q(F)$ um produto dado por

$$(D, x) \cdot (E, y) = (D \cdot E \cdot \Delta(x, y), x \cdot y)$$

então $(B(F) \times Q(F), \cdot)$ é um grupo abeliano isomorfo a $BW(F)$.

Teorema 5.25.

(1) $\Delta((1, a), (1, b)) = \Delta((0, a), (0, b)) = \left(\frac{a,b}{F}\right) \in \mathrm{Quat}(F)$.
(2) $\Delta((1, a), (0, b)) = \Delta((0, b), (1, a)) = \left(\frac{-a,b}{F}\right) \in \mathrm{Quat}(F)$.

Demonstração. Por definição

$$\begin{aligned}\Delta((1,a),(1,b)) &= C(\langle a\rangle)\widehat{\otimes}\langle b\rangle\widehat{\otimes}\langle 1,ab\rangle^{-1}\\ &= \Gamma(\langle a,b,-1,-ab\rangle) = \left(\frac{a,b}{F}\right)\in B(F)\end{aligned}$$

através de 5.21. Os cálculos restantes são inteiramente análogos. □

Esse teorema nos fornece a seguinte tabela de multiplicação em $BW(F)\simeq (B(F)\times Q(F),\cdot)$

Teorema 5.26. Para quaisquer $a,b\in F^*$

(1) $(D,1,a)\cdot(E,1,b)=(D\cdot E\cdot\left(\frac{a,b}{F}\right),0,-ab)\in BW(F)$
(2) $(D,0,a)\cdot(E,0,b)=(D\cdot E\cdot\left(\frac{a,b}{F}\right),0,ab)\in BW(F)$
(3) $(D,0,a)\cdot(E,1,b)=(D\cdot E\left(\frac{a,-b}{F}\right),1,ab)\in BW(F)$
(4) $(D,0,a)^{-1}=(D^{-1}\cdot\left(\frac{a,a}{F}\right),0,a)$
(5) $(D,1,a)^{-1}=(D^{-1},1,a)$.

Teorema 5.27.

(1) Se $\text{type}(A)=1$ então $\langle A\rangle=([A_0],1,\delta(A))\in BW(F)$.
(2) Se $\text{type}(B)=0$ então $\langle B\rangle=([B],0,\delta B)\in BW(F)$.

Demonstração. (1) Temos nesse caso $A\simeq(A_0)\widehat{\otimes}Z(A)$, como álgebras graduadas, e $Z(A)\simeq C(\langle\delta\rangle)$ $(\delta=\delta(A))$. Assim. temos $\langle A\rangle=[A_0]t(1,\delta)$ e isso implica $\langle A\rangle=([A_0],1,\delta(A))$.

(2) Escrevendo $\langle B\rangle=(x,0,\delta)$ $(\delta=\delta(B))$ devemos determinar x. Consideremos a multiplicação de $\langle B\rangle$ por $\langle C(\langle 1\rangle)\rangle$, usando 5.26(3) o resultado é

$$\langle C(\langle 1\rangle\widehat{\otimes}B)\rangle=(x\cdot\left(\frac{\delta}{F}\right),1,-\delta).$$

Como $\text{type}(B)=0$, x é a classe da componente zero de $C(\langle -1\rangle)\widehat{\otimes}B$. Usando 2.21 temos

$$x=[(C\langle -1\rangle\widehat{\otimes}B)_0]=[F\otimes B]=[B]\in B(F).$$

□

Corolário 5.28. Sejam $A,B\in\text{AGCS}(F)$. Assumamos que ou A,B são ambas do tipo ímpar ou $\delta(A)$, $\delta(B)$ são diferentes de 1. Então $A\simeq B$ se, e somente se, $\langle A\rangle=\langle B\rangle\in BW(F)$ e $\dim A=\dim B$.

Continuando o uso da notação tripla, podemos expressar o invariante de Clifford de um espaço quadrático V na forma

$$\Gamma(V)=(c(V),\dim{}_0V,d_{\pm}V)$$

onde $c(V) \in B(F)$ e $\dim {}_0V$ significa $\dim V (\mathrm{mod}\ 2)$. Por 5.27 temos:

$$c(V) = \begin{cases} [C_0(V)] \in B(F) \text{ se } \dim V \text{ impar} \\ [C(V)] \in B(F) \text{ se } \dim V \text{ par} \end{cases}$$

Essa c é então uma função $c : W(F) \to B(F)$ e é conhecida como **invariante de Witt**. Ela não é um homomorfismo sobre $W(F)$ embora seja sobre I^2F (no qual $c = \gamma$). As fórmulas de $c(U \perp V)$ em vários casos podem ser interpretadas imediatamente de 5.26 como segue:

PROPOSIÇÃO 5.29. Sejam (U, f) e (V, q) espaços quadráticos, então:

$$c(U \perp V) = c(U) \cdot c(V) \cdot \left(\frac{d_\pm U, d_\pm V}{F}\right)$$

se $\dim U$ e $\dim V$ são ambos ímpares ou ambos pares, e

$$c(U \perp V) = c(U) \cdot c(V) \cdot \left(-\frac{d_\pm U, d_\pm V}{F}\right)$$

se $\dim U$ é ímpar e $\dim V$ é par.

DEFINIÇÃO 5.30. Se $\langle a_1, \ldots, a_n\rangle$ é uma diagonalização de V definimos o **invariante de Hasse** , $s(V)$, como sendo a classe de

$$\prod_{i<j} \left(\frac{a_i, a_j}{F}\right)$$

em $B(F)$.

PROPOSIÇÃO 5.31. $s(V)$ não depende da diagonalização escolhida para defini-lo.

DEMONSTRAÇÃO. Relembremos que quaisquer duas diagonalizações de um mesmo espaço quadrático são cadeia equivalentes. Assim, é suficiente comparar os dois produtos definidos por $\langle a, b, a_3, \ldots, a_n\rangle$ e $\langle c, d, a_3, \ldots, a_n\rangle$, onde $\langle a, b\rangle \cong \langle c, d\rangle$. A última isometria implica que $ab = cd \in F^*/F^{*2}$ e $\left(\frac{a,b}{F}\right) \simeq \left(\frac{c,d}{F}\right)$. O produto formado pela diagonalização $\langle a, b, a_3, \ldots, a_n\rangle$ é igual a

$$\left(\frac{a, b}{F}\right)\left(\frac{a, a_3 \cdots a_n}{F}\right)\left(\frac{b, a_3 \cdots a_n}{F}\right)\prod_{3\le i<j}\left(\frac{a_i, a_j}{F}\right)$$

$$= \left(\frac{c, d}{F}\right)\left(\frac{cd, a_3 \cdots a_n}{F}\right)\prod_{3\le i<j}\left(\frac{a_i, a_j}{F}\right)$$

o qual é precisamente o produto formado pela segunda diagonalização $\langle c, d, a_3, \ldots, a_n\rangle$. □

PROPOSIÇÃO 5.32. Seja $n = \dim V$.

(1) Se $n \equiv 1, 2\ (\mathrm{mod} 8)$ então $c(V) = s(V)$.

(2) Se $n \equiv 3,4 \pmod 8$ então $c(V) = s(V) \cdot \left(\frac{-1,-d(V)}{F}\right)$.
(3) Se $n \equiv 5,6 \pmod 8$ então $c(V) = s(V) \cdot \left(\frac{-1,-1}{F}\right)$.
(4) Se $n \equiv 7,8 \pmod 8$ então $c(V) = s(V) \cdot \left(\frac{-1,d(V)}{F}\right)$.

Podemos escrever essas quatro afirmações numa única fórmula por

$$(A) \quad c(V) = s(V) \cdot \left(\frac{-1, d(V)}{F}\right)^{\epsilon} \cdot \left(\frac{-1,-1}{F}\right)^{\delta}$$

onde $\epsilon = \frac{(n-1)(n-2)}{2}$ e $\delta = \frac{(n+1)n(n-1)(n-2)}{24}$. Nesse caso, se $[V] \in I^2F$ com $\dim V = 2m$ temos

$$(B) \quad c(V) = s(V) \cdot \left(\frac{-1,-1}{F}\right)^{\frac{m(m-1)}{2}}.$$

Demonstração. Aplicaremos indução sobre n, e mostraremos como fazer a etapa de indução no caso $n = 8r + 1$. escrevamos $V \cong \langle a \rangle \perp U$, onde $\dim U \equiv 0 \pmod 8$. Por 5.29 temos

$$c(V) = c(U) \cdot \left(\frac{-a, d(U)}{F}\right)$$

e por indução

$$c(U) = s(U) \cdot \left(\frac{-1, d(U)}{F}\right).$$

Combinando essas equações, vem

$$c(V) = s(U) \cdot \left(\frac{a, d(U)}{F} = s(V)\right),$$

como em (1). Os outros casos são semelhantes, e as fórmulas (A) e (B) seguem por mera inspeção. □

Vejamos agora como esses invariantes podem determinar completamante uma forma quadrática dadas certas hipóteses.

Teorema 5.33. Para formas q, q' tais que $\dim q = \dim q' \leq 3$ as seguintes sentenças são equivalentes.

(1) q, q' são isométricas;
(2) $d(q) = d(q')$ e $c(q) = c(q')$;
(3) $d(q) = d(q')$ e $s(q) = s(q')$.

Demonstração. Precisamos provar somente (3) $\Rightarrow$ (1), pois o resto é trivial. O caso binário ja foi tratado no Corolário 2.20, assim, asumamos q e q' formas ternárias. Consideremos d ser o determinante comum de q q'. Cálculos imediatos fornecem,

$s(\langle -d\rangle \cdot q) = s(q)\left(\frac{-d,-d}{F}\right)$. Substituindo q e q' por $\langle -d\rangle q$ e $\langle -d\rangle q'$, podemos assumir que o determinante comum é -1. Escrevamos

$$q = \langle x, y, -xy\rangle,\ q' = \langle x', y', x'y'\rangle.$$

Então $s(q) = \left(\frac{x,y}{F}\right)$ e $s(q') = \left(\frac{x',y'}{F}\right)$. Como elas são iguais (por (3)) temos

$$\langle 1, -x, -y, xy\rangle \cong \langle 1, -x', -y', x'y'\rangle.$$

Por 2.15. Cancelando $\langle 1\rangle$ deduzimos que $q \cong q'$. □

Proposição 5.34. Suponha que toda forma de dimensão 5 sobre F é isotrópica. Então duas formas q, q' são isométricas se, e somente se, $\dim q = \dim q'$, $d(q) = d(q')$ e $s(q) = s(q')$.

Demonstração. ($\Rightarrow$) Óbvio.

($\Leftarrow$) Se a dimensão comum n é ≤ 3, o resultado segue do Teorema 5.33. Agora suponhamos $n \geq 4$. As hipóteses então implicam que q, q' representam 1. Digamos que $q \simeq \langle 1\rangle \perp \varphi$ e $q' \simeq \langle 1\rangle \perp \varphi'$. Claramente, φ, φ' têm a mesma dimensão, determinante, e invariante de Hasse. Por indução, temos $\varphi \simeq \varphi'$ e dai $q \simeq q'$. □

Atualmente existem resultados melhores na literatura. Por exmplo, em 1972, R. Elman e T.Y.Lam, provaram que formas quadráticas sobre um corpo F são classificadas por dimensão, determinante e invariante de Hasse se, e somente se, $I^3F = \mathbf{0}$. Muitas outras informações podem ser ditas a respeito desses invariantes sobre as formas quadráticas, contudo pararemos nossa discussão por aqui.

2. Periodicidade Real e Módulos de Clifford

Nessa seção estamos inicialmente interessados em calcular a álgebra de Clifford de espaços quadráticos da forma

$$p\langle 1\rangle \perp q\langle -1\rangle,$$

com $p, q \geq 0$. Em seguida discutiremos a questão da representação dessas álgebras. Para simplificar a notação escrevemos

$$C^{p,q} := C(p\langle 1\rangle \perp q\langle -1\rangle).$$

Proposição 5.35. Existe um isomorfismo de álgebras graduadas

$$C^{p+n,q+n} \simeq \widehat{M}_{2^n}(C^{p,q}).$$

Demonstração. Da decomposição ortogonal

$$\varphi_{p+n,q+n} \cong \varphi_{p,q} \perp \varphi_{n,n}$$

temos

$$C^{p+n,q+n} \simeq C^{p,q}\widehat{\otimes}C^{n,n}.$$

Mas, pelo Corolário 5.12

$$C^{n,n} \simeq \widehat{M}_{2^n}(F).$$

Assim, pelo Corolário 4.40 do capítulo 4, vem:

$$C^{p+n,q+n} \simeq C^{p,q}\widehat{\otimes}\widehat{M}_{2^n}(F) \simeq \widehat{M}_{2^n}(C^{p,q}).$$

□

PROPOSIÇÃO 5.36. (**"Periodicidade 8"**) $C^{p+8,q} \simeq \widehat{M}_{16}(C^{p,q}) \simeq C^{p,q+8}$.

DEMONSTRAÇÃO. É suficiente provarmos o primeiro isomorfismo pois o segundo é análogo. Consideremos inicialmente o caso quando $p = q = 0$. □

Assim, reduzimos nosso problema ao cálculo de $C^{p,0}$ e $C^{0,q}$, com $0 \leq p, q \leq 7$. Podemos calcular essas álgebras em termos das álgebras graduadas $C^{1,0}$, $C^{2,0}$, $C^{0,1}$ e $C^{0,2}$ denotadas respectivamente por X, Y, Z e W. Como sabemos, via exmplos 5.7 e 5.8,

$$X \simeq F\langle\sqrt{-1}\rangle,\ \ Y \simeq \left\langle \frac{-1,-1}{F} \right\rangle,\ \ Z \simeq F\langle\sqrt{1}\rangle \ \text{ e } \ W \simeq \left\langle \frac{-1,-1}{F} \right\rangle.$$

As outras álgebras de Clifford são dadas como segue:

n	0	1	2	3	4	5	6	7
$C^{n,0}$	F	X	Y	$Y \otimes Z$	$Y \otimes W$	$\widehat{M}_2(X \otimes W)$	$\widehat{M}(W)$	$\widehat{M}_8(Z)$
$C^{0,n}$	F	Z	W	$X \otimes W$	$Y \otimes W$	$\widehat{M}_2(X \otimes W)$	$\widehat{M}_4(W)$	$\widehat{M}_8(X)$

Especializaremos nossas informações agora para as álgebras não graduadas. Como tais, $Z \simeq F \times F$ e $W = M_2(F)$ porém, X e Y dependem de certas propriedades de corpo F. Precisamente, existem três casos a serem considerados:

Caso 1 $-1 \in F^{*2}$ ($X \simeq F \times F$, $Y \simeq M_2(F)$).

Caso 2 $-1 \notin F^{*2}$ mas é uma soma de dois quadrados ($X = F(\sqrt{-1})$ é um corpo e $Y = M_2(F)$).

Caso 3 -1 não é uma soma de dois quadrados ($X = F(\sqrt{-1})$ é um corpo e $Y = \left(\frac{-1,-1}{F}\right)$ é uma álgebra com divisão).

No Caso 1 temos $C^{n,0} \simeq C^{0,n}$. Além disso, $C^{2,0}$ é hiperbólico e

$$C^{p+2,0} \simeq C^{p,0}\widehat{\otimes}\widehat{M}_2(F) \simeq \widehat{M}_2(C^{0,p}).$$

Temos então "periodicidade 2"nesse caso:

$Caso\ 1$	0	1	2	3
$C^{n,0} \simeq C^{0,n}$	F	$F \times F$	$M_2(F)$	$M_2(F) \times M_2(F)$
	4	5	6	7
$C^{n,0} \simeq C^{0,n}$	$M_4(F)$	$M_4(F) \times M_4(F)$	$M_8(F)$	$M_8(F) \times M_8(F)$

No Caso 2 temos $\langle 1,1\rangle \simeq \langle -1,-1\rangle$ e assim,

$$C^{p+4,0} \simeq C^{p,0}\widehat{\otimes}\widehat{M_4}(F) \simeq \widehat{M_4}(C^{p,0}).$$

Desse modo, temos aqui "periodicidade 4".

$Caso\ 2$	0	1	2	3
$C^{n,0}$	F	X	$M_2(F)$	$M_2(F) \times M_2(F)$
$C^{0,n}$	F	$F \times F$	$M_2(F)$	$M_2(X)$
	4	5	6	7
$C^{n,0}$	$M_4(F)$	$M_4(X)$	$M_8(F)$	$M_8(F) \times M_8(F)$
$C^{0,n}$	$M_4(F)$	$M_4(F) \times M_4(F)$	$M_8(F)$	$M_8(X)$

No Caso 3 não temos simplificações maiores além das usuais $X \times M_n(F) \simeq M_n(X), M_r(M_s(F)) \simeq M_{rs}(F), \ldots$, etc. Temos assim a seguinte tabela de leitura.

$Caso\ 2$	0	1	2	3
$C^{n,0}$	F	X	Y	$Y \times Y$
$C^{0,n}$	F	$F \times F$	$M_2(F)$	$M_2(X)$
	4	5	6	7
$C^{n,0}$	$M_2(Y)$	$M_4(X)$	$M_8(F)$	$M_8(F) \times M_8(F)$
$C^{0,n}$	$M_2(Y)$	$M_2(Y) \times M_2(Y)$	$M_4(Y)$	$M_8(X)$

Nosso objetivo agora é saber qual o valor máximo $k = \rho_F(n)$ tal que $C^{k-1,0}$ admite uma represntação n-dimensional sobre F. Os resultados a seguir trarão a resposta procurada e para a demonstração dos mesmos faremos uso de certas propriedades dos anéis semisimples (vide Apêndice B).

LEMA 5.37. $M_m(F)$ é mapeado em $M_n(F)$ (como uma F-álgebra) se, e somente se, m divide n.

DEMONSTRAÇÃO. Usaremos a equivalência óbvia segundo a qual uma tal função existe se, e somente se, F^n pode ser tornado um $M_m(F)$-módulo. Como $M_n(F)$ é simples, então todo F^n é M_m-módulo semi-simples. Seja então $U_1 \oplus \ldots \oplus U_r$ a decomposição em soma direta em módulos simples. Como o único módulo simples de $M_n(F)$ é F^m temos

$$n = r \cdot m$$

Para mostrar a recíproca basta identificarmos F^n com $M_{m\times r}(F)$ e definirmos a ação de $M_m(F)$ sobre $M_{m\times r}$ através da multiplicação de matrizes. □

TEOREMA 5.38. Suponha $n = 2^a n_0$, onde n_0 é ímpar. Então $\rho_F(n) = 2a + 2$.

DEMONSTRAÇÃO. Escrevamos $m - 1 = 2s + i$ ($i = 0$ ou 1). Pelo Caso 1, $C^{m-1,0}(F) \simeq M_{2^s}(F)$ se $i = 0$, e

$$C^{m-1,0} \simeq M_{2^s}(F) \times M_{2^s}(F)$$

se $i = 1$. Assim, pelo Lema 5.37, $C^{m-1,0}$ é mapeado em $M_n(F)$ se, e somente se, $2^s|n$, i.e., se, e somente se, $s \leq a$. O maior valor possível para m nesse caso é $\rho(n) = 2a + 2$. □

LEMA 5.39. $M_m(X)$ é mapeado em $M_n(F)$ (como uma F-álgebra) se, e somente se, $2m$ divide n.

DEMONSTRAÇÃO. A prova é analóga a feita no Lema 5.37. A única observação a a ser feita é que o único $M_n(X)$-módulo simples tem dimensão $2m$. □

TEOREMA 5.40. Suponhamos $n = 2^{2a+b}n_0$ onde n_0 é ímpar e $b = 0$ ou 1. Então $\rho_F(n) = 4a + 4^b$.

DEMONSTRAÇÃO. Escrevamos $m-1 = 4s+i$ ($0 \leq i \leq 3$). Pela "4-periodicidade", $C^{m-1,0}$ é

$$M_{2^{2s}}(F), \text{ ou } M_{2^{2s}}(X), \text{ ou } M_{2^{2s+1}}(F) \text{ ou } M_{2^{2s+1}}(F) \times M_{2^{2s+1}}(F),$$

de acordo com $i = 0, 1, 2$ ou 3. Se $b = 0$, o maior m para o qual $C^{m-1,0}$ é mapeado em $M_n(F)$ é obtido considerando $s = a$ e $i = 0$, e isso fornece $m = 4a+1$. Analogamente, para $b = 1$, o maior m é obtido considerando $s = 0$ e $i = 3$, o qual fornece $m = 4a + 4$ □

LEMA 5.41. $M_m(Y)$ é mapeado em $M_n(F)$ (como uma F-álgebra) se, e somente se, $4m$ divide n.

DEMONSTRAÇÃO. A demonstração desse lema se da de forma análoga a do Lema 5.39. □

TEOREMA 5.42. Suponha $n = 2^{4a+b}n_0$, onde n_0 é ímpar e $0 \leq b \leq 3$. Então, $\rho_F(n) = 8a + 2^b$.

DEMONSTRAÇÃO. Escrevamos $m-1 = 8s+i$ $(0 \leq i \leq 7)$. Pela "8-periodicidade", $C^{m-1}, 0$ é dado por

	$C^{m-1,0}$
$i=0$	$M_{2^{4s}}(F)$
$i=1$	$M_{2^{4s}}(X)$
$i=2$	$M_{2^{4s}}(Y)$
$i=1$	$M_{2^{4s}}(Y) \times M_{2^{4s}}(Y)$

	$C^{m-1,0}$
$i=4$	$M_{2^{4s+1}}(Y)$
$i=5$	$M_{2^{4s+2}}(X)$
$i=6$	$M_{2^{4s+3}}(F)$
$i=7$	$M_{2^{4s+3}}(F) \times M_{2^{4s+3}}(F)$

Por 5.37, 5.39 e 5.41 temos os seguintes casos

	caso
$i=0$	$4s \leq 4a+b$
$i=1$	$4s+1 \leq 4a+b$
$i=2$	$4s+2 \leq 4a+b$
$i=3$	$4s+2 \leq 4a+b$

	caso
$i=4$	$4s+3 \leq 4a+b$
$i=5$	$4s+3 \leq 4a+b$
$i=6$	$4s+3 \leq 4a+b$
$i=7$	$4s+3 \leq 4a+b$

Para $b=0$, encontramos o valor máximo de m considerando $s=a$ e $i=0$, i.e, $m = 8a+1$. Para $b=1$, ele é obtido para $s=a$ e $i=1$, i.e., $m=8a+2$. Para $b=2$, ele é obtido para $s=a$ e $i=3$, i.é., $m=8a+4$. Para $b=3$ ele é obtido para $s=a$ e $i=7$, i.e., $m=8a+8$. □

Também podemos estudar os casos onde $k = \rho'_F(n)$ é o valor máximo para o qual $C^{0,k-1}$ tem uma representação n-dimensional sobre F. Os resultados para essas situações são totalmente análogos e os cálculos são paralelos aos anteriores, por isso, seguem aqui apenas seus enunciados.

TEOREMA 5.43. Suponha $n = 2^a n_0$, onde n_0 é ímpar. Então, $\rho'_F(n) = \rho_F(n) = 2a+2$.

TEOREMA 5.44. Suponha $n = 2^{2a+b}n_0$, one n_0 é ímpar e $b=0$ ou 1. Então, $\rho'_F(n) = 4a+b+2$.

TEOREMA 5.45. Suponha $n = 2^{4a+b}n_0$, onde n_0 é ímpar e $0 \leq b \leq 3$. Então, $\rho'_F(n) = 8a+b+\lfloor \frac{b}{3} \rfloor + 2$.

Apresentaremos na seção seguinte uma aplicação das ferramentas desenvolvidas até agora. Trata-se do problema das formas quadráticas de composição que é assunto de interesse nos estudos de espaços projetivos, variedades Grassmanianas, campos de vetores sobre esfera, etc.

3. Formas Quadráticas de Composição

No **Disquisitiones arithmeticae,** obra prima de Gauss publicada em 1801, existe uma seção dedicada a um estudo sistemático da aritmética das formas quadráticas binárias, mais especificamente, aquelas cujos coeficientes são inteiros. Em suas pesquisas a respeito desse assunto, Gauss introduziu o conceito de formas quadráticas de composição. Se f, g, h são formas quadráticas binárias com coeficientes $a, b, c; a', b', c'; A, B, C$ respectivamente, então ele dizia que h é a composta de f e g (ou o resultado da composição de f e g) se a equação

$$f(\xi_1, \xi_2) \cdot g(\eta_1, \eta_2) = h(\zeta_1, \zeta_2)$$

é verdadeira para quaisquer ξ_1, ξ_2 e η_1, η_2, onde ζ_1 e ζ_2 são formas bilineares com coeficientes inteiros.

Seguindo os passos de Gauss, álgebras de composição mais gerais foram consideradas. Num artigo de Hurwitz ele expõe o seguinte:

"No domínio das formas quadráticas de dimensão n, uma teoria de composição existe se para qualquer três formas quadráticas φ, ψ, χ de formas quadráticas regulares a equação

$$\varphi(x_1, \ldots, x_n)\psi(y_1, \ldots, y_n) = \chi(z_1, \ldots, z_n)$$

pode ser satisfeita por uma escolha de uma aplicação bilinear conveniente que envia $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ em $(z_1, \ldots, z_n)$.

No texto presente estudaremos o seguinte problema: Sejam (V, φ), (U, λ) espaços quadráticos. Existe uma aplicação bilinear de $V \times U$ em V, $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{xy}$, tal que

$$\varphi(\mathbf{xy}) = \varphi(\mathbf{x})\lambda(\mathbf{y}) \tag{29}$$

quaisquer que sejam $\mathbf{x} \in V$ e $\mathbf{y} \in U$?

Façamos algumas deduções a respeito de (29). Denotemos por A e B as formas bilineares sobre U e V associadas as formas quadráticas λ e φ respectivamente. Para $\mathbf{x} \in U$ e $\mathbf{y}, \mathbf{z} \in V$, temos

$$\begin{aligned} B(\mathbf{x} \cdot \mathbf{y}, \mathbf{x} \cdot \mathbf{z}) &= \frac{1}{2}[\varphi(\mathbf{x} \cdot (\mathbf{y} + \mathbf{z})) - \varphi(\mathbf{x} \cdot \mathbf{y}) - \varphi(\mathbf{x} \cdot \mathbf{z})] \\ &= \lambda(\mathbf{x}) \cdot \frac{1}{2}[\varphi(\mathbf{x} + \mathbf{y}) - \varphi(\mathbf{y}) - \varphi(\mathbf{z})] \\ &= \lambda(\mathbf{x})B(\mathbf{y}, \mathbf{z}) \end{aligned} \tag{30}$$

Da mesma maneira, para $B(\mathbf{x} \cdot \mathbf{y}, \mathbf{w} \cdot \mathbf{y})$ $(\mathbf{x}, \mathbf{w} \in U,\ \mathbf{y} \in V)$ obtemos

$$B(\mathbf{x} \cdot \mathbf{y}, \mathbf{w} \cdot \mathbf{y}) = A(\mathbf{x}, \mathbf{w})\varphi(\mathbf{y}) \tag{31}$$

Exibimos agora uma normalização para facilitar os cálculos futuros. Considere $\mathbf{u} \in U$ um vetor qualquer com $\lambda(\mathbf{u}) = a \neq 0$. Então, a ação de $\mathbf{u}$ por multiplicação sobre V é um isomorfismo linear. de fato, se $\mathbf{u} \cdot \mathbf{y} = \mathbf{0}$, então para cada $\mathbf{z} \in V$,

$$0 = B(\mathbf{u} \cdot \mathbf{y}, \mathbf{u} \cdot \mathbf{z}) = a \cdot B(\mathbf{y}, \mathbf{z}) \Rightarrow B(\mathbf{y}, \mathbf{z}) = 0.$$

Como B é regular, $\mathbf{y}$ deve ser igual a zero. Definiremos agora uma nova aplicação bilinear. Para $\mathbf{x} \in U$ e $\mathbf{y} \in V$, seja $\mathbf{x} * \mathbf{y}$ o único vetor em V tal que $\mathbf{u} \cdot (\mathbf{x} * \mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$. Avaliando φ em ambos os lados, obtemos $a\varphi(\mathbf{x} * \mathbf{y}) = \lambda(\mathbf{x})\varphi(\mathbf{y})$. Se λ' denota a forma quadrática $a^{-1}\lambda$ sobra U temos $\varphi(\mathbf{x} * \mathbf{y}) = \lambda'(\mathbf{x})\varphi(\mathbf{y})$. Facilmente checa-se que $*$ é uma aplicação bilinear. Finalmente, notemos que $\lambda'(\mathbf{u}) = 1$ e que a definição de $*$ força $\mathbf{u} * \mathbf{y} = \mathbf{y}$ para todo $\mathbf{y} \in V$.

Com essa normalização podemos assumir que $\lambda(\mathbf{u}) = 1$ e $\mathbf{u}$ age como a identidade sobre V.

Teorema 5.46. Suponhamos que encontramos uma tal normalização. Considere U_0 o complemento ortogonal de $F \cdot \mathbf{u}$. Então a álgebra de Clifford $C(U_0, -\lambda)$ admite uma F-representação sobre V.

Demonstração. Para qualquer $\mathbf{x} \in U_0$, denotemos por $L_{\mathbf{x}}$ a multiplicação por $\mathbf{x}$ sobre V. Se $\mathbf{y} \in V$, temos

$$B(\mathbf{y}, L_{\mathbf{x}}(\mathbf{y})) = B(\mathbf{u} \cdot \mathbf{y}, \mathbf{x}\mathbf{y}) = A(\mathbf{u}, \mathbf{x})\varphi(\mathbf{y}) = 0.$$

De $0 = B(\mathbf{y} + \mathbf{z}, L_{\mathbf{x}}(\mathbf{y} + \mathbf{z}))$ obtemos

$$B(\mathbf{y}, L_{\mathbf{x}}(\mathbf{z})) + B(\mathbf{z}, L_{\mathbf{x}}(\mathbf{y})) = 0 \tag{32}$$

Se trocarmos $\mathbf{z}$ por $L_{\mathbf{x}}(\mathbf{z})$ vem

$$B(\mathbf{y}, L_{\mathbf{x}}^2(\mathbf{z})) = -B(\mathbf{x} \cdot \mathbf{z}, \mathbf{x} \cdot \mathbf{y}) = -\lambda(\mathbf{x})B(\mathbf{y}, \mathbf{z}),$$

i.e.,

$$B(\mathbf{y}, (L_{\mathbf{x}}^2 + \lambda(\mathbf{x}) \cdot 1_V)\mathbf{z}) = 0$$

onde 1_V denota a aplicação identidade sobre V. Consequentemente,

$$L_{\mathbf{x}}^2 = -\lambda(\mathbf{x})1_V \in \mathrm{End}_F V,$$

sempre que $\mathbf{x} \in U_0$. Isso mostra que a regra $\mathbf{x} \mapsto L_{\mathbf{x}}$ define um homomorfismo de F-álgebras de $C(U_0, -\lambda)$ em $\mathrm{End}_F V$. □

Aplicaremos o Teorema 5.46 ao caso clássico $\lambda \simeq m\langle 1 \rangle$. Como λ representa 1, na normalização isso não muda. Iniciando com qualquer $\mathbf{u} \in U$ tal que $\lambda(\mathbf{u}) = 1$, o espaço quadrático $(U_0, -\lambda)$ do Teorema 5.46 é justamente $(m-1) \cdot \langle 1 \rangle$. Usando a notação $C(U_0, -\lambda) = C^{m-1,0}$ cocluímos o seguinte de Teorema 5.46.

TEOREMA 5.47. Se $\lambda \cong m\langle 1\rangle$, uma condição necessária para a fórmula de composição (29) existir é que $m \leq \rho_F(n)$, onde $\rho_F(n)$ é determinado como em 5.38, 5.40 e 5.42. Analogamente, se $\lambda \cong \langle 1\rangle \perp (m-1)\langle -1\rangle$, então uma condição suficiente para que (29) exista é que $m \leq \rho'_F(n)$, onde $\rho'_F(n)$ é determinado como em 5.43, 5.44 e 5.45.

COROLÁRIO 5.48. Em geral (sem restrições sobre λ), uma condição nescessária para a fórmula de composição (29) existir é que $m \leq 2a+2$, onde $n = 2^a n_0$ (n_0 ímpar).

DEMONSTRAÇÃO. Suponhamos 29 verdadeira. Seja K um extensão de corpo qualquer de F. Podemos mostrar, mediante cálculos, que $(K \otimes U, K \otimes \lambda)$ e $(K \otimes V, K \otimes \varphi)$ têm as mesma fórmulas de composição que U, V, sobre a extensão escalar da aplicação bilinear original. Passando ao fecho algébrico de F, podemos assumir que $\lambda \simeq m\langle 1\rangle$. A função $\rho_F(n)$, nesse caso, nos da $m \leq 2a+2$, onde $n = 2^a n_0$. □

TEOREMA 5.49. (**Hurwitz**) Seja (V, φ) um espaço quadrático regular sobre F. Se existe uma aplicação bilinear $V \times V \to V$, denotada por $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \cdot \mathbf{y}$, tal que $\varphi(\mathbf{x} \cdot \mathbf{y}) = \varphi(\mathbf{x})\varphi(\mathbf{y})$para todo $\mathbf{x}, \mathbf{y} \in V$, então $\dim V = 1, 2, 4,$ ou 8.

DEMONSTRAÇÃO. Nesse caso epecial $U = V$, $m = n$ e $\lambda = \varphi$. Se $n = 2^a n_0$ (n_0 ímpar), então 5.48 força $2a + 2 \geq 2^a n_0$. Isso só é possível para $0 \leq a \leq 3$ e $n_0 = 1$. Assim $n = 1, 2, 4$ ou 8. □

CAPíTULO 6

Álgebras Cíclicas

Nesse capítulo vamos construir uma classe de álgebras centrias simples utilizando ferramentas básicas da teoria de Galois. Uma das aplicações importantes é a construção, onde for possível, de álgebras com divisão não comutativas sobre corpos.

Seja K uma extensão galoisiana cíclica finita, de grau n, do corpo F com grupo de Galois $G = \mathrm{Gal}(K|F)$. Seja θ o gerador de G. Dado um elemento $a \in F$, estamos interessados em saber a respeito da existência de uma F-álgebra A, tal que A como um K-espaço vetorial esquerdo tem base consistindo das potências $1, j, \ldots, j^{n-1}$ de um elemento j e valem as relações

$$j^n = a, \quad j\alpha = \theta(\alpha)j \ \ (\forall \alpha \in K.)$$

Uma tal álgebra é chamada de **álgebra cíclica** e a representamos por $A = (K|F, \theta, a)$ (ou $\mathcal{C}(a)$ caso K e θ estiverem claros pelo contexto).

A motivação para a definição e o estudo dessa classe de álgebras nesta dissertação são basicamente duas. A primeira decorre do fato de que tais álgebras são uma generalização da álgebra dos quatérnios $\mathbb{H}$. Confirmamos essa afirmação com o exemplo a seguir.

Exemplo 6.1. Consideremos a álgebra dos quatérnios $\mathbb{H}$. Como sabemos, $\mathbb{C}$ é uma extensão cíclica de $\mathbb{R}$ de grau 2 e com grupo de Galois $G = \{\mathbb{I}, \theta\}$ onde θ é a conjugação complexa. Notamos facilmente que $\mathbb{H}$ é gerado por $\mathbb{R}$ e j e que

$$j\alpha = \theta(\alpha)j, \ \ j^2 = -1.$$

Portanto, $\mathbb{H}$ é uma álgebra cíclica.

A segunda é que para determinadas classes de corpos toda álgebra central simples é cíclica, como ilustrado pelo importante e celebrado teorema:

Teorema 6.2. (**Hasse-Brauer-Noether**) Se F é um corpo numérico, então toda F-álgebra central simples é cíclica.

Existem outras classes de corpos, por exemplo os corpos da forma $F(t)$ com F algebricamente fechado, para as quais toda álgebra central simples é cíclica. Por outro lado, existem exemplos de Albert e Amitsur (ver [**10**]) que mostram que a inclusão

$$\{\text{álgebras cíclicas sobre } F\} \subseteq \{ \text{ álgebras centrais simples sobre } F\}$$

pode ser estrita.

Faremos agora a exposição de alguns resultados a respeito dessas álgebras que mostram como elas são fontes de exemplos de álgebras com divisão não comutativa. Um resultado importante nesse sentido é o **Critério da Norma de Wedderburn** que discutiremosmais adiante.

Para fixar notação escreveremos os elementos de F por $a, b, \ldots$ os elementos de K por $\alpha, \beta, \ldots$ e os elementos de G por $\theta, \varphi, \ldots$. A norma de um elemento γ será denotada por $N(\gamma)$ e o conjunto das normas de elementos de K^* por $N(K^*)$.

Proposição 6.3. Se existe $\gamma \in K^*$ tal que $b = N(\gamma)a$ então $\mathcal{C}(a)$ é isomorfo a $\mathcal{C}(b)$ como F-álgebras. Em particular, se $a \in N(K^*)$ então $\mathcal{C}(a) \simeq \mathcal{C}(1) \simeq M_n(F)$.

Demonstração. Para a primeira parte é suficiente considerar o isomorfismo que é a identidade sobre K e que envia γj em j. Para a segunda parte, resta-nos demonstrar que $\mathcal{C}(1) \simeq M_n(F)$. Para isso, denotemos o anel das aplicações F-lineares de K em K por $\mathrm{End}_F(K)$ e identifiquemos o subanel

$$\{\alpha I_n : \ \alpha \in K\}$$

com o corpo K. Com essa identificação, considere o subanel A de $\mathrm{End}_F(K)$ gerado por produtos dos elementos de K com elementos de G. Temos,

$$\theta\alpha(\beta) = \theta(\alpha\beta) = \theta(\alpha)\theta(\beta),$$

ou seja, $\theta\alpha = \theta(\alpha)\theta$. Com isso concluimos que A, como um K-espaço vetorial, é gerado por G. Pelo lema da independência de Dedekind, os elementos de G são linearmente independentes sobre K. Logo, $\dim\ {}_KA = n$. Como $\dim\ {}_FK = n$, então $\dim\ {}_FA = n^2$ e dai que $A = M_n(F)$. Do fato que G é cíclico segue que A é gerado por $1, \theta, \ldots, \theta^{n-1}$ e

$$\theta\alpha = \theta(\alpha)\theta, \quad \theta^n = 1.$$

Portanto, de fato $\mathcal{C}(1) \simeq M_n(F)$. □

Traduzamos esse teorema no caso onde $F = \mathbb{R}$, $K = \mathbb{C}$ e $\theta =$ conjugação complexa. Para $\alpha = a + b\mathbf{i}$ temos

$$N(a + b\mathbf{i}) = (a + bi)(a - b\mathbf{i}) = a^2 + b^2$$

Como $F^*/F^{*2} = \pm 1$ então, a menos de isomorfismos, temos exatamente duas álgebras cíclicas correspondentes a $a = 1$ e $a = -1$; elas são respectivamente, $M_2(\mathbb{R})$ e $\mathbb{H}$.

Proposição 6.4. $A = (K|F, \theta, a) \in \mathrm{ACS}(F)$ e $\dim\ {}_FA = n^2$.

Demonstração. Cálculos imediatos sobre elementos da forma $\alpha_s j^s$ mostram que A é associativa. Mostraremos agora que A é simples. Para isso, assumamos $\mathfrak{a} \subseteq A$ um ideal bilateral não nulo. Seja $f = \alpha_0 + \alpha_1 j + \ldots + \alpha_{n-1} j^{n-1} \in \mathfrak{a}$ não nulo com $\alpha_i \in K$. Para todo $\alpha \in K$ temos

$$\begin{aligned} f_1 &= (\alpha_0 + \alpha_1 j + \ldots + \alpha_{n-1} j^{n-1})\alpha - \alpha(\alpha_0 + \alpha_1 j + \ldots + \alpha_{n-1} j^{n-1}) \\ &= \alpha_1(\theta(\alpha) - \alpha)j + \ldots + \alpha_{n-1}(\theta^{n-1}(\alpha) - \alpha)j^{n-1} \in \mathfrak{a}. \end{aligned}$$

Multiplicando f_1 por j obtemos um elemento não nulo da mesma forma de f mas com menos parcelas. Repetimos o argumento acima até o resultado ser um elemento da forma $\alpha j^l \in \mathfrak{a}$ que como sabemos, é um elemento invertível. Para provarmos que A é central, consideremos $f = \alpha_0 + \alpha_1 j + \ldots + \alpha_{n-1} j^{n-1} \in Z(A)$. Para todo $\alpha \in K$ temos

$$\alpha f = f\alpha. \tag{33}$$

Se existisse $1 \leq i \leq n-1$ tal que $\alpha_i \neq 0$ então de (33) $\theta^i(\alpha) = \alpha$ para todo $\alpha \in K$. Mas isso é um absurdo, logo $f = \alpha_0$. Que $\alpha \in F$ segue da igualdade

$$j\alpha = \theta(\alpha)j.$$

□

Observação 6.5. Outra propriedade de uma álgebra cíclica $A = (K|F, \theta, a)$ é que ela se decompõe sobre K. Essa propriedade é consequência de 4.20.

Seja V o grupo aditivo subjacente de $\mathcal{C}(a)$, $V = K1 + Kj + \ldots + Kj^{n-1}$. Olharemos para os elementos de V como polinômios em j com coeficientes em K.

Lema 6.6.

(1) Sejam $f, g \in V$. Se $\mathrm{gr}(f) + \mathrm{gr}(g) < n$ então $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$ e o produto fg em $\mathcal{C}(a)$ é independente de a.

(2) Se $f = j^r + \alpha_{r-1} j^{r-1} + \ldots + \alpha_0 \in V$, com $1 \leq r \leq n-1$, então existe $g = j^{n-r} + \beta_{n-r-1} j^{n-r-1} + \ldots + \beta_0$ (independente de a) tal que para cada $a \in F^*$, $\mathrm{gr}(gf) < \mathrm{gr}(f)$. Além disso, os termos não constantes de gf são independentes de a e o termo constante de gf em $\mathcal{C}(a)$ é $a + \beta_0\alpha_0$.

Demonstração. (1) Imediato

(2) Consideremos um produto

$$(j^{n-r} + \beta_{n-r-1} j^{n-r-1} + \ldots + \beta_0)(j^r + \alpha_{r-1} j^{r-1} + \ldots + \alpha_0),$$

onde os β_s são determinados recursivamente. Fazendo o coeficiente de j^{n-r} no produto igual a zero determinamos β_{n-r-1}, fazendo o coeficiente de j^{n-r-1} igual a zero determinamos β_0. □

PROPOSIÇÃO 6.7. $\mathcal{C}(a)$ é isomorfo a $\mathcal{C}(1)$ se, e somente se, $a \in N(K^*)$.

DEMONSTRAÇÃO. **se**) Ver Proposição 6.3.
somente se) $\mathcal{C}(a) \simeq \mathcal{C}(1) \simeq M_n(F)$ tem um ideal esquerdo I tal que o espaço quociente $\mathcal{C}(a)/I$ tem dimensão n sobre F (dimensão 1 sobre K). Em $\mathcal{C}(a)$ um ideal esquerdo principal é gerado por um polinômio mônico de grau mínimo. Como $\mathcal{C}(a)/I$ é unidimensional sobre K, $I = \mathcal{C}(a)(j - \alpha)$ para algum $\alpha \in K$. Para $f = j - \alpha$ e g, como no Lema 6.6, gf tem grau menor ou igual a 1 e f não é a unidade, logo $gf = 0$. Calculando os coeficientes de g segue que $a = N(\alpha)$. □

COROLÁRIO 6.8. Temos os seguintes resultados

(1) Se $a \notin N(K^*)$ então $\mathcal{C}(a)$ é um anel de matrizes sobre uma álgebra com divisão central.
(2) Seja $n = [K : F]$ um número primo. Se $a \notin N(K^*)$, então $\mathcal{C}(a)$ é uma álgebra com divisão.

DEMONSTRAÇÃO. (1) Pelas proposições 6.4 e 6.7, $\mathcal{C}(a) \in \mathrm{ACS}(F)$ e $\mathcal{C}(a) \ncong M_n(F)$. Assim, $\mathcal{C}(a) \simeq M_s(D)$, onde D é uma álgebra com divisão central simples. (2) Como $\mathcal{C}(a) \simeq M_s(D)$ calculando as dimensões temos $n^2 = s^2 t$, onde $t = \dim {}_F D$. Dessa maneira, ou $s = n$ e $t = 1$ com $\mathcal{C}(a) \simeq M_n(F)$ ou $s = 1$ e $t = n^2$. Pela Proposição 6.7 segue a segunda possibilidade e daí que $\mathcal{C}(a) \simeq D$. □

No capítulo 2 mostramos como representar a álgebra cíclica $\mathbb{H}$ por matrizes sobre $\mathbb{C}$. Agora estamos interessados em realizar o mesmo procedimento para uma álgebra cíclica qualquer. Para isso, consideremos $\mathcal{C}(a)$ como um K-espaço vetorial esquerdo. Para cada $f \in \mathcal{C}(a)$ a multiplicação direita por f é uma transformação K-linear e podemos representá-la por uma matriz $M(f)$, digamos, através de uma K-base escolhida, por exemplo, a base $1, j, \ldots, j^{n-1}$. Calculemos $M(f)$ de um elemento f geral de $\mathcal{C}(a)$. Para $\alpha \in K$, $j^s \alpha = \theta^s(\alpha) j^s$ e assim $M(\alpha)$ é uma matriz diagoanal com entradas $\alpha, \theta(\alpha), \ldots, \theta^{n-1}(\alpha)$. Agora

$$j^s j^r = \begin{cases} j^{s+r} & \text{se} \quad s + r \leq n - 1 \\ a j^{s+r-n} & \text{se} \quad s + r \geq n \end{cases}$$

assim

$$M(j^r) = \begin{pmatrix} 0 & I_{n-r} \\ aI_r & 0 \end{pmatrix}$$

Agora considere $1 \leq r \leq n - 1$ e $f = j^r + \alpha_{r-1} j^{r-1} + \ldots + \alpha_0$. Então $M(f) = M(j^r) + M(\alpha_{r-1}) M(j^{r-1}) + \ldots + M(\alpha_0)$.

TEOREMA 6.9. (**Critério da Norma de Wedderburn**) Seja F um corpo infinito. Se $a_0^r \notin N(K^*)$ para algum $1 \leq r \leq n-1$, então $\mathcal{C}(a_0)$ é uma álgebra com divisão.

DEMONSTRAÇÃO. Se $\mathcal{C}(a_0)$ não é uma álgebra com divisão, então ela tem divisores de zero. Escolhamos um divisor de zero f de grau mínimo e sem perda de generalidade com f mônico. Digamos que

$$f = j^r + \alpha_{r-1}j^{r-1} + \ldots + \alpha_0$$

onde $1 \leq r \leq n-1$. Pelo Lema 6.6, existe um g com $\mathrm{gr}(gf) < \mathrm{gr}(f)$, assim, pela escolha de f, $gf = 0$ (f é uma unidade se gf é uma unidade) e, em particular, seu termo constante é zero. O Lema 6.6 assegura que $a_0 + \beta_0\alpha_0 = 0$, e dai $\beta_0\alpha_0 = -a_0$. Agora consideremos o produto gf em $\mathcal{C}(a)$ para um a arbitrário. Para todo $a \in F^*$, novamente do Lema 6.6, temos que

$$gf = a + \beta_0\alpha_0 = a - a_0,$$

e assim $M(g)M(f) = M(a - a_0)$. Calculando o determinante temos

$$[(-1)^{r(n-r)}a^{n-r} + \ldots + N(\beta_0)][(-1)^{(n-r)r}a^r + \ldots + N(\alpha_0)] = (a - a_0)^n.$$

Isso é verdadeiro para todo a não nulo no corpo infinito F, e desse modo essa expressão é uma identidade em a, i.e., se substituirmos a por uma indeterminada x, então essa relação é verdadeira no anel de polinômios $K[x]$. Como $K[x]$ é um dominio fatorial então o lado esquerdo tem fatoração $(x-a)^n$. Assim, para o segundo fator temos

$$(-1)^{(n-r)r}a^r + \ldots + N(\alpha_0) = (-1)^{(n-r)r}(a - a_0)^r.$$

O termo constante é então

$$N(\alpha_0) = (-1)^{(n-r)r}(-1)^r(a_0)^r = (-1)^{nr}a_0^r,$$

com $r^2 \equiv r \bmod 2$. Finalmente,

$$N((-1)^r\alpha_0) = N((-1)^r)N(\alpha_0) = a_0^r$$

como desejávamos. □

Enunciaremos agora uma série de resultados relacionados aos anteriores, cujas demonstrações originais dadas por Brauer eram muito difíceis sendo hoje em dia corolários de teorias mais sofisticadas de cohomologia de Galois.

Se A é uma algebra central simples sobre F e se $A \simeq M_n(F) \otimes D$, com D uma álgebra com divisão sobre F, definimos o **índice de** A, indicado por $\mathrm{ind}(A)$, na maneira seguinte

$$\text{ind}(A) = \dim_F(D).$$

Temos portanto $[A] \neq 0$ em $B(F)$ se e somente se $\text{ind}(A) \geq 2$.

A demonstração do teorema a seguir pode ser encontrada nas seções 4.4 e 4.5 de [**9**]. Indicaremos a ordem de $[A]$ em $B(F)$ por $o(A)$.

Teorema 6.10. (**Brauer**) Com as notações acima temos:

(1) $B(F)$ é um grupo abeliano de torção, i.e. cada elemento $[A] \neq 0$ tem ordem finita;
(2) $o(A)$ divide $\text{ind}(A)$ para cada $[A] \in B(F) \setminus 0$;
(3) $o(A)$ e $\text{ind}(A)$ tem os mesmos fatores primos;
(4) se D é uma álgebra com divisão central sobre F e se $\text{ind}(D) = p_1^{m_1} \cdots p_r^{m_r}$, entao existem $D_i, i = 1, \ldots, r$, álgebras com divisão centrais sobre F com $\text{ind}(D_i) = p_i^{m_i}$ e tais que

$$D \simeq D_1 \otimes \cdots \otimes D_r.$$

As álgebras D_i são únicas a menos de isomorfismo.

Um resultado importante e que também descreve álgebras centrais simples em termos de álgebras cíclicas é

Teorema 6.11. (**Merkurjev-Suslin**) Suponhamos que F contém uma m-ésima raiz primitiva da unidade ω. Então toda F-álgebra central simples cuja a ordem no grupo de Brauer $B(F)$ divide m é semelhante a um produto tensorial de álgebras cíclicas da forma

$$(F(\sqrt[m]{a_1})|F, \theta_1, b_1) \otimes_F \ldots \otimes_F (F(\sqrt[m]{a_r})|F, \theta_r, b_r).$$

Demonstração. Vide [**9**]. □

Para corpos como nas hipóteses desse teorema ou de 6.11, ou para corpos do tipo $F(t)$, F algebricamente fechado, temos que o grupo de Brauer para estes é gerado por álgebras cíclicas e, em particular, usando os fatos:

(1) $\mathcal{C}(a, \theta) \otimes_F \mathcal{C}(b, \theta) = \mathcal{C}(ab, \theta) \otimes_F M_n(F)$ (ver demonstração em [**10**])
(2) $a \in F^* \Longrightarrow N(a) = a^n$

concluimos, por 6.3, $[\mathcal{C}(a, \theta)]^n = 1$ e que portanto o grupo de Brauer de tais corpos são de fato de torção como previsto por 6.10 (1).

Fechamos a dissertação lembrando que Hasse provou que se A é cíclica então $o(A) = \text{ind}(A)$ e que Brauer construiu um exemplo de álgebra com divisão central

sobre um corpo com ordem menor do que o índice, que pode ser considerado o primeiro exemplo de álgebra com divisao central sobre F não cíclica, vide-se nota final de [**6**].

APÊNDICE A

O Teorema de Wedderburn

DEFINIÇÃO A.1. Um ideal esquerdo $I \subseteq A$, próprio, é dito ser **ideal esquerdo minimal** se: para I' ideal esquerdo de A, $(0) \subsetneqq I' \subseteq I \Rightarrow I' = I$

OBSERVAÇÃO A.2. Todo ideal esquerdo I de uma F-álgebra A é um F-subespaço vetorial. Uma consequência disso é que toda F-álgebra A admite um ideal esquerdo minimal.

PROPOSIÇÃO A.3. Se I é um ideal esquerdo minimal de A então $\mathrm{End}_A(I)$ é uma álgebra com divisão.

DEMONSTRAÇÃO. É suficiente mostrar que todo $\varphi \in \mathrm{End}_A(I)$ não nulo é invertível. Como $\varphi(I) \subseteq I$ e I é minimal então $\varphi(I) = I$. Como $\ker\varphi \subseteq I$ segue novamente da minimalidade de I que $\ker\varphi = \{\mathbf{0}\}$. Portanto, $\mathrm{End}_A(I)$ é de fato uma F-álgebra com divisão. □

PROPOSIÇÃO A.4. Se I e J são ideais esquerdo minimais em uma álgebra simples A então

$$\mathrm{End}_A(I) \simeq \mathrm{End}_A(J)$$

como F-álgebras.

PROPOSIÇÃO A.5. Se D é uma F-álgebra com divisão central então existe um isomorfismo de F-álgebras

$$M_n(F) \otimes D \simeq M_n(D).$$

DEMONSTRAÇÃO. Consideremos as seguintes subálgebras de $M_n(D)$:

$$\overline{D} = \{d \cdot I_{n\times n};\ d \in D\}$$

e

$$A = \{[d_{ij}];\ d_{ij} \in F\}$$

Temos os isomorfismos de álgebras: $\overline{D} \simeq D$ e $A \simeq M_n(F)$.

Obviamente $1 \in \overline{D} \cap A$ e esses dois conjuntos comutam elemento com elemento. Desse modo, podemos concluir sem dificuldades que $\overline{D}$ e A geram $M_n(D)$ e podemos

escrever cada elemento de $M_n(D)$ da forma $\sum da$ com $d \in D$ e $a \in A$. Consideremos agora a seguinte aplicação bilinear:

$$w : \overline{D} \times A \to M_n(D)$$

definida por $w(d, a) = d \cdot a$. Então existe um único homomorfismo de F-álgebras

$$\varphi : \overline{D} \otimes A \to M_n(D)$$

tal que $\varphi(d \otimes a) = da$ quaisquer que sejam $d \in \overline{D}$ e $a \in A$. Logo essa φ é claramente sobrejetiva. Como $\overline{D} \otimes A$ é simples, então $\ker \varphi = \{\mathbf{0}\}$. Portanto,

$$M_n(F) \otimes D \simeq A \otimes \overline{D} \simeq M_n(D).$$

□

Observação A.6.

(1) Para uma F-álgebra com divisão e V é um D-módulo esquerdo finitamente gerado então existe uma D-base tal como para os espaços vetoriais sobre corpos. Por isso, podemos falar, em tal situação, da dimensão de V sobre D
(2) Sejam D uma F-álgebra com divisão e V um D-módulo. Então $\mathrm{End}_D(V) \simeq M_n(D)$ como F-álgebras, onde $n = \dim {}_DV$.

Após esses resultados e definições chegamos ao objetivo principal desse apêndice.

Teorema A.7. (**Wedderburn**) Seja $A \in \mathrm{ACS}(F)$. Então existe uma álgebra com divisão $D \in \mathrm{ACS}(F)$ tal que

$$A \simeq M_n(F) \otimes_F D.$$

Além disso, o número n é unicamente determinado e D é única a menos de isomorfismos.

Demonstração. Seja I um ideal esquerdo minimal de A. Pela Proposição A.3 $D = \mathrm{End}_A(I)$ é uma F-álgebra com divisão. Provaremos que esse é o D do teorema. Dividiremos a demonstração em seis etapas:

1) Da definição da lei de composição em D temos

$$\varphi(\mathbf{x} + \mathbf{y}) = \varphi\mathbf{x} + \varphi\mathbf{y},\ (\varphi + \psi)\mathbf{x} = \varphi\mathbf{x} + \psi\mathbf{x},$$

$$(\varphi\psi)x = \varphi(\psi\mathbf{x}),\ \mathbf{1}_D\mathbf{x} = \mathbf{x}.$$

Daí, podemos pensar I como um D-módulo.
2) Procuraremos agora definir um isomorfismo natural da álgebra A na álgebra $\mathrm{End}_D(I)$. Dado $\mathbf{a} \in A$ considere $\sigma_\mathbf{a} : I \to I$ definida pela equação

$$\sigma_\mathbf{a}(\mathbf{x}) = \mathbf{ax} \quad \forall \mathbf{x} \in A.$$

Claramente $\sigma_{\mathbf{a}}$ é uma aplicação D-linear. Assim, temos uma aplicação

$$A \to \mathrm{End}_D(I)$$

definida por $\mathbf{a} \rightarrowtail \sigma_{\mathbf{a}}$. Facilmente verifica-se que essa aplicação é um homomorfismo de F-álgebras. O núcleo dessa aplicação é um ideal bilateral logo, ele tem de ser o ideal nulo. Encontramos portanto um homomorfismo injetivo de álgebras.

4) Denotamos o anulador de um D-submódulo W de I por W_i^0. Para mostrar que a aplicação $\mathbf{a} \mapsto \sigma_a$ é sobrejetiva devemos mostrar que dado $\sigma \in \mathrm{End}_D(I)$ existe $\mathbf{a} \in A$ tal que $\sigma_a = \sigma$. Para isso, consideremos uma D-base $\{\mathbf{z}_1, \ldots, \mathbf{z}_2\}$ para I Seja W_i o hiperplano gerado por todos os vetores da D-base dada exceto $\mathbf{z}_i$. Não podemos ter $W_i^0\mathbf{z}_i = \mathbf{0}$, pois caso contrário, $W_i^0 I = \mathbf{0}$ e assim $W_i = W_i^{00} = I$ o que é um absurdo. Logo, $W_i^0\mathbf{z}_i \neq \mathbf{0}$ e $W_i^0 I = I$. Seja $\mathbf{a}_i \in W_i^0$ tal que $\mathbf{a}_i\mathbf{z}_i = \sigma\mathbf{z}_i$; então $\mathbf{a}_i\mathbf{z}_i = \mathbf{0}$ para $j \neq i$. Façamos $\mathbf{a} = \mathbf{a}_1, \ldots, \mathbf{a}_n$. Então

$$\sigma_{\mathbf{a}}\mathbf{z}_i = \mathbf{a}\mathbf{z}_i = \mathbf{a}_i\mathbf{z}_i = \sigma\mathbf{z}_i$$

Portanto, $\sigma_{\mathbf{a}} = \sigma$ e de fato

$$A \to \mathrm{End}_D(I)$$

é um isomorfismo de F-álgebras.

5) $D \in \mathrm{ACS}(F)$ segue das implicações:

$$\mathbf{d} \in Z(D) \Rightarrow \mathbf{d}I_{n\times n} \in Z(M_n(D)) = F \cdot I_{n\times n} \Rightarrow \mathbf{d} \in F \cdot 1.$$

6) Sejam $A' = M_n(D)$ e $\theta : A \to A'$ um isomorfismo. Uma observação imediata é que θ envia ideal esquerdo minimal I de A em ideal esquerdo minimal I' de A', e esse mesmo θ induz um isomorfismo $\xi : \mathrm{End}_A(I) \to \mathrm{End}_{A'}(I')$. Para provar a unicidade de D mostraremos que se $\mathrm{End}_{A'}(I')$ é isomorfo a D para algum ideal minimal esquerdo I' de A' então ele será isomorfo a D qualquer que seja I' de A' . Desse modo, pela Proposição A.4, $\mathrm{End}_A(I)$ será isomorfo a D para qualquer ideal esquerdo minimal I de A . Esses fatos certamente acarretam a unicidade de D e a unicidade de n segue do isomorfismo

$$A \simeq M_n(F) \otimes_F D.$$

Consideremos então o conjunto I' das matrizes em A' da forma

$$(\mathbf{d}_1 \cdot I_{n\times n})\mathbf{e}_{11} + \ldots + (\mathbf{d}_n \cdot I_{n\times n})\mathbf{e}_{n1}$$

onde $\mathbf{e}_{ij}$ denota as matrizes com 1 na entrada ij e 0 nas demais. Facilmente verifica-se que I' é um ideal à esquerda em A'. Notemos que se J é também

um ideal a esquerda em A' com

$$(\mathbf{0}) \subsetneqq J \subseteq I',$$

então, dado

$$(\mathbf{d}_1 \cdot I_{n\times n})\mathbf{e}_{11} + \ldots + (\mathbf{d}_n \cdot I_{n\times n})\mathbf{e}_{n1} \in J$$

não nulo, digamos $\mathbf{d}_1 \neq \mathbf{0}$, temos

$$(\mathbf{d} \cdot I_{n\times n})\mathbf{e}_{j1} = (\mathbf{d}\mathbf{d}_1^{-1} \cdot I_{n\times n})\mathbf{e}_{ji}[(\mathbf{d}_1 \cdot I_{n\times n})\mathbf{e}_{11} + \ldots + (\mathbf{d}_n \cdot I_{n\times n})\mathbf{e}_{n1}] \in J$$

qualquer que seja $\mathbf{d} \in D$ e qualquer que seja $1 \leq j \leq n$. Logo, I' é minimal.

Agora considere o homomorfismo

$$D \to \mathrm{End}_{A'}(I')$$

que envia $\mathbf{d} \in D$ em $\psi_{\mathbf{d}} \in \mathrm{End}_{A'}(I')$ definido pela equação

$$\psi_{\mathbf{d}}(\mathbf{x}) = \mathbf{x}(\mathbf{d} \cdot I_{n\times n}).$$

Obviamente esse homomorfismo é injetivo. Suponha $\psi \in \mathrm{End}_{A'}(I')$. Ora

$$\psi(\mathbf{e}_{11}) = (\mathbf{d}_1 \cdot I_{n\times n})\mathbf{e}_{11} + \ldots + (\mathbf{d}_1 \cdot I_{n\times n})\mathbf{e}_{n1}]$$

então, para $1 < i \leq n$,

$$\mathbf{d}_i \cdot I_{n\times n} = \mathbf{e}_{1i}[(\mathbf{d}_1 \cdot I_{n\times n})\mathbf{e}_{11} + \ldots + (\mathbf{d}_1 \cdot I_{n\times n})\mathbf{e}_{n1}] = \psi(\mathbf{e}_{1i}\mathbf{e}_{11}) = \mathbf{0}.$$

Desse modo $\psi(\mathbf{e}_{11}) = (\mathbf{d}_1 \cdot I_{n\times n})\mathbf{e}_{11}$ e

$$\psi(\mathbf{e}_{i1}) = \psi(\mathbf{e}_{i1}\mathbf{e}_{11}) = \mathbf{e}_{i1}(\psi(\mathbf{e}_{11})) = (\mathbf{d} \cdot I_{n\times n})\mathbf{e}_{i1}.$$

Logo, $\psi = \psi_{\mathbf{d}_1}$, ou seja, a aplicação

$$D \to \mathrm{End}_{A'}(I')$$

é um isomorfismo.

□

APÊNDICE B

Anéis Semi-simples.

Uma boa referência para a demonstração dos resultados desse apêndice encontra-se em [**3**].

DEFINIÇÃO B.1. Seja R um anel, e M um R-módulo (esquerdo).

(1) M é chamado um R-módulo **simples** se $M \neq \mathbf{0}$ e não possui R-submódulos além de $(\mathbf{0})$ e M.
(2) M é chamado um R-módulo **semi-simples** se todo R-submódulo de M possui um completamento.

Uma observação imediata é que qualquer submódulo de um R-submódulo semi-simples é também um módulo semi-simples.

LEMA B.2. Qualquer R-módulo esquerdo semi-simples M contém um submódulo simples.

TEOREMA B.3. Para um R-módulo M, as seguintes propriedades são equivalentes:

(1) M é simples;
(2) M é a soma direta de uma família de submódulos semi-simples;
(3) M é a soma de uma família de submódulos simples.

DEFINIÇÃO B.4. Um anel R é dito **semi-simples esquerdo** se todo R-módulo esquerdo é semi-simples

TEOREMA B.5. Sejam D uma álgebra com divisão e $R = M_n(D)$. Então

(1) R é simples e semi-simples esquerdo.
(2) R possui (a menos de isomorfismo) um único módulo simples V.

Bibliografia

[1] Curtis, Charles W. **Linear algebra: an introductory approach**, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1984.

[2] Ebbinghaus, H. D., H.Hermes,F. Hirzebruch, M. Koecher, K.Mainzer, J.Neukirch, A.Prestel, R. Remmert. **Numbers**,Graduate Texts in Mathematics, Springer, 1991.

[3] Lam, T. Y. **A First Course in Noncommutative Rings**, Graduate Texts in Mathematics, 2. ed., Springer, 2001.

[4] Lam, T. Y. **Introduction to Quadraticic Forms over Fields**, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, 2005.

[5] Lounesto, Pertti. **Clifford Algebras Spinor**,London Mathematical Lecture Note Series, 286, Cambridige University Press, 2001.

[6] McConnell, J.C. **Division Algebras-Beyond the Quaternions**, The American Mathematical Monthly, vol.105, No. 2, (fev. 1998), pg. 154-162.

[7] O.T.O'Meara. **Introduction to Quadratic Forms**, Grundl. Math. Wiss., vol. 117, Springer-Verlag, Berlin-Gottigen-Heidelberg, 1963.

[8] Pfister, Albrecht. **Quadratic Forms with Aplications To Algebraic and Topology**, London Mathematical Lecture Note Series, 217, Cambridige University Press, 1996.

[9] P. Gille, T. Szamuely. **Central Simple Algebras Galois Comology**, Cambridge Studies in Advanced Mathematics, 00, Cambridge University Press, 2006.

[10] Pierce, Richard S. **Associative Algebras**, Graduate Texts in Mathematics, vol. 88, Springer-Verlag, New York-Heidelberg-Berlin, 1980.

[11] Porteous, Ian R..**Clifford Algebras and Classical Groups**, Cambridge Studies in Advanced Mathematics, 50, Cambridge University Press, 2000.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo