Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Álgebras Biquaterniônicas:

Construção, Classificação e Condições de Existência via Formas Quadráticas e Involuções

por

Maurício de Araújo Ferreira

Mestrado em Matemática

Orientador: Prof. Dr. Antônio José Engler

Campinas, SP

Fevereiro/2006

Álgebras Biquaterniônicas: Construção, Classificação e Condições de Existência via Formas Quadráticas e Involuções

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Maurício de Araujo Ferreira e aprovada pela comissão julgadora.

Campinas, 17 de fevereiro de 2006

_____

Prof. Dr. Antônio José Engler
Orientador

Banca Examinadora

Prof. Dr. Paulo Roberto Brumatti (IMECC - UNICAMP)

Prof. Dr. Vitor de Oliveira Ferreira (IME - USP)

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para a obtenção do título de MESTRE em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Bibliotecário: Maria Júlia Milani Rodrigues – CRB8a / 2116

Ferreira, Maurício de Araujo

F413a Álgebras biquaterniônicas: construção, classificação e condições de existência via formas quadráticas e involuções / Maurício de Araujo Ferreira -- Campinas, [S.P. :s.n.], 2006.

Orientador : Antônio José Engler

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Formas quadráticas. 2. Brauer, Grupo de. 3. Galois, Teoria de. 4. Álgebras de dimensão finitas. 5. Anéis não-comutativos. I. Engler, Antônio José. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Biquaternion algebras: construction, classification and existence condition through quadratic forms and involutions.

Palavras-chave em inglês (Keywords): 1. Quadratic forms. 2. Brauer group. 3. Galois theory. 4. Finite dimensional algebras. 5. Non-commutative rings.

Área de concentração: Álgebra

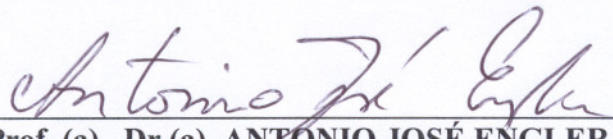
Titulação: Mestre em Matemática

Banca examinadora: Prof. Dr. Antonio José Engler (IMECC-UNICAMP)
Prof. Dr. Paulo Roberto Brumatti (IMECC-UNICAMP)
Prof. Dr. Vitor de Oliveira Ferreira (IME-USP)

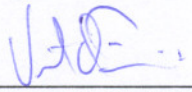
Data da defesa: 17/02/2006

Dissertação de Mestrado defendida em 17 de fevereiro de 2006 e aprovada

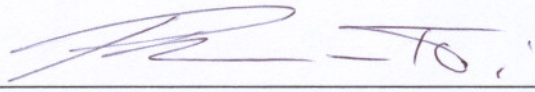
Pela Banca Examinadora composta pelos Profs. Drs.



Prof. (a). Dr (a). ANTONIO JOSÉ ENGLER



Prof. (a). Dr (a). VITOR DE OLIVEIRA FERREIRA



Prof. (a). Dr (a). PAULO ROBERTO BRUMATTI

Dedicatória

Para minha avó
Emília Lopes de Araújo.

Agradecimentos

Agradeço a Deus em primeiro lugar, por tudo o que tem me proporcionado.

Ao meu orientador, o professor Antônio José Engler, pela orientação, amizade e motivação nos momentos de dificuldade.

À minha avó, por ter me criado e amado como a um filho.

À minha mãe, a quem eu devo tudo. A sua criação e educação me fizeram chegar até aqui. Agradeço também por todo apoio, amor e carinho em todos os momentos da minha vida.

À minha namorada Márcia, a mulher que eu amo. Agradeço por todo amor e carinho em todo esse tempo de união, principalmente quando estávamos longe. Sem o seu apoio e compreensão teria sido muito mais difícil.

À toda a minha família, por sempre me apoiarem e torcerem muito por mim.

À minha tia Zenaide, por ter sempre me recebido de maneira muito calorosa a cada volta para casa.

Aos grandes amigos Eduardo e Nolmar, companheiros desde a graduação e que vieram comigo da Bahia para começar o mestrado.

À Renata, pela grande amizade durante todo o mestrado e por ter me ajudado a corrigir a introdução deste trabalho.

Aos demais amigos do IMECC, especialmente os colegas que participaram diretamente comigo desta jornada: Andrielber, Eduardo Estrada, Eliana, José Antônio, Karina, Lien, Mauro, Paula e Rodrigo.

Aos professores da banca: Paulo Roberto Brumatti e Vitor de Oliveira Ferreira, por terem lido o meu trabalho e pelas valiosas correções e sugestões.

À todos aqueles que prestigiaram a minha defesa, especialmente tia Bela, minha mãe e minha namorada.

Aos demais professores do IMECC com os quais fiz cursos ou que de alguma maneira contribuíram para a minha formação.

Aos funcionários do IMECC, por sempre terem me atendido em tudo o que precisei.

Aos professores da graduação: Haroldo Golçalves Benatti, Jean Fernandes Barros e Maria Hildete de Magalhães França, os quais muito me ajudaram a chegar até o mestrado.

Ao CNPq, pelo apoio financeiro.

Resumo

Neste trabalho, estudamos as álgebras biquaterniônicas, que são um tipo especial de álgebra central simples de dimensão 16, obtida como produto tensorial de duas álgebras de quatérnios. A teoria de formas quadráticas é aplicada para estudarmos critérios de decisão sobre quando uma álgebra biquaterniônica é de divisão e quando duas destas álgebras são isomorfas. Além disso, utilizamos o u-invariante do corpo para discutirmos a existência de álgebras biquaterniônicas de divisão sobre o corpo. Provamos também um resultado atribuído a A. A. Albert, que estabelece critérios para decidir quando uma álgebra central simples de dimensão 16 é de fato uma álgebra biquaterniônica, através do estudo de involuções. Ao longo do trabalho, construímos vários exemplos concretos de álgebras biquaterniônicas satisfazendo propriedades importantes.

Sumário

Lista de Símbolos

$\mathbb{K}$, $\mathbb{F}$, $\mathbb{L}, \ldots$	-	Corpo com característica diferente de 2.
$\mathrm{M}_n(\mathbb{A})$	-	Álgebra de matrizes $n \times n$ com coeficientes em A.
$(a_{ij})_{n\times n}$	-	Matriz $n \times n$.
E_{ij}	-	Matriz que tem 1 na posição (i, j) e 0 nas demais entradas.
A^{op}	-	Álgebra oposta de A.
$A \backsim B$	-	Álgebras Brauer equivalentes.
$\mathrm{Br}(\mathbb{K})$	-	Grupo de Brauer do corpo $\mathbb{K}$.
$[B]$	-	Classe da álgebra B no grupo de Brauer.
$\deg(A)$	-	Grau da álgebra A.
$\mathrm{ind}(A)$	-	Índice da álgebra A.
$\exp(A)$	-	Expoente de A.
$A_{\mathbb{L}}$	-	$A \otimes_{\mathbb{K}} \mathbb{L}$.
$\imath_u$	-	Automorfismo interno.
$N_{\mathbb{L}/\mathbb{K}}(\alpha)$	-	Norma do elemento α na extensão de corpos $\mathbb{L}/\mathbb{K}$.
$T_{\mathbb{L}/\mathbb{K}}(\alpha)$	-	Traço do elemento α na extensão de corpos $\mathbb{L}/\mathbb{K}$.
$\mathrm{Nrd}_A(\alpha)$	-	Norma reduzida de α na álgebra A.
$\mathrm{Trd}_A(\alpha)$	-	Traço reduzido de α na álgebra A.
$\mathrm{Prd}_{A,\alpha}(x)$	-	Polinômio característico reduzido.
$\mathrm{End}_{\mathbb{K}}(A)$	-	Conjunto dos $\mathbb{K}$–endomorfismos de A.
$\mathbb{N}$	-	Números naturais.
$\mathbb{Z}$	-	O anel dos números inteiros.
$\mathbb{Q}$	-	O corpo dos números racionais.
$\mathbb{R}$	-	O corpo dos números reais.
$\mathbb{C}$	-	O corpo dos números complexos.
$\mathbb{K}(x)$	-	Corpo de funções racionais sobre $\mathbb{K}$.
$\mathbb{K}[t]$	-	Anel de polinômios na variável t.

$\mathbb{K}((t))$	-	O corpo das séries de Laurent formais na variável t.
$\mathbb{K}[[t]]$	-	Anel das séries de potência na variável t.
$\mathbb{K}^\times$	-	$\mathbb{K}\backslash\{0\}$.
$\mathbb{K}^\times/\mathbb{K}^{\times 2}$	-	Grupo das classes de quadrados de $\mathbb{K}$.
$\Sigma\mathbb{K}^2$	-	Conjunto das somas de quadrados de $\mathbb{K}$.
$\langle a_1, \ldots, a_n\rangle$	-	Forma quadrática $a_1X_1^2 + \cdots + a_nX_n^2$.
$\phi \cong \psi$.	-	Formas quadráticas isométricas.
$\phi \approx \psi$.	-	Formas quadráticas simplesmente equivalentes.
$\phi \perp \psi$.	-	Soma ortogonal de formas quadráticas.
$\phi \otimes \psi$.	-	Produto tensorial de formas quadráticas.
$(a, b)_\mathbb{K}$	-	$\mathbb{K}$–álgebra de quatérnios.
$X_\mathbb{K}$	-	Conjunto das ordens do corpo $\mathbb{K}$.
$u(\mathbb{K})$	-	u–invariante de $\mathbb{K}$.
$D_\mathbb{K}(\phi)$	-	Conjunto dos valores não nulos de $\mathbb{K}$ representados por ϕ.
$c\phi$	-	O produto $\langle c\rangle \otimes \phi$.
$n \times \phi$	-	A soma $\phi \perp \ldots \perp \phi$ n-vezes.
$c(\phi)$	-	Invariante de Witt de ϕ.
$s(\phi)$	-	Invariante de Hasse de ϕ.
$d(\phi)$	-	Discriminate de ϕ.
x^t	-	Transposta da matriz x.
$\mathrm{Sym}(A, \sigma)$	-	Elementos simétricos de A por σ.
$\mathrm{Skew}(A, \sigma)$	-	Elementos anti-simétricos de A por σ.
$\mathrm{disc}(\sigma)$	-	Discriminante da involução σ.
$\mathrm{Sub}(G)$	-	Família dos subgrupos de G.
$\mathrm{Lat}(\mathbb{L}/\mathbb{K})$	-	Família dos corpos intermediários da extensão $\mathbb{L}/\mathbb{K}$.
S_n	-	Grupo das permutações de n símbolos.
$(\mathbb{L}/\mathbb{K}, \sigma, \alpha)$	-	Álgebra cíclica.

Introdução

Neste trabalho, estudamos as álgebras biquaterniônicas, que são um tipo especial de álgebra central simples de dimensão 16, obtida como produto tensorial de duas álgebras de quatérnios.

As álgebras biquaterniônicas têm importância histórica. Até 1914 as únicas álgebras com divisão conhecidas eram as álgebras de quatérnios. Neste ano, L. E. Dickson apresentou uma forma de produzir exemplos de álgebras centrais simples de dimensão n^2. Estas álgebras são hoje conhecidas como álgebras cíclicas.

Veremos no texto que as álgebras de quatérnios são álgebras cíclicas. Além disso, Wedderburn provou que toda álgebra de dimensão 9 sobre seu centro é uma álgebra cíclica.

A partir daí, era natural se perguntar se existiam álgebras com divisão que não fossem álgebras cíclicas. Em 1932, as álgebras biquaterniônicas foram utilizadas por A. A. Albert [4], um dos estudantes de doutorado de Dickson, para construir o primeiro exemplo da história de uma álgebras com divisão não cíclica.

Desde então, as álgebras biquaterniônicas despertaram o interesse de estudo de vários matemáticos. Durante o século passado, a teoria se desenvolveu bastante e em várias direções. Desta forma, nesta dissertação, optamos por não estudar um problema específico e sim trabalhar estas álgebras num contexto mais abrangente, visando o contato com uma quantidade maior de problemas com as quais estas álgebras estão relacionadas.

O nosso trabalho está dividido em cinco capítulos. O primeiro é introdutório, consistindo apenas de uma breve revisão de alguns conceitos básicos sobre álgebras centrais simples, formas quadráticas e álgebras de quatérnios. Desta maneira, omitimos a demonstração da maior parte dos resultados deste capítulo.

No segundo capítulo, começamos de fato a estudar as álgebras biquaterniônicas. O objetivo principal deste capítulo é provar um resultado atribuído a Albert, que estabelece critérios para decidir quando uma álgebra central simples de dimensão 16 é uma álgebra

biquaterniônica, através do estudo de involuções. Além disso, obtemos alguns resultados interessantes sobre as involuções simpléticas e ortogonais nestas álgebras.

Problemas relacionando álgebras biquaterniônicas com formas quadráticas são abordados no terceiro capítulo, onde definimos a forma de Albert. Trata-se de uma forma quadrática de dimensão 6, através da qual podemos decidir se uma álgebra biquaterniônica é de divisão e quando duas destas álgebras são isomorfas. Além disso, utilizamos o u-invariante para discutirmos a existência de álgebras biquaterniônicas de divisão sobre um corpo não formalmente real.

O professor Albert publicou vários trabalhos estudando a ciclicidade das álgebras biquaterniônicas. Inspirados nestes trabalhos, no quarto capítulo, construímos exemplos de álgebras biquaterniônicas com divisão cíclicas e não cíclicas. Nas duas primeiras seções deste capítulo, revisamos alguns conceitos básicos sobre Teoria de Galois e Álgebras Cíclicas em geral.

No quinto e último capítulo, construímos exemplos concretos de corpos que atentem aos problemas levantados nas observações 4.15 e 3.30. Isto é, um corpo não-SAP e um corpo com u-invariante 8 sobre o qual não existe álgebra biquaterniônica de divisão. Para apresentarmos estes exemplos, revisamos algumas noções de valorização discreta e ordem, necessárias para lidarmos com o corpo das séries formais de Laurent.

Ao longo de todo trabalho estamos assumindo que os corpos têm sempre característica diferente de 2, mesmo que em alguns resultados essa hipótese seja desnecessária.

Capítulo 1

Noções Elementares

1.1 Álgebras Centrais Simples

O objetivo desta seção é apresentar os principais conceitos e resultados sobre álgebras centrais simples, buscando introduzir as notações que serão utilizadas ao longo do texto. Esta teoria pode ser encontrada facilmente na literatura e sendo assim, omitiremos demonstrações. Aqui utilizamos como referência Felfenswalb [12], Reiner [29] e Scharlau [32].

Seja A uma $\mathbb{K}$–álgebra de dimensão finita. Por uma $\mathbb{K}$–álgebra de dimensão finita entendemos um espaço vetorial de dimensão finita sobre $\mathbb{K}$, dotado de uma operação de multiplicação associativa e distributiva em relação à soma de vetores. Assumiremos sempre a existência de 1. Vamos também identificar $\mathbb{K}$ com $\mathbb{K} \cdot 1$, dessa forma podemos escrever $\mathbb{K} \subset A$ e temos que a restrição da multiplicação de A a $\mathbb{K} \cdot 1$ coincide com a multiplicação inicial de escalares de $\mathbb{K}$. Dado um subconjunto S de A, definimos o **centralizador** de S em A, como sendo o subconjunto de A formado por todos os elementos $a \in A$, tais que $as = sa$, para todo s em S, que será denotado por $\mathcal{C}_A S$. Em particular, $\mathcal{C}_A A$ é o **centro** de A.

Nas condições acima, A é dita uma $\mathbb{K}$–**álgebra central simples** se o seu centro é o corpo $\mathbb{K}$ e os seus únicos ideais bilaterais são os triviais, a saber 0 e A. A álgebra de matrizes $\mathrm{M}_n(\mathbb{K})$ é central simples, pois se $x = (a_{ij})_{n\times n}$ está no centro de $\mathrm{M}_n(\mathbb{K})$, para cada $i, j \in \{1, \ldots, n\}$ com $i \neq j$ teremos que $\mathrm{E}_{ij}x = x\mathrm{E}_{ij}$, onde E_{ij} denota a matriz que tem 1 na posição (i, j) e 0 nas demais entradas. Dessa igualdade segue que $a_{ij} = 0$ e $a_{ii} = a_{jj}$. Portanto, $x \in \mathbb{K}$. Mais ainda, se I é um ideal bilateral não nulo de $\mathrm{M}_n(\mathbb{K})$

e se $x = (a_{ij})_{n\times n} \in I$ com algum $a_{ij} \neq 0$, teremos que $1 = \frac{1}{a_{ij}} \sum_{k=1}^{n} \mathrm{E}_{ki} x \mathrm{E}_{jk}$ e assim, $I = \mathrm{M}_n(\mathbb{K})$. Além disso, se todos os elementos não nulos de uma álgebra central simples A são invertíveis, então dizemos que A é um **anel de divisão**. Por outro lado, temos o célebre **Teorema de Wedderburn**, segundo o qual, toda álgebra central simples é isomorfa a uma álgebra de matrizes $\mathrm{M}_n(D)$ com coeficientes em um anel de divisão. Mais ainda, n é unicamente determinado e D é determinado a menos de isomorfismo.

Se A e B são simples centrais sobre $\mathbb{K}$ então $A \otimes_{\mathbb{K}} B$ é uma $\mathbb{K}$–álgebra central simples. Reciprocamente, se A e B são álgebras e $A \otimes_{\mathbb{K}} B$ é simples central sobre $\mathbb{K}$ então A e B também o serão.

Definimos a **álgebra oposta** $A^{op} = \{a^{op} \mid a \in A\}$ que coincide com A como espaço vetorial e a multiplicação é dada por $a^{op}b^{op} = (ba)^{op}$. Se A é central simples então A^{op} também o será e a aplicação canônica $\varphi : A \otimes_{\mathbb{K}} A^{op} \to \mathrm{End}_{\mathbb{K}}(A)$ que associa a cada $a \otimes b^{op}$ a aplicação linear $x \mapsto axb$, é um isomorfismo. Logo, $A \otimes_{\mathbb{K}} A^{op} \cong \mathrm{M}_n(\mathbb{K})$, onde $n = \dim_{\mathbb{K}} A$.

Com base nas propriedades acima, podemos definir uma relação de equivalência no conjunto das $\mathbb{K}$–álgebras centrais simples. Se A e B são simples centrais sobre $\mathbb{K}$, pelo Teorema de Wedderburn $A \cong \mathrm{M}_n(D)$ e $B \cong \mathrm{M}_m(D')$, onde D e D' são anéis de divisão. Dizemos que A e B são **Brauer equivalentes**, $A \backsim B$, se D e D' são isomorfas. Esta relação de equivalência pode ser reformulada da seguinte maneira, $A \backsim B$, se, e somente se, existem inteiros positivos n e m tais que $A \otimes_{\mathbb{K}} \mathrm{M}_n(\mathbb{K}) \cong B \otimes_{\mathbb{K}} \mathrm{M}_m(\mathbb{K})$. Seja $\mathrm{Br}(\mathbb{K})$ o conjunto das classes de equivalência de $\mathbb{K}$–álgebras centrais simples segundo a relação $\backsim$. Definimos em $\mathrm{Br}(\mathbb{K})$ uma operação da seguinte forma: $[A][B] = [A \otimes_{\mathbb{K}} B]$. Segue das propriedades de produto tensorial que a operação acima definida é associativa e comutativa. Além disso, como $A \otimes_{\mathbb{K}} \mathbb{K} \cong A$ e $A \otimes_{\mathbb{K}} A^{op} \cong \mathrm{M}_n(\mathbb{K})$, segue que $[A][\mathbb{K}] = [A]$, $[A][A^{op}] = [\mathbb{K}]$ e $[A] = [D]$, se D é o anel de divisão dado pelo Teorema de Wedderburn. Com a operação acima definida, $\mathrm{Br}(\mathbb{K})$ é um grupo abeliano, que é chamado de **grupo de Brauer**.

A dimensão de uma álgebra central simples A sobre seu centro é sempre um quadrado, e assim, $\sqrt{\dim_{\mathbb{K}} A}$ é chamado de **grau** de A e denotado por $\deg(A)$. Se $A \cong \mathrm{M}_n(D)$ então o grau de D é chamado **índice** de A e denotado por $\mathrm{ind}(A)$. Daí, é claro que o índice de A divide o grau de A e que A é um anel de divisão se, e somente se, $\mathrm{ind}(A) = \deg(A)$. Dado $[A] \in \mathrm{Br}(\mathbb{K})$, nós temos que $[A]^{\mathrm{ind}(A)} = 1$ em $\mathrm{Br}(\mathbb{K})$. Em particular, o grupo de Brauer é de torsão. A ordem de $[A]$ no grupo $\mathrm{Br}(\mathbb{K})$ é chamada de **expoente** de A e é denotada por $\exp(A)$.

Para uma extensão de corpos $\mathbb{L}/\mathbb{K}$ nós vamos denotar por $A_{\mathbb{L}}$ a $\mathbb{L}$–álgebra central simples $A \otimes_{\mathbb{K}} \mathbb{L}$. Dizemos que $\mathbb{L}$ **cinde** A se $A_{\mathbb{L}}$ é a álgebra das transformações lineares em um espaço vetorial sobre $\mathbb{L}$. Neste caso dizemos que $\mathbb{L}$ é um **corpo de decomposição** para A. Se $A \cong \mathrm{M}_n(\mathbb{K})$ então diremos que A é **cindida**. Como $\dim_{\mathbb{L}} A_{\mathbb{L}} = \dim_{\mathbb{K}} A = n$, $\mathbb{L}$ cinde A se, e somente se, $A_{\mathbb{L}} \cong \mathrm{M}_n(\mathbb{L})$ se, e somente se, $[A]$ pertence ao núcleo do homomorfismo de grupos $\psi : \mathrm{Br}(\mathbb{K}) \to \mathrm{Br}(\mathbb{L})$, $[A] \mapsto [A_{\mathbb{L}}]$. Desta maneira, se $A \cong \mathrm{M}_n(D)$ então $\mathbb{L}$ é um corpo de decomposição para A se, e somente se, $\mathbb{L}$ cinde D. E, assim, o estudo sobre corpos de decomposição para uma álgebra fica resumido aos anéis de divisão.

Se D é um anel de divisão de centro $\mathbb{K}$ então um subcorpo $\mathbb{L}$ de D é um **subcorpo maximal** se não está contido propriamente em nenhum subcorpo maior de D. Segue que $\mathbb{L}$ é um subcorpo maximal de D se, e somente se, $\mathcal{C}_{\mathbb{L}} D = \mathbb{L}$. A Teoria nos garante muito mais. De fato, $\mathbb{L}$ é um subcorpo maximal de D se, e somente se, $\dim_{\mathbb{K}} D = (\dim_{\mathbb{K}} \mathbb{L})^2$. Além disso, todo subcorpo maximal é um corpo de decomposição.

Todo anel de divisão D de centro $\mathbb{K}$ admite um subcorpo maximal que é uma extensão separável de $\mathbb{K}$. Mais ainda, se $\mathbb{L}$ cinde D então toda extensão de $\mathbb{L}$ também cinde D. Resulta das duas afirmações anteriores que D sempre admite um corpo de decomposição que é uma extensão galoisiana de $\mathbb{K}$. Por outro lado, não é sempre verdade que um anel de divisão admite um subcorpo maximal que é uma extensão galoisiana do seu centro. Entretanto, temos o seguinte resultado:

Teorema 1.1 *Se D é um anel de divisão de centro $\mathbb{K}$ então, no grupo de Brauer $\mathrm{Br}(\mathbb{K})$, $[D] = [B]$, onde B contém um subcorpo maximal que é uma extensão galoisiana de $\mathbb{K}$.*

Para concluir esta seção, apresentamos dois resultados clássicos da teoria que serão muito utilizados ao longo do texto:

Teorema 1.2 (Duplo Centralizador) *Seja A uma $\mathbb{K}$–álgebra central simples e B uma subalgebra simples de A contendo $\mathbb{K}$. Então valem as seguintes propriedades:*

1. *$\mathcal{C}_A B$ é uma $\mathbb{K}$–subalgebra simples de A.*
2. *$\dim_{\mathbb{K}} A = \dim_{\mathbb{K}} B . \dim_{\mathbb{K}} \mathcal{C}_A B$.*
3. *$\mathcal{C}_A(\mathcal{C}_A B) = B$.*
4. *Se B é simples e central sobre $\mathbb{K}$ então $A = B \otimes_{\mathbb{K}} \mathcal{C}_A B$.*
5. *Se B é um corpo então $\mathcal{C}_A B$ é uma B–álgebra central simples.*

Teorema 1.3 (Skolem-Nöther) *Seja A uma $\mathbb{K}$–álgebra central simples e B e C subalgebras simples de A que contém $\mathbb{K}$. Se $\varphi : B \to C$ é um isomorfismo que fixa os elementos de $\mathbb{K}$, então existe um elemento inversível $u \in A$ tal que $\varphi(x) = u^{-1}xu$, para todo elemento $x \in B$.*

Obs 1.4 *Um automorfismo do tipo $\imath_u : A \to A$, $\imath_u(x) = u^{-1}xu$ é chamado de **automorfismo interno**. Segue do teorema acima que todo automorfismo de A é interno.*

1.2 Norma e Traço

Nesta seção vamos revisar alguns resultados sobre norma e traço em extensões finitas de corpos e em álgebras centrais simples. Omitiremos a demonstração dos resultados, para detalhes ver [14] e [32].

Se $\mathbb{L}/\mathbb{K}$ é uma extensão finita de corpos de grau n então $\mathbb{L}$ é um $\mathbb{K}$–espaço vetorial de dimensão n. Desta forma, se $\alpha \in \mathbb{L}$ então a aplicação

$$\begin{aligned} \varphi_\alpha : \mathbb{L} &\longrightarrow \mathbb{L} \\ x &\longmapsto \alpha x \end{aligned}$$

é uma transformação linear. Se $B = \{\beta_1, \ldots, \beta_n\}$ é uma base de $\mathbb{L}$ com respeito a $\mathbb{K}$ e (a_{ij}) é a matriz definida por:

$$\varphi_\alpha(\beta_i) = \sum_{j=1}^{n} a_{ij}\beta_j$$

então o polinômio

$$f_\alpha(t) = \det(tI - (a_{ij}))$$

é o **polinômio característico** do elemento α relativo a extensão $\mathbb{L}/\mathbb{K}$, onde I denota a matriz identidade $n \times n$.

O polinômio característico $f_\alpha(t)$ é uma potência do seu polinômio minimal $p_\alpha(t)$. Segue daí que $f_\alpha(t)$ independe da escolha da base B.

Se $f_\alpha(t) = x^n + f_1x^{n-1} + \ldots + f_n$ então definimos o **traço** e a **norma** de α em relação a $\mathbb{L}/\mathbb{K}$ por

$$T_{\mathbb{L}/\mathbb{K}}(\alpha) = -f_1 = \sum_{i=1}^{n} a_{ii} \qquad \text{e}$$

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = (-1)^n f_n = \det(a_{ij}).$$

Segue das propriedades de traço e determinante de matrizes que $\forall \alpha, \beta \in \mathbb{L}$ e $\forall a, b \in \mathbb{K}$ que

$$N_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}/\mathbb{K}}(\alpha)N_{\mathbb{L}/\mathbb{K}}(\beta), \qquad N_{\mathbb{L}/\mathbb{K}}(a) = a^n,$$

$$T_{\mathbb{L}/\mathbb{K}}(a\alpha + b\beta) = aT_{\mathbb{L}/\mathbb{K}}(\alpha) + bT_{\mathbb{L}/\mathbb{K}}(\beta) \quad \text{e} \quad T_{\mathbb{L}/\mathbb{K}}(a) = na.$$

Se $\mathbb{L}$ for uma extensão separável de $\mathbb{K}$ e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{K}$–automorfismos de $\mathbb{L}$ no seu fecho algébrico Ω então

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{e} \quad T_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Voltemos agora a trabalhar com álgebras centrais simples.

Sejam A uma $\mathbb{K}$ álgebra central simples, $\mathbb{L}$ um corpo de decomposição para A e um isomorfismo:

$$\varphi : A \otimes_{\mathbb{K}} \mathbb{L} \to \mathrm{M}_n(\mathbb{L}).$$

Nestas condições, para cada elemento $\alpha \in A$, definimos o **polinômio característico reduzido** $\mathrm{Prd}_{A,\alpha}(x)$ como sendo o polinômio característico da matriz $\varphi(\alpha)$.

O polinômio $\mathrm{Prd}_{A,\alpha}(x)$ independe da escolha do corpo de decomposição $\mathbb{L}$ e do isomorfismo φ e tem coeficientes em $\mathbb{K}$.

Se escrevermos $\mathrm{Prd}_{A,\alpha}(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ então definimos a **norma reduzida** e o **traço reduzido** com sendo, respectivamente,

$$\mathrm{Nrd}_A(\alpha) = (-1)^n a_0 = \det(\varphi(\alpha)) \quad \text{e} \quad \mathrm{Trd}_A(\alpha) = -a_{n-1} = tr(\varphi(\alpha)).$$

A norma reduzida e o traço reduzido satisfazem as seguintes propriedades:

$$\mathrm{Nrd}_A(\alpha\beta) = \mathrm{Nrd}_A(\alpha)\mathrm{Nrd}_A(\beta), \qquad \mathrm{Nrd}_A(a\alpha) = a^n \mathrm{Nrd}_A(\alpha),$$

$$\mathrm{Trd}_A(\alpha + \beta) = \mathrm{Trd}_A(\alpha) + \mathrm{Trd}_A(\beta) \quad \text{e} \quad \mathrm{Trd}_A(a\alpha) = a\mathrm{Trd}_A(\alpha),$$

para todo $\alpha, \beta \in A$ e $a \in \mathbb{K}$.

Apresentamos agora o seguinte resultado que relaciona a norma e a norma reduzida definidas acima.

Proposição 1.5 *Se A é uma $\mathbb{K}$–álgebra central simples e $\mathbb{L}$ é um subcorpo maximal de A então*

$$\mathrm{Nrd}_A(\alpha) = N_{\mathbb{L}/\mathbb{K}}(\alpha), \quad \forall \alpha \in \mathbb{L}.$$

Para concluir essa seção, trazemos um resultado sobre álgebras centrais simples. Como é de natureza muito técnica e utiliza o traço reduzidos, daremos uma demonstração.

Lema 1.6 *Se A é uma $\mathbb{K}$-álgebra central simples então existe $u \in A \otimes_{\mathbb{K}} A$ tal que $u^2 = 1$ e $u(a \otimes b)u = b \otimes a, \forall a, b \in A$.*

Demonstração: Como $A \otimes_{\mathbb{K}} A$ e $A \otimes_{\mathbb{K}} A^{op}$ coincidem como espaços vetoriais, do isomorfismo canônico $A \otimes_{\mathbb{K}} A^{op} \cong \mathrm{End}_{\mathbb{K}}(A)$ obtemos o seguinte isomorfismo de $\mathbb{K}$-espaços vetoriais:

$$\begin{array}{rcccl} \sigma & : & A \otimes_{\mathbb{K}} A & \longrightarrow & \mathrm{End}_{\mathbb{K}}(A) \\ & & a \otimes b & \longmapsto & \sigma(a \otimes b) \end{array} \quad : \quad \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & axb. \end{array}$$

Por outro lado, a função traço reduzido $\mathrm{Trd}_A : A \to \mathbb{K}$ pode ser visto como um elemento de $\mathrm{End}_{\mathbb{K}}(A)$. Desta maneira, pelo isomorfismo construído acima, existe um único $u \in A \otimes_{\mathbb{K}} A$ tal que $\sigma(u) = \mathrm{Trd}_A$, que é chamado de **elemento goldman** de A. Vamos verificar que este elemento satisfaz as propriedades desejadas.

Suponhamos inicialmente que A é cindida e u é o elemento goldman de A. Se $\mathrm{E}_{ij} \in A$ denota a matriz que tem 1 na posição (i, j) e zero nas demais entradas então $u = \sum_{i,j} \mathrm{E}_{ij} \otimes \mathrm{E}_{ji}$ pois, dado $x = (x_{ij})_{n\times n} \in \mathrm{M}_n(\mathbb{K})$ teremos que

$$\sigma(u)(x) = \sum_{i,j} \mathrm{E}_{ij} x \mathrm{E}_{ji} = \sum_i x_{ii} \mathrm{I}_n = \sum_i x_{ii} = \mathrm{Trd}_A(x).$$

Além disso,

$$u^2 = \sum_{i,j} \mathrm{E}_{ij} \otimes \mathrm{E}_{ji} \sum_{s,l} \mathrm{E}_{ls} \otimes \mathrm{E}_{sl} = \sum_{i,j,s,l} \mathrm{E}_{ij}\mathrm{E}_{ls} \otimes \mathrm{E}_{ji}\mathrm{E}_{sl}.$$

$$\mathrm{E}_{ij}\mathrm{E}_{ls} = \begin{cases} \mathrm{E}_{is} & \text{se } j = l \\ 0 & \text{se } j \neq l \end{cases}$$

$$\mathrm{E}_{ji}\mathrm{E}_{sl} = \begin{cases} \mathrm{E}_{jl} & \text{se } i = s \\ 0 & \text{se } i \neq s \end{cases}$$

$$\mathrm{E}_{ij}\mathrm{E}_{ls} \otimes \mathrm{E}_{ji}\mathrm{E}_{sl} = \begin{cases} \mathrm{E}_{ii} \otimes \mathrm{E}_{jj} & \text{se } i = s \text{ e } j = l \\ 0 & \text{caso contrário} \end{cases}$$

assim, $u^2 = \sum_{i,j} \mathrm{E}_{ii} \otimes \mathrm{E}_{jj} = 1$. Mais ainda, se $a = (a_{ij})_{n\times n}$ e $b = (b_{ij})_{n\times n} \in \mathrm{M}_n(\mathbb{K})$, então

$$u(a \otimes b)u = (\sum_{i,j} \mathrm{E}_{ij} \otimes \mathrm{E}_{ji})(a \otimes b)(\sum_{r,s} \mathrm{E}_{rs} \otimes \mathrm{E}_{sr}) = \sum_{i,j,r,s} (\mathrm{E}_{ij} a \mathrm{E}_{rs}) \otimes (\mathrm{E}_{ji} b \mathrm{E}_{sr}) =$$

$$= \sum_{i,j,r,s} (a_{jr}\mathrm{E}_{is}) \otimes (b_{is}\mathrm{E}_{jr}) = \sum_{i,j,r,s} (b_{is}\mathrm{E}_{is}) \otimes (a_{jr}\mathrm{E}_{jr}) =$$

$$= (\sum_{i,s} b_{is}\mathrm{E}_{is}) \otimes (\sum_{j,r} a_{jr}\mathrm{E}_{jr}) = b \otimes a.$$

Para o caso geral, tomamos $\mathbb{L}$ um corpo de decomposição para A e u o elemento goldman de A. Nestas condições, para $u = \sum_i a_i \otimes b_i \in A \otimes_{\mathbb{K}} A$, escrevemos $u = \sum_i (a_i \otimes 1) \otimes (b_i \otimes 1) \in (A \otimes_{\mathbb{K}} \mathbb{L}) \otimes_{\mathbb{L}} (A \otimes_{\mathbb{K}} \mathbb{L})$. Como $\mathrm{Trd}_A(x) = \mathrm{Trd}_{A\otimes_{\mathbb{K}}\mathbb{L}}(x \otimes 1)$, se tomarmos $x = \sum_j x_j \otimes l_j \in A \otimes_{\mathbb{K}} \mathbb{L}$ e $\sigma_{\mathbb{L}} : A_{\mathbb{L}} \to \mathrm{End}_{\mathbb{L}}(A_{\mathbb{L}})$, o isomorfismo construído acima, teremos que

$$\sigma_{\mathbb{L}}(u)(x) = \sum_{i,j} a_i x_j b_i \otimes l_j = \sum_j l_j(\sum_i a_i x_j b_i \otimes 1) = \sum_j l_j(\sum_i a_i x_j b_i) =$$

$$= \sum_j l_j(\sigma(u)(x_j)) = \sum_j l_j(\mathrm{Trd}_A(x_j)) = \sum_j l_j(\mathrm{Trd}_{A\otimes_{\mathbb{K}}\mathbb{L}}(x_j \otimes 1)) =$$

$$= \mathrm{Trd}_{A\otimes_{\mathbb{K}}\mathbb{L}}(\sum_j l_j(x_j \otimes 1)) = \mathrm{Trd}_{A\otimes_{\mathbb{K}}\mathbb{L}}(\sum_j x_j \otimes l_j) = \mathrm{Trd}_{A\otimes_{\mathbb{K}}\mathbb{L}}(x).$$

E assim, u é também o elemento goldman de $A_{\mathbb{L}}$. Como $A_{\mathbb{L}}$ é cindida, pelo que vimos anteriormente, u satisfaz as propriedades desejadas. □

1.3 Formas Quadráticas

Nesta seção vamos expor alguns conceitos básicos sobre formas quadráticas. As duas referências clássicas sobre o assunto são Lam [20] e Scharlau [32].

Uma forma quadrática φ sobre um corpo $\mathbb{K}$ é um polinômio homogêneo de grau 2 a n variáveis em $\mathbb{K}$, isto é,

$$\varphi(X) = \varphi(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j \in \mathbb{K}[X_1, \ldots, X_n] = \mathbb{K}[X].$$

Como $X_i X_j = X_j X_i$, podemos reescrever φ da seguinte maneira:

$$\varphi(X) = \sum_{i,j=1}^{n} \frac{1}{2}(a_{ij} + a_{ji}) X_i X_j = \sum_{i,j=1}^{n} b_{ij} X_i X_j.$$

Desta forma, $b_{ij} = b_{ji}$ e φ determina uma única matriz $n \times n$ simétrica $M_\varphi = (b_{ij})$, tal que, $\varphi(X) = X^t M_\varphi X$, olhando $X = (X_1, \ldots, X_n)$ como um vetor coluna. Uma forma

quadrática φ é dita **regular** se a matriz M_φ é não singular. Além disso, definimos o **determinante** $\det(\varphi)$ como sendo o determinante da matriz simétrica M_φ e o inteiro n como a **dimensão** da forma quadrática φ, que denotamos por $\dim(\varphi)$. De agora em diante, vamos considerar apenas as formas quadráticas regulares e se φ é uma forma quadrática de dimensão n, diremos apenas que φ é uma n–forma. Em particular, se $n = 2$ dizemos também que φ é uma **forma binária**.

Duas formas quadráticas φ e ψ são ditas **isométricas** se existe uma matriz inversível C tal que $\varphi(X) = \psi(CX)$, ou ainda, $M_\varphi = C^t M_\psi C$. Esta é claramente uma relação de equivalência e escrevemos $\varphi \cong \psi$. Note que $\dim(\varphi)$ é um invariante dessa relação de equivalência e que $\det(\varphi)$, visto como um elemento de $\mathbb{K}^\times/\mathbb{K}^{\times 2}$, é também um invariante da classe de equivalência de φ.

Como estamos assumindo que o corpo $\mathbb{K}$ tem sempre característica diferente de dois, toda forma quadrática pode ser diagonalizada. Sendo assim, dados $a_1, \ldots, a_n \in \mathbb{K}^\times$, utilizaremos a notação clássica $\langle a_1, \ldots, a_n\rangle$ para denotar a forma quadrática $\varphi(X) = a_1X_1^2 + \cdots + a_nX_n^2$. Com isto, podemos definir uma relação de equivalência no conjunto das formas quadráticas de mesma dimensão. Dadas duas n–formas $\phi = \langle a_1, \ldots, a_n\rangle$ e $\psi = \langle b_1, \ldots, b_n\rangle$, dizemos que ϕ e ψ são **simplesmente equivalentes** ($\phi \approx \psi$), se existem dois índices, i e j, tais que $\langle a_i, a_j\rangle \cong \langle b_i, b_j\rangle$ e $a_k = b_k$ para cada k diferente de i e j. Segue do Teorema de Equivalência por Cadeias de Witt que se $\phi \cong \psi$ então $\phi \approx \psi$.

Sejam $\varphi = \langle a_1, \ldots, a_n\rangle$ e $\psi = \langle b_1, \ldots, b_m\rangle$ duas formas quadráticas sobre $\mathbb{K}$. Definimos a **soma ortogonal** como sendo a $(n + m)$–forma $\varphi \perp \psi = \langle a_1, \ldots, a_n, b_1, \ldots, b_m\rangle$ e o **produto tensorial** como a (nm)–forma $\varphi \otimes \psi = \langle a_1b_1, \ldots, a_1b_m, \ldots, a_nb_1, \ldots, a_nb_m\rangle$. Para todo $a \in \mathbb{K}^\times$, escreveremos $a\varphi$ para denotar a forma $\langle a\rangle \otimes \varphi$. Dado $m \in \mathbb{N}$ escrevemos $m \times \varphi$ para representar a soma $\varphi \perp \ldots \perp \varphi$ de m cópias de φ. Se $\varphi, \psi, \tilde{\varphi}, \tilde{\psi}$ são formas quadráticas, segue das propriedades de matrizes que $\varphi \perp \psi \cong \psi \perp \varphi$, $\det(\varphi \perp \psi) = \det(\varphi)\det(\psi)$ e se $\psi \cong \tilde{\psi}$ e $\varphi \cong \tilde{\varphi}$ então $\varphi \perp \psi \cong \tilde{\varphi} \perp \tilde{\psi}$.

Uma forma quadrática $\langle a_1, \ldots, a_n\rangle$ sobre $\mathbb{K}$ é dita **isotrópica** se existem $x_1, \ldots, x_n \in \mathbb{K}$, não todos nulos, tais que $a_1x_1^2 + \ldots + a_nx_n^2 = 0$ e dita **anisotrópica** caso contrário. A 2–forma $\langle 1, -1\rangle$ é a forma quadrática isotrópica de menor dimensão e é chamada de **plano hiperbólico**. Uma forma é dita **hiperbólica** se é isométrica a uma soma de planos hiperbólicos.

Se φ, ψ e γ são formas quadráticas sobre $\mathbb{K}$ e $\varphi \perp \gamma \cong \psi \perp \gamma$ então $\varphi \cong \psi$ pela **Lei do Cancelamento de Witt**.

Toda forma quadrática φ pode ser escrita da forma $\varphi \cong \varphi' \perp n \times \langle 1, -1\rangle$, onde φ' é anisotrópica e $n \in \mathbb{N}$. Esta é a chamada **decomposição de Witt**. O inteiro n é o **índice de Witt** e φ' é a **parte anisotrópica** de φ. Em particular, toda forma quadrática φ isotrópica pode ser escrita como $\varphi \cong \langle 1, -1\rangle \perp \psi$. Duas formas quadráticas ϕ e ψ sobre $\mathbb{K}$ são ditas **Witt equivalentes** se as suas partes anisotrópicas são isométricas. Neste caso, escrevemos $\psi \sim \psi$.

Seja $W\mathbb{K}$ o conjunto das classes de equivalência determinado pela relação de equivalência de Witt no conjunto de todas as formas quadrática definidas sobre um corpo $\mathbb{K}$. A soma ortogonal e o produto tensorial de formas quadráticas induzem uma estrutura de anel comutativo em $W\mathbb{K}$. Ese anel é chamado de **Anel de Witt** de $\mathbb{K}$. Note que o 0 de $W\mathbb{K}$ é dado pela classe das formas hiperbólicas, a identidade multiplicativa pela classe da 1–forma $\langle 1\rangle$ e o inverso aditivo da classe de $\langle a_1, \ldots, a_n\rangle$ é a classe de $\langle -a_1, \ldots, -a_n\rangle$.

Uma forma $\varphi \cong \langle a_1, \ldots a_n\rangle$ representa um certo elemento $a \in \mathbb{K}^\times$ se, e somente se, existem $x_1, \ldots, x_n \in \mathbb{K}$ tais que $a_1x_1^2 + \ldots + a_nx_n^2 = a$ se, e somente se, $\varphi \cong \langle a\rangle \perp \psi$ para alguma forma ψ. Denotamos por $D_{\mathbb{K}}(\varphi)$ o subconjunto de $\mathbb{K}^\times$ formado pelos elementos que são representados por φ. Se $\phi \cong \psi$ então $D_{\mathbb{K}}(\phi) = D_{\mathbb{K}}(\psi)$.

Duas formas φ e ψ são ditas **similares** se $\varphi \cong \lambda\psi$, para algum $\lambda \in \mathbb{K}^\times$. A similaridade define uma relação de equivalência que preserva o índice de Witt. A forma ϕ é dita **multiplicativa** se é hiperbólica ou então, é anisotrópica e satisfaz $\phi \cong a\phi$ para todo $a \in D_{\mathbb{K}}(\phi)$.

Dados $a_1, \ldots, a_n \in \mathbb{K}^\times$, a forma quadrática $\langle 1, a_1\rangle \otimes \ldots \otimes \langle 1, a_n\rangle$ é chamada de **forma de Pfister de n folhas**. Simplificando a notação escrevemos $\langle\langle a_1, \ldots, a_n\rangle\rangle$ no lugar de $\langle 1, a_1\rangle \otimes \ldots \otimes \langle 1, a_n\rangle$. Estas formas quadráticas têm a particularidade de serem sempre hiperbólicas ou anisotrópicas.

A classe das forma de dimensão par formam um ideal em $W\mathbb{K}$, denotado por $I\mathbb{K}$ e chamado de **ideal fundamental**. Para cada $n \in \mathbb{N}$, escrevemos $I^n\mathbb{K}$ como a n-ésima potência do ideal fundamental. Como $\langle a, b\rangle \perp \langle 1, -1\rangle \cong \langle 1, a\rangle \perp -\langle 1, -b\rangle$, $I\mathbb{K}$ é aditivamente gerado pelas 2–formas $\langle 1, a\rangle$. Segue que $I^n\mathbb{K}$ é gerado, como grupo abeliano, pelas classes das formas de Pfister de n folhas $\langle\langle a_1, \ldots, a_n\rangle\rangle$.

Para uma forma quadrática φ sobre $\mathbb{K}$ e uma extensão de corpos $\mathbb{L}/\mathbb{K}$, utilizaremos $\varphi_{\mathbb{L}}$ para denotar φ vista como uma forma quadrática sobre $\mathbb{L}$. Para finalizar esta seção, vejamos dois resultados de natureza técnica que serão úteis ao longo do texto. A demonstração de ambos pode ser vista em Lam [20], página 200.

Proposição 1.7 *Seja φ uma forma anisotrópica sobre $\mathbb{K}$ e $\mathbb{L} = \mathbb{K}(\sqrt{d})$, onde $d \in \mathbb{K}^\times \setminus {\mathbb{K}^\times}^2$. Então $\varphi_\mathbb{L}$ é isotrópica sobre $\mathbb{L}$ se, e somente se, φ contém uma subforma $\langle a, -ad\rangle$ para algum $a \in \mathbb{K}^\times$. Em outras palavras, $\varphi \cong \langle a, -ad\rangle \perp \psi$ para alguma forma ψ sobre $\mathbb{K}$.*

Proposição 1.8 *Se ϕ é uma n–forma anisotrópica sobre $\mathbb{K}$, $\mathbb{L} = \mathbb{K}(\sqrt{d})$ e $\phi_\mathbb{L}$ é hiperbólica, então $\phi \cong \langle 1, -d\rangle \otimes \psi$, para alguma forma quadrática ψ.*

1.4 Álgebra de Quatérnios

Como nosso principal objetivo é estudar as álgebras do tipo $A \otimes_\mathbb{K} B$, onde A e B são álgebras de quatérnios, nesse momento convém olharmos os quatérnios um pouco mais de perto. Sendo assim, neste parágrafo, vamos caracterizar estas álgebras através do estudo de formas quadráticas.

Definição 1.9 *Dados $a, b \in \mathbb{K}^\times$ definimos a Álgebra de Quatérnios $(a, b)_\mathbb{K}$ como sendo o $\mathbb{K}$–espaço vetorial das combinações lineares formais:*

$$(a, b)_\mathbb{K} = \{x + y\mathfrak{i} + z\mathfrak{j} + w\mathfrak{K} \mid x, y, z, w \in \mathbb{K}\},$$

onde os elementos da base são multiplicados pelas seguintes regras:

$$\mathfrak{i}^2 = a, \quad \mathfrak{j}^2 = b \quad \mathfrak{K} = \mathfrak{ij} = -\mathfrak{ji} \quad \text{e} \quad x\mathfrak{i} = \mathfrak{i}x, \quad x\mathfrak{j} = \mathfrak{j}x, \quad x\mathfrak{K} = \mathfrak{K}x, \quad \forall x \in \mathbb{K}.$$

Estendemos a multiplicação aos outros elementos por distributividade.

Proposição 1.10 *Toda álgebra de quatérnios $(a, b)_\mathbb{K}$ é simples central.*

Demonstração: Seja $q = x + y\mathfrak{i} + z\mathfrak{j} + w\mathfrak{K}$ no centro de $(a, b)_\mathbb{K}$. Como q comuta com todos os elementos de $(a, b)_\mathbb{K}$, obtemos que

$$q\mathfrak{i} = \mathfrak{i}q \Rightarrow x\mathfrak{i} + ya - z\mathfrak{K} - aw\mathfrak{j} = x\mathfrak{i} + ya + z\mathfrak{K} + aw\mathfrak{j} \Rightarrow z\mathfrak{K} + aw\mathfrak{j} = 0 \Rightarrow z = w = 0$$

e

$$q\mathfrak{j} = \mathfrak{j}q \Rightarrow z\mathfrak{j} + y\mathfrak{K} = x\mathfrak{j} - y\mathfrak{K} \Rightarrow y = 0.$$

Portanto, $q \in \mathbb{K}$.

Por outro lado, seja I um ideal bilateral não nulo de $(a, b)_\mathbb{K}$ e seja $q = x + y\mathfrak{i} + z\mathfrak{j} + w\mathfrak{K}$ um elemento não nulo em I. Devemos verificar que $1 \in I$. Se $y = z = w = 0$, então $q \in \mathbb{K}^\times$ e $1 = qq^{-1} \in I$. Sem perda de generalidade, suponhamos que $y \neq 0$.

$$\mathfrak{i}q\mathfrak{i} = (x\mathfrak{i} + ya + z\mathfrak{K} + wa\mathfrak{j})\mathfrak{i} = xa + ya\mathfrak{i} - az\mathfrak{j} - wa\mathfrak{K} = a(x + y\mathfrak{i} - z\mathfrak{j} - w\mathfrak{K}) \in I \Rightarrow$$
$$x + y\mathfrak{i} - z\mathfrak{j} - w\mathfrak{K} \in I \Rightarrow x + y\mathfrak{i} \in I \Rightarrow \mathfrak{j}(x + y\mathfrak{i})\mathfrak{j} = xb - by\mathfrak{i} = b(x - y\mathfrak{i}) \in I \Rightarrow x - y\mathfrak{i} \in$$
$$I \Rightarrow 2y\mathfrak{i} \in I \Rightarrow y \in I \Rightarrow 1 = yy^{-1} \in I.$$

Portanto, $I = (a, b)_{\mathbb{K}}$ e a álgebra é central simples. □

Um pouco mais interessante é a recíproca desse resultado:

Teorema 1.11 *Toda $\mathbb{K}$–álgebra central simples de grau 2 é uma álgebra de quatérnios.*

Demonstração: Seja A uma $\mathbb{K}$–álgebra central simples de grau 2. Pelo Teorema de Wedderburn, $A \cong \mathrm{M}_n(D)$, onde D é um anel de divisão. Por conta da dimensão, temos apenas duas possibilidades: $A \cong \mathrm{M}_2(\mathbb{K})$ ou A é um anel de divisão de grau 2. No primeiro caso, basta tomarmos $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{K}\}$ a base de $(1, 1)_{\mathbb{K}}$ e definirmos a aplicação linear $\varphi : (1, 1)_{\mathbb{K}} \to \mathrm{M}_2(\mathbb{K})$ na base:

$$1 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathfrak{i} \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ \mathfrak{j} \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \mathfrak{K} \longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Como estas matrizes são L.I, φ é um isomorfismo de espaços vetoriais. É fácil também ver que elas verificam as mesmas relações que os elementos $1, \mathfrak{i}, \mathfrak{j}, \mathfrak{K}$. Portanto, φ é um isomorfismo de $\mathbb{K}$-álgebras.

Se A é um anel de divisão, então A admite um subcorpo $\mathbb{L}$ da forma $\mathbb{K}(e_1)$, onde $e_1 \in A\backslash\mathbb{K}$ e ${e_1}^2 = a \in \mathbb{K}$. Seja σ o automorfismo não trivial de $\mathbb{L}$. Pelo Teorema de Skolem-Nöther, este automorfismo pode ser estendidos a um automorfismo interno de A. Desta forma, existe $e_2 \in A$ tal que ${e_2}^{-1}e_1e_2 = -e_1$. Como e_2 não comuta com e_1, obtemos que $e_2 \notin \mathbb{L}$, e assim, $A = \mathbb{L} \oplus \mathbb{L}e_2$. Observe agora que e_2^2 comuta com todos os elementos da base $\{1, e_1, e_2, e_1e_2\}$ de A, logo $e_2^2 = b \in \mathbb{K}$. Fazendo $e_3 = e_1e_2$, obtemos que a base $\{1, e_1, e_2, e_3\}$ de A satisfaz as propriedades: $e_1^2 = a$, $e_2^2 = b$ e $e_3 = e_1e_2 = -e_2e_1$. Portanto, podemos identificar A com a álgebra de quatérnios $(a, b)_{\mathbb{K}}$. □

Seja $(a, b)_{\mathbb{K}}$ uma $\mathbb{K}$–álgebra de quatérnios e $\alpha, \beta \in (a, b)_{\mathbb{K}}$. Se $\alpha = x + y\mathfrak{i} + z\mathfrak{j} + w\mathfrak{K}$ então definimos o **conjugado** de α como $\overline{\alpha} = x - y\mathfrak{i} - z\mathfrak{j} - w\mathfrak{K}$. Um cálculo simples mostra que $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$, $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$, $\overline{\overline{\alpha}} = \alpha$ e $\overline{\lambda\beta} = \lambda\overline{\beta}$, $\forall\lambda \in \mathbb{K}$. Além disso, $\overline{\alpha} = \alpha$ se, e somente se, $\alpha \in \mathbb{K}$. Se $\alpha = y\mathfrak{i} + z\mathfrak{j} + w\mathfrak{K}$ então dizemos que α é um **quatérnio puro**.

Podemos também definir a **norma** de α como $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha$. Se escrevermos $\alpha = x + y\mathfrak{i} + z\mathfrak{j} + w\mathfrak{K}$ podemos ver que $\mathrm{N}(\alpha) = x^2 - ay^2 - bz^2 + abw^2$. Portanto, a função norma define uma forma quadrática $\langle 1, -a, -b, ab\rangle$ em $(a, b)_{\mathbb{K}}$, que será chamada de **forma norma**.

A seguir apresentamos uma série de resultados clássicos, através dos quais a álgebra de quatérnios pode ser totalmente classificada a partir da sua forma norma. As demonstrações podem ser vistas em Scharlau [32], páginas 76-78 e 85.

Teorema 1.12 *Para $a, b, c, d \in \mathbb{K}^\times$ as seguintes afirmações são equivalentes:*

1. $\langle 1, -a, -b, ab\rangle \cong \langle 1, -c, -d, cd\rangle$
2. $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle$
3. $(a, b)_{\mathbb{K}} \cong (c, d)_{\mathbb{K}}$

Teorema 1.13 *Dados $a, b \in \mathbb{K}^\times$, as seguintes afirmações são equivalentes:*

1. $\langle -a, -b, ab\rangle$ *é isotrópica.*
2. $\langle 1, -a, -b, ab\rangle$ *é hiperbólica.*
3. $(a, b)_{\mathbb{K}} \cong (1, 1)_{\mathbb{K}}$.

Corolário 1.14 *Duas formas binárias $\langle a, b\rangle$ e $\langle c, d\rangle$ são isométricas se, e somente se, $(a, b)_{\mathbb{K}} \cong (c, d)_{\mathbb{K}}$ e $ab = cd$ em $\mathbb{K}^\times/{\mathbb{K}^\times}^2$.*

Corolário 1.15 *Para todo $a, b, c, d \in \mathbb{K}^\times$, temos que:*

1. $(a, b)_{\mathbb{K}} \cong (ac^2, bd^2)_{\mathbb{K}}$.
2. $(a, b)_{\mathbb{K}} \cong (b, a)_{\mathbb{K}}$.
3. $(1, 1)_{\mathbb{K}} \cong (1, a)_{\mathbb{K}} \cong (b, -b)_{\mathbb{K}} \cong (c, 1 - c)_{\mathbb{K}}$ *se* $c \neq 0, 1$.
4. $(a, a)_{\mathbb{K}} \cong (a, -1)_{\mathbb{K}}$.
5. $(a, b)_{\mathbb{K}} \cong (a, -ab)_{\mathbb{K}}$.
6. $[(ab, c)_{\mathbb{K}}] = [(a, c)_{\mathbb{K}}][(b, c)_{\mathbb{K}}]$ *no grupo de Brauer* $\mathrm{Br}(\mathbb{K})$

Capítulo 2

Álgebras Biquaterniônicas I (Involuções)

Como o primeiro capítulo foi apenas uma revisão de boa parte da teoria básica que será utilizada neste trabalho, neste capítulo começaremos de fato a estudar as álgebras biquaterniônicas, que, como já foi dito na introdução deste trabalho, são um tipo especial de álgebra central simples de dimensão 16, obtida como produto tensorial de duas álgebras de quatérnios. Ao longo deste capítulo vamos utilizar as involuções para discutir quando uma álgebra central simples é uma álgebra biquaterniônica. Além disso, vamos extrair algumas propriedades importantes sobre as involuções dessas álgebras.

2.1 Involuções em Álgebras Centrais Simples

Uma **involução** em uma $\mathbb{K}$–álgebra central simples A é uma aplicação $\sigma : A \to A$ que satisfaz as seguintes propriedades:

1. $\sigma(a+b) = \sigma(a) + \sigma(b)$, para $a, b \in A$;
2. $\sigma(ab) = \sigma(b)\sigma(a)$, para $a, b \in A$;
3. $\sigma^2(a) = a$, para $a \in A$.

Uma involução σ é dita do **primeiro tipo** se $\sigma(x) = x$, $\forall x \in \mathbb{K}$ e dita do **segundo tipo**, caso contrário.

Como nosso estudo nesse capítulo estará voltado prioritariamente para as involuções do primeiro tipo, usaremos apenas a palavra "involução" para nos referirmos às involuções do primeiro tipo.

Note que se σ é uma involução em uma $\mathbb{K}$–álgebra central simples A e $\mathbb{L}$ é uma extensão de $\mathbb{K}$ contida em A então $\sigma_{|_{\mathbb{L}}}$ é um automorfismo.

Exemplo 2.1 *1. Se A é a álgebra de matrizes $\mathrm{M}_n(\mathbb{K})$ então a aplicação $\sigma(x) = x^t$ que associa a cada matriz x a sua transposta é uma involução em A.*

2. Se A é a álgebra de quatérnios $(a,b)_{\mathbb{K}}$ então a aplicação $\sigma(u) = \overline{u}$ é uma involução em A, que é chamada de involução canônica.

3. Se σ é uma involução em uma álgebra central simples e $\imath_c$ é um automorfismo interno de A, tal que $\sigma(c) = \pm c$, então a aplicação $\imath_c \circ \sigma$ é uma involução em A.

4. Sejam A_1 e A_2 são duas $\mathbb{K}$–álgebras centrais simples. Se $\varphi : A_1 \to A_2$ é um isomorfismo e σ é uma involução em A_1 então $\varphi \circ \sigma \circ \varphi^{-1}$ é uma involução em A_2.

5. Se A_1 e A_2 são duas $\mathbb{K}$–álgebras centrais simples com involuções σ_1 e σ_2, respectivamente, então a aplicação $\sigma_1 \otimes \sigma_2 : A_1 \otimes_{\mathbb{K}} A_2 \to A_1 \otimes_{\mathbb{K}} A_2$, induzida por $a_1 \otimes a_2 \longmapsto \sigma(a_1) \otimes \sigma(a_2)$, é uma involução em $A_1 \otimes_{\mathbb{K}} A_2$.

Proposição 2.2 *Seja σ uma involução em uma $\mathbb{K}$–álgebra central simples A. Se τ é outra involução em A então existe um único $u \in A^{\times}$, a menos de fator em $\mathbb{K}^{\times}$, tal que*

$$\tau = \imath_u \circ \sigma \quad \text{e} \quad \sigma(u) = \pm u,$$

onde $\imath_u$ denota um automorfismo interno de A.

Demonstração: Se σ e τ são involuções em A então $\sigma \circ \tau$ é um automorfismo que fixa os elementos de $\mathbb{K}$. Pelo Teorema de Skolem–Nöther, existe $u \in A^{\times}$, unicamente determinado a menos de fator em $\mathbb{K}^{\times}$, tal que $\tau \circ \sigma = \imath_u$, assim, $\tau = \tau \circ \sigma^2 = \imath_u \circ \sigma$. Agora, para cada $x \in A$ teremos que

$$x = \tau^2(x) = (\imath_u \circ \sigma)^2(x) = (\imath_u \circ \sigma)(u^{-1}\sigma(x)u) = (u^{-1}\sigma(u))x(\sigma(u)^{-1}u).$$

Isto implica que $(u^{-1}\sigma(u))x = x(u^{-1}\sigma(u))$, e assim, $(u^{-1}\sigma(u)) = \lambda \in \mathbb{K}^{\times}$ e $\sigma(u) = \lambda u$. Conseqüentemente, $u = \sigma^2(u) = \sigma(\lambda u) = \lambda\sigma(u) = \lambda^2 u$ e $\lambda = \pm 1$. □

Seja σ uma involução em uma $\mathbb{K}$–álgebra central simples A e uma extensão galoisiana $\mathbb{L}/\mathbb{K}$ que cinde A, isto é, existe um isomorfismo

$$\varphi : A \otimes_{\mathbb{K}} \mathbb{L} \to \mathrm{M}_n(\mathbb{L}).$$

Desta forma, $\sigma \otimes 1$ é uma involução em $A \otimes_{\mathbb{K}} \mathbb{L}$ e então, $\tau = \varphi \circ (\sigma \otimes 1) \circ \varphi^{-1}$ é uma involução em $\mathrm{M}_n(\mathbb{L})$. Sendo assim, aplicando a proposição anterior às involuções τ e transposição, obtemos que existe $u \in \mathrm{M}_n(\mathbb{L})$ tal que $\tau(x) = \imath_u(x^t)$, $\forall x \in \mathrm{M}_n(\mathbb{L})$ e $u^t = \varepsilon u$, onde $\varepsilon = \pm 1$.

Seja $\psi : A \otimes_{\mathbb{K}} \mathbb{L}' \to \mathrm{M}_n(\mathbb{L}')$ outra decomposição. Como podemos substituir $\mathbb{L}$ e $\mathbb{L}'$ por uma outra extensão $\mathbb{L}''$ que contém $\mathbb{L}$ e $\mathbb{L}'$, então podemos assumir que $\mathbb{L} = \mathbb{L}'$. Sendo assim, $\tau' = \psi \circ (\sigma \otimes 1) \circ \psi^{-1}$ é uma involução em $\mathrm{M}_n(\mathbb{L})$, que satisfaz, $\tau'(x) = \imath_v(x^t)$, $\forall x \in \mathrm{M}_n(\mathbb{L})$, com $v^t = \varepsilon' v$. Assim,

$$\tau' = \psi \circ (\sigma \otimes 1) \circ \psi^{-1} = \psi \circ (\varphi^{-1} \circ \tau \circ \varphi) \circ \psi^{-1} = (\psi \circ \varphi^{-1}) \circ \tau \circ (\psi \circ \varphi^{-1})^{-1}.$$

Com $\psi \circ \varphi^{-1}$ é um automorfismo de $\mathrm{M}_n(\mathbb{L})$, podemos escrever $\psi \circ \varphi^{-1} = \imath_c$. Segue que para cada $x \in \mathrm{M}_n(\mathbb{L})$,

$$vx^tv^{-1} = \tau'(x) = (\imath_c \circ \tau \circ \imath_{c^{-1}})(x) = c\tau(c^{-1}xc)c^{-1} = cu(c^{-1}xc)^t u^{-1}c^{-1} = cuc^t x^t (c^{-1})^t u^{-1}c^{-1}.$$

Assim, $x^t v^{-1} cuc^t = v^{-1}cuc^t x^t$, para cada $x \in \mathrm{M}_n(\mathbb{L})$. Logo $v^{-1}cuc^t = \lambda \in \mathbb{L}$ e

$$\lambda v = cuc^t. \tag{2.1}$$

Aplicando a transposição em ambos os membros da igualdade 2.1 obtemos que $\varepsilon'\lambda v = \varepsilon cuc^t$. Portanto concluímos que $\varepsilon' = \varepsilon$ e ε independe da escolha da decomposição. Com isso, podemos definir que σ é do **tipo simplética** se $\varepsilon = -1$ e do **tipo ortogonal** se $\varepsilon = 1$.

Consideremos σ uma involução em A e definimos o conjunto dos elementos simétricos em anti-simétricos respectivamente por:

$$\mathrm{Sym}(A,\sigma) = \{u \in A | \sigma(u) = u\} \quad \text{e} \quad \mathrm{Skew}(A,\sigma) = \{u \in A | \sigma(u) = -u\}.$$

Observe que $\mathrm{Skew}(A,\sigma)$ e $\mathrm{Sym}(A,\sigma)$ são subespaços vetoriais de A que satisfazem

$$\mathrm{Skew}(A,\sigma) \cap \mathrm{Sym}(A,\sigma) = \{0\}.$$

Além disso, como $u - \sigma(u) \in \mathrm{Skew}(A,\sigma)$, $u + \sigma(u) \in \mathrm{Sym}(A,\sigma)$ e $u = \frac{1}{2}(u + \sigma(u)) + \frac{1}{2}(u - \sigma(u))$, $\forall u \in A$, conseguimos que $A = \mathrm{Skew}(A,\sigma) \oplus \mathrm{Sym}(A,\sigma)$. No caso em que A é a álgebra de matrizes $\mathrm{M}_n(\mathbb{K})$ e σ é a transposição então escreveremos $\mathrm{SymM}_n(\mathbb{K})$ e $\mathrm{SkewM}_n(\mathbb{K})$ para denotar $\mathrm{Sym}(A,\sigma)$ e $\mathrm{Skew}(A,\sigma)$, respectivamente.

Proposição 2.3 *Seja A uma $\mathbb{K}$–álgebra central simples de grau n com uma involução σ. Então valem:*

1. *Se σ é ortogonal então* $\dim \mathrm{Sym}(A,\sigma) = n(n+1)/2$.
2. *Se σ é simplética então* $\dim \mathrm{Skew}(A,\sigma) = n(n+1)/2$.

Demonstração: Seja $\alpha : A \otimes_{\mathbb{K}} \mathbb{L} \to \mathrm{M}_n(\mathbb{L})$ uma decomposição para A. Desta forma, se $\tau = \alpha \circ (\sigma \otimes 1) \circ \alpha^{-1}$ então $\tau(x) = i_u(x^t)$, $\forall x \in \mathrm{M}_n(\mathbb{L})$, onde $u^t = \varepsilon u$ e $\varepsilon = 1$ se σ é ortogonal e $\varepsilon = -1$ se σ é simplética. Suponhamos inicialmente que σ é ortogonal, isto é, $u^t = u$. Uma verificação direta mostra que:

$$u\mathrm{Sym}\mathrm{M}_n(\mathbb{L}) = \mathrm{Sym}(\mathrm{M}_n(\mathbb{L}),\tau) = \alpha(\mathrm{Sym}(A \otimes_{\mathbb{K}} \mathbb{L}, \sigma \otimes 1)).$$

Como

$$\dim_{\mathbb{K}} \mathrm{Sym}(A,\sigma) = \dim_{\mathbb{L}} \mathrm{Sym}(A \otimes_{\mathbb{K}} \mathbb{L}, \sigma \otimes 1)$$

e α é um isomorfismo,

$$\dim_{\mathbb{K}} \mathrm{Sym}(A,\sigma) = \dim_{\mathbb{K}} u\mathrm{Sym}\mathrm{M}_n(\mathbb{L}) = \dim_{\mathbb{K}} \mathrm{Sym}\mathrm{M}_n(\mathbb{L}) = \frac{n(n+1)}{2}.$$

Isto prova (1). A verificação de (2) é análoga, supondo que $u^t = -u$. □

Proposição 2.4 *Seja A uma $\mathbb{K}$–álgebra central simples com uma involução σ. Suponhamos que $\tau = \imath_u \circ \sigma$, onde $\sigma(u) = \pm u$. Então σ e τ têm o mesmo tipo se, e somente se, $\sigma(u) = u$.*

Demonstração: Um cálculo direto mostra que

$$\mathrm{Sym}(A,\tau) = \begin{cases} u\mathrm{Sym}(A,\sigma) = \mathrm{Sym}(A,\sigma)u^{-1} & \text{se } \sigma(u) = u \\ u\mathrm{Skew}(A,\sigma) = \mathrm{Skew}(A,\sigma)u^{-1} & \text{se } \sigma(u) = -u \end{cases} \tag{2.2}$$

e

$$\mathrm{Skew}(A,\tau) = \begin{cases} u\mathrm{Skew}(A,\sigma) = \mathrm{Skew}(A,\sigma)u^{-1} & \text{se } \sigma(u) = u \\ u\mathrm{Sym}(A,\sigma) = \mathrm{Sym}(A,\sigma)u^{-1} & \text{se } \sigma(u) = -u \end{cases} \tag{2.3}$$

Pela Proposição 2.3, σ e τ têm o mesmo tipo se e somente se $\mathrm{Sym}(A,\sigma)$ e $\mathrm{Sym}(A,\tau)$ têm a mesma dimensão. As equações 2.2 e 2.3 mostram que esta condição vale se e somente se $\sigma(u) = u$. □

2.2 Involuções em Álgebras de Quatérnios

Nesta seção vamos obter alguns resultados a respeito das involuções na álgebras de quatérnios que serão úteis ao longo do capítulo.

Proposição 2.5 *A única involução simplética numa $\mathbb{K}$–álgebra de quatérnios A é a involução canônica.*

Demonstração: Pela Proposição 2.3, a involução canônica σ é simplética pois

$$\dim_{\mathbb{K}} \mathrm{Skew}(A, \sigma) = 3.$$

Agora, se τ é outra involução simplética em A então, pelas Proposições 2.2 e 2.4 existe $u \in A^{\times}$ tal que $\tau = \imath_u \circ \sigma$ e $\sigma(u) = u$. Mas neste caso, teremos que $u \in \mathbb{K}$ e portanto, $\tau = \sigma$. □

Proposição 2.6 *Seja H uma $\mathbb{K}$–álgebra de quatérnios de divisão e $\mathbb{L}$ um subcorpo maximal de H. Então existe uma involução σ em H tal que σ é a identidade em $\mathbb{L}$.*

Demonstração: Seja $\mathbb{L} = \mathbb{K}(a)$, onde a é um quatérnio puro e τ a involução canônica em H. Então $\tau(a) = -a$. Como $a^2 \in \mathbb{K}$, se φ denota o automorfismo não trivial de $\mathbb{L}$ então $\varphi(a) = -a$. Agora estendemos φ a um automorfismo interno $\imath_c$ de H. Desta forma, se definirmos $\sigma = \imath_c \circ \tau$ teremos que σ é uma involução em H e satisfaz:

$$\sigma(a) = c\tau(a)c^{-1} = -cac^{-1} = -\varphi(a) = a.$$

Portanto, σ é a identidade em $\mathbb{L}$. □

Lema 2.7 *Seja A um anel de divisão sobre $\mathbb{K}$ e $\mathbb{L}$ um subcorpo maximal de A. Se τ é uma involução em A tal que $\tau_{|_{\mathbb{L}}} = \imath_{u|_{\mathbb{L}}}$, então $\tau(u) = \pm u$.*

Demonstração: Como $\tau(x) = uxu^{-1}, \quad \forall x \in \mathbb{L}$, obtemos que

$$x = \tau^2(x) = \tau(uxu^{-1}) = \tau(u)^{-1}\tau(x)\tau(u).$$

Isto implica que $\tau(x) = \tau(u)x\tau(u)^{-1}$. Igualando as duas expressões obtidas para $\tau(x)$ conseguimos que $xu^{-1}\tau(u) = u^{-1}\tau(u)x$, isto é, $u^{-1}\tau(u)$ comuta com todo elemento de $\mathbb{L}$. Como $\mathbb{L}$ é maximal, $u^{-1}\tau(u) = \lambda \in \mathbb{L}$. Segue que:

$$u^{-1}\tau(u) = \lambda \Rightarrow \tau(u) = u\lambda \Rightarrow \tau(\lambda)\tau(u) = u \Rightarrow u\lambda u^{-1}\tau(u) = u \Rightarrow \tau(u) = u\lambda^{-1}.$$

Portanto, $u\lambda = \tau(u) = u\lambda^{-1}$ e conseqüentemente, $\lambda = \pm 1$. □

Proposição 2.8 *Seja H uma $\mathbb{K}$–álgebra de quatérnios de divisão e x e y dois quatérnios puros em H. Então existe uma involução σ em H tal que $\sigma(x) = x$ e $\sigma(y) = y$.*

Demonstração: Seja τ a involução canônica em H. Então $\tau(x) = -x$ e $\tau(y) = -y$. Desta forma, τ é uma automorfismo quando restrito aos subcorpos maximais $\mathbb{K}(x)$ e $\mathbb{K}(y)$. Logo existe $u, v \in H$ tais que $\tau_{|_{\mathbb{K}(x)}} = \imath_{u|_{\mathbb{K}(x)}}$ e $\tau_{|_{\mathbb{K}(y)}} = \imath_{v|_{\mathbb{K}(y)}}$. Pelo Lema 2.7, $\tau(u) = \pm u$ e $\tau(v) = \pm v$. Como u e v não podem estar em $\mathbb{K}$, conseguimos que $\tau(u) = -u$ e $\tau(v) = -v$. Um cálculo direto mostra que para todo $z \in \mathbb{K}(x)$, como $\tau(z) = uzu^{-1}$, então $\tau(uz) = -uz$. Igualmente para $z \in \mathbb{K}(y)$. Logo, $\tau(ux) = -ux$ e $\tau(vy) = -vy$. Assim, $u\mathbb{K}(x)$ e $v\mathbb{K}(y)$ são ambos $\mathbb{K}$–espaços vetoriais de dimensão 2 que só contém quatérnios puros. Assim existe $z \in u\mathbb{K}(x) \cap v\mathbb{K}(y)$, com $z \neq 0$. Desta forma, se definirmos $\sigma = \imath_z \circ \tau$ teremos que σ é uma involução em H. Se escrevermos $z = u(a + bx)$, com $a, b \in \mathbb{K}$, teremos que

$$\sigma(x) = z\tau(x)z^{-1} = -u(a + bx)x(a + bx)^{-1}u^{-1} = -uxu^{-1} = -\tau(x) = x.$$

Do mesmo modo, $\sigma(y) = y$ e σ satisfaz as propriedades desejadas. □

2.3 Anéis de Divisão de grau 4 com Involuções

Nesta seção vamos apenas demonstrar resultados que trazem algumas propriedades dos anéis de divisão de grau 4 com involução. A demonstração é um pouco técnica, mas o esforço será recompensado com os importantes resultados que obteremos nas três seções seguintes.

Lema 2.9 *Seja A um anel de divisão de grau 4 e centro $\mathbb{K}$. Se A admite uma involução σ, então existe em A uma extensão quadrática $\mathbb{L} = \mathbb{K}(a)$ de $\mathbb{K}$ e uma involução $\tau : A \to A$ tal que $\tau(a) = -a$ e $a^2 \in \mathbb{K}$.*

Demonstração: Começamos tomando um elemento não nulo u em $\mathrm{Skew}(A, \sigma)$. Como $u \notin \mathbb{K}$ e $\sigma(u^2) = u^2$, obtemos que $\mathbb{K} \subset \mathbb{K}(u^2) \subsetneq \mathbb{K}(u)$. Como $\dim_{\mathbb{K}} A = 16$, temos apenas duas possibilidades: $[\mathbb{K}(u) : \mathbb{K}] = 2$ ou $\mathbb{K}(u)$ é um subcorpo maximal de A. Se o primeiro

caso ocorrer, o lema esta demonstrado. Suponhamos então que $[\mathbb{K}(u) : \mathbb{K}] = 4$. Neste caso, $\mathbb{K}(u^2)$ é uma extensão quadrática de $\mathbb{K}$ e podemos escrever $\mathbb{K}(u^2) = \mathbb{K}(a)$, onde $a^2 \in \mathbb{K}$. Pelo Teorema de Skolem-Nöther, o automorfismo não trivial de $\mathbb{K}(a)$ pode ser estendido a um automorfismo interno $\imath_c$ de A, isto é, $\imath_c(x) = cxc^{-1}, \forall x \in A$ e $\imath_c(a) = -a$.

Seja $\tau = \imath_c \circ \sigma$. Se $\sigma(c) = -c$ então τ é uma involução em A que satisfaz $\tau(a) = \imath_c(\sigma(a)) = \imath_c(a) = -a$.

Suponhamos que $\sigma(c) \neq -c$. Neste caso, $\sigma(\sigma(c) + c) = \sigma(c) + c \neq 0$. Como $a \in \mathbb{K}(u^2)$ e σ é a identidade em $\mathbb{K}(u^2)$ então teremos que $\sigma(c)c^{-1}$ comuta com a pois

$$\sigma(c)c^{-1}a(\sigma(c)c^{-1})^{-1} = \sigma(c)(c^{-1}ac)\sigma(c)^{-1} = -\sigma(c)a\sigma(c^{-1}) =$$

$$= -\sigma(c)\sigma(a)\sigma(c^{-1}) = -\sigma(c^{-1}ac) = -\sigma(-a) = \sigma(a) = a.$$

Tome $b = c + \sigma(c)$ e considere $\tau = \imath_b \circ \sigma$. Como $\sigma(b) = b$, então τ é uma involução em A. Além disso,

$$ab = a(c + \sigma(c)) = ac + a\sigma(c) = cc^{-1}ac + a\sigma(c)c^{-1}c =$$

$$= -ca + \sigma(c)c^{-1}ac = -ca - \sigma(c)a = -ba$$

e daí obtemos que $\tau(a) = b\sigma(a)b^{-1} = bab^{-1} = -a$.

Em ambos os casos, conseguimos em A uma extensão quadrática $\mathbb{L}$ de $\mathbb{K}$ e uma involução que restrita a $\mathbb{L}$ é o automorfismo não trivial. □

Lema 2.10 *Seja A uma $\mathbb{K}$–álgebra de divisão de grau 4 contendo uma extensão quadrática $\mathbb{L} = \mathbb{K}(a)$ de $\mathbb{K}$ e uma involução $\sigma : A \to A$ tal que $\sigma(a) = -a$ e $a^2 \in \mathbb{K}$. Se definirmos $B = \mathcal{C}_A\mathbb{L}$ então existe uma $\mathbb{K}$–subalgebra de quatérnios Q de A tal que $A \cong Q \otimes_{\mathbb{K}} \mathcal{C}_A Q$ e $B = Q \otimes_{\mathbb{K}} \mathbb{L}$.*

Demonstração: Segue do Teorema do Duplo Centralizador que $B = \mathcal{C}_A\mathbb{L}$ é uma $\mathbb{L}$-álgebra central simples. Como $\dim_{\mathbb{L}} B = 4$, B é uma $\mathbb{L}$-álgebra de quatérnios.

Vamos então obter um elemento $x_o \in B \setminus \mathbb{L}$ tal que $\sigma(x_o) = x_o$. Primeiramente, note que um cálculo simples mostra que $\sigma(x) \in B$, $\forall x \in B$. Com isso, B é invariante por σ e daí, σ é uma involução do segundo tipo em B. Agora, observe que neste caso, também podemos escrever $B = B_1 \oplus B_2$, onde $B_1 = \{b \in B \mid \sigma(b) = b\}$ e $B_2 = \{b \in B \mid \sigma(b) = -b\}$. Dado $u \in B \setminus \mathbb{L}$, escrevemos $u = v + w$ onde $\sigma(v) = -v$ e $\sigma(w) = w$. Como σ restrito a $\mathbb{L}$ é um automorfismo não trivial, se $w \notin \mathbb{K}$ então $w \notin \mathbb{L}$ e assim, faça $x_o = w$. Caso

contrário, $w \in \mathbb{K}$ e $v \in B \setminus \mathbb{L}$. Tomamos então $x_o = av$. Nestas condições, $\mathbb{L}(x_o)$ é uma extensão quadrática de $\mathbb{L}$ em B, portanto maximal e galoisiana, com grupo de Galois $\mathrm{Gal}(\mathbb{L}(x_o)|\mathbb{L}) = \{1, s\}$. Sendo assim, B é cíclica com $\mathbb{L}$-base $\beta = \{1, x_o, y, x_o y\}$, onde $zy = ys(z), \forall z \in \mathbb{L}(x_o)$ e $y^2 = \gamma \in \mathbb{L}$. Como σ é a identidade em $\mathbb{K}(x_o)$ então devemos ter $\mathbb{K}(x_o) \subsetneq \mathbb{L}(x_o)$. Segue que $\mathbb{K}(x_o)$ é uma extensão quadrática galoisiana de $\mathbb{K}$ e terá grupo de Galois $\mathrm{Gal}(\mathbb{K}(x_o)|\mathbb{K}) = \{1, s|_{\mathbb{K}(x_o)}\}$.

Desejamos construir uma $\mathbb{K}$-álgebra de quatérnios em B. Desta forma, precisamos obter $y_o \in B$ tal que $y_o^2 \in \mathbb{K}$ e $zy_o = y_o s(z), \forall z \in \mathbb{K}(x_o)$. Com efeito, se $\sigma(y) = -y$ então $\sigma(\gamma) = \sigma(y^2) = (-y)^2 = \gamma$ e assim, $\gamma \in \mathbb{K}$. Neste caso, basta tomarmos $y_o = y$. Suponhamos então $\sigma(y) \neq -y$. Como $s(x_o) \in \mathbb{K}(x_o)$, resulta que $\sigma(s(x_0)) = s(x_0)$ e portanto,

$$s(x_o)\sigma(y) = \sigma(s(x_o))\sigma(y) = \sigma(ys(x_o)) = \sigma(x_o y) = \sigma(y)\sigma(x_o) = \sigma(y)x_o$$

logo, $y\sigma(y)x_o = ys(x_o)\sigma(y) = x_o y\sigma(y)$ e assim, $y\sigma(y)$ comuta com x_o. Portanto, $y\sigma(y) \in \mathbb{L}(x_o)$, pois $y\sigma(y) \in B = \mathcal{C}_A\mathbb{L}$ e $\mathbb{L}(x_o)$ é maximal. Como $y\sigma(y)$ é σ-invariante, $y\sigma(y) = x_2 \in \mathbb{K}(x_o)$. Desta forma, $\sigma(y) = \gamma^{-1}y^2\sigma(y) = \gamma^{-1}yx_2$. E assim, façamos $y_o = y + \sigma(y) = y + y\gamma^{-1}x_2 = y(1 + \gamma^{-1}x_2)$. Como $1 + \gamma^{-1}x_2 \in \mathbb{L}(x_o), \forall z \in \mathbb{L}(x_o)$ teremos que

$$zy_o = zy(1 + \gamma^{-1}x_2) = ys(z)(1 + \gamma^{-1}x_2) = y(1 + \gamma^{-1}x_2)s(z) = y_o s(z), \qquad (2.4)$$

e assim, $zy_o^2 = y_o s(z) y_o = y_o^2 s^2(z) = y_o^2 z$. Portanto, $y_o^2 \in \mathbb{L}(x_o)$, pois sendo $\mathbb{L}(x_o)$ maximal em B, coincide com o seu centralizador.

Se $y_o^2 \notin \mathbb{L}$ então $\mathbb{L}(y_o) = \mathbb{L}(y_o^2) = \mathbb{L}(x_o)$, o que não é possível, pois y_o e x_o não comutam, como pode ser visto na equação 2.4. Logo $y_o^2 \in \mathbb{L}$. Como y_o^2 é σ-invariante, obtemos que $y_o^2 \in \mathbb{K}$.

Desta forma, construímos em A uma $\mathbb{K}$-subalgebra de quatérnios $Q = (x_o^2, y_o^2)_{\mathbb{K}}$. Pelo Teorema do Duplo Centralizador, $A = Q \otimes_{\mathbb{K}} \mathcal{C}_A Q$. Para provar a última afirmação afirmação do lema, veja que $Q \subseteq B = \mathcal{C}_A\mathbb{L}$ implica que $\mathbb{L} \subseteq \mathcal{C}_A Q$, e daí, $Q \otimes_{\mathbb{K}} L$ é uma $\mathbb{L}$–álgebra de quatérnios contida em A. Portanto, $Q \otimes_{\mathbb{K}} L \subseteq \mathcal{C}_A\mathbb{L} = B$. Como $\dim_{\mathbb{L}} B = \dim_{\mathbb{L}} Q \otimes_{\mathbb{K}} \mathbb{L}$, concluímos que $B = Q \otimes_{\mathbb{K}} \mathbb{L}$. □

Lema 2.11 *Seja A um anel de divisão de grau 4 contendo uma extensão quadrática $\mathbb{L} = \mathbb{K}(a)$ de $\mathbb{K}$ e uma involução σ. Se $a^2 \in \mathbb{K}$ e τ denota o automorfismo não trivial de $\mathbb{L}$ então existe um elemento $u \in A$ tal que $\sigma(u) = u$ e $(\sigma \circ \tau)(x) = uxu^{-1}$, $\forall x \in \mathbb{L}$. Segue que A admite uma involução ρ que coincide com τ quando restrita a $\mathbb{L}$.*

Demonstração: Seja $B = \mathcal{C}_A\mathbb{L}$. Como $\sigma \circ \tau$ é um isomorfismo do corpo $\mathbb{L}$ no corpo $\sigma(\tau(\mathbb{L}))$ então, pelo Teorema de Skolem–Nöther, existe $y \in A$ tal que $(\sigma \circ \tau)(x) = yxy^{-1}$, $\forall x \in \mathbb{L}$. Então

$$(y^{-1}\sigma(y))^{-1}x(y^{-1}\sigma(y)) = (\sigma(y))^{-1}\sigma(\tau(x))\sigma(y) = \sigma(y\tau(x)y^{-1}) = \sigma^2(x) = x, \qquad (2.5)$$

e daí, $y^{-1}\sigma(y) \in B$. Assim, $\sigma(y) \in yB$. Suponhamos que todo elemento não nulo de yB é anti-simétrico com respeito a σ. Assim, para cada $a \in B$, teremos que

$$-ya = \sigma(ya) = \sigma(a)\sigma(y) = -\sigma(a)y \Rightarrow \sigma(a) = yay^{-1}.$$

Desta forma, se $a_1, a_2 \in B$ então

$$\sigma(a_1a_2) = \sigma(a_2)\sigma(a_1) = (ya_2y^{-1})(ya_1y^{-1}) = y(a_2a_1)y^{-1} = \sigma(a_1a_2).$$

Mas isto implica que $a_1a_2 = a_2a_1$ e B é comutativo. Como isto não é possível, existe um elemento $z \in yB^{\times}$ tal que $\sigma(z) \neq -z$. Se escrevermos $z = ya$ e $x \in \mathbb{L}$ então

$$zxz^{-1} = (ya)x(ya)^{-1} = y(axa^{-1})y^{-1} = yxy^{-1} = \sigma(\tau(x)),$$

e assim, se repetirmos o cálculo feito em 2.5 chegaremos que $z^{-1}\sigma(z) \in B$, logo, $\sigma(z) \in yB$. Desta forma, $u = z + \sigma(z)$ é um elemento simétrico e não nulo em yB que satisfaz $uxu^{-1} = \sigma(\tau(x))$, $\forall x \in \mathbb{L}$. Para última afirmação basta tomarmos $\rho = \imath_u \circ \sigma$ que teremos as propriedades desejadas. □

2.4 O Teorema de Albert

É claro que toda álgebra biquaterniônica é central simples, pois é o produto tensorial de duas álgebras de quatérnios, que por sua vez, são sempre centrais simples. Como vimos no teorema 1.11, toda álgebra central simples de grau 2 é uma álgebra de quatérnios. Uma pergunta natural então seria: Toda álgebra central simples A de grau 4 é uma álgebra biquaterniônica? Infelizmente, isto não é verdade em geral. Pelo Teorema de Wedderburn, $A \cong \mathrm{M}_n(D)$. Como $\dim_{\mathbb{K}} A = 16$, temos três possibilidades: A é um anel de divisão, A é cindida ou $A \cong \mathrm{M}_2(D)$, onde D é uma álgebra de quatérnios de divisão. Nos dois últimos casos, temos uma resposta afirmativa, pois $A \cong \mathrm{M}_4(\mathbb{K}) \cong \mathrm{M}_2(\mathbb{K}) \otimes_{\mathbb{K}} \mathrm{M}_2(K) \cong (1,1)_{\mathbb{K}} \otimes_{\mathbb{K}} (1,1)_{\mathbb{K}}$ ou $A \cong \mathrm{M}_2(D) \cong \mathrm{M}_2(\mathbb{K}) \otimes_{\mathbb{K}} D \cong (1,1)_{\mathbb{K}} \otimes_{\mathbb{K}} D$. Para o caso em que A é um anel de divisão, temos o seguinte resultado:

Teorema 2.12 (Albert) *Seja A um anel de divisão de grau 4 sobre $\mathbb{K}$. Então as seguintes afirmações são equivalentes:*

1. *A é uma álgebra biquaterniônica.*
2. *A tem uma involução do primeiro tipo.*
3. $\exp[A] = 2$ *no grupo de Brauer* $\mathrm{Br}(\mathbb{K})$.

Demonstração:
(1)⇒(3) Se A é biquaterniônica então podemos escrever $A = B \otimes_{\mathbb{K}} C$, onde B e C são álgebras de quatérnios de divisão. Como $\mathrm{ind}(B) = \mathrm{ind}(C) = 2$, $[A]^2 = [B \otimes_{\mathbb{K}} C]^2 = [B]^2[C]^2 = 1$

(2)⇒(1) Pelos lemas 2.9 e 2.10, $A \cong Q \otimes_{\mathbb{K}} \mathcal{C}_A Q$. Como Q e $\mathcal{C}_A Q$ são ambas centrais simples de grau 2, concluímos que A é uma álgebra biquaterniônica.

(3)⇒(2) Se $[A]^2 = 1$ em $\mathrm{Br}(\mathbb{K})$ então $[A] = [A^{op}]$, e assim, existe um isomorfismo de $\mathbb{K}$-álgebras $\tau : A \to A^{op}$. Ao mesmo tempo, podemos olhar $\tau : A \to A$ como um anti-automorfismo. Desta forma, se $\tau^2 = 1$ então τ é uma involução e nada temos a fazer. Suponhamos então $\tau^2 \neq 1$. Por outro lado, se estendermos τ ao isomorfismo $A \otimes_{\mathbb{K}} A \cong A \otimes_{\mathbb{K}} A^{op}$ e compormos com isomorfismo canônico $A \otimes_{\mathbb{K}} A^{op} \cong \mathrm{End}_{\mathbb{K}}(A)$, obteremos o seguinte isomorfismo de $\mathbb{K}$-álgebras:

$$\begin{array}{rcccl} \varphi & : & A \otimes_{\mathbb{K}} A & \longrightarrow & \mathrm{End}_{\mathbb{K}}(A) \\ & & a \otimes b & \longmapsto & \varphi(a \otimes b) \end{array} \quad : \quad \begin{array}{rcl} A & \longrightarrow & A \\ x & \longmapsto & ax\tau(b). \end{array}$$

Pelo lema 1.6, existe $u \in A \otimes_{\mathbb{K}} A$ tal que $u^2 = 1$ e $u(a \otimes b) = (b \otimes a)u, \forall a, b \in A$. Seja então $\psi : A \to A$ dado por $\varphi(u)$. Note que $\psi^2 = 1$ pois $\forall x \in A$,

$$\psi^2(x) = (\varphi(u) \circ \varphi(u))(x) = \varphi(u^2)(x) = \varphi(1)(x) = x.$$

Mais ainda, $\psi(ax\tau(b)) = b\psi(x)\tau(a)$, pois $\forall a, b \in A$

$$\psi(ax\tau(b)) = \psi(\varphi(a \otimes b)(x)) = (\varphi(u) \circ \varphi(a \otimes b))(x) = \varphi(u(a \otimes b))(x) =$$

$$= \varphi((b \otimes a)u)(x) = (\varphi(b \otimes a) \circ \varphi(u))(x) = \varphi(b \otimes a)(\psi(x) = b\psi(x)\tau(a).$$

Seja $w = \psi(1) \in A$. Pelo que vimos acima, $1 = \psi(w) = \psi(w\cdot 1) = 1\cdot\psi(1)\tau(w) = w\tau(w)$ e $1 = \psi(1 \cdot w) = \psi(1 \cdot \tau(\tau^{-1}(w))) = \tau^{-1}(w)\psi(1) = \tau^{-1}(w)w$. Portanto, $\tau(w) = \tau^{-1}(w)$ e $1 = w\tau(w) = \tau(w)w$. Além disso, $\forall x \in A$ temos que

$$x = \psi^2(x) = \psi(\psi(x \cdot 1)) = \psi(\psi(1)\tau(x)) = \psi(w\tau(x)) = \psi(\tau(x))\tau(w) =$$

$$= \psi(\tau(x) \cdot 1)\tau(w) = w\tau^2(x)\tau(w) = w\tau^2(x)w^{-1},$$

assim, $x = (\imath_w \circ \tau^2)(x)$ e $\tau^2 = (\imath_w)^{-1}$, onde $\imath_w$ denota o automorfismo interno.

Como $\tau^2 \neq 1$, $\imath_w \neq 1$ e assim, $w \notin \mathbb{K}$. Portanto, $1 + w = 1 + \psi(1) \neq 0$. Seja então $a = 1+w$ e definimos $\sigma = \imath_a \circ \tau$. Como τ é um anti-automorfismo e $\imath_a$ é um automorfismo interno, então $\sigma|_{\mathbb{K}} = 1$, $\sigma(x + y) = \sigma(x) + \sigma(y)$ e $\sigma(xy) = \sigma(y)\sigma(x), \forall x, y \in A$. Além disso,

$$a = 1 + \psi(1) = \psi^2(1) + \psi(1) = \psi(\psi(1) + 1) = \psi(a) = \psi(1)\tau(a) = w\tau(a),$$

logo $w = a\tau(a)^{-1}$, e assim

$$\sigma^2(x) = (\imath \circ \tau)^2(x) = (\imath_a \circ \tau \circ \imath_a \circ \tau)(x) = \imath_a(\tau(a\tau(x)a_{-1})) = \imath_a(\tau(a_{-1})\tau^2(x)\tau(a)) =$$

$$= a\tau(a^{-1})\tau^2(x)\tau(a)a^{-1} = w\tau^2(a)w^{-1} = (\imath_w \circ \tau^2)(x) = x.$$

Portanto, $\sigma^2 = 1$ e σ é uma involução do primeiro tipo em A. □

Obs 2.13 *Pelo que acabamos de ver, toda álgebra biquaterniônica A admite uma involução σ. Seria interessante se para $A \cong Q_1 \otimes_{\mathbb{K}} Q_2$, conseguíssemos escrever σ da forma $\sigma_1 \otimes \sigma_2$, onde σ_i é uma involução em Q_i. Uma condição necessária e suficiente para que isto ocorra é termos que A contém uma subalgebra de quatérnios que é invariante por σ. Se Q_1 é uma tal subalgebra, isto é, $\sigma(Q_1) \subseteq Q_1$ então $\sigma(Q_1) = Q_1$, pois $\sigma^2 = 1$. Agora, se $Q_2 = \mathcal{C}_A Q_1$ então $A \cong Q_1 \otimes_{\mathbb{K}} Q_2$ e dado $x \in Q_2$, $\sigma(x)$ também comuta com todo elemento de Q_1, implicando que Q_2 também é invariante por σ. Assim, as restrições σ_1 e σ_2 de σ a Q_1 e Q_2, respectivamente, são involuções e $\sigma = \sigma_1 \otimes \sigma_2$. Neste caso dizemos que σ é decomponível. Vamos então analisar quando essa situação pode ocorrer, estudando separadamente os casos em que a involução é do tipo simplético e do tipo ortogonal.*

2.5 Involuções Simpléticas

Veremos agora que toda involução simplética σ em uma álgebra biquaterniônica é decomponível. Pela observação acima, basta mostrarmos que a álgebra contém uma subalgebra de quatérnios que é invariante por σ. Mas antes precisaremos do seguinte lema:

Lema 2.14 *Se A é uma $\mathbb{K}$–álgebra biquaterniônica com uma involução simplética σ então o polinômio característico reduzido de todo elemento simétrico é um quadrado. Segue que todo elemento simétrico satisfaz um polinômio quadrático em $\mathbb{K}$.*

Demonstração: Seja $\mathbb{F}$ uma extensão galoisiana de $\mathbb{K}$ e $\alpha : A \otimes_{\mathbb{K}} \mathbb{F} \to \mathrm{M}_4(\mathbb{F})$ uma decomposição. Para cada elemento simétrico $a \in A$ temos que $\mathrm{Prd}_{A,a}(X) = \det(X.I - \alpha(a))$. Por outro lado, podemos extender $\mathbb{F}$ a uma extensão galoisiana $\mathbb{L}$ de $\mathbb{K}$, tal que $\mathrm{Prd}_{A,a}(X)$ se fatore completamente. Como σ é simplética, a involução

$$\alpha \circ (\sigma \otimes 1) \circ \alpha^{-1} : \mathrm{M}_4(\mathbb{L}) \to \mathrm{M}_4(\mathbb{L})$$

é da forma $\imath_u \circ t$, onde t é a transposição de $\mathrm{M}_4(\mathbb{L})$ e $u^t = -u$. Sendo assim,

$$u\alpha(a)^t u^{-1} = (\alpha \circ (\sigma \otimes 1) \circ \alpha^{-1})(\alpha(a)) = \alpha(\sigma \otimes 1(a \otimes 1)) = \alpha(a).$$

Isto implica que $u\alpha(a)^t = \alpha(a)u$ e daí

$$(\alpha(a)u)^t = u^t\alpha(a)^t = -u\alpha(a)^t = -\alpha(a)u.$$

Com isso, u^{-1} e $X.u - u\alpha(a)$ são matrizes alternadas. Como o determinante de toda matriz alternada é um quadrado,

$$\mathrm{Prd}_{A,a}(X) = \det(X.1 - \alpha(a)) = \det(u^{-1}) \det(X.u - \alpha(a)u)$$

é um quadrado em $\mathbb{L}[X]$. Portanto, podemos escrever $\mathrm{Prd}_{A,a}(X) = (X - a_1)^2(X - a_2)^2$. Como a ação pelo grupo de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ só permuta as raízes, conseguimos que $\mathrm{Prd}_{A,a}(X)$ é um quadrado em $\mathrm{M}_4(\mathbb{K})$. A última afirmação do Lema segue do fato de que $\mathrm{Prd}_{A,a}(a) = 0$. □

Teorema 2.15 *Se A é uma $\mathbb{K}$–álgebra biquaterniônica com uma involução simplética σ então A contém uma σ–invariante subalgebra de quatérnios.*

Demonstração: Começamos com um elemento simétrico $x \in A \setminus \mathbb{K}$. Pelo Lema anterior, $[\mathbb{K}(x) : \mathbb{K}] = 2$. Escrevemos $\mathbb{K}(x) = \mathbb{K}(a)$, onde $a^2 \in \mathbb{K}$. Pelo Lema 2.11, existe em A um elemento simétrico y tal que $yay^{-1} = -a$, isto é, $ya = -ay$. Novamente pelo Lema anterior, $[\mathbb{K}(y) : \mathbb{K}] = 2$. Como y^2 comuta com a, não podemos ter $[\mathbb{K}(y^2) : \mathbb{K}] = 2$, pois neste caso, $\mathbb{K}(y) = \mathbb{K}(y^2)$, e assim, y também comutaria com a. Portanto $y^2 \in \mathbb{K}$, logo, y e a geram uma álgebra de quatérnios $(a^2, y^2)_{\mathbb{K}}$ em A que é invariante por σ. □

2.6 Involuções Ortogonais

Toda álgebra biquaterniônica admite uma involução ortogonal decomponível, para isto, escrevemos $A = Q_1 \otimes_{\mathbb{K}} Q_2$ e tomamos σ_1 e σ_2 involuções em Q_1 e Q_2, respectivamente. Se $\sigma = \sigma_1 \otimes \sigma_2$ então teremos que

$$\mathrm{Sym}(A, \sigma) = [\mathrm{Sym}(Q_1, \sigma_1) \otimes_{\mathbb{K}} \mathrm{Sym}(Q_2, \sigma_2)] \oplus [\mathrm{Skew}(Q_1, \sigma_1) \otimes_{\mathbb{K}} \mathrm{Skew}(Q_2, \sigma_2)] \quad (2.6)$$

e

$$\mathrm{Skew}(A, \sigma) = [\mathrm{Sym}(Q_1, \sigma_1) \otimes_{\mathbb{K}} \mathrm{Skew}(Q_2, \sigma_2)] \oplus [\mathrm{Skew}(Q_1, \sigma_1) \otimes_{\mathbb{K}} \mathrm{Sym}(Q_2, \sigma_2)]. \quad (2.7)$$

Desta forma, se σ_1 e σ_2 são as involuções canônicas então, pela Proposição 2.3, σ é uma involução ortogonal em A.

Por outro lado, ao contrário do que ocorre com as involuções simpléticas, nem toda involução ortogonal é decomponível. E isto é justamente o que discutiremos nesta seção. Veremos que este problema está ligado ao discriminante da involução que definiremos agora.

Definição 2.16 *Se A é uma $\mathbb{K}$–álgebra central simples e σ é uma involução ortogonal em A então definimos o* ***discriminante*** *de σ por*

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_A(a).\mathbb{K}^{\times 2} \in \mathbb{K}^{\times}/\mathbb{K}^{\times 2},$$

onde a percorre todos os elementos invertíveis tais que $\sigma(a) = -a$.

Obs 2.17 *Seja A uma $\mathbb{K}$–álgebra biquaterniônica de divisão e escrevermos $A = Q_1 \otimes_{\mathbb{K}} Q_2$. Consideremos $Q_1 = [1, i_1, j_1, k_1]$ e $Q_2 = [1, i_2, j_2, k_2]$ com involuções canônicas σ_1 e σ_2, respectivamente. Assim,* $\mathrm{Skew}(Q_1, \sigma_1) = [i_1, j_1, k_1]$ *e* $\mathrm{Skew}(Q_2, \sigma_2) = [i_2, j_2, k_2]$. *Logo,*

$$\mathrm{Skew}(A, \sigma_1 \otimes \sigma_2) = \mathrm{Skew}(Q_1, \sigma_1) \oplus \mathrm{Skew}(Q_2, \sigma_2) \quad \text{e}$$

$$\mathrm{Sym}(A, \sigma_1 \otimes \sigma_2) = \mathbb{K} \oplus \mathrm{Skew}(Q_1, \sigma_1) \otimes_{\mathbb{K}} \mathrm{Skew}(Q_2, \sigma_2).$$

Lema 2.18 *Com a notação da observação acima, para todo* $a = v_1 + v_2 \in \mathrm{Skew}(A, \sigma_1 \otimes \sigma_2)$*, com* $v_i \in \mathrm{Skew}(Q_i, \sigma_i)$ *nós temos* $v_i^2 \in \mathbb{K}$ *e*

$$\mathrm{Nrd}_A(a) = (v_1^2 - v_2^2)^2 \in \mathbb{K}^2.$$

Demonstração: Como v_1 e v_2 são quatérnios puros, já temos que $v_1^2, v_2^2 \in \mathbb{K}$. Como $v_1 v_2 = v_2 v_1$, $\mathbb{L} = \mathbb{K}(v_1, v_2)$ é um subcorpo maximal de A. E mais, $\mathbb{L}$ é uma extensão galoisiana de $\mathbb{K}$ com grupo de Galois $\mathbb{Z}_2 \times \mathbb{Z}_2$, com geradores $\sigma_1 \otimes 1$ e $1 \otimes \sigma_2$. Assim, a ação pelo grupo de Galois em a resulta em $\{v_1 + v_2, v_1 - v_2, -v_1 + v_2, -v_1 - v_2\}$. Portanto, pela Proposição 1.5,

$$\mathrm{Nrd}_A(a) = N_{\mathbb{L}/\mathbb{K}}(a) = (v_1 + v_2)(v_1 - v_2)(-v_1 + v_2)(-v_1 - v_2) = (v_1^2 - v_2^2)^2 \in \mathbb{K}^2.$$

□

Lema 2.19 *Ainda com a notação da observação 2.17, se* τ_i *é uma involução ortogonal em* Q_i *e* $\tau = \tau_1 \otimes \tau_2$ *então* $\mathrm{disc}(\tau) = 1$.

Demonstração: Como τ_i é ortogonal, existe $t_i \in \mathrm{Skew}(Q_i, \sigma_i)$ tal que $\tau_i(r) = t_i \sigma_i(r) t_i^{-1}$, $\forall r \in Q_i$. Assim, para cada $a \otimes b \in A$,

$$\tau(a \otimes b) = \tau_1(a) \otimes \tau_2(b) = (t_1 \sigma_1(a) t_1^{-1}) \otimes (t_2 \sigma_2(b) t_2^{-1}) = (t_1 \otimes t_2)\sigma_1 \otimes \sigma_2(a \otimes b)(t_1 \otimes t_2)^{-1}.$$

Assim, como visto na demonstração da Proposição 2.4, $\mathrm{Skew}(A, \tau) = (t_1 \otimes t_2)\mathrm{Skew}(A, \sigma)$. Logo

$$\begin{aligned} \mathrm{disc}(\tau) &= \mathrm{Nrd}_A(x).\mathbb{K}^2, \forall x \in \mathrm{Skew}(A, \tau)^{\times}; \\ &= \mathrm{Nrd}_A(t_1 \otimes t_2)\mathrm{Nrd}_A(y).\mathbb{K}^2, \forall y \in \mathrm{Skew}(A, \sigma)^{\times}; \\ &= \mathrm{Nrd}_A(t_1 \otimes t_2).\mathbb{K}^2. \end{aligned}$$

A última igualdade segue do lema anterior. Desta forma, falta apenas calcular a norma reduzida de $t_1 \otimes t_2$. Temos que $\mathbb{L} = \mathbb{K}(t_1 \otimes 1, 1 \otimes t_2)$ é um subcorpo maximal de A. Procedendo como na demonstração do lema anterior,

$$\mathrm{Nrd}_A(t_1 \otimes t_2) = N_{\mathbb{L}/\mathbb{K}}(t_1 \otimes t_2) = (t_1 \otimes t_2)(-t_1 \otimes t_2)(t_1 \otimes -t_2)(-t_1 \otimes -t_2) =$$

$$= t_1^4 \otimes t_2^4 = (t_1^2.t_2^2)^2 \in \mathbb{K}^2.$$

Portanto, $\mathrm{disc}(\tau) = 1$. □

Proposição 2.20 *Se A é uma álgebra biquaterniônica de divisão e τ é uma involução ortogonal decomponível então* $\mathrm{disc}(\tau) = 1$.

Demonstração: Seja $A = Q_1 \otimes_{\mathbb{K}} Q_2$ e $\tau = \tau_1 \otimes \tau_2$. Se τ é ortogonal então segue das equações 2.6 e 2.7 que τ_1 e τ_2 devem ser do mesmo tipo. Se τ_1 e τ_2 são ambas simpléticas, então τ_i é justamente a involução canônica de Q_i. Assim, pelo Lema 2.18, $\mathrm{Nrd}_A(a) \in \mathbb{K}^2$, $\forall a \in \mathrm{Skew}(A, \tau)$, logo, $\mathrm{disc}(\tau) = 1$. Se τ_1 e τ_2 são ambas ortogonais então o resultado segue do Lema 2.19. □

O resultado acima diz que para uma involução ortogonal não ser decomponível, basta encontrarmos uma elemento anti-simétrico cuja norma reduzida não seja um quadrado. Entretanto, não me parece tão natural encontrar tal elemento. Vejamos então um resultado que simplifica esse trabalho.

Teorema 2.21 *Seja A uma álgebra biquaterniônica sobre $\mathbb{K}$ e $\mathbb{L}$ um subcorpo maximal de A contendo uma extensão quadrática de $\mathbb{K}$. Então existe uma involução ortogonal de A que é a identidade em $\mathbb{L}$ e de discriminante 1.*

Demonstração: Como $\mathbb{L}$ contém uma extensão quadrática $\mathbb{K}$, nós escolhemos $a \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(a)$ e $[\mathbb{K}(a) : \mathbb{K}(a^2)] = 2$. Seja $\mathbb{L}_1 = \mathbb{K}(a^2) = \mathbb{K}(\sqrt{d})$ e consideremos $B = \mathcal{C}_A\mathbb{L}_1$, que é uma $\mathbb{L}_1$–álgebra de quatérnios. Pelo Lema 2.11, existe em A uma involução τ que restrita a $\mathbb{L}_1$ é o automorfismo não trivial. Assim, segue do Lema 2.10 que existe em A uma subalgebra de quatérnios H_1 tal que $B = H_1 \otimes_{\mathbb{K}} \mathbb{L}_1$ e $A = H_1 \otimes_{\mathbb{K}} H_2$, onde $H_2 = \mathcal{C}_A H_1$.

Como $a \in \mathbb{L} \subseteq B$, podemos escrever $a = x \otimes 1 + y \otimes \sqrt{d}$, onde $x, y \in H_1$. Como

$$a^2 = (x \otimes 1 + y \otimes \sqrt{d})^2 = (x^2 + dy^2) \otimes 1 + (xy + yx) \otimes \sqrt{d}$$

está em $\mathbb{K}(\sqrt{d})$, devemos ter $xy + yx \in \mathbb{K}$. Se x e y comutam então $\mathbb{K}(x, y)$ é um subcorpo maximal de H_1, pois, caso contrário, teríamos $\mathbb{K}(x, y) = \mathbb{K}$ e $\mathbb{L} = \mathbb{K}(a) = \mathbb{K}(\sqrt{d})$, contradizendo o fato de que $\mathbb{L}$ é maximal. Assim, pela Proposição 2.6 podemos construir uma involução σ_1 em H_1 que é a identidade em $\mathbb{K}(x, y)$ e outra involução σ_2 em H_2 que é a identidade em $\mathbb{K}(\sqrt{d})$. Então $\sigma = \sigma_1 \otimes \sigma_2$ é uma involução ortogonal em A, pois σ_1 e σ_2 são ortogonais. Além disso, como $\sigma(a) = a$, σ é a identidade em $\mathbb{L}$ e pelo Lema 2.19, $\mathrm{disc}(\sigma) = 1$. Por outro lado, se x e y não comutam então $\{1, x, y, xy\}$ forma uma $\mathbb{K}$–base de H_1. Se escrevermos $xy + yx = \lambda \in \mathbb{K}$ então

$$x^2y + xyx = x\lambda = \lambda x = xyx + yx^2 \quad \text{e}$$

$$yxy + y^2 = y\lambda = \lambda y = xy^2 + yxy.$$

Assim, $x^2y = yx^2$ e $y^2x = xy^2$. Isto implica que x^2 e y^2 comutam com todos os elementos de H_1, e daí, $x^2, y^2 \in \mathbb{K}$. Portanto x e y são quatérnios puros. Pela Proposição 2.8, existe uma involução σ_1' em H_1, tal que $\sigma_1'(x) = x$ e $\sigma_1'(y) = y$. Desta forma, $\sigma = \sigma_1' \otimes \sigma_2$ é uma involução ortogonal em A que satisfaz $\sigma(a) = a$ e $\mathrm{disc}(\sigma) = 1$. □

Podemos então exibir uma $\mathbb{K}$–álgebra biquaterniônica de divisão A que tem uma involução não decomponível. Esta construção ficará mais clara depois que falarmos de álgebras cíclicas no capítulo 4. Por hora, considere que A contém como subcorpo maximal que é uma extensão galoisiana cíclica $\mathbb{L} = \mathbb{K}(u)$ com grupo de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \langle\rho\rangle$. Além disso, considere que $u = \sqrt{e + f\sqrt{d}}$ e $\rho(\sqrt{e + f\sqrt{d}}) = \sqrt{e - f\sqrt{d}}$, onde $e, f \in \mathbb{K}$, $d \in \mathbb{K}^\times \backslash \mathbb{K}^{\times 2}$ e $d(e^2 - df^2)$ é um quadrado em $\mathbb{K}$. Desta forma,

$$\mathrm{Nrd}_A(u) = N_{\mathbb{L}/\mathbb{K}}(u) = (\sqrt{e + f\sqrt{d}})(\sqrt{e - f\sqrt{d}})(-\sqrt{e + f\sqrt{d}})(-\sqrt{e - f\sqrt{d}}) =$$

$$= (e + f\sqrt{d})(e - f\sqrt{d}) = e^2 - f^2 d.$$

Nestas condições, como $\mathbb{L}$ contém um subcorpo quadrático $\mathbb{K}(\sqrt{d})$, pelo Teorema anterior, existe em A uma involução ortogonal σ de discriminante 1 e que é a identidade em $\mathbb{L}$. Assim, se definirmos $\tau = \imath_u \circ \sigma$, como $\sigma(u) = u$, teremos que τ é uma involução ortogonal em A e $\mathrm{Skew}(A, \tau) = u\mathrm{Skew}(A, \sigma)$. Segue que:

$$\begin{aligned}
\mathrm{disc}(\tau) &= \mathrm{Nrd}_A(x).\mathbb{K}^2, \forall x \in \mathrm{Skew}(A, \tau)^\times; \\
&= \mathrm{Nrd}_A(u)\mathrm{Nrd}_A(y).\mathbb{K}^2, \forall y \in \mathrm{Skew}(A, \sigma)^\times; \\
&= \mathrm{Nrd}_A(u)\mathrm{disc}(\sigma); \\
&= (e^2 - df^2)\mathbb{K}^2; \\
&= d\mathbb{K}^2.
\end{aligned}$$

Portanto, o discriminante de τ não é trivial e conseqüentemente, τ não é decomponível.

No capítulo 4, veremos que as condições impostas ao longo da construção sobre o subcorpo maximal $\mathbb{L}$ valem em geral. Com isso, conseguiremos que toda álgebra biquaterniônica de divisão cíclica admite uma involução ortogonal não decomponível.

Capítulo 3

Álgebras Biquaterniônicas II (Formas Quadráticas)

Como vimos capítulo 1, a função norma de um quatérnio define uma forma quadrática de dimensão 4 e dela podemos classificar as álgebras de quatérnios. Desta forma, desejamos obter resultados análogos aos teoremas 1.12 e 1.13, de tal forma a podermos decidir, através de formas quadráticas, quando um álgebra biquaterniônica é de divisão e quando duas destas álgebras são isomorfas. Ao final no capítulo, vamos discutir a existência de álgebras biquaterniônicas sobre um corpo e veremos que no caso do corpo ser não formalmente real, este problema está relacionado com o u–invariante do corpo.

3.1 Invariantes de Formas Quadráticas

Nesta seção, definiremos e estabeleceremos alguns resultados sobre invariantes de formas quadráticas, a saber, o discriminante, o invariante de Hasse e o invariante de Witt. Ao longo deste capítulo, vamos escrever apenas (a, b) para denotar a classe da álgebra de quatérnios $(a, b)_{\mathbb{K}}$ no grupo de Brauer $\mathrm{Br}(\mathbb{K})$. Além disso, escrevemos $\mathrm{Br}_2(\mathbb{K})$ como o subgrupo do grupo de Brauer formado pelos elemento de ordem menor ou igual a dois.

Definição 3.1 *Para uma n-forma ϕ o discriminante $d(\phi)$ é definido por*

$$d(\phi) = (-1)^{\frac{n(n-1)}{2}}\det(\phi) \in \mathbb{K}^{\times}/\mathbb{K}^{\times 2}.$$

Podemos reformular a definição acima escrevendo $d(\phi) = (-1)^n\det(\phi)$, onde $\dim(\phi) = 2n$ ou $2n+1$. Além disso, como veremos na proposição abaixo, o discriminante independe da escolha do representante da classe no anel de Witt.

Proposição 3.2 *A aplicação $d : W\mathbb{K} \to \mathbb{K}^{\times}/\mathbb{K}^{\times 2}$ está bem definida.*

Demonstração: Primeiramente notamos que o discriminante de uma forma hiperbólica é 1, pois, se $\phi = n \times \langle 1, -1\rangle$ então $\dim(\phi) = 2n$ e assim, $d(\phi) = (-1)^n \det(\phi) = (-1)^n(\det(\langle 1, -1\rangle))^n = (-1)^n(-1)^n = 1$. Sendo assim, se ϕ é uma n–forma e $\phi = \psi \perp k \times \langle 1, -1\rangle = \psi \perp h$ é a decomposição de Witt para ϕ então $n = m + 2k$, onde $m = \dim(\psi)$. Sendo assim,

$$\begin{aligned} d(\phi) &= (-1)^{\frac{n(n-1)}{2}} \det(\phi) \\ &= (-1)^{\frac{(m+2k)(m+2k-1)}{2}} \det(\phi)\det(h) \\ &= (-1)^{\frac{m(m-1)}{2}} (-1)^{\frac{2k(2k-1)}{2}} (-1)^{2mk} \det(\phi)\det(h) \\ &= (-1)^{\frac{m(m-1)}{2}} (-1)^{\frac{2k(2k-1)}{2}} \det(\phi)\det(h) \\ &= d(\psi)d(h) \\ &= d(\psi). \end{aligned}$$

Portanto, o discriminante depende apenas da forma anisotrópica dada pela decomposição de Witt. □

Vale notar que esta aplicação não é em geral um homomorfismo. Por exemplo, $d(\langle 1\rangle) = 1$ mas $d(\langle 1\rangle \perp \langle 1\rangle) = -1$. Entretanto, se nos restringirmos ao ideal fundamental $I\mathbb{K}$ visto como um subgrupo aditivo de $W\mathbb{K}$ temos o seguinte resultado:

Proposição 3.3 $I\mathbb{K}/I^2\mathbb{K} \cong \mathbb{K}^{\times}/\mathbb{K}^{\times 2}$.

Demonstração: Consideremos a aplicação $d : I\mathbb{K} \to \mathbb{K}^{\times}/\mathbb{K}^{\times 2}$. Se tomarmos uma $2n$–forma ϕ e uma $2m$–forma ψ em $I\mathbb{K}$ então

$$d(\phi \perp \psi) = (-1)^{n+m}\det(\phi \perp \psi) = (-1)^n(-1)^m\det(\phi)\det(\psi) = d(\phi)d(\psi)$$

e $d(-\phi) = (-1)^n\det(-\phi) = (-1)^n\det(\phi) = d(\phi)$. Além disso, $d(\langle 1, -1\rangle) = 1$ e $d(\langle 1, -a\rangle) = a, \forall a \in \mathbb{K}^{\times}/\mathbb{K}^{\times 2}$. Portanto, d é um homomorfismo sobrejetivo de grupos. Se $\psi \in I^2\mathbb{K}$ então

$$\psi = \langle 1, a_1, b_1, a_1b_1\rangle \perp \ldots \perp \langle 1, a_n, b_n, a_nb_n\rangle,$$

e assim,

$$d(\psi) = \prod_{i=1}^{n} d(\langle 1, a_i, b_i, a_ib_i\rangle) = 1.$$

Agora observe que

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

Desta forma, toda forma $\phi \in I\mathbb{K}$ pode ser escrita como $\phi = \langle 1,x\rangle \perp \psi$ tal que $\psi \in I^2\mathbb{K}$. Sendo assim , se $d(\phi) = 1$ então $d(\phi) = d(\langle 1,x\rangle)d(\psi) = d(\langle 1,x\rangle) = -x = 1$, logo, $x = -1$ em $\mathbb{K}^\times/\mathbb{K}^{\times 2}$ e $\phi = \langle 1,x\rangle \perp \psi = \langle 1,-1\rangle \perp \psi = \psi$. Portanto, o ideal $I^2\mathbb{K}$ é precisamente o $\ker(d)$ e $I\mathbb{K}/I^2\mathbb{K} \cong \mathbb{K}^\times/\mathbb{K}^{\times 2}$. □

Segue da proposição acima que o ideal $I^2\mathbb{K}$ é formado pelas classes das formas pares de discriminante 1.

Definição 3.4 *Se $\phi = \langle a_1,\ldots,a_n\rangle$ é uma n–forma então definimos o* ***invariante de Hasse*** *$s(\phi)$ pela seguinte fórmula:*

$$s(\phi) = \prod_{i<j}(a_i,a_j) \in \mathrm{Br}_2(\mathbb{K}).$$

Para $n = 1$ definimos $s(\phi) = 1$.

Proposição 3.5 *Se ϕ e ψ são duas formas quadráticas então*

$$s(\phi \perp \psi) = s(\phi)s(\psi)(\det(\phi),\det(\psi)).$$

Demonstração: Escrevendo $\phi = \langle a_1,\ldots,a_n\rangle$ e $\psi = \langle a_{n+1},\ldots,a_{n+m}\rangle$ teremos que

$$s(\phi \perp \psi) = \prod_{i,j=1;i<j}^{n+m}(a_i,a_j) = \prod_{i,j=1;i<j}^{n}(a_i,a_j)\prod_{i,j=n+1;i<j}^{m}(a_i,a_j)\prod_{i=1}^{n}\prod_{j=n+1}^{n+m}(a_i,a_j),$$

como

$$\prod_{i=1}^{n}\prod_{j=n+1}^{n+m}(a_i,a_j) = \prod_{i=i}^{n}(a_i,\prod_{j=n+1}^{n+m}a_j) = \prod_{i=i}^{n}(a_i,\det(\psi)) =$$

$$= (\prod_{i=i}^{n}a_i,\det(\psi)) = (\det(\phi),\det(\psi)),$$

segue que $s(\phi \perp \psi) = s(\phi)s(\psi)(\det(\phi),\det(\psi))$. □

Proposição 3.6 *Se ϕ e ψ são duas formas quadráticas satisfazendo $\phi \cong \psi$ então $s(\phi) = s(\psi)$.*

Demonstração: Se $\phi = \langle a_1, \dots a_n\rangle$, $\psi = \langle b_1, \dots b_n\rangle$ e $\phi \cong \psi$ então, pelo Teorema da Cadeia Equivalência de Witt, $\phi \approx \psi$, isto é, $\phi \cong \langle a, b, a_3, \dots, a_n\rangle$ e $\psi \cong \langle c, d, a_3, \dots, a_n\rangle$, onde $\langle a, b\rangle \cong \langle c, d\rangle$. Pelo Corolário 1.14, $ab = cd$ em $\mathbb{K}^\times/\mathbb{K}^{\times 2}$ e $(a, b)_\mathbb{K} \cong (c, d)_\mathbb{K}$. Sendo assim, segue da proposição anterior que

$$\begin{aligned} s(\phi) &= s(\langle a, b\rangle)s(\langle a_3, \dots, a_n\rangle)(ab, a_3 \dots a_n) \\ &= (a, b)s(\langle a_3, \dots, a_n\rangle)(ab, a_3 \dots a_n) \\ &= (c, d)s(\langle a_3, \dots, a_n\rangle)(cd, a_3 \dots a_n) \\ &= s(\langle c, d\rangle)s(\langle a_3, \dots, a_n\rangle)(cd, a_3 \dots a_n) \\ &= s(\psi). \end{aligned}$$

□

Entretanto, s não está bem definida no anel de Witt, pois temos que $s(\langle 1, -1\rangle) = 1$ e $s(\langle 1, -1, 1, -1\rangle) = (-1, -1)$, mas sob os racionais, $(-1, -1) \neq 1$. Para corrigir esse problema temos a seguinte definição:

Definição 3.7 *Definimos o* ***invariante de Witt*** $c(\phi)$ *de uma n–forma ϕ pelas seguintes fórmulas:*

$$\begin{aligned} c(\phi) &:= s(\phi) && \text{se } n \equiv 1, 2 (\mathrm{mod}\, 8) \\ &:= s(\phi)(-1, -\det(\phi)) && \text{se } n \equiv 3, 4 (\mathrm{mod}\, 8) \\ &:= s(\phi)(-1, -1) && \text{se } n \equiv 5, 6 (\mathrm{mod}\, 8) \\ &:= s(\phi)(-1, \det(\phi)) && \text{se } n \equiv 7, 8 (\mathrm{mod}\, 8). \end{aligned}$$

Proposição 3.8 *A aplicação $c : W\mathbb{K} \to \mathrm{Br}_2(\mathbb{K})$ está bem definida.*

Demonstração: Seja ϕ uma n–forma. Suponhamos que $\dim(\phi) \equiv 5, 6 (\mathrm{mod}\, 8)$. Neste caso, $\dim(\phi \perp \langle 1, -1\rangle) \equiv 7, 8 (\mathrm{mod}\, 8)$. Assim,

$$\begin{aligned} c(\phi \perp \langle 1, -1\rangle) &= s(\phi \perp \langle 1, -1\rangle)(-1, \det(\phi \perp \langle 1, -1\rangle) \\ &= s(\phi)s(\langle 1, -1\rangle)(\det(\phi), \det(\langle 1, -1\rangle)(-1, \det(\phi)\det(\langle 1, -1\rangle) \\ &= s(\phi)(1, -1)(\det(\phi), -1)(-1, -\det(\phi)) \\ &= s(\phi)(\det(\phi), -1)(-1, \det(\phi))(-1, -1) \\ &= s(\phi)(-1, -1) \\ &= c(\phi). \end{aligned}$$

A verificação de que $c(\phi \perp \langle 1, -1\rangle) = c(\phi)$ nos demais casos é análoga. Segue daí que $c(\phi \perp h) = c(\phi)$ para qualquer forma hiperbólica h. Portanto, $c(\phi)$ só depende classe de Witt equivalência de ϕ. □

3.2 Teoremas de Classificação

Nesta seção vamos utilizar os invariantes definidos na seção anterior para classificar formas quadráticas de dimensão baixa (menor ou igual a 10). A partir desses resultados vamos obter os dois principais teoremas deste capítulo. O leitor deve ficar atento, pois ao longo dessa seção, estaremos utilizando a todo momento as equações do Corolário 1.15 sem citá-lo, a fim de não nos tornarmos repetitivos. Começamos então com um teorema de classificação para formas quadráticas de dimensão 3.

Teorema 3.9 *Sejam ϕ e ψ duas formas quadráticas de dimensão $\leq$ 3. Se* $\dim(\phi) = \dim(\psi)$, $\det(\phi) = \det(\psi)$ *e* $s(\phi) = s(\psi)$ *então* $\phi \cong \psi$.

Demonstração: Para dimensão 1, $\phi \cong \langle \det(\phi)\rangle \cong \langle \det(\psi)\rangle \cong \psi$. Se ϕ e ψ são duas formas binárias então o resultado segue imediatamente do Corolário 1.14. Agora, sejam $\phi = \langle a, b, c\rangle$ e $\psi = \langle d, e, f\rangle$. Estamos assumindo que $\det(\phi) = \det(\psi)$, assim, $abc = def$. Daí obtemos que

$$\phi' = -abc\phi = \langle -a^2bc, -ab^2c, -abc^2\rangle \cong \langle -bc, -ac, -ab\rangle \cong \langle x, y, -xy\rangle \quad \text{e}$$

$$\psi' = -def\psi = \langle -d^2ef, -de^2f, -def^2\rangle \cong \langle -ef, -df, -de\rangle \cong \langle z, w, -zw\rangle,$$

onde $x = -bc$, $y = -ac$, $z = -ef$ e $w = -df$. Note agora que para uma 3–forma $\varphi = \langle a, b, c\rangle$ e $\lambda \in \mathbb{K}^\times$ temos que

$$\begin{aligned} s(\lambda\varphi) &= s(\langle \lambda a, \lambda b, \lambda c\rangle) \\ &= (\lambda a, \lambda b)(\lambda a, \lambda c)(\lambda b, \lambda c) \\ &= (\lambda a, -ab)(ab, \lambda c) \\ &= (\lambda a, -1)(\lambda a, ab)(ab, \lambda c) \\ &= (\lambda, \lambda)(a, a)(ab, ac) \\ &= (\lambda, \lambda)(a, b)(a, c)(b, c) \\ &= s(\varphi)(\lambda, \lambda). \end{aligned}$$

Sendo assim,

$$s(\phi') = s(\lambda\phi) = (\lambda, \lambda)s(\phi) = (\lambda, \lambda)s(\psi) = s(\lambda\psi) = s(\psi').$$

Por outro lado, $s(\phi') = (x, y)(x, -xy)(y, -xy) = (x, y)(xy, -xy) = (x, y)$ e, pela mesma razão, $s(\psi') = (z, w)$. Como duas álgebras de quatérnios Brauer equivalentes são obrigatoriamente isomorfas, então $(x, y)_{\mathbb{K}} \cong (z, w)_{\mathbb{K}}$. Segue do Teorema 1.12 que $\langle x, y, -xy\rangle \cong \langle z, w, -zw\rangle$. Portanto, $\phi \cong \psi$. □

Corolário 3.10 *Uma 3–forma φ é isotrópica se, e somente se, $c(\varphi) = 1$.*

Demonstração: Se φ é isotrópica então, pelo Teorema da Decomposição de Witt, $\varphi \cong \langle 1, -1, a\rangle$, logo,

$$c(\varphi) = s(\varphi)(-1, -\det(\varphi)) = (1, -1)(1, a)(-1, a)(-1, a) = 1.$$

Reciprocamente, suponhamos que $c(\varphi) = 1$. Fazendo $\varphi = \langle a, b, c\rangle$ e $\varphi' = \langle 1, -1, -abc\rangle$, temos que $\det(\varphi) = abc = \det(\varphi')$ e

$$s(\varphi') = (-1, -abc) = (-1, -\det(\varphi)) = s(\varphi),$$

pois, $c(\varphi) = s(\varphi)(-1, -abc) = 1$. Portanto, pelo Teorema 3.9, $\varphi \cong \varphi'$, logo, φ é isotrópica. □

O teorema 3.9 não pode ser estendido para formas de dimensão 4. Por exemplo, sobre os racionais, se tomarmos $\phi = \langle 1, 1, 1, 1\rangle$ e $\psi = \langle -1, -1, -1, -1\rangle$ temos que $\det(\phi) = 1 = \det(\psi)$ e $s(\phi) = s(\psi)$, entretanto, ϕ e ψ não são isométricas. Em contrapartida, temos alguns importantes resultados que classificam essas formas quadráticas, como veremos agora.

Teorema 3.11 *Sejam ϕ e ψ duas 4–formas satisfazendo $d(\phi) = d(\psi) = 1$ e $c(\phi) = c(\psi)$. Então $\phi = \lambda\psi$, para algum $\lambda \in \mathbb{K}^{\times}$.*

Demonstração: Escrevendo $\phi = \langle x, y, z, w\rangle$ teremos que $d(\phi) = (-1)^2 \det(\phi) = xyzw = 1$ em $\mathbb{K}^{\times}/\mathbb{K}^{\times 2}$. Desta forma,

$$\phi \cong \langle x^2yzw, xy^2zw, xyz^2w, xyzw^2\rangle \cong \langle yzw, xzw, xyw, xyz\rangle \cong \langle a, b, c, abc\rangle,$$

onde, $a = yzw$, $b = xzw$ e $c = xyw$. Do mesmo modo, podemos escrever $\psi \cong \langle d, e, f, def\rangle$. Agora, para cada $\lambda \in \mathbb{K}^\times$, temos:

$$\begin{aligned} c(\lambda\psi) &= s(\lambda\psi)(-1, -\det(\lambda\psi)) \\ &= (\lambda a, \lambda a)(\lambda b, ab)(\lambda c, \lambda abc)(-1,-1) \\ &= (\lambda a, -1)(\lambda b, ab)(\lambda c, \lambda c)(\lambda c, ab)(-1,-1) \\ &= (\lambda a, -1)(bc, ab)(\lambda c, -1)(-1,-1) \\ &= (ac, -1)(b, ab)(c, abc)(-1,-1) \\ &= c(\psi). \end{aligned}$$

Escrevendo $\phi \cong \langle a\rangle \perp \phi'$ e $ad\psi = \langle a, ade, adf, aef\rangle \cong \langle a\rangle \perp \psi'$ teremos que $\det(\phi') = a = \det(\psi')$, $c(\phi) = s(\phi)(-1,-1) = s(\phi')(a,a)(-1,-1)$ e $c(ad\psi) = s(ad\psi)(-1,-1) = s(\psi')(a,a)(-1,-1)$. Como $c(ad\psi) = c(\phi)$, então $s(\phi') = s(\psi')$. Pelo Teorema 3.9, $\phi' \cong \psi'$, e assim, $\phi \cong ad\psi$. □

Proposição 3.12 *Seja ϕ uma 4–forma com discriminante d e $\mathbb{L} = \mathbb{K}(\sqrt{d})$. Então ϕ é isotrópica se, e somente se, $\phi_{\mathbb{L}}$ é isotrópica.*

Demonstração: É claro que se ϕ é isotrópica então $\phi_{\mathbb{L}}$ é isotrópica. Reciprocamente, se d é um quadrado então $\mathbb{L} = \mathbb{K}$, e nada temos a fazer. Suponhamos então que $d \notin \mathbb{K}^{\times 2}$ e que $\phi_{\mathbb{L}}$ é isotrópica. Se ϕ fosse anisotrópica então teríamos, pela Proposição 1.7, que $\phi \cong \langle a, -ad\rangle \perp \langle x, y\rangle$ para alguns a, x, $y \in \mathbb{K}^\times$. Sendo assim,

$$d = \det(\phi) = -dxy \Rightarrow xy = -1 \Rightarrow \langle x, y\rangle \cong \langle x, -x\rangle.$$

Assim, $\langle x, y\rangle$ é um plano hiperbólico e ϕ é isotrópica. □

Teorema 3.13 *Seja ϕ uma 4–forma sobre $\mathbb{K}$ com discriminante d e $\mathbb{L} = \mathbb{K}(\sqrt{d})$. Então valem:*

(i) ϕ é hiperbólica se, e somente se, $d(\phi) = 1$ e $c(\phi) = 1$.

(ii) ϕ é isotrópica se, e somente se, $c(\phi_{\mathbb{L}}) = 1$.

Demonstração: *(i)* Suponhamos inicialmente que $d(\phi) = 1$ e $c(\phi) = 1$. Sendo assim, podemos escrever $\phi \cong \langle a, b, c, abc\rangle$ e

$$\begin{aligned} c(\phi) &= (a,a)(b,ab)(c,abc)(-1,-1) \\ &= (a,-1)(b,-1)(a,b)(c,-ab)(-1,-1) \\ &= (a,-b)(-b,-b)(c,-ab) \\ &= (-ab,-ac). \end{aligned}$$

Como $c(\phi) = (-ab,-ac) = 1$, pelo Teorema 1.13, a forma $\langle 1, ab, ac, bc\rangle$ é hiperbólica, logo $\phi \cong a\langle 1, ab, ac, bc\rangle$ é hiperbólica. Reciprocamente, se ϕ é hiperbólica então, é claro que $d(\phi) = 1$ e $c(\phi) = 1$.

(ii) Se ϕ é isotrópica então $\phi \cong \langle 1, -1, x, y\rangle$. Sendo assim, $d(\phi) = -xy$ e

$$\begin{aligned} c(\phi) &= (1,-xy)(-1,xy)(x,y)(-1,-1) \\ &= (-1,x)(-1,y)(x,y)(-1,-1) \\ &= (-1,-y)(x,-y) \\ &= (-x,-y). \end{aligned}$$

Em $\mathrm{Br}(\mathbb{L})$, $(-x,-y) = (-x,-y(-xy)) = (-x,x)$, e assim, $c(\phi_{\mathbb{L}}) = 1$. Suponhamos agora que $c(\phi_{\mathbb{L}}) = 1$. Como $d(\phi_{\mathbb{L}}) = 1$ em $\mathbb{L}^{\times}/\mathbb{L}^{\times 2}$, segue da parte *(i)* que $\phi_{\mathbb{L}}$ é hiperbólica. Pela Proposição 3.12, ϕ é isotrópica. □

Veremos agora um resultado semelhante ao teorema anterior para formas de dimensão 6.

Teorema 3.14 *Se ϕ é uma 6–forma sobre $\mathbb{K}$ com discriminante 1 então:*

(i) ϕ é hiperbólica se, e somente se, $c(\phi) = 1$

(ii) Se $c(\phi)$ é a classe de uma álgebra de quatérnios $(a,b)_{\mathbb{K}}$ então ϕ é isotrópica.

Demonstração: *(i)* Se ϕ é hiperbólico então um cálculo simples mostra que $c(\phi) = 1$. Reciprocamente, suponhamos que $c(\phi) = 1$. Desta forma, $s(\phi) = c(\phi)(-1,-1) = (-1,-1)$. Como $d(\phi) = 1$, podemos escrever $\phi \cong \langle a, b, c, d, e, -abcde\rangle$. Agora escrevemos

$\phi = \psi \perp (-\psi')$, onde $\psi = \langle a, b, c\rangle$ e $\psi' = \langle -d, -e, abcd\rangle$. Sendo assim,

$$\begin{aligned} s(\phi) &= s(\psi)(a, -abc)(b, -abc)(c, -abc)s(-\psi') \\ &= s(\psi)(a, bc)(b, ac)(c, ab)s(-\psi') \\ &= s(\psi)(a, b)(a, c)(b, a)(b, c)(c, a)(c, b)s(-\psi') \\ &= s(\psi)s(-\psi'). \end{aligned}$$

Como vimos na demonstração do Teorema 3.9, $s(-\psi') = s(\psi')(-1, -1)$. Assim, $s(\psi)s(\psi') = s(\phi)(-1, -1) = 1$. Logo, $s(\psi) = s(\psi')$. Como $\det(\psi) = abc = \det(\psi')$, segue do Teorema 3.9 que $\psi \cong \psi'$. Portanto, $\phi \cong \psi \perp (-\psi')$ é hiperbólica.

(ii) Suponhamos que ϕ é anisotrópica. Seja $\mathbb{L} = \mathbb{K}(\sqrt{-ab})$. Em $\mathrm{Br}(\mathbb{L})$, $c(\phi_{\mathbb{L}}) = (a, b) = (a, b(-ab)) = (a, -a) = 1$. Como $d(\phi) = d(\phi_{\mathbb{L}}) = 1$, temos, pelo parte *(i)* que $\phi_{\mathbb{L}}$ é hiperbólica. Pela Proposição 1.8, $\phi \cong \langle 1, ab\rangle \otimes \psi$. Escrevendo $\psi = \langle x, y, z\rangle$, teremos que $\phi \cong \langle x, y, z, ab, yab, zab\rangle$ e $d(\phi) = -ab = 1$. Assim, $-ab \in \mathbb{K}^{\times 2}$. Portanto, $\mathbb{L} = \mathbb{K}$ e ϕ é hiperbólica, o que é um absurdo. Logo, ϕ é isotrópica. □

Corolário 3.15 *Uma 8–forma ϕ é hiperbólica se, e somente se, é isotrópica, $d(\phi) = 1$ e $c(\phi) = 1$.*

Demonstração: Suponhamos que ϕ é isotrópica, $d(\phi) = 1$ e $c(\phi) = 1$. Desta forma, escrevemos $\phi \cong \langle 1, -1\rangle \perp \psi$. Sendo assim, $1 = d(\phi) = \det(\phi) = -\det(\psi) = d(\psi)$ e

$$\begin{aligned} c(\phi) &= s(\phi)(-1, \det(\psi)) \\ &= (1, -\det(\psi))(-1, \det(\psi))s(\psi)(-1, 1) \\ &= (-1, -1)s(\psi) \\ &= c(\psi). \end{aligned}$$

Portanto, $d(\psi) = 1$ e $c(\psi) = 1$ e, pela parte *(i)* do Teorema 3.14, ψ é hiperbólica. Logo ϕ é hiperbólica. A outra implicação é imediata. □

Corolário 3.16 *Se ϕ é uma 10–forma que satisfaz $d(\phi) = 1$ e $c(\phi) = 1$ então ϕ é isotrópica.*

Demonstração: Como $\det(\phi) = -d(\phi) = -1$, podemos escrever:

$$\phi \cong \langle x, y, z, w\rangle \perp \psi \cong \langle x, y, z, -xyz\det(\psi)\rangle \perp \psi \cong a\langle 1, b, c, d\rangle \perp \psi$$

Se ψ é isotrópica, nada temos a fazer. Suponhamos então que ψ é anisotrópica e tomamos $\mathbb{L} = \mathbb{K}(\sqrt{bcd})$. Como $\det(\phi) = bcd\det(\psi) = -1$, então $d(\psi_{\mathbb{L}}) = -\det(\psi_{\mathbb{L}}) = bcd = 1$. Além disso, fazendo $\gamma = a\langle 1, b, c, d\rangle$, teremos que

$$c(\phi_{\mathbb{L}}) = s(\phi_{\mathbb{L}}) = s(\psi_{\mathbb{L}})s(\gamma_{\mathbb{L}})(\det(\psi_{\mathbb{L}}), \det(\gamma_{\mathbb{L}}) = s(\psi_{\mathbb{L}})s(\gamma_{\mathbb{L}})(-1, 1) = s(\psi_{\mathbb{L}})s(\gamma_{\mathbb{L}}).$$

Como $\gamma_{\mathbb{L}} \cong a\langle 1, b, c, bc\rangle$, então

$$\begin{aligned} c(\psi_{\mathbb{L}}) &= s(\psi_{\mathbb{L}})(-1,-1) \\ &= s(\gamma_{\mathbb{L}})(-1,-1) \\ &= (a,a)(ab,b)(ac,abc)(-1,-1) \qquad (*) \\ &= (a,-1)(a,b)(b,-1)(ac,-b) \\ &= (a,-b)(-b,1)(c,-b)(a,-b) \\ &= (-b,-c). \end{aligned}$$

Assim, $d(\psi_{\mathbb{L}}) = 1$ e $c(\psi_{\mathbb{L}}) = 1$, logo, pela parte *(ii)* do Teorema 3.13, $\psi_{\mathbb{L}}$ é isotrópica. Pela Proposição 1.7,

$$\psi \cong \langle e, -e(bcd)\rangle \perp \psi' = e\langle 1, bcd\rangle \perp \psi',$$

e assim,

$$d(\psi') = \det(\psi') = -bcd\det(\psi) = (-bcd)^2 = 1.$$

Logo, $\psi' \cong \langle f, g, h, fgh\rangle = f\langle 1, fg, fh, gh\rangle$. Se escrevermos

$$\varphi = a\langle 1, b, c, d\rangle \perp e\langle 1, -bcd\rangle,$$

teremos que $\phi \cong \varphi \perp \psi'$, $d(\varphi) = -\det(\varphi) = 1$ e

$$c(\phi) = s(\phi) = s(\varphi)s(\psi')(\det(\varphi), \det(\psi')) = s(\varphi)s(\psi')(-1, 1) = s(\varphi)s(\psi') = 1.$$

Assim, pelas equações $(*)$ acima,

$$c(\varphi) = s(\varphi)(-1,-1) = s(\psi')(-1,-1) = (-fg, -fh).$$

Portanto, pelo Teorema 3.13, φ é isotrópica e ϕ também é isotrópica. □

3.3 A forma de Albert

Vamos agora retornar ao estudo das álgebras biquaterniônicas. Como foi visto na seção 3 do capítulo 1, podemos classificar as álgebras de quatérnios $(a,b)_{\mathbb{K}}$ através da sua forma norma $\langle 1,-a,-b,ab\rangle$. Desta maneira, desejamos obter resultados análogos aos Teoremas 1.12 e 1.13, de tal forma, a podermos classificar as álgebra biquaterniônicas por meio de formas quadráticas. Sendo assim, se $A \cong (a,b)_{\mathbb{K}} \otimes_{\mathbb{K}} (c,d)_{\mathbb{K}}$ então definimos uma **forma de Albert** associada a A como sendo a 6-forma $\langle -a,-b,ab,c,d,-cd\rangle$.

Obs 3.17 *Seja ϕ uma forma quadrática do tipo*

$$\phi \cong \langle a,b,c,d,e,-abcde\rangle$$

então,

$$abc\phi \cong \langle bc,ac,ab,abcd,abce,-de\rangle \cong \langle -x,-y,xy,z,w,-zw\rangle,$$

onde $x=-bc$, $y=-ac$, $z=abcd$ e $w=abce$. Portanto, toda 6 forma de discriminante 1 é similar a uma forma de Albert.

Obs 3.18 *A decomposição de uma álgebra biquaterniônica como o produto de duas álgebras de quatérnios não é essencialmente única. Como exemplo, basta tomarmos o corpo dos números racionais que teremos: $(1,1)_{\mathbb{K}} \otimes_{\mathbb{K}} (1,1)_{\mathbb{K}} \cong (-1,-1)_{\mathbb{K}} \otimes_{\mathbb{K}} (-1,-1)_{\mathbb{K}}$, mas $(-1,-1)_{\mathbb{K}} \ncong (1,1)_{\mathbb{K}}$, pois a forma $\langle 1,1,1\rangle$ é anisotrópica. Como também não é única a forma de Albert associada a A. Por exemplo, ainda sob os racionais, é claro que $(-1,-1)_{\mathbb{K}}\otimes_{\mathbb{K}}(1,1)_{\mathbb{K}} \cong (1,1)_{\mathbb{K}}\otimes_{\mathbb{K}}(-1,-1)_{\mathbb{K}}$ mas, $\langle 1,1,1,1,1,-1\rangle$ e $\langle -1,-1,1,-1,-1,-1\rangle$ não são isométricas.*

Mesmo não sendo única, uma forma de Albert é capaz de classificar uma álgebra biquaterniônica à qual está associada, como veremos no resultado abaixo:

Teorema 3.19 *Seja A uma álgebra biquaterniônica e φ uma forma de Albert associada. Então:*

1. *A é cindida se, e somente se, φ é hiperbólica;*
2. *$A \cong \mathrm{M}_2(D)$, onde D é uma álgebra de quatérnios de divisão se, e somente se, φ tem índice de Witt 1;*
3. *A é um anel de divisão se, e somente se, φ é anisotrópica.*

Demonstração: Note que pelo Teorema de Wedderburn e pelo Teorema da Decomposição de Witt, as três situações acima são as únicas que podem ocorrer. Assim, precisamos provar apenas duas delas. Seja $A = (a,b)_{\mathbb{K}} \otimes_{\mathbb{K}} (c,d)_{\mathbb{K}}$ uma álgebra biquaterniônica e $\phi = \langle -a, -b, ab, c, d, -cd\rangle$ uma forma de Albert associada. Note que o invariante de Witt leva essa forma quadrática na classe do grupo de Brauer de A, pois

$$\begin{aligned} c(\phi) &= (-a,a)(-b,-ab)(ab,-1)(c,-c)(d,-cd)(-1,-1) \\ &= (-1,-1)(-1,ab)(b,-ab)(ab,-1)(d,-cd)(-1,-1) \\ &= (b,-ab)(d,-cd) \\ &= (a,b)(c,d). \end{aligned}$$

Como $d(\phi) = 1$, pela parte *(i)* o Teorema 3.13, A é cindida se, e somente se, $c(\phi) = 1$ se, e somente se, ϕ é hiperbólica. Isto prova (1). Para verificar a parte (2), escrevemos $A \cong \mathrm{M}_2(D)$, onde D é uma álgebra de quatérnios de divisão $(a,b)_{\mathbb{K}}$. Como $d(\phi) = 1$ e $c(\phi) = [A] = [B] = (a,b)$, teremos pela parte *(ii)* do Teorema 3.13, que ϕ é isotrópica. Sendo assim, ϕ tem índice de Witt 1, 2 ou 3. Os dois últimos casos não são possíveis pois ϕ seria hiperbólica e daí $c(\phi) = [D] = 1$. Reciprocamente, se ϕ tem índice de Witt 1, então podemos escrever $\phi \cong \langle 1, -1\rangle \perp \psi$, com $\psi \cong \langle a, b, c, abc\rangle$ é anisotrópica. Assim,

$$\begin{aligned} c(\phi) &= (1,-1)(-1,1)(a,a)(b,ab)(c,abc)(-1,-1) \\ &= (a,-1)(b,-a)(c,-ab)(-1,-1) \\ &= (-a,-a)(b,-a)(c,-ab) \\ &= (-a,-ab)(c,-ab) \\ &= (-ac,-ab). \end{aligned}$$

Como $\langle ac, ab, bc\rangle \cong a\langle b, c, abc\rangle$ é anisotrópica, pelo Teorema 1.13, $[A] = c(\phi)$ é a classe de uma álgebra de quatérnios de divisão. □

Para ilustrar o resultado acima, vamos utilizá-lo para construir uma álgebra biquaterniônica de divisão.

Exemplo 3.20 *Consideremos o corpo das funções racionais a quatro variáveis* $\mathbb{K} = \mathbb{F}(x_1, x_2, x_3, x_4)$ *com coeficiente no corpo* $\mathbb{F}$*. Então a álgebra biquaterniônica*

$$A = (x_1, x_2)_{\mathbb{K}} \otimes_{\mathbb{K}} (x_3, x_4)_{\mathbb{K}}$$

é de divisão sobre $\mathbb{K}$*. Suponhamos que* A *não é de divisão. Pelo teorema acima, a forma de Albert associada a* A *é isotrópica, isto é, existem* $a_1, \ldots, a_6$ *não todos nulos em* $\mathbb{K}(x_1, x_2, x_3, x_4)$ *tais que*

$$-x_1a_1^2 - x_2a_2^2 + x_1x_2a_3^2 + x_3a_4^2 + x_4a_5^2 - x_3x_4a_6^2 = 0. \qquad (*)$$

Podemos assumir que $a_1, \ldots, a_6$ *estão* $\mathbb{K}(x_1, x_2, x_3)[x_4]$ *e que algum* a_i *não é divisível por* x_4*. Suponhamos* a_1, a_2, a_3, a_4 *são todos divisíveis por* x_4*. Desta forma,*

$$x_4^2|(-x_1a_1^2 - x_2a_2^2 + x_1x_2a_3^2 + x_3a_4^2) \Rightarrow x_4^2|(x_4a_5^2 - x_3x_4a_6^2) \Rightarrow x_4|(a_5^2 - x_3a_6^2).$$

Como x_4 *não divide* a_5 *ou* a_6*, fazendo* $x_4 = 0$ *obtemos que a equação* $x^2 - a_3y^2$ *admite solução não trivial em* $\mathbb{K}(x_1, x_2, x_3)$*. Mas daí teríamos que* x_3 *é um quadrado em* $\mathbb{K}(x_1, x_2, x_3)$*, o que é um absurdo. Portanto, um dos* a_1, a_2, a_3, a_4 *não é divisível por* x_4*. Fazendo* $x_4 = 0$ *na equação* $(*)$ *obtemos que existem* $b_1, \ldots, b_4$ *não todos nulos em* $\mathbb{K}(x_1, x_2, x_3)$ *tais que*

$$-x_1b_1^2 - x_2b_2^2 + x_1x_2b_3^2 + x_3b_4^2 = 0. \qquad (**)$$

Do mesmo modo, podemos assumir que b_1, b_2, b_3, b_4 *estão todos em* $\mathbb{K}(x_1, x_2)[x_3]$ *e que um deles não é divisível por* x_3*. Daí, se* x_3 *não pode dividir algum dos* a_1, a_2, a_3*, pois, caso contrário, também dividiria* a_4*. Assim, substituindo* $x_3 = 0$ *na equação* $(**)$ *teremos*

$$-x_1c_1^2 - x_2c_2^2 + x_1x_2c_3^2 = 0,$$

onde c_1, c_2, c_2 *não são todos nulos em* $\mathbb{K}(x_1, x_2)$*. Aplicando o mesmo truque, chegaremos que a equação*

$$x_1d_1^2$$

tem solução não trivial em $\mathbb{K}(x_1)$*. Isto de fato é uma contradição. Portanto,*

$$\langle -x_1, -x_2, x_1x_2, x_3, x_4, -x_3x_4 \rangle$$

é anisotrópica e A *é de divisão.*

Vamos agora ver dois resultados imediatos do Teorema 3.19, que também nos ajudarão a classificar as álgebras biquaterniônicas.

Corolário 3.21 *Uma álgebra biquaterniônica* $A = B \otimes_{\mathbb{K}} C$ *não é um anel de divisão se, e somente se, existem* $x, y, z \in \mathbb{K}^{\times}$ *tais que* $B \cong (x, z)_{\mathbb{K}}$ *e* $C \cong (y, z)_{\mathbb{K}}$*. Neste caso, dizemos que as álgebra de quatérnios* B *e* C *são ligadas e* $[A] = (xy, z)$ *no grupo de Brauer* $\mathrm{Br}(\mathbb{K})$

Demonstração: Suponhamos que A não é uma álgebra de divisão. Se $B \cong (a,b)_{\mathbb{K}}$ ou $C \cong (c,d)_{\mathbb{K}}$ é cindida, digamos B, então $B \cong (1,d)_{\mathbb{K}}$. Suponhamos então que B e C são de divisão, desta forma, pelo Teorema 1.13, $\phi \cong \langle -a,-b,ab\rangle$ e $\psi \cong \langle -c,-d,cd\rangle$ são anisotrópicas. Pelo Teorema 3.19, a forma $\langle -a,-b,ab,c,d,-cd\rangle$ é isotrópica, então ψ e ϕ representam um comum valor $-z \in \mathbb{K}^{\times}$. Assim, $\phi \cong \langle -z,-x,v\rangle$ e $\psi \cong \langle -z,-y,u\rangle$. Como $\det(\phi) = \det(\psi) = 1$, obtemos que $\phi \cong \langle -z,-x,xz\rangle$ e $\psi \cong \langle -z,-y,yz\rangle$. Portanto, pelo Teorema 1.12, $B \cong (x,z)_{\mathbb{K}}$ e $C \cong (y,z)_{\mathbb{K}}$. A recíproca é imediata. □

Corolário 3.22 *Sejam B e C duas álgebra de quatérnios de divisão. $A \cong B \otimes_{\mathbb{K}} C$ não é uma álgebra biquaterniônica de divisão se, e somente se, B e C possuem um subcorpo quadrático comum.*

Demonstração: Pelo corolário acima, A não é de divisão se, e somente se, $B \cong (x,z)_{\mathbb{K}}$ e $C \cong (y,z)_{\mathbb{K}}$ se, e somente se, $\mathbb{K}(\sqrt{z})$ é uma extensão quadrática de $\mathbb{K}$ em B e C. □

Uma demonstração independente do resultado acima foi dada pelo próprio Albert [6], numa publicação póstuma.[1]

Como vimos na observação 3.18, $(-1,-1)_{\mathbb{K}} \otimes_{\mathbb{K}} (1,1)_{\mathbb{K}} \cong (1,1)_{\mathbb{K}} \otimes_{\mathbb{K}} (-1,-1)_{\mathbb{K}}$ mas, $\langle 1,1,1,1,1,-1\rangle$ e $\langle -1,-1,1,-1,-1,-1\rangle$ não são isométricas. Entretanto, note que

$$\langle 1,1,1,1,1,-1\rangle \cong -1\langle -1,-1,1,-1,-1,-1\rangle,$$

isto é, as duas forma quadráticas são similares. Veremos agora que este fato é geral.

Teorema 3.23 (Jacobson) *Sejam A e B duas álgebras biquaterniônicas sobre $\mathbb{K}$ e φ_A e φ_B formas de Albert associadas a A e B, respectivamente. Nestas condições, $A \cong B$ se, e somente se, φ_A e φ_B são **similares**, isto é, $\varphi_A \cong \lambda\varphi_B$, para algum λ em $\mathbb{K}^{\times}$. Em particular, duas formas de Albert associadas a uma álgebra biquaterniônica são sempre similares.*

Este teorema foi demonstrado inicialmente por Jacobson [13], utilizando a teoria de normas de Jordan em álgebras centrais simples com involuções. Entretanto, a fim de continuarmos trabalhando com a teoria de formas quadráticas, seguiremos os passos dados por Mammone e Shapiro [23]. De qualquer forma, precisaremos de mais alguns resultados que veremos nas duas seções seguintes.

[1] Professor Albert faleceu em 6 de junho de 1972.

3.4 O Teorema de Pfister

De acordo com o célebre **Teorema de Merkurjev** (Ver [8] ou [34]), se restringirmos a aplicação $c : W\mathbb{K} \to \mathrm{Br}_2(\mathbb{K})$, obtida em 3.8, ao ideal $I^2\mathbb{K}$, então

$$c : I^2\mathbb{K} \to \mathrm{Br}_2(\mathbb{K})$$

é um homomorfismo sobrejetivo de grupos, cujo núcleo é dado por $I^3\mathbb{K}$. Como o ideal $I^2\mathbb{K}$ é aditivamente gerado pelas formas $\langle 1, -a, -b, ab\rangle$ e

$$c(\langle 1, -a, -b, ab\rangle) = (a, b),$$

segue que toda álgebra de expoente 2 é Brauer equivalente a um produto tensorial de álgebras de quatérnios.

De qualquer forma, como estamos interessados apenas em formas quadráticas de dimensão baixa, vamos evitar o uso desse difícil teorema e provar um resultado parcial a esse, que é atribuído a Pfister [25].

Teorema 3.24 (Pfister) *Suponhamos que $\phi \in I^2\mathbb{K}$ e $\dim(\phi) \leq 12$. Se $c(\phi) = 1$ então $\phi \in I^3\mathbb{K}$.*

Demonstração: Pela Proposição 3.3, se $\phi \in I^2\mathbb{K}$ então $\dim(\phi)$ é par $d(\phi) = 1$. Desta forma, se $\dim(\phi) = 2$, 4 ou 6, segue dos Teoremas 3.9, 3.13 e 3.14, respectivamente, que ϕ é hiperbólica e assim, $\phi \in I^3\mathbb{K}$.

Suponhamos agora que $\dim(\phi) = 8$. Se ϕ é isotrópica então, pelo Corolário 3.15, ϕ é hiperbólica. Consideremos então o caso em que ϕ é anisotrópica. Como $\det(\phi) = 1$, escrevemos:

$$\phi \cong \langle a, y\rangle \perp \psi \cong \langle a, a\det(\psi)\rangle \perp \psi \cong \langle a, -ab\rangle \perp \psi,$$

onde, $b = -\det(\psi)$. Se $\mathbb{L} = \mathbb{K}(\sqrt{b})$ teremos que $\phi_{\mathbb{L}}$ é isotrópica. Como $d(\phi_{\mathbb{L}}) = 1$ e $c(\phi_{\mathbb{L}}) = 1$, pelo Corolário 3.15, $\phi_{\mathbb{L}}$ é hiperbólica, logo, $\psi_{\mathbb{L}}$ é isotrópica. Como estamos supondo que ψ é anisotrópica, segue da Proposição 1.7 que $\psi \cong \langle c, -bc\rangle \perp \psi'$. Assim,

$$\phi \cong \langle a, -ab\rangle \perp \langle c, -bc\rangle \perp \psi' \cong \langle a, c\rangle \otimes \langle 1, -b\rangle \perp \psi'.$$

Escrevendo $\phi' = \langle a, -ab\rangle \perp \langle c, -bc\rangle = \langle a, c\rangle \otimes \langle 1, -b\rangle$, teremos que, $\phi \cong \phi' \perp \psi'$ e $d(\psi') = \det(\psi') = d(\psi') = 1$. Além disso,

$$\begin{aligned} c(\phi) &= s(\phi)(-1, \det(\phi)) \\ &= s(\phi')s(\psi')(\det(\phi'), \det(\psi'))(-1, 1) \\ &= s(\phi')s(\psi'), \end{aligned}$$

logo, $s(\phi') = s(\psi')$ e $c(\phi') = s(\phi')(-1, -\det(\phi') = s(\psi')(-1, -\det(\psi') = c(\psi')$. Desta forma, pelo Teorema 3.11, existe $\lambda \in \mathbb{K}^\times$ tal que $\phi' \cong \lambda\psi'$. Portanto,

$$\phi \cong \phi' \perp \psi' \cong \phi' \perp \lambda\phi' \cong \phi' \otimes \langle 1, \lambda\rangle \cong \langle a, c\rangle \otimes \langle 1, -b\rangle \otimes \langle 1, \lambda\rangle \in I^3\mathbb{K}.$$

Se $\dim(\phi) = 10$ então, pelo Corolário 3.16, ϕ é isotrópica. Sendo assim, podemos escrever $\phi \cong \langle 1, -1\rangle\psi$. Como ψ é uma 8–forma que satisfaz

$$d(\psi) = \det(\psi) = -\det(\phi) = d(\phi) = 1$$

e

$$c(\phi) = s(\phi) = (1, -\det(\psi))(-1, \det(\psi))s(\psi) = c(\psi) = 1.$$

Teremos, pelo caso anterior, que $\psi \in I^3\mathbb{K}$. Portanto, $\phi \in I^3\mathbb{K}$.

Resta-nos o caso em que ϕ é uma 12–forma. Se ϕ é isotrópica então $\phi \cong \langle 1, -1\rangle \perp \psi$. Sendo assim, $d(\phi) = \det(\phi) = -\det(\psi) = d(\phi) = 1$ e

$$c(\phi) = s(\phi)(-1, -1) = (1, -1)s(\psi)(-1, -\det(\psi))(-1, -1) = s(\psi) = c(\psi) = 1.$$

Pelo caso anterior, $\psi \in I^3\mathbb{K}$ e assim, $\phi \in I^3\mathbb{K}$. Suponhamos então que ϕ é anisotrópica e escrevemos $\phi \cong \langle a, -ab\rangle \perp \psi$. Se $\mathbb{L} = \mathbb{K}(\sqrt{b})$ então $d(\psi_\mathbb{L}) = -\det(\psi_\mathbb{L}) = b\det(\phi_\mathbb{L}) = b = 1$ e

$$c(\phi_\mathbb{L}) = (a, a)(-a, -1)s(\psi_\mathbb{L})(-1, -1) = s(\psi_\mathbb{L}) = c(\psi_\mathbb{L}).$$

Assim, pelo Corolário 3.16, $\psi_\mathbb{L}$ é isotrópica e pela Proposição 1.7, podemos escrever:

$$\psi \cong \langle c, -cb\rangle \perp \psi', \text{ logo, } \phi \cong \langle a, -ab\rangle \perp \langle c, -cb\rangle \perp \psi'.$$

Como $\det(\psi') = \det(\phi) = 1$, então escrevemos $\psi' \cong \langle e, -ed\rangle \perp \gamma$. Segue que $\det(\psi') = -d\det(\gamma) = 1$, logo $d(\gamma_{\mathbb{K}(\sqrt{d})}) = -\det(\gamma_{\mathbb{K}(\sqrt{d})}) = 1$ e como

$$\phi \cong \langle a, -ab\rangle \perp \langle c, -cb\rangle \perp \langle e, -ed\rangle \perp \gamma,$$

teremos que

$$\begin{aligned}
c(\phi) &= (a, a)(-ab, -b)(c, -cb)(-cb, 1)(e, e)(-ed, -d)s(\gamma)\\
&= (a, -1)(-a, -b)(c, b)(e, -1)(-e, -d)s(\gamma)\\
&= (a, -1)(-a, -1)(-a, b)(c, b)(e, -1)(d, -e)(-1, -e)s(\gamma)\\
&= (-1, -1)(-ac, b)(-1, -1)(d, -e)s(\gamma)\\
&= (-1, -1)(-ac, b)(-1, -1)(d, -e)s(\gamma)\\
&= (-ac, b)(d, -e)s(\gamma).
\end{aligned}$$

Segue daí que

$$c(\gamma_{\mathbb{K}(\sqrt{d})}) = s(\gamma_{\mathbb{K}(\sqrt{d})})(-1, -\det(\gamma_{\mathbb{K}(\sqrt{d})})) = (-ac, b)(d, -e)(-1, d) = (-ac, b).$$

Novamente, pelo Teorema 3.14 e pela Proposição 1.7, teremos que $\gamma_{\mathbb{K}(\sqrt{d})}$ é isotrópica e $\gamma \cong \langle f, -df\rangle \perp \phi_3$. Desta forma, se escrevermos

$$\phi_1 \cong \langle a, c\rangle \otimes \langle 1, -b\rangle \text{ e } \phi_2 \cong \langle e, f\rangle \otimes \langle 1, -d\rangle,$$

teremos que

$$\phi \cong \langle a, -ab\rangle \perp \langle c, -cb\rangle \perp \langle e, -ed\rangle \perp \langle f, -fd\rangle \perp \phi_3 \cong \phi_1 \perp \phi_2 \perp \phi_3.$$

Desta forma, $d(\phi_1) = d(\phi_2) = d(\phi_3) = 1$ e

$$c(\phi_1)c(\phi_2)c(\phi_3) = s(\phi_1)(-1,-1)s(\phi_2)(-1,-1)s(\phi_3)(-1,-1) =$$

$$= s(\phi_1)s(\phi_2)s(\phi_3)(-1,-1) = s(\phi)(-1,-1) = c(\phi) = 1.$$

Sendo assim, se tomarmos $\phi' \cong f\phi_1 \perp (-a)\phi_2 \perp \phi_3$, então $d(\psi') = 1$ e

$$\begin{aligned} c(\phi') &= s(\phi')(-1,-1) \\ &= s(f\phi_1)s(-a\phi_2)s(\phi_3)(-1,-1) \\ &= c(f\phi_1)c(-a\phi_2)c(\phi_3) \\ &= c(\phi_1)c(\phi_2)c(\phi_3) \\ &= 1. \end{aligned}$$

Além disso, como ϕ' é isotrópica, $\phi' \cong \langle 1, -1\rangle \perp \rho$, onde, $d(\rho) = 1$ e $c(\rho) = 1$. Segue do caso de dimensão 10 que $\rho \in I^3\mathbb{K}$, logo, $\phi' \in I^3\mathbb{K}$. Como, em $W\mathbb{K}$,

$$\phi = \phi' \perp \langle 1, f\rangle \otimes \phi_1 \perp \langle 1, a\rangle \otimes \phi_2,$$

concluímos que $\phi \in I^3\mathbb{K}$. □

3.5 Mais sobre formas de dimensão 4

Começamos com o seguinte resultado de Wadsworth [33](Teorema 7).

Teorema 3.25 (Wadsworth) *Sejam ϕ e ϕ' duas 4–forma que representam 1 e com discriminante d e seja $\mathbb{L} = \mathbb{K}(\sqrt{d})$. Nestas condições, se $\phi_{\mathbb{L}} \cong \phi'_{\mathbb{L}}$ então ϕ e ϕ' são similares.*

Demonstração: Suponhamos que $d \notin \mathbb{K}^{\times 2}$, caso contrário, nada teríamos a fazer. Se ϕ é isotrópica então ϕ' também é isotrópica e podemos escrever:

$$\phi \cong \langle 1, -1\rangle \perp \langle a, b\rangle \qquad \text{e} \qquad \phi' \cong \langle 1, -1\rangle \perp \langle c, d\rangle.$$

Assim, $d = -ab = -cd$ e, em $\mathbb{K}^{\times}/\mathbb{K}^{\times 2}$, podemos escrever $\lambda = ac = bd$, logo

$$\lambda\phi \cong \langle \lambda, -\lambda\rangle \perp \langle \lambda a, \lambda b\rangle \cong \langle 1, -1\rangle \perp \langle a^2c, b^2d\rangle \cong \langle 1, -1\rangle \perp \langle c, d\rangle \cong \phi'.$$

Podemos supor então que ϕ e ϕ' são anisotrópicas. Escrevemos $\phi \cong \langle 1\rangle \perp \psi$ e $\phi' \cong \langle 1\rangle \perp \psi'$ e seja $\gamma \cong \psi \perp -\psi'$. Como $\psi_{\mathbb{L}} \cong \psi'_{\mathbb{L}}$, então $\gamma_{\mathbb{L}}$ é hiperbólica. Se γ fosse anisotrópica, pela Proposição 1.8, teríamos $\gamma \cong \langle 1, -d\rangle \otimes \rho$ e daí, $\det(\gamma) = -d$. Por outro lado,

$$\det(\gamma) = \det(\psi)(-\det(\psi')) = -\det(\phi)\det(\phi') = -d^2 = -1,$$

o que não é possível, portanto, γ é isotrópica. Como ψ e ψ' são anisotrópicas, existe $a \in \mathbb{K}^{\times}$, que é representado por ψ e ψ'. Então ficamos com

$$\phi \cong \langle 1, a, b, c\rangle \qquad \text{e} \qquad \phi \cong \langle 1, a, b', c'\rangle.$$

Como $abc = d = ab'c'$ então $c = abd$ e $c' = ab'd$ logo,

$$\phi \cong \langle 1, a, b, abd\rangle \qquad \text{e} \qquad \phi \cong \langle 1, a, b', ab'd\rangle.$$

Seja agora, $\tau \cong \langle 1, a, -bb', -bb'ad\rangle$. Note que $\det(\tau) = d$ e

$$b\tau_{\mathbb{L}} \cong \langle b, ab, -b', -b'ad\rangle \cong \langle b, abd, -b', -b'ad\rangle.$$

Como $\phi_{\mathbb{L}} \perp -\phi'_{\mathbb{L}} \cong \langle 1, a, -1, -a\rangle \perp b\tau_{\mathbb{L}}$ é hiperbólica, assim como $\langle 1, a, -1, -a\rangle$, obtemos que $\tau_{\mathbb{L}}$ é hiperbólica. Se τ fosse anisotrópica, teríamos que $\tau \cong \langle 1, -d\rangle \otimes \sigma$ e $\det(\tau) = 1$. Portanto, τ é isotrópica. Agora, do fato de ϕ ser anisotrópica, segue que $\langle 1, a\rangle$ é anisotrópica, e daí, $\langle 1, a\rangle$ e $\langle bb', bb'ad\rangle$ representam um comum valor $t \in \mathbb{K}^{\times}$. Desta forma, $\langle 1, a\rangle \cong \langle t, x\rangle$ e assim, $a = tx$ e $x = at$ em $\mathbb{K}^{\times}/\mathbb{K}^{\times 2}$, logo $\langle 1, a\rangle \cong \langle t, at\rangle \cong t\langle 1, a\rangle$. Do mesmo modo, $\langle bb', bb'ad\rangle \cong \langle t, y\rangle$, e assim, $ad = ty$ e $y = adt$ em $\mathbb{K}^{\times}/\mathbb{K}^{\times 2}$. Logo

$$\langle bb', bb'ad\rangle \cong \langle t, adt\rangle \cong t\langle 1, ad\rangle \Rightarrow \langle b', b'ad\rangle \cong t\langle b, bad\rangle.$$

Finalmente,

$$\phi' \cong \langle 1, a, b', ab'd\rangle \cong t\langle 1, a, b, abd\rangle \cong t\phi.$$

□

Corolário 3.26 *Sejam ϕ e ϕ' duas 4–forma com discriminante d e seja $\mathbb{L} = \mathbb{K}(\sqrt{d})$. Sendo assim, se $\phi_{\mathbb{L}}$ e $\phi'_{\mathbb{L}}$ são similares então ϕ e ϕ' são similares.*

Demonstração: Supondo que $\det(\phi) = \det(\phi') = d$, podemos escrever

$$\phi \cong \langle a, b, c, abcd\rangle \cong a\langle 1, ab, ac, bcd\rangle \cong a\langle 1, x, y, xyd\rangle \cong a\psi.$$

Do mesmo modo, obtemos $\phi' \cong a'\langle 1, x', y', x'y'd\rangle \cong a'\psi'$. Se $\phi_{\mathbb{L}}$ e $\phi'_{\mathbb{L}}$ são similares então existe $\alpha \in \mathbb{L}^{\times}$ tal que $\phi_{\mathbb{L}} \cong \alpha\phi'_{\mathbb{L}}$, e assim, $\psi_{\mathbb{L}} \cong aa'\alpha\psi'_{\mathbb{L}}$. Note que $\psi_{\mathbb{L}}$ e $\psi'_{\mathbb{L}}$ são formas de Pfister. Como toda forma de Pfister é multiplicativa, segue que duas formas de Pfister similares são isométricas. Daí concluímos que ψ e ψ' cumprem as hipóteses do teorema anterior. Desta forma, existe $\lambda \in \mathbb{K}^{\times}$ tal que $\psi \cong \lambda\psi'$. Assim, $aa'\psi \cong aa'\lambda\psi'$ e daí, $a'\phi \cong a\lambda\phi'$. Portanto, ϕ e ϕ' são similares. □

Proposição 3.27 *Suponhamos que ϕ e ψ são 4–formas satisfazendo $d(\phi) = d(\psi)$ e $c(\phi) = c(\psi)$. Então ϕ e ψ são similares.*

Demonstração: Suponhamos que $d(\phi) = d(\psi) = d$. Se $d = 1$ então o resultado está provado em 3.11. Se $d \neq 1$ então consideramos a extensão $\mathbb{L} = \mathbb{K}(\sqrt{d})$ e assim, $d(\phi_{\mathbb{L}}) = d(\psi_{\mathbb{L}}) = 1$. Pelo mesmo resultado, temos que $\phi_{\mathbb{L}}$ e $\psi_{\mathbb{L}}$ são similares. Segue do corolário precedente que ϕ e ψ são similares. □

3.6 O Teorema de Jacobson

Antes de demonstramos o Teorema de Jacobson 3.23, vejamos o seguinte lema:

Lema 3.28 *Suponhamos que ϕ e ψ são 6–formas satisfazendo $d(\phi) = d(\psi) = 1$ e $c(\phi) = c(\psi)$. Então ϕ e ψ são similares.*

Demonstração: Se ϕ e ψ forem isotrópicas então o resultado segue imediatamente da Proposição 3.27. Suponhamos então que ambas são anisotrópicas. Note que $\dim(\phi \perp -\psi) =$

12, $d(\phi \perp -\psi) = 1$ e $c(\phi \perp -\psi) = 1$. Pelo Teorema 3.24, $\phi \perp -\psi \in I^3\mathbb{K}$. Agora escrevermos $\phi \cong a\phi_1$ e $\psi \cong b\psi_1$ de tal forma que ϕ_1 e ψ_1 ambas representem 1. Assim,

$$d(\phi_1) = d(a\phi) = d(\phi) = 1 = d(\psi) = d(b\psi) = d(\psi_1)$$

e

$$c(\phi_1) = c(a\phi) = c(\phi) = c(\psi) = c(b\psi) = c(\psi_1).$$

Portanto, $\phi_1 \perp -\psi_1 \in I^3\mathbb{K}$. Fazendo $\phi_1 \cong \langle 1\rangle \perp \phi_2$ e $\psi_1 \cong \langle 1\rangle \perp \psi_2$, teremos que $\phi_2 \perp -\psi_2 \in I^3\mathbb{K}$. Desta maneira, $\phi_2 \perp -\psi_2$ é uma 10–forma com $d(\phi_2 \perp -\psi_2) = 1$ e $c(\phi_2 \perp -\psi_2) = 1$. Pelo Corolário 3.16, $\phi_2 \perp -\psi_2$ é isotrópica. Como ϕ e ψ são anisotrópicas, ϕ_2 e ψ_2 representam um comum valor d. Assim, $\phi_2 \cong \langle d\rangle \perp \phi_3$ e $\psi_2 \cong \langle d\rangle \perp \psi_3$. Desta forma, $\phi_3 \perp -\psi_3 \in I^3\mathbb{K}$ e assim, $d(\phi_3 \perp \psi_3) = 1$ e $c(\phi_3 \perp \psi_3) = 1$. Segue daí que $d(\phi_3) = d(\psi_3)$ e $c(\phi_3) = c(\psi_3)$. Pela Proposição 3.27, ϕ_3 e ψ_3 são similares, isto é, existe $x \in \mathbb{K}^\times$ tal que, $\phi_3 \cong x\psi_3$. Como $c(\phi_3) = c(x\psi_3) = (x, d(\psi_3))c(\psi_3)$, $(x, d(\psi_3)) = 1$. Mas $\psi_1 \cong \langle 1, d\rangle \perp \psi_3$ e assim,

$$\det(\psi_1) = d\det(\psi_3) = -1 \Rightarrow \det(\psi_3) = -d \Rightarrow d(\psi_3) = -d.$$

Logo, $(x, -d) = 1$ e $\langle 1, -x, d, -xd\rangle \cong \langle 1, d\rangle \perp -x\langle 1, d\rangle$ é hiperbólica, e assim, $\langle 1, d\rangle \cong x\langle 1, d\rangle$. Conseqüentemente,

$$abx\psi \cong ax\psi_1 \cong as(\langle 1, d\rangle \perp \psi_3) \cong a(x\langle 1, d\rangle \perp x\psi_3) \cong$$

$$\cong a(\langle 1, d\rangle \perp \phi_3) \cong a\phi_1 \cong \phi,$$

isto é, ϕ e ψ são similares.

□

De posse do lema acima e da teoria desenvolvida nas seções anteriores, a demonstração do teorema torna-se trivial.

Prova do Teorema de Jacobson

Demonstração: Sejam ϕ_A e ϕ_B as formas de Albert associadas as álgebras biquaterniônicas A e B. Se $\phi_A \cong \lambda\phi_B$ então, no grupo de Brauer $\mathrm{Br}(\mathbb{K})$, teremos que

$$[A] = c(\phi_A) = c(\lambda\phi_B) = c(\phi_B)(x, d(\phi_B)) = c(\phi_B) = [B].$$

Portanto, $A \cong B$. Reciprocamente, se $A \cong B$ então $c(\phi_A) = [A] = [B] = c(\phi_B)$. Como $d(\phi_A) = d(\phi_B) = 1$, pelo lema acima, ϕ_A e ϕ_B são similares. □

3.7 O u-invariante

Vimos anteriormente como decidir se uma álgebra biquaterniônica é um anel de divisão através da sua forma de Albert. Entretanto, será que todo corpo admite uma álgebra biquaterniônica de divisão? A resposta para essa pergunta é um sonoro não. Um antigo resultado atribuído a George Frobenius, datado de 1878, garante que o único anel de divisão sobre os reais $\mathbb{R}$ é a álgebra de quatérnios. Para uma demonstração, ver Polcino[26]. Posteriormente, Albert[3] provou que toda álgebra com divisão de grau 4 tendo como centro qualquer extensão finita dos racionais tem ordem 4 no grupo de Brauer. Veremos agora que para o caso em que o corpo é não formalmente real, a questão da existência de álgebras biquaterniônicas de divisão pode ser relacionada com o u–invariante do corpo.

Um corpo $\mathbb{K}$ é dito **formalmente real** se -1 não pode ser escrito como soma de quadrados e **não formalmente real**, caso contrário. Ao longo desta seção, $\mathbb{K}$ denota sempre um corpo não formalmente real. Neste caso definimos o **u–invariante** de $\mathbb{K}$ como sendo a dimensão máxima das formas anisotrópicas. Note que este número pode ser ∞, para isto basta tomarmos o corpo $\mathbb{C}(x_1, x_2, \ldots)$ (infinitas variáveis).

Obs 3.29 *Pelo Teorema 3.19, se um corpo $\mathbb{K}$ admite uma álgebra biquaterniônica de divisão então este possui uma 6–forma anisotrópica. Portanto, devemos ter $u(\mathbb{K}) \geq 6$.*

Com esta informação, podemos exibir vários exemplos de corpos que não admitem uma álgebra biquaterniônica de divisão:

1. $\mathbb{K}$ = um corpo quadraticamente fechado então $u(\mathbb{K}) = 1$.
2. $\mathbb{K}$ = um corpo finito então $u(\mathbb{K}) \leq 2$.
3. $\mathbb{K}$ = um corpo com grau de transcendência 1 sobre um corpo real fechado então $u(\mathbb{K}) \leq 2$.
4. $\mathbb{K}$ = um corpo local então $u(\mathbb{K}) = 4$. Este é o caso do corpo das séries de Laurent formais $\mathbb{F}(\!(t)\!)$, onde $\mathbb{F}$ é um corpo finito.

5. $\mathbb{K}$ = um corpo global, como qualquer extensão finita de $\mathbb{F}(x)$, o corpo das funções racionais em uma variável, onde $\mathbb{F}$ denota um corpo finito, então $u(\mathbb{K}) = 4$.

6. $\mathbb{K}$ = um corpo com grau de transcendência ≤ 2 sobre um corpo algebricamente fechado então $u(\mathbb{K}) = 1$, 2 ou 4. Por exemplo, $u(\mathbb{C}) = 1, u(\mathbb{C}(x)) = 2$ e $u(\mathbb{C}(x, y)) = 4$, onde $\mathbb{C}$ denota o corpo dos números complexos.

Como o cálculo do u–invariante dos corpos acima citados fogem um pouco dos objetivos principais desse trabalho, deixamos como referências [20](pg 316) e [11] (pg 152).

Obs 3.30 *Infelizmente, a recíproca da observação 3.29 não é sempre verdadeira. A construção do contra-exemplos será deixada para o capítulo 5, onde trabalharemos com o corpo das séries de Laurent formais* $\mathbb{K} = \mathbb{C}(\!(x)\!)(\!(y)\!)(\!(z)\!)$.

Por outro lado, temos um resultado um pouco mais fraco, porém interessante:

Teorema 3.31 *Se* $\mathbb{K}$ *é um corpo com* $u(\mathbb{K}) = 6$ *então existe uma álgebra biquaterniônica de divisão sobre* $\mathbb{K}$.

Demonstração: Suponha que $u(\mathbb{K}) = 6$ e tome uma 6–forma anisotrópica ϕ. Considere $\det(\phi) = d$ e escreva $\gamma = \langle 1, d\rangle \perp \phi$. Desta forma, γ é isotrópica e podemos escrever $\gamma \cong \langle 1, -1\rangle \perp \psi$, onde ψ é uma 6–forma que satisfaz $\det(\psi) = -\det(\gamma) = -1$. Vamos provar que ψ é anisotrópica. Suponhamos então por absurdo que ψ é isotrópica e escrevemos $\psi \cong \langle 1, -1\rangle \perp \psi'$. Segue daí que

$$\langle 1, d\rangle \perp \phi \cong \gamma \cong 2 \times \langle 1, -1\rangle \perp \psi' \cong \langle 1, d\rangle \perp \langle -1, -d\rangle \perp \psi'.$$

Pela Lei do cancelamento de Witt, obtemos $\phi \cong \langle -1, -d\rangle \perp \psi'$. Como $\det(\psi') = 1$, podemos escrever $\psi' \cong a\langle\langle b, c\rangle\rangle$. Sendo assim, como $u(\mathbb{K}) = 6$ e toda forma de Pfister isotrópica é hiperbólica, obtemos que $\langle\langle -a, b, c\rangle\rangle$ é hiperbólica. Assim,

$$\begin{aligned}\langle\langle -a, b, c\rangle\rangle &\cong \langle 1, b, c, bc, -a, -ab, -ac, -abc\rangle \\ &\cong \langle a, -a, ab, -ab, ac, -ac, abc, -abc\rangle.\end{aligned}$$

Pelo cancelamento de Witt, teremos que $\langle\langle b, c\rangle\rangle \cong a\langle\langle b, c\rangle\rangle$. Logo,

$$\phi \cong \langle -1, -d\rangle \perp \psi' \cong \langle -1, -d\rangle \perp \langle 1, b, c, bd\rangle$$

e ϕ é isotrópica, o que é um absurdo. Portanto, ψ é anisotrópica. Como $d(\psi) = 1$, segue da observação 3.17 que ψ é similar a uma forma de Albert anisotrópica

$$\langle -x, -y, xy, z, w, -zw \rangle.$$

Do Teorema 3.19, obtemos que $(x, y)_{\mathbb{K}} \otimes_{\mathbb{K}} (z, w)_{\mathbb{K}}$ é uma álgebra biquaterniônica de divisão sobre $\mathbb{K}$. □

Entretanto, o teorema acima não torna tão simples a construção de corpos que admitem álgebras biquaterniônicas de divisão. Na verdade, a existência de corpos com u–invariante 6 é um problema que permaneceu em aberto por mais de 30 anos e foi respondido por A. Merkurjev em 1988. Para uma construção, ver Lam [22].

Capítulo 4

Álgebras Biquaterniônicas Cíclicas e não-Cíclicas

Neste capítulo vamos estudar a ciclicidade das álgebras biquaterniônicas, construindo exemplos de álgebras cíclicas e não cíclicas. Veremos que a condição para uma álgebra de divisão ser cíclica está ligada à existência de um subcorpo maximal que é uma extensão galoisiana cíclica do seu centro. Neste sentido, começamos revisando algumas noções de Teoria de Galois e apresentando alguns resultados que caracterizam as extensões cíclicas de grau 4.

4.1 Elementos da Teoria de Galois

Começamos com o célebre Teorema Fundamental da Teoria de Galois (TFTG). Por se tratar de um resultado clássico e que pode ser facilmente encontrado na literatura, omitiremos a demonstração e por ora recomendamos Rotman [30].

Teorema 4.1 (TFTG) *Seja* $\mathbb{L}/\mathbb{K}$ *uma extensão galoisiana com grupo de Galois* $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. *Se denotarmos por* $\mathrm{Sub}(G)$ *a família dos subgrupos de* G, $\mathrm{Lat}(\mathbb{L}/\mathbb{K})$ *a família de todos os corpos intermediários da extensão* $\mathbb{L}/\mathbb{K}$ *e se para cada* $H \in \mathrm{Sub}(G)$ *escrevermos* $\mathbb{L}^H = \{x \in \mathbb{L} \mid \sigma(x) = x, \forall \sigma \in H\}$, *então teremos que:*

1. *A aplicação* $\varphi : \mathrm{Sub}(G) \to \mathrm{Lat}(\mathbb{L}/\mathbb{K})$, *definida por* $H \longmapsto \mathbb{L}^H$ *é uma bijeção que inverte inclusão.*

2. $\mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{F})} = \mathbb{F}$ *e* $\mathrm{Gal}(\mathbb{L}/\mathbb{L}^{\mathbb{H}}) = H$.

3. $[\mathbb{F} : \mathbb{K}] = [G : \mathrm{Gal}(\mathbb{L}/\mathbb{F})]$ *e* $[G : H] = [\mathbb{L}^H : \mathbb{K}]$.

4. $\mathbb{F}/\mathbb{K}$ *é uma extensão galoisiana se, e somente se,* $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ *é um subgrupo normal de* G.

Definição 4.2 *Seja* $f(x) \in \mathbb{K}[x]$ *um polinômio de grau* n *tendo como corpo de decomposição uma extensão separável* $\mathbb{L}/\mathbb{K}$ *e seja* $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. *Se* $a_1, \ldots, a_n$ *são as raízes de* $f(x)$ *em* $\mathbb{L}$ *e definirmos*

$$\Delta = \prod_{i<j}(a_i - a_j),$$

então, o ***discriminante*** *do polinômio* $f(x)$ *é* $D = \Delta^2$.

Note que Δ só depende da indexação das raízes, uma nova indexação poderia apenas alterar o sinal de Δ. Desta forma, o discriminante D só depende do conjunto de raízes. Além disso, como $G \subseteq S_n$ (grupo das permutações de n símbolos), então, para cada $\sigma \in G$, $\sigma(\Delta) = \pm\Delta$, e assim, $D \in \mathbb{L}^G = \mathbb{K}$. Mais ainda, $\sigma(\Delta) = \Delta$ se, e somente se, $\sigma \in A_n$ (subgrupo de S_n formado pelas permutações pares).

Proposição 4.3 *Seja* $f(x) \in \mathbb{K}[x]$ *com discriminante* $D = \Delta^2 \neq 0$ *e grupo de Galois* $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. *Se* $H = G \cap A_n$, *então* $\mathbb{L}^H = \mathbb{K}(\Delta)$. *Além disso,* $\Delta \in \mathbb{K}$ *se, e somente se,* G *é um subgrupo de* A_n.

Demonstração: Como $H \subseteq A_n$, então $\mathbb{K}(\Delta) \subseteq \mathbb{L}^H$. Além disso, pelo TFTG, temos que $[\mathbb{L}^H : \mathbb{K}] = [G : H] \leq 2$. Vamos verificar que $[\mathbb{K}(\Delta) : \mathbb{K}] = [G : H]$. Se $[G : H] = 2$ então existe $\sigma \in G$ tal que $\sigma(\Delta) = -\Delta$ e assim, $\Delta \notin \mathbb{L}^G = \mathbb{K}$ e $[\mathbb{K}(\Delta) : \mathbb{K}] = 2$. Por outro lado, se $[G : H] = 1$ então $G = H$ e $\mathbb{K}(\Delta) \subseteq \mathbb{L}^H = \mathbb{L}^G = \mathbb{K}$, logo $[\mathbb{K}(\Delta) : \mathbb{K}] = 1$. Finalmente, segue do TFTG que:

$$\Delta \in \mathbb{K} \iff \mathbb{K}(\Delta) = \mathbb{L}^H = \mathbb{K} \iff G = H \iff G \subseteq A_n.$$

□

Veremos agora dois resultados que serão necessários para conhecermos a estrutura das extensões cíclicas de grau 4.

Teorema 4.4 *Seja* $\mathbb{L}$ *uma extensão cíclica de grau 4 sobre* $\mathbb{K}$. *Então existem* $e, f \in \mathbb{K}$ *e* $d \in \mathbb{K}^\times \backslash \mathbb{K}^{\times 2}$ *tal que* $\mathbb{L} = \mathbb{K}(\sqrt{e + f\sqrt{d}})$ *e* d *é a soma de dois quadrados em* $\mathbb{K}$.

Demonstração: Pelo TFTG, existe um único subcorpo intermediário $\mathbb{F}$ na extensão $\mathbb{L}/\mathbb{K}$. Escrevemos $\mathbb{F} = \mathbb{K}(\sqrt{d})$ e $\mathbb{L} = \mathbb{F}(\theta)$, tal que d não é um quadrado e $\theta^2 = e + f\sqrt{d} \in \mathbb{F}$. Como $\theta^2 - e = f\sqrt{d}$ então θ é uma raíz do polinômio:

$$p(x) = x^4 - 2ex^2 + (e^2 - df^2) = (x^2 - (e + f\sqrt{d}))(x^2 - (e - f\sqrt{d})).$$

Assim, $p(x)$ é irredutível sobre $\mathbb{K}$ e tem como raízes $\theta, -\theta, \phi, -\phi$, onde $\phi^2 = e - f\sqrt{d}$. Como $\mathbb{L}/\mathbb{K}$ é galoisiana então $\theta\phi = \sqrt{e^2 - f^2 d} \in \mathbb{L}^\times$ e daí, $e^2 - f^2 d \in {\mathbb{L}^\times}^2$. Agora, como ${\mathbb{L}^\times}^2 \cap \mathbb{F} = {\mathbb{F}^\times}^2 \cup (e + f\sqrt{d})\mathbb{F}$ e $e^2 - f^2 d \in \mathbb{K}$ então, $e^2 - f^2 d \in {\mathbb{F}^\times}^2 \cap \mathbb{K} = {\mathbb{K}^\times}^2 \cup d{\mathbb{K}^\times}^2$. Por outro lado, temos que o discriminante de $p(x)$ é dado por:

$$\begin{aligned}
\Delta^2 &= (2\theta)^2(2\phi)^2(\theta - \phi)(\theta + \phi)(-\theta - \phi)(-\theta + \phi) && (4.1)\\
&= 16(e + f\sqrt{d})(e - f\sqrt{d})(\theta^2 - \phi^2)^4 && (4.2)\\
&= 16(e^2 - f^2 d)(2f\sqrt{d})^4 && (4.3)\\
&= 16^2(e^2 - f^2 d)f^4 d^2. && (4.4)
\end{aligned}$$

Como $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ é um grupo cíclico de ordem 4, então este não pode ser um subgrupo de A_n. Pela Proposição 4.3, $\Delta \notin \mathbb{K}$, e assim, $(e^2 - f^2 d)$ não é um quadrado em $\mathbb{K}$, logo, $(e^2 - f^2 d) \in d{\mathbb{K}^\times}^2$ e $e^2 - f^2 d = da^2$. Finalmente, se $e \neq 0$ então $d = (\frac{fd}{e})^2 + (\frac{da}{e})^2$ e se $e = 0$ então $\langle 1, 1\rangle \cong \langle d, -d\rangle$ e $\langle 1, 1\rangle$ representa d. Em ambos os casos, d é a soma de dois quadrados. □

Teorema 4.5 *Se $d \in \mathbb{K}^\times \backslash {\mathbb{K}^\times}^2$ e $f, e \in \mathbb{K}$ tais que $d(e^2 - df^2)$ é um quadrado em $\mathbb{K}$, então $\mathbb{L} = \mathbb{K}(\sqrt{e + f\sqrt{d}})$ é uma extensão cíclica de grau 4 sobre $\mathbb{K}$ e $p(x) = x^4 - 2ex^2 + (e^2 - df^2)$ é o polinômio minimal de $\sqrt{e + f\sqrt{d}}$ sobre $\mathbb{K}$.*

Demonstração: Se $d(e^2 - f^2 d)$ é um quadrado então $(e^2 - f^2 d)$ não é um quadrado em $\mathbb{K}$. Segue que $e + f\sqrt{d}$ também não é um quadrado em $\mathbb{K}(\sqrt{d})$. Isto nos dá as seguintes extensões:

$$\mathbb{K} \subset \mathbb{K}(\sqrt{d}) = \mathbb{F} \subset \mathbb{F}(\sqrt{e + f\sqrt{d}}) = \mathbb{L}.$$

Escrevendo $\theta = \sqrt{e + f\sqrt{d}}$, teremos que θ é raíz do polinômio irredutível $p(x) = x^4 - 2ex^2 + (e^2 - f^2 d)$, que tem como raízes θ, $-\theta$, ϕ e $-\phi$, onde $\phi^2 = e^2 - f^2 d$. Agora veja que:

$d(e^2 - f^2 d) \in {\mathbb{K}^\times}^2 \Rightarrow e^2 - f^2 d \in d{\mathbb{K}^\times}^2 \Rightarrow e^2 - f^2 d \in {\mathbb{L}^\times}^2 \Rightarrow \theta\phi = \sqrt{e^2 - f^2 d} \in \mathbb{L}^\times \Rightarrow \phi \in \mathbb{L}.$

Assim, $\mathbb{L}$ é o corpo de raízes de $p(x)$ sobre $\mathbb{K}$. Como em característica diferente de dois toda extensão de grau 4 é separável, obtemos que $\mathbb{L}/\mathbb{K}$ é galoisiana. Finalmente, como $(e^2 - f^2 d)$ não é um quadrado em $\mathbb{K}$, então $\Delta = 16^2(e^2 - f^2 d)f^4 d^2 \notin \mathbb{K}$, e assim, pela Proposição 4.3, $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ não é um subgrupo de A_n. Portanto, $\mathbb{L}/\mathbb{K}$ é cíclica. □

Obs 4.6 *Poderíamos substituir no teorema acima a hipótese de que $d(e^2 - df^2)$ é um quadrado por d ser a soma de dois quadrados, pois neste caso, se $d = a^2 + b^2$, com $a, b \in \mathbb{K}$, então tomado $e = \frac{1}{b}$ e $f = \frac{a}{db}$, teremos que*

$$d(e^2 - f^2 d) = d\left(\frac{1}{b^2} - d\left(\frac{a}{db}\right)^2\right) = d\left(\frac{1}{b^2} - \frac{a^2}{db^2}\right) = \frac{d - a^2}{b^2} = \frac{a^2 + b^2 - a^2}{b^2} = 1.$$

4.2 Álgebras Cíclicas

Vamos agora estudar uma classe muito especial de álgebras centrais simples que são as álgebras cíclicas.

Para construir uma álgebra cíclica de dimensão n^2, começamos com um corpo $\mathbb{K}$ e uma extensão galoisiana cíclica $\mathbb{L}/\mathbb{K}$ de grau n com grupo de Galois $G = \langle\sigma\rangle$. Agora escolhemos um elemento $\alpha \in \mathbb{K}^\times$, um símbolo e e consideramos A o conjunto formado por todas as combinações lineares formais

$$x = a_0 + a_1 e + \ldots + a_{n-1} e^{n-1},$$

com $a_i \in \mathbb{L}$. Definimos a soma de dois destes elementos e o produto de um deles por um elemento de $\mathbb{K}$ componente a componente. Isto faz de A um $\mathbb{K}$–espaço vetorial com $\dim_{\mathbb{K}} A = n^2$. Para definir o produto de dois destes elementos, procedemos distributivamente de acordo com as seguintes regras:

1. $(ae^j)(be^i) = a\sigma^j(b)e^{i+j}, \quad \forall a, b \in \mathbb{L} \quad \text{e} \quad i, j = 0, \ldots, n-1;$
2. $e^n = \alpha.$

Como a multiplicação já foi definida de maneira distributiva e para cada $a, b, c \in \mathbb{L}$

temos que

$$\begin{aligned}[(ae^i)(be^j)](ce^k) &= (a\sigma^i(b)e^{i+j})(ce^k)\\ &= a\sigma^i(b)\sigma^{i+j}(c)e^{i+j+k}\\ &= a\sigma^i(b\sigma^j(c))e^{i+j+k}\\ &= (ae^i)(b\sigma^j(c)e^{j+k})\\ &= (ae^i)[(be^j)(ce^k)],\end{aligned}$$

obtemos que A é uma $\mathbb{K}$–álgebra associativa.

Uma álgebra definida como acima diz-se uma **álgebra cíclica** e é denotada por $A = (\mathbb{L}/\mathbb{K}, \sigma, \alpha)$.

Teorema 4.7 *Toda álgebra cíclica $A = (\mathbb{L}/\mathbb{K}, \sigma, \alpha)$ é uma álgebra central simples sobre $\mathbb{K}$.*

Demonstração: Seja $x = a_0 + a_1e + \ldots + a_{n-1}e^{n-1}$ um elemento do centro de A. Veja que

$$xe = a_0e + a_1e^2 + \ldots + a_{n-1}e^n = a_{n-1}\alpha + a_0e + a_1e^2 + \ldots + a_{n-2}e^{n-1} \qquad \text{e}$$

$$ex = ea_0 + ea_1e + \ldots + ea_{n-1}e^{n-1} = a_0e + \sigma(a_1)e^2 + \ldots + \sigma(a_{n-1})e^n =$$

$$= \sigma(a_{n-1})\alpha + a_0e + \sigma(a_1)e^2 + \ldots + \sigma(a_{n-2})e^{n-1}.$$

Neste caso, $xe = ex$ e daí, $a_i \in \mathbb{K}$. Por outro lado, $\forall \lambda \in \mathbb{L}$ teremos que $\lambda x = x\lambda$ e assim,

$$x\lambda = a_0\lambda + a_1e\lambda + \ldots + a_{n-1}e^{n-1}\lambda = a_0\lambda + a_1\sigma(\lambda)e + \ldots + a_{n-1}\sigma(\lambda)e^{n-1} =$$

$$= \lambda a_0 + \lambda a_1e + \ldots + \lambda a_{n-1}e^{n-1}.$$

Portanto, para cada $i = 1, \ldots, n-1$, teremos $\lambda a_i = a_i\sigma(\lambda) = \sigma(\lambda)a_i, \forall \lambda \in \mathbb{L}$ e isto implica que $a_i = 0$. Logo, $x = a_0 \in \mathbb{K}$.

Para provar que A é simples, tomamos I um ideal bilateral não nulo de A e seja

$$x = a_{i_1}e^{i_1} + \ldots + a_{i_r}e^{i_r} \in I\backslash\{0\}, \quad 0 \leq i_1 < \ldots < i_r \leq n-1$$

de tal forma que r seja o menor possível. Desta forma, $\forall b \in \mathbb{L}$ teremos que

$$xb = a_{i_1}e^{i_1}b + \ldots + a_{i_r}e^{i_r}b = a_{i_1}\sigma^{i_1}(b)e^{i_1} + \ldots + a_{i_r}\sigma^{i_r}(b)e^{i_r} \in I,$$

$$\sigma^{i_1}(b)x = \sigma^{i_1}(b)a_{i_1}e^{i_1} + \ldots + \sigma^{i_1}(b)a_{i_r}e^{i_r} = a_{i_1}\sigma^{i_1}(b)e^{i_1} + \ldots + a_{i_r}\sigma^{i_1}(b)e^{i_r} \in I \quad \text{e}$$

$$xb - \sigma^{i_1}(b)x = a_{i_2}(\sigma^{i_2}(b) - \sigma^{i_1}(b))e^{i_2} + \ldots + a_{i_r}(\sigma^{i_r}(b) - \sigma^{i_1}(b))e^{i_r} \in I.$$

Como esta última expressão tem comprimento menor do que a expressão para x, então $xb - \sigma^{i_1}(b)x = 0$, logo, $\sigma^{i_r}(b) - \sigma^{i_1}(b) = 0$, $\forall b \in \mathbb{L}$. Assim, $i_r = i_1$ e x é da forma $a_i e^i$ com $a_i \in \mathbb{L}^\times$. Temos então que

$$(a_i e^i)(\sigma^i(a_i^{-1})e^{n-i}) = a_i a_i^{-1} e^i e^{n-i} = e^n = \alpha \in I.$$

Como $\alpha \in \mathbb{K}^\times$, concluímos que $I = A$. Portanto, A é uma $\mathbb{K}$–álgebra central simples. □

Obs 4.8 *Note que se $A = (\mathbb{L}/\mathbb{K}, \sigma, \alpha)$ e $\dim_{\mathbb{K}} A = n^2$, então, como $\mathbb{L} \subset A$ e $[\mathbb{L} : \mathbb{K}] = n$, $\mathbb{L}$ é um subcorpo maximal de A.*

Agora veremos a recíproca do Teorema 4.7.

Teorema 4.9 *Se A é uma $\mathbb{K}$–álgebra central simples de dimensão n^2 e $\mathbb{L}$ é um subcorpo maximal de A que é uma extensão galoisiana cíclica de $\mathbb{K}$ então A é isomorfa a uma álgebra cíclica.*

Demonstração: Seja $\text{Gal}(\mathbb{L}/\mathbb{K}) = \langle\sigma\rangle$. Como σ é uma automorfismo de $\mathbb{L}$ então, pelo Teorema de Skolem-Nöther, existe um elemento $e \in A^\times$ tal que $\sigma(x) = exe^{-1}$, $\forall x \in \mathbb{L}$. Note que para cada $x \in \mathbb{L}$ teremos que:

$$x = \sigma^n(x) = e^n x (e^n)^{-1} \Rightarrow e^n x = x e^n.$$

como $\mathbb{L}$ é maximal, $e_n \in \mathbb{L}$. Agora, como $\sigma(e^n) = ee^n e^- 1 = e^n$, obtemos que $e^n \in \mathbb{K}$. Falta então verificar que $\beta = \{1, e, e^2, \ldots, e^{n-1}\}$ é L.I. sobre $\mathbb{L}$. Suponhamos o contrário e seja $\{e^{i_1}, \ldots, e^{i_r}\}$ o menor subconjunto L.D. de β. Desta forma, existem $a_{i_1}, \ldots, a_{i_r} \in \mathbb{L}$, não todos nulos, tais que

$$x = a_{i_1}e^{i_1} + \ldots + a_{i_r}e^{i_r} = 0.$$

Assim, $\forall b \in \mathbb{L}$ teremos que

$$xb = a_{i_1}e^{i_1}b + \ldots + a_{i_r}e^{i_r}b = a_{i_1}\sigma^{i_1}(b)e^{i_1} + \ldots + a_{i_r}\sigma^{i_r}(b)e^{i_r} = 0,$$

$$\sigma^{i_1}(b)x = \sigma^{i_1}(b)a_{i_1}e^{i_1} + \ldots + \sigma^{i_1}(b)a_{i_r}e^{i_r} = a_{i_1}\sigma^{i_1}(b)e^{i_1} + \ldots + a_{i_r}\sigma^{i_1}(b)e^{i_r} = 0 \quad \text{e}$$

$$xb - \sigma^{i_1}(b)x = a_{i_2}(\sigma^{i_2}(b) - \sigma^{i_1}(b))e^{i_2} + \ldots + a_{i_r}(\sigma^{i_r}(b) - \sigma^{i_1}(b))e^{i_r} = 0.$$

Como $\{e^{i_2}, \ldots, e^{i_n}\}$ é L.I., $\sigma^{i_r}(b) = \sigma^{i_1}(b)$, $\forall b \in \mathbb{L}$, logo, $i_r = i_1$. Mas daí teríamos que $\{e^i\}$ é L.D., o que é um absurdo. Portanto, $\{1, e, e^2, \ldots, e^{n-1}\}$ é uma $\mathbb{L}$–base para A e a multiplicação verifica as propriedades desejadas, logo, $A \cong (\mathbb{L}/\mathbb{K}, \sigma, e^n)$. □

Exemplo 4.10 *Toda álgebra de quatérnios $(a, b)_{\mathbb{K}}$ é cíclica, pois $(a, b)_{\mathbb{K}}$ sempre contém uma subcorpo quadrático que é necessariamente cíclico. Mais explicitamente,*

$$(a, b)_{\mathbb{K}} \cong (\mathbb{K}(\sqrt{a})/\mathbb{K}, \sigma, b).$$

4.3 Álgebras Biquaterniônicas não-Cíclicas

Como vimos no exemplo 4.10, uma álgebra de quatérnios é sempre cíclica. Veremos agora que isso não é sempre verdade para as álgebras biquaterniônicas. Começamos com dois lemas técnicos. Lembre que um corpo $\mathbb{K}$ é dito Pitagórico se $\mathbb{K}^2 + \mathbb{K}^2 = \mathbb{K}^2$.

Lema 4.11 *Seja γ uma forma binária e φ uma forma de dimensão ≥ 2 sobre um corpo $\mathbb{F}$. Se $\gamma \otimes \varphi$ é isotrópica então φ contém uma subforma $\psi \cong \langle a, b\rangle$ tal que $\gamma \otimes \psi$ é hiperbólica.*

Demonstração: Se φ fosse isotrópica então poderíamos simplesmente tomar ψ como um plano hiperbólico. Suponhamos então que φ é anisotrópica e escrevemos $\gamma \cong \langle s, t\rangle$. Como $\gamma \otimes \varphi \cong s\varphi \perp t\varphi$ é isotrópica, então existem $x, y \in D_{\mathbb{F}}(\varphi)$ tais que $sx + ty = 0$. Desta forma, escrevemos $\varphi \cong \langle x\rangle \perp \varphi_1$ e teremos que existem $w \in \mathbb{F}$ e $z \in D_{\mathbb{F}}(\varphi_1)$ tais que $y = xw^2 + z$. Se $z = 0$ então

$$y = xw^2 \Rightarrow sx + txw^2 = 0 \Rightarrow s + tw^2 = 0 \Rightarrow \langle s, t\rangle \cong \langle 1, -1\rangle.$$

Neste caso, a forma $\gamma \otimes \psi$ é hiperbólica para qualquer escolha de ψ. Agora, se $z \neq 0$ então podemos escrever $\varphi \cong \langle x\rangle \perp \varphi_1 \cong \langle x, z\rangle \perp \varphi_2$. Tomando $\psi \cong \langle x, z\rangle$, obtemos da equação $y = xw^2 + z$ que $\phi \cong \langle y, a\rangle$. Como $xz = \det(\psi) = \det(\langle y, a\rangle) = ya$, segue que $a = xyz$ e $\psi \cong \langle y, xyz\rangle$. Finalmente, como $x^2sy = -y^2tx$,

$$\langle s, t\rangle \otimes \psi \cong s\langle y, xyz\rangle \perp t\langle x, z\rangle \cong \langle sy, syxz\rangle \perp \langle tx, tz\rangle \cong \langle -tx, -txxz\rangle \perp \langle tx, tz\rangle,$$

e assim, $\gamma \otimes \psi$ é hiperbólica. □

Lema 4.12 *Seja ϕ uma forma quadrática sobre um corpo não-pitagórico $\mathbb{F}$. Então as seguintes afirmações são equivalentes:*

1. *ϕ é isotrópica sobre alguma extensão quadrática $\mathbb{K} \supset \mathbb{F}$, da forma $\mathbb{K} = \mathbb{F}(\sqrt{r^2+s^2})$ onde $r, s \in \mathbb{F}$;*

2. *$2 \times \phi$ é isotrópica sobre $\mathbb{F}$.*

Demonstração: (1) $\Rightarrow$ (2). Podemos assumir que ϕ é anisotrópica. Como $\phi_{\mathbb{K}}$ é isotrópica então, pela Proposição 1.7, ϕ possui uma subforma binária $b\langle 1, -(r^2+s^2)\rangle$. Conseqüentemente, $2 \times \phi$ contém a subforma $b(2 \times \langle 1, -(r^2+s^2)\rangle) \cong b\langle 1, 1, -r^2-s^2, -r^2-s^2\rangle$, que é isotrópica.
(2) $\Rightarrow$ (1). Podemos supor que ϕ é anisotrópica, pois, caso contrário, poderíamos tomar qualquer extensão quadrática da forma $\mathbb{K} = \mathbb{F}(\sqrt{r^2+s^2})$ que a afirmação (1) estaria satisfeita. Agora, aplicamos o lema anterior para a $\gamma \cong \langle 1, 1\rangle$. Como $\dim \phi \geq 2$ e $\gamma \otimes \phi = 2 \times \phi$ é isotrópica, então, ϕ contém uma subforma binária $\langle a, b\rangle$ tal que $2 \times \langle a, b\rangle$ é hiperbólica. Assim, $a\langle 1, 1, ab, ab\rangle$ é hiperbólica, e daí, $\langle 1, 1\rangle \cong \langle -ab, -ab\rangle$. Desta forma, existem $r, s \in \mathbb{F}$ tais que $-ab = r^2 + s^2$. Como $\langle a, b\rangle$ é anisotrópica, $-ab \notin \mathbb{F}^2$, e assim, ϕ é isotrópica sobre a extensão quadrática $\mathbb{K} = \mathbb{F}(\sqrt{r^2+s^2})$. □

Definição 4.13 *Uma corpo $\mathbb{K}$ é dito SAP (*Strongly Approximation Propriety*) se para quaisquer $a, b \in \mathbb{K}^\times$, existe $n \in \mathbb{N}$ tal que a forma $n \times \langle 1, a, b, -ab\rangle$ é isotrópica.*

Veremos agora que todo corpo não SAP admite uma álgebra biquaterniônica de divisão não cíclica.

Proposição 4.14 *Seja $\mathbb{K}$ um corpo que não é SAP, isto é, existem $x, y \in \mathbb{K}^\times$ tais que $n \times \langle 1, x, y, -xy\rangle$ é anisotrópica para cada $n \in \mathbb{N}$. Então se $B = (-1, -1)_{\mathbb{K}}$ e $C = (x, y)_{\mathbb{K}}$ então a álgebra biquaterniônica $A = B \otimes_{\mathbb{K}} C$ é uma $\mathbb{K}$–álgebra de divisão não cíclica.*

Demonstração: Como $3 \times \langle 1, x, y, -xy\rangle$ é anisotrópica então a forma de Albert de A

$$\varphi_A \cong \langle 1, 1, 1, x, y, -xy\rangle$$

é também anisotrópica e pelo Teorema 3.19, A é de divisão. Suponhamos por absurdo que A é uma álgebra cíclica. Pela observação 4.8, A admite um subcorpo maximal $\mathbb{L}$ que

é uma extensão galoisiana cíclica de $\mathbb{K}$. Pela Proposição 4.4, a única extensão quadrática $\mathbb{F}$ de $\mathbb{K}$ dentro de $\mathbb{L}$ é da forma $\mathbb{F} = \mathbb{K}(\sqrt{r^2+s^2})$, com $r, s \in \mathbb{K}^\times$. Como $\mathbb{L}$ cinde A então $\varphi_\mathbb{L}$ é hiperbólica. Se $\varphi_\mathbb{F}$ for anisotrópica e $\mathbb{L} = \mathbb{F}(\sqrt{d})$ então, pela Proposição 1.8, teremos que

$$\varphi_\mathbb{F} \cong \langle 1, -d\rangle \otimes \langle a, b, c\rangle \cong \langle a, b, c, -ad, -bd, -cd\rangle.$$

Desta forma,

$$-1 = \det(\varphi) = \det(\langle a, b, c, -ad, -bd, -cd\rangle) = -d$$

Portanto, $d = 1$ em $\mathbb{F}^\times/\mathbb{F}^{\times 2}$, o que é um absurdo, logo, φ é isotrópica em $\mathbb{F}$. Pelo lema anterior obtemos que $2 \times \varphi$ é isotrópica sobre $\mathbb{K}$. Mas então $6 \times \langle 1, x, y, -xy\rangle$ é também isotrópica sobre $\mathbb{K}$. Como isso contraria a hipótese inicial de que $n \times \langle 1, x, y, -xy\rangle$ é anisotrópica, obtemos que A não pode ser uma álgebra cíclica. □

Obs 4.15 *Para que o resultado acima torne-se mais significativo, construiremos no capítulo 5 um exemplo concreto de um corpo não SAP.*

4.4 Álgebras Biquaterniônicas Cíclicas

Nesta seção, vamos construir diretamente um exemplo de álgebra biquaterniônica de divisão cíclica. Dividiremos o nosso trabalho em três passos.

Passo 1: Construir uma álgebra A cíclica de grau 4 sobre o corpo $\mathbb{Q}(x, y)$.

Consideremos $\mathbb{K} = \mathbb{Q}(x, y)$, o corpo das funções racionais em duas variáveis sobre o corpo dos números racionais. Tomando

$$d = 2, \qquad v = \frac{-y}{4x^2} \qquad \text{e} \qquad w = -2v = \frac{y}{2x^2},$$

teremos que

$$d(w^2 - dv^2) = d(-2v)^2 - d^2v^2 = 4dv^2 - d^2v^2 = 8v^2 - 4v^2 = 4v^2.$$

Portanto, $d(w^2 - dv^2)$ é um quadrado e, pelo Teorema 4.5, $\mathbb{L} = \mathbb{K}(\sqrt{w + v\sqrt{d}})$ é uma extensão cíclica de grau 4 sobre $\mathbb{K}$ que tem $\mathbb{K}(\sqrt{d})$ como a única extensão intermediária e

$$p(\alpha) = \alpha^4 - 2w\alpha^2 + (w^2 - dv^2) = \alpha^4 + 4v\alpha^2 + 2v^2$$

é o polinômio minimal de $\theta = \sqrt{w + v\sqrt{d}}$ sobre $\mathbb{K}$. Para $u = \sqrt{2}$, como

$$\theta^2 = w + vu = -2v + uv = v(u-2),$$

fazendo $\alpha = \theta(u+1)$, teremos que:

$$\alpha^2 = \theta^2(u+1)^2 = v(u-2)(3+2u) = v(3u + 2u^2 - 6 - 4u) = -v(u+2);$$

$$\alpha^4 = v^2(u+2)^2 = v^2(u^2 + 4u + 4) = v^2(4u+6);$$

$$p(\alpha) = v^2(4u+6) - 4v^2(u+2) + 2v^2 = v^2(4u + 6 - 4u - 8 + 2) = 0.$$

Portanto, $\theta(u+1)$ é uma raíz de $p(\alpha)$ diferente de θ e $-\theta$. Sendo assim, podemos tomar $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \{1, \sigma, \sigma^2, \sigma^3\}$, onde $\sigma(\theta) = \theta(u+1)$.

Com essas informações, podemos utilizar a construção apresentada na seção 4.2 para exibir a álgebra cíclica

$$A = \mathbb{L} \oplus \mathbb{L}e \oplus \mathbb{L}e^2 \oplus \mathbb{L}e^3,$$

onde a multiplicação é definida por:

$$(ae^i)(be^j) = a\sigma^i(b)e^{i+j} \qquad \text{e} \qquad e^4 = -x^2.$$

Passo 2: Provar que A é uma álgebra biquaterniônica.

Procedemos construindo duas subalgebras de quatérnios B e C contidas em A, tais que $\mathcal{C}_A B = C$. Nestas condições teremos, pelo Teorema do Duplo Centralizador que $A \cong B \otimes_{\mathbb{K}} C$. Denotamos por $(a_1, \ldots, a_n)$ o subespaço de A gerado pelos elementos $a_1, \ldots, a_n$ e definimos:

$$B = (1, u, s, us) \qquad \text{e} \qquad C = (1, j, t, jt) \qquad \text{onde,}$$

$$s = xe + e^3, \qquad j = e^2, \qquad t = \theta e^2 + x\sigma(\theta)$$

e u como foi obtido no passo 1. Assim teremos que $u^2 = 2$, $j^2 = e^4 = -x^2$, e mais:

$$s^2 = (xe + e^3)^2 = x^2e^2 + xe^4 + e^3xe + e^6 = x^2e^2 - 2x^3 - x^2e^2 = -2x^3;$$

$$\begin{aligned} t^2 &= (\theta e^2)^2 + \theta e^2 x\sigma(\theta) + x\sigma(\theta)\theta e^2 + (x\sigma(\theta))^2 \\ &= \theta\sigma^2(\theta)e^4 + x\theta\sigma^3(\theta)e^2 + x\sigma(\theta)\theta e^2 + x^2(\sigma(\theta))^2 \\ &= \theta^2 x^2 - x\theta\sigma(\theta)e^2 + x\sigma(\theta)\theta e^2 + x^2(\sigma(\theta))^2 \\ &= x^2(\theta^2 + \sigma(\theta)^2) \\ &= 2x^2 w \\ &= y; \end{aligned}$$

$$su = (xe + e^3)u = x\sigma(u)e + \sigma^3(u)e^3 = -xue - ue = -u(xe + e^3) = -us;$$

$$tj = (\theta e^2 + x\sigma(\theta))e^2 = e^2\sigma^2(\theta)e^2 + xe^2\sigma^3(\theta) = e^2(\sigma^2(\theta)e^2 + x\sigma^3(\theta)) =$$

$$= e^2(-\theta e^2 + -x\sigma(\theta)) = -jt;$$

Desta forma, obtemos que B e C são subalgebras de quatérnios satisfazendo:

$$B \cong (2, -2x^3)_{\mathbb{K}} \cong (2, -2x)_{\mathbb{K}} \qquad \text{e} \qquad C \cong (-x^2, y)_{\mathbb{K}} \cong (-1, y)_{\mathbb{K}}.$$

Agora vamos verificar que todos os elementos de B comutam com os elementos de C.

$$sj = (xe + e^3)e^2 = xe^3 + e^5 = e^2(xe) + e^2e^3 = e^2(xe + e^3) = js;$$

$$tu = (\theta e^2 + x\sigma(\theta))u = \theta e^2u + x\sigma(\theta)u = \theta ue^2 + ux\theta = u(\theta e^2 + x\sigma(\theta)) = ut;$$

$$\begin{aligned} st &= (xe + e^3)(\theta e^2 + x\sigma(\theta)) \\ &= xe\theta e^2 + xex\sigma(\theta) + e^3\theta e^2 + e^3x\sigma(\theta) \\ &= x\sigma(\theta)e^3 + x^2\sigma^2(\theta)e + \sigma^3(\theta)e^5 + x\sigma^4(\theta)e^3 \\ &= x\theta e^3 - x^2\theta e + x^2\sigma(\theta)e + x\sigma(\theta)e^3 \\ &= x\theta e^3 - \theta e^5 + x^2\sigma(\theta)e + x\sigma(\theta)e^3 \\ &= (\theta e^2 + x\sigma(\theta))(xe + e^3); \\ &= ts. \end{aligned}$$

Como $uj = ue^2 = e^2u = ju$, obtemos que $C \subseteq \mathcal{C}_A B$. Como $\dim_{\mathbb{K}} B = \dim_{\mathbb{K}} C = 4$ e $A \cong B \otimes_{\mathbb{K}} \mathcal{C}_A B$, concluímos que $A \cong B \otimes_{\mathbb{K}} C$.

Passo 3: Provar que A é uma álgebra de divisão.

No passo anterior, conseguimos que $A \cong B \otimes_{\mathbb{K}} C \cong (2, -2x)_{\mathbb{K}} \otimes_{\mathbb{K}} (-1, y)_{\mathbb{K}}$. Sendo assim, pelo Teorema 3.19, para provar que A é uma álgebra de divisão, devemos verificar que a forma de Albert

$$\varphi_A \cong \langle 2, -2x, -x, 1, -y, -y \rangle$$

é anisotrópica sobre $\mathbb{K} = \mathbb{Q}(x)(y)$. Suponhamos o contrário, sejam $a_1, \ldots, a_6 \in \mathbb{K}$ não todos nulos tais que

$$2a_1^2 - 2xa_2^2 + xa_3^2 = -a_4^2 + y(a_5^2 + a_6^2). \tag{4.5}$$

Podemos supor que $a_1, \ldots, a_6$ são polinômios com coeficientes racionais e que não têm um fator comum. Agora, substituindo $y = 0$ ficamos com

$$b_4^2 + 2b_1^2 = 2x(b_2^2 - 2b_3^2),$$

onde $b_1, \ldots, b_4$ são polinômios na variável x. Suponhamos que para cada i, b_i tenha grau r_i e coeficiente líder β_i. Sendo assim, temos as seguintes possibilidades para o termo de maior grau de $b_4^2 + 2b_1^2$:

$$\beta_4^2 x^{2r_4}, \qquad 2\beta_1^2 x^{2r_1}, \qquad (\beta_4^2 + 2\beta_1^2)x^{2r_1},$$

e para $2x(b_2^2 - 2b_3^2)$:

$$2\beta_2^2 x^{2r_2+1}, \qquad -4\beta_3^2 x^{2r_3+1}, \qquad 2(\beta_2^2 - 2\beta_3^2)x^{2r_2+1}.$$

Note que como ± 2 não é um quadrado em $\mathbb{Q}$, $\beta_4^2 + 2\beta_1^2$ e $\beta_2^2 - 2\beta_3^2$ não podem se anular. Assim, em 4.5 temos a igualdade de um polinômio de grau ímpar com um de grau par. Logo, $b_1 = \ldots = b_4 = 0$, e conseqüentemente, $a_1, \ldots, a_4$ são todos divisíveis por y. Escrevendo $a_i = yc_i$ para $i = 1, \ldots, 4$, ficamos com

$$y^2(c_1^2 - 2xc_2^2 + xc_3^2 + c_4^2) = y(a_5^2 + a_6^2).$$

Assim, $a_5^2 + a_6^2$ é divisível por y. Se a_5^2 e a_6^2 tem como termos constantes com respeito a y, ϑ_5 e ϑ_5, respectivamente, então $\vartheta_5^2 + \vartheta_6^2 = 0$. Como -1 não é um quadrado, então $\vartheta_5 = \vartheta_6 = 0$. Seque que a_5 e a_6 também são divisíveis por y. Como partimos da hipótese de que $a_1, \ldots, a_6$ não têm fator comum, chegamos a um absurdo e concluímos que φ é anisotrópica.

Portanto, temos construído um exemplo de uma álgebra biquaterniônica cíclica de divisão.

Capítulo 5

Construção de Exemplos Sobre $\mathbb{K}(\!(t)\!)$

O objetivo desse último capítulo é apenas construir exemplos concretos para os problemas apresentados nas observações 4.15 e 3.30. Para isso, utilizaremos as noções de valorização e ordens sobre $\mathbb{K}(\!(t)\!)$, que é definido como o corpo das séries de Laurent formais na variável t

$$f = \sum_{i=n}^{\infty} a_i t^i \qquad (a_i \in \mathbb{K},\ n \in \mathbb{Z} \text{ e } a_n \neq 0)$$

sobre $\mathbb{K}$, onde a adição é dada por

$$\sum_{i=n}^{\infty} a_i t^i + \sum_{i=m}^{\infty} b_i t^i = \sum_{i=l}^{\infty} (a_i + b_i) t^i,$$

sendo $l = \min\{i \mid a_i + b_i \neq 0\}$ e a multiplicação é definida por

$$(\sum_{i=n}^{\infty} a_i t^i)(\sum_{i=m}^{\infty} b_i t^i) = \sum_{i=l}^{\infty} c_i t^i,$$

onde $l = \min\{i \mid c_i \neq 0\}$ e $c_i = \sum_{r+s=i} a_r b_s$.

5.1 Valorização Discreta

Começamos revisando algumas noções básicas sobre valorização.

Um corpo $\mathbb{K}$ é dito um **corpo valorizado** se admite uma **valorização discreta**, que é uma aplicação sobrejetiva $v : \mathbb{K}^{\times} \to \mathbb{Z}$ satisfazendo:

1. $v(ab) = v(a) + v(b)$
2. $v(a + b) \geq \min\{v(a), v(b)\}$.

Além disso, convencionamos que $\upsilon(0) = \infty$. O conjunto

$$A = \{x \in (K) \mid \upsilon(x) \geq 0\}$$

é um subanel de $\mathbb{K}$, chamado de **anel de valorização**. Nestas condições, A tem um único ideal maximal

$$\mathfrak{m} = \{x \in \mathbb{K} \mid \upsilon(x) \geq 1\},$$

que é gerado por um elemento π, tal que $\upsilon(\pi) = 1$. Isto nos dá a seguinte cadeia de ideais

$$A \supsetneq \mathfrak{m} \supsetneq \mathfrak{m}^2 \supsetneq \ldots \supsetneq 0 \quad \text{e} \quad \bigcap_{i=1}^{\infty} \mathfrak{m}^i = 0.$$

O grupo das unidades de A é dado por

$$U = \{x \in A \mid x \notin \mathfrak{m}\} = \{x \in \mathbb{K} \mid \upsilon(x) = 0\},$$

e o corpo $\overline{\mathbb{K}} = A/\mathfrak{m}$ é chamado de **corpo de resíduos** de A, sendo que a projeção de A sobre $\overline{\mathbb{K}}$ será expressa por $x \longmapsto \overline{x} = x + \mathfrak{m}$.

Podemos definir uma métrica d sobre um corpo valorizado $(\mathbb{K}, \upsilon)$, pondo para cada $x, y \in \mathbb{K}$

$$d(x, y) = e^{-\upsilon(x-y)}.$$

Sendo assim, $(\mathbb{K}, \upsilon)$ é dito **completo** se toda seqüência de Cauchy é convergente com respeito a métrica d.

Proposição 5.1 *Se $(\mathbb{K}, \upsilon)$ uma corpo valorizado completo então, para cada $u \in U$, u é um quadrado em $\mathbb{K}$ se, e somente se, $\overline{u}$ é um quadrado em $\overline{\mathbb{K}}$.*

Demonstração: Seja $u \in U$ tal que $\overline{u} \in \overline{\mathbb{K}}^{\times 2}$. Vamos construir indutivamente uma seqüência (b_i) em U, tal que $b_i - u \in \mathfrak{m}^2$ e $b_{i+1} - b_i \in \mathfrak{m}^2$. Como $\overline{u} \in \overline{\mathbb{K}}^{\times 2}$, então $\overline{u} = \overline{b_1^2}$ para algum $b_1 \in U$, logo, $b_1^2 - u \in \mathfrak{m}$. Agora, suponhamos que temos construído um elemento b_i tal que $b_i^2 - u = \pi^i c$, para algum $c \in A$. Seja $z \in A$ tal que $c + 2b_i z = \pi$ e tomamos $b_{i+1} = b_i + \pi_i z$ Desta forma, $b_{i+1} \in U$, $b_{i+1} - b_i \in \mathfrak{m}^i$ e

$$b_{i+1}^2 - u = (b_i + \pi^i z)^2 - u = b_i^2 + 2b_i\pi^i z + z^2\pi^{2i} - u = \pi^i c + 2b_i\pi^i z + z^2\pi^{2i} =$$

$$= \pi^i(c + 2b_i z) + z^2\pi^{2i} = \pi^{i+1} + z^2\pi^{2i} \in \mathfrak{m}^{i+1}.$$

Como a seqüência (b_i) construída acima é de Cauchy, então existe $b \in A$ tal que $\lim b_i = b$. Desta forma, $\lim(b_i^2 - b^2) = 0$. Como $\lim b_i^2 = u$, obtemos que $u = b^2$. A recíproca é

imediata. □

Agora podemos aplicar as idéias trabalhadas acima para o corpo $\mathbb{F} = \mathbb{K}((t))$. Se definirmos, para cada $f \in \mathbb{F}^{\times}$

$$v(f) = v(\sum_{i=n}^{\infty} a_i t^i) = n$$

teremos que v é uma valorização discreta, o anel de valorização de v será dado pelo domínio das séries de potência formais $\mathbb{K}[[t]] = \sum_{i=0}^{\infty} a_i t^i$, $\mathfrak{m} = (t)$ e o corpo de resíduos $\overline{\mathbb{F}}$ será isomorfo ao corpo $\mathbb{K}$. Além disso, $(\mathbb{F}, v)$ é completo e, pela proposição acima, todo elemento de $\mathbb{F}$ da forma $1 + ta$, onde $a = \sum_{i=0}^{\infty} a_i t^i$, é sempre um quadrado. Sendo assim, podemos caracterizar o grupo $\mathbb{F}^{\times}/\mathbb{F}^{\times 2}$.

Proposição 5.2 *Seja $\mathbb{F} = \mathbb{K}((t))$ e suponhamos que $\mathbb{K}^{\times}/\mathbb{K}^{\times 2}$ é um conjunto finito. Se $\mathbb{K}^{\times}/\mathbb{K}^{\times 2} = \{x_1, \ldots, x_m\}$ então*

$$\mathbb{F}^{\times}/\mathbb{F}^{\times 2} = \{x_1, \ldots, x_m, x_1 t, \ldots, x_m t\}.$$

Demonstração: Dado $f \in \mathbb{F}$ escrevemos

$$f = \sum_{i=n}^{\infty} a_i t^i = a_n t^n + \sum_{i=n+1}^{\infty} a_i t^i = a_n t^n (1 + \sum_{i=n+1}^{\infty} a_n^{-1} a_i t^{i-n}) = a_n t^n (1 + \sum_{j=0}^{\infty} b_j t^{i+1}), \quad (5.1)$$

onde $b_j = a_n^{-1} a_{n+1+j}$. Pela Proposição 5.1, $1 + \sum_{j=0}^{\infty} b_j t^{i+1} = 1 + t \sum_{j=0}^{\infty} b_j t^i$ é um quadrado em $\mathbb{F}$. Desta forma, se n é par então f está na classe de algum dos x_i e, caso contrário, se n é ímpar então $f = t x_i$ em $\mathbb{F}^{\times}/\mathbb{F}^{\times 2}$. Agora, vejamos que de fato $x_1, \ldots, x_m, x_1 t, \ldots, x_m t$ representam distintas classes de quadrados em $\mathbb{F}$. Não podemos ter $x_i = x_j (\sum_{i=n}^{\infty} a_i t^i)^2$, pois neste caso,

$$0 = v(x_i) = v(x_j (\sum_{i=n}^{\infty} a_i t^i)^2) = v(x_j) + v((\sum_{i=n}^{\infty} a_i t^i)^2) = 2n,$$

e assim, $x_i = a_0^2 x_j$. Se $t x_i = t x_j (\sum_{i=n}^{\infty} a_i t^i)^2$ então $x_i = x_j (\sum_{i=n}^{\infty} a_i t^i)^2$ e nos reduzimos ao caso anterior. Finalmente, se $x_i = t x_j (\sum_{i=n}^{\infty} a_i t^i)^2$ então

$$0 = v(x_i) = v(t x_j (\sum_{i=n}^{\infty} a_i t^i)^2) = 1 + 2n,$$

o que não é possível. □

5.2 O corpo $\mathbb{C}((x))((y))((z))$

Na observação 3.29, vimos que se um corpo $\mathbb{K}$ admite uma álgebra biquaterniônica de divisão então, devemos ter o u-invariante $u(\mathbb{K}) \geq 6$. Entretanto, afirmamos na observação 3.30 que a recíproca desse resultado não é sempre verdadeira. Veremos agora que o contra-exemplo para tal afirmação virá do corpo $\mathbb{K} = \mathbb{C}((x))((y))((z))$.

Como $\mathbb{C}$ tem única classe de quadrados, então, pela Proposição 5.2, teremos que $\mathbb{K}$ tem exatamente 8 classes de quadrados, a saber

$$\{1, x, y, z, xy, xz, yz, xyz\}.$$

Como -1 é um quadrado em $\mathbb{K}$ então já temos que $u(\mathbb{K}) \leq 8$. Vamos então provar que a forma

$$\varphi = \langle 1, x, y, z, xy, xz, yz, xyz\rangle$$

é anisotrópica. Suponhamos o contrário, isto é, existem $a_1, \ldots, a_8 \in \mathbb{K}$ tais que

$$a_1^2 + xa_2^2 + ya_3^2 + za_5^2 + xya_4^2 + xza_6^2 + yza_7^2 + xyza_8^2 = 0.$$

Reescrevendo,

$$a_1^2 + xa_2^2 + ya_3^2 + xya_4^2 = z(a_5^2 + xa_6^2 + ya_7^2 + xya_8^2).$$

Por definição,

$$\upsilon(a_1^2 + xa_2^2 + ya_3^2 + xya_4^2) \geq \min\{\upsilon(a_1^2), \upsilon(xa_2^2), \upsilon(ya_3^2), \upsilon(xya_4^2)\} =$$

$$= 2\min\{\upsilon(a_1), \upsilon(a_2), \upsilon(a_3), \upsilon(a_4)\},$$

e da mesma forma,

$$\upsilon(z(a_5^2 + xa_6^2 + ya_7^2 + xya_8^2)) \geq 1 + 2\min\{\upsilon(a_5), \upsilon(a_6), \upsilon(a_7), \upsilon(a_8)\}.$$

Sendo assim, não podemos ter a igualdade em ambas as equações acima, suponhamos então que:

$$\upsilon(a_1^2 + xa_2^2 + ya_3^2 + xya_4^2) > \min\{\upsilon(a_1^2), \upsilon(xa_2^2), \upsilon(ya_3^2), \upsilon(xya_4^2)\}.$$

Neste caso, a forma $\langle 1, x, y, zy\rangle$ é isotrópica sobre $\mathbb{C}((x))((y))$, isto é, $b_1^2 + xb_2^2 = y(b_3^2 + xb_4^2)$ para alguns $b_1, \ldots, b_4 \in \mathbb{C}((x))((y))$ não todos nulos. Repetindo o mesmo argumento, chegamos que $\langle 1, x\rangle$ é isotrópica sobre $\mathbb{C}((x))$. Mas isto não é possível pois se $c_1^2 = xc_2^2$ então $2\upsilon(c_1) = \upsilon(c_1^2) = \upsilon(xc_2^2) = 1 + 2\upsilon(c_2)$. Portanto, φ é anisotrópica e $u(\mathbb{K}) = 8$.

Novamente, como -1 é um quadrado e $\mathbb{K}$ tem oito classes de quadrados, concluímos que $\mathbb{K}$ admite no máximo oito álgebra de quatérnios, a saber:

$$(1,1)_{\mathbb{K}}, \qquad (x,y)_{\mathbb{K}}, \qquad (x,z)_{\mathbb{K}}, \qquad (y,z)_{\mathbb{K}},$$

$$(x,yz)_{\mathbb{K}}, \quad (y,xz)_{\mathbb{K}}, \quad (z,xy)_{\mathbb{K}}, \quad (xy,xz)_{\mathbb{K}}.$$

Podemos calcular diretamente, e ver que o conjunto formado pelas classes dessas álgebras de quatérnios formam um subgrupo do grupo de Brauer, e assim, $\mathbb{K}$ não admite álgebra biquaterniônica de divisão.

5.3 Ordem

Definição 5.3 *Uma ordem em um corpo $\mathbb{K}$ é um subconjunto $P \neq \mathbb{K}$ que satisfaz:*

1. $P + P \subseteq P$;
2. $P.P \subseteq P$;
3. $P \cup -P = \mathbb{K}$;

onde denotamos por $-P$ o conjunto $\{-x \mid x \in P\}$.

Segue da definição que $P \cap -P = 0$, $-1 \notin P$ e P contém $\sum \mathbb{K}^2$, o conjunto de todas as somas de quadrados em $\mathbb{K}$. Vamos denotar por $X_{\mathbb{K}}$ o conjunto de todas as ordens do corpo $\mathbb{K}$. Se $\mathbb{K} \subseteq \mathbb{F}$ e $P \in X_{\mathbb{F}}$ então $P \cap \mathbb{K} \in X_{\mathbb{K}}$. Além disso, se $\mathbb{K} = \mathbb{Q}$ então $X_{\mathbb{K}} = \{\sum \mathbb{Q}^2\}$.

Proposição 5.4 *Se P é uma ordem de um corpo $\mathbb{K}$ então $\mathbb{F} = \mathbb{K}(\!(t)\!)$ admite pelo menos duas ordens, a saber:*

1. $P_1 = \{\sum_{i=n}^{\infty} a_i t^i \mid a_n \in P\}$
2. $P_2 = \{\sum_{i=n}^{\infty} a_i t^i \mid (-1)^n a_n \in P\}$.

Além disso, $P_1 \cap P_2 = P\mathbb{F}^2$.

Demonstração: Dados $f = \sum_{i=n}^{\infty} a_i t^i$ e $g = \sum_{i=m}^{\infty} b_i t^i \in P_1$, teremos que a_n e $b_m \in P$. Sendo assim, $f + g = \sum_{i=l}^{\infty} c_i t^i$, onde $c_i = a_i + b_i$ e $l = \min\{i \mid c_i \neq 0\}$. Desta forma, c_l será dado por a_n, b_m ou $a_n + b_m$. Em qualquer caso, $c_l \in P$ e $f + g \in P_1$. Logo $P_1 + P_1 \subseteq P_1$. Analogamente, $fg = \sum_{i=l}^{\infty} c_i t^i$, onde $c_i = \sum_{r+s=i} a_r b_s$ e $l = \min\{i \mid c_i \neq 0\}$.

Neste caso, $c_l = a_n b_m$ e $fg \in P_1$. Logo $P_1P_1 \subseteq P_1$. Agora, se $f = \sum_{i=n}^{\infty} a_i t^i \in \mathbb{F}$ então temos duas possibilidades $a_n \in P$ ou $-a_n \in P$. No primeiro caso, $f \in P_1$ e no segundo, $-f = \sum_{i=n}^{\infty} -a_i t^i \in P_1$ e daí $f \in -P_1$. Portanto, $\mathbb{F} = P_1 \cup -P_1$. Finalmente, como $-1 \notin P_1$ obtemos que de fato P_1 é uma ordem de $\mathbb{F}$. De modo análogo, verifica-se facilmente que P_2 também é uma ordem de $\mathbb{F}$. Agora, se $f \in P_1 \cup P_2$ então $f = \sum_{i=n}^{\infty} a_i t^i$ com $a_n \in P$ e $(-1)^n a_n \in P$. Como $a_n \neq 0$ obtemos que $n = 2k$ para algum $k \in \mathbb{Z}$. Sendo assim, escrevendo f como na equação 5.1 da Proposição 5.2 obtemos

$$f = a_{2k} t^{2k}(1 + tg) \in a_{2k}\mathbb{F}^2.$$

Como $a_{2k} \in P$, teremos que $f \in P\mathbb{F}^2$. Por outro lado, como $P \subseteq P_1 \cap P_2$ e $\mathbb{F}^2 \subseteq P_1 \cap P_2$, concluímos que $P_1 \cap P_2 = P\mathbb{F}^2$. □

Proposição 5.5 *Nas hipóteses na proposição anterior, P_1 e P_2 são as únicas ordens de $\mathbb{F}$ com a propriedade de que $P_1 \cap \mathbb{K} = P_2 \cap \mathbb{K} = P$.*

Demonstração: Seja P_3 é uma ordem de $\mathbb{F}$ satisfazendo $P_3 \cap \mathbb{K} = P$. Seja $f = \sum_{i=n}^{\infty} a_i t^i$ e, como na equação 5.1, escrevemos $f = a_n t^n(1 + tg) \in a_n t^n \mathbb{F}^2$. Agora, se $t \in P_3$, então teremos que:

$$f \in P_3 \Longleftrightarrow a_n \in P_3 \Longleftrightarrow a_n \in P \Longleftrightarrow f \in P_1$$

Neste caso, $P_3 = P_1$. Se $-t \in P_3$ então escrevemos $f = (-1)^n a_n (-t)^n (1 + tg)$, e assim:

$$f \in P_3 \Longleftrightarrow (-1)^n a_n \in P_3 \Longleftrightarrow (-1)^n a_n \in P \Longleftrightarrow f \in P_2,$$

implicando que $P_3 = P_2$.

□

5.4 O corpo $\mathbb{Q}((x))((y))$

Na Proposição 4.14, provamos que todo corpo não SAP, admite uma álgebra biquaterniônica de divisão não-cíclica. Nesta seção, vamos utilizar as noções de ordem desenvolvidas na seção anterior para apresentar um exemplo concreto de um corpo não SAP. Lembre que um corpo $\mathbb{K}$ é dito não SAP se existem $a, b \in \mathbb{K}^{\times}$, tais que a forma $n \times \langle 1, a, b, -ab\rangle$ é anisotrópica para todo $n \in \mathbb{N}$. Desta forma, tomamos $\mathbb{F} = \mathbb{K}((y))$, onde $\mathbb{K} = \mathbb{Q}((x))$ e vamos mostrar que $\mathbb{F} = \mathbb{Q}((x))((y))$ é um corpo não SAP.

Como $\mathbb{Q}$ tem uma única ordem $P = \sum \mathbb{Q}^2$, pelas Proposições 5.4 e 5.5, $\mathbb{K}$ tem exatamente duas ordens P_1 e P_2 e estas satisfazem $x \in P_1$ e $-x \in P_2$. Conseqüentemente, $X_{\mathbb{F}} = \{P_1^1, P_1^2, P_2^1, P_2^2\}$, onde $P_i^j \cap \mathbb{K} = P_i$. E assim, teremos:

$$\{1, x, y, xy\} \subset P_1^1, \qquad \{1, x, -y, -xy\} \subset P_1^2,$$

$$\{1, -x, y, -xy\} \subset P_2^1 \qquad \text{e} \qquad \{1, -x, -y, xy\} \subset P_2^2.$$

Vamos agora verificar que $P_1^1 \cap P_1^2 \cap P_2^1 \subset P_2^2$. Ainda pela Proposição 5.4, $P_1^1 \cap P_1^2 = P_1\mathbb{F}^2$. Logo $P_1^1 \cap P_1^2 \cap P_2^1 = P_2^1 \cap P_1\mathbb{F}^2$. Já sabemos que $P\mathbb{F}^2 \subseteq P_2^1 \cap P_1\mathbb{F}^2$. Reciprocamente, se $f \in P_2^1 \cap P_1\mathbb{F}^2$, então existem $g \in P_1 \subseteq \mathbb{K}$, $h \in \mathbb{F}$ e $z \in P_2^1$ tais que $f = gh^2 = z$. Sendo assim, escrevemos:

$$z = \sum_{i=n}^{\infty} a_i y^i, \quad \text{com} \quad a_n \in P_2 \quad \text{e}$$

$$h = \sum_{i=m}^{\infty} b_i y^i \Rightarrow h^2 = \sum_{i=2m}^{\infty} c_i y^i, \quad \text{com} \quad c_{2m} = b_m^2$$

Logo obtemos que $f = gh^2 = \sum_{i=2m}^{\infty} g c_i y^i$. Portanto, $n = 2m$ e $g b_m^2 = a_n \in P_1 \cap P_2 = P\mathbb{K}^2$. Segue que $g \in P_1 \cap P_2 = P\mathbb{K}^2$, e daí, $f = gh^2 \in P\mathbb{F}^2$. Portanto, $P_1^1 \cap P_1^2 \cap P_2^1 = P\mathbb{F}^2$. Como $P\mathbb{F}^2 \subseteq P_2^2$, conseguimos que $P_1^1 \cap P_1^2 \cap P_2^1 \subset P_2^2$.

Com um procedimento semelhante podemos verificar o resultado acima para quaisquer três ordens escolhidas de $\mathbb{F}$. Finalmente, vamos verificar que $\mathbb{F}$ não é SAP.

Suponhamos então que $n \times \langle 1, -x, -y, -xy\rangle$ é isotrópica para algum $n \in \mathbb{N}$, isto é, existem $a_i, b_i, c_i, d_i \in \mathbb{F}$ não todos nulos tais que

$$\sum_{i=1}^{n}(a_i^2 - xb_i^2 - yc_i^2 - xyd_i^2) = (\sum_{i=1}^{n} a_i^2) - x(\sum_{i=1}^{n} b_i^2) - y(\sum_{i=1}^{n} c_i^2) - xy(\sum_{i=1}^{n} d_i^2) = 0.$$

Desta forma, podemos escrever $bx + cy + dxy = a$, para $a, b, c, d \in \sum \mathbb{F}^2$ não todos nulos. Como $-dxy \in P_2^1 \cap P_1^2$, então $bx + cy \in P_1^1 \cap P_2^1 \cap P_1^2 \subset P_2^2$. Mas $bx, cy \in P_2^2$ implica que $b = c = 0$. Mas daí chegaríamos que $dxy = a$, e assim, $d = a = 0$. Portanto, $n \times \langle 1, -x, -y, -xy\rangle$ é anisotrópica e $\mathbb{F}$ é um corpo não SAP.

Considerações Finais

Como pôde ser visto, o objetivo deste trabalho não foi estudar um problema específico e sim, realmente, dissertar sobre as álgebras biquaterniônicas. Por essa razão, buscamos demonstrar alguns resultados clássicos e construir exemplos concretos, a fim de entendermos um pouco a estrutura dessas álgebras.

Entretanto, esta dissertação está muito longe de ser um trabalho completo sobre as álgebras biquaterniônicas. Muito mais pode ser encontrado na literatura, inclusive nos textos que deixamos como referências.

De acordo com o Teorema de Merckurjev, toda álgebra central simples de expoente 2 é Brauer equivalente a um produto de álgebras de quatérnios. Em contrapartida, Amitsur, Rowen e Tignol tem construíram em [7] um exemplo de uma álgebra de divisão de expoente 2 que não se decompõe como um produto tensorial de álgebras de quatérnios.

Tendo em vista estes resultados, alguns dos principais problemas da teoria atualmente giram em torno de investigar sobre que condições, uma álgebra de divisão é isomorfa a um produto tensorial de álgebras de quatérnios. E neste sentido, acredito que conhecer a estrutura das álgebras biquaterniônicas torna-se imprescindível.

Referências Bibliográficas

[1] A. A. Albert, *On the Wedderburn norm condition for cyclic algebras*, Bull. Amer. Math. Soc. **37**, (1931), 301–312.

[2] A. A. Albert, *A note on cyclic algebras of order sixteen*, Bull. Amer. Math. Soc. **37**, (1931), 727–730.

[3] A. A. Albert, *Division algebras over an algebraic field*, Bull. Amer. Math. Soc. **37**, (1931), 777–784.

[4] A. A. Albert, *A construction of non-cyclic normal division algebras*, Bull. Amer. Math. Soc. **38**, (1932), 449–456.

[5] A. A. Albert, *Struture of Algebras*, Coll. Publ. **24** Amer. Math. Soc., Providence, R. I., 1961.

[6] A. A. Albert, *Tensor product of quaternion algebras*, Proc. Amer. Math. Soc. **35** (1972), 65–66.

[7] S. A. Amitsur, L. H. Rowen e J.-P. Tignol, *Division algebras of degree 4 and 8 with involution*, Israel J. Math. **33** (1979), 133–148.

[8] J. Kr. Arason, *A proof of Merkurjev's theorem*, Quadratic and Hermitian forms (Hamilton, Ont., 1983), 121–130, CMS Conf. Proc., 4, Amer. Math. Soc., Providence, RI, 1984.

[9] Richard A. Dean, *A rational polynomial whose group is the quaternions*, Amer. Math. Monthly **88** (1981), 42–45.

[10] R. Elman e T. Y. Lam, *Quadratic forms and the u–invariant I*, Math. Z. **131** (1973), 283–304.

[11] R. Elman e T. Y. Lam, *Quadratic forms and u–invariant. II*, Invent. Math. **2** (1973), 125–137.

[12] B. Felzenszwalb, *Álgebras de Dimensão Finita,* 12º Colóquio Brasileiro de Matemática, IMPA, Rio de Janeiro, 1991.

[13] N. Jacobson, *Some applications of Jordan norms to involutorial simple associative algebras*, Adv. in Math. **48** (1983), 149–165.

[14] G. Karpilovsky, *Field Theory: Classical Foundations and Multiplicative Groups*, Monographs and textbooks in pure ans applied mathematics **120** Marcel Dekker, Inc. New York, 1988.

[15] M.-A. Knus, A. Merkurjev, M. Rost e J.-P. Tignol, *The book of involutions*. Amer. Math. Soc. Coll. Publ., **44**, Amer. Math. Soc., Providence, RI, (1998).

[16] M.-A. Knus, R. Parimala e R. Sridharan, *Involutions on rank 16 central simple algebras*, J. Indian Math. Soc. **57** (1991), 143-151.

[17] M.-A. Knus, R. Parimala e R. Sridharan, *On the discriminant of an involution*, Bull. Soc. Math. Belg. Sér. A **43** (1991), 89-98.

[18] M.-A. Knus, T. Y. Lam, D. B. Shapiro e J.-P. Tignol, *Discriminants of involutions on biquaternion algebras*. K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), Proc. Sympos. Pure Math. **58** Part 2. Amer. Math. Soc., Providence, RI, (1995) 279–303.

[19] T. Y. Lam, D. B. Leep e J.-P. Tignol, *Biquaternion algebras and quartic extensions*, Inst. Hautes Études Sci. Publ. Math. **77** (1993), 63–102.

[20] T. Y. Lam, *The Algebraic Theory of qruadratic forms*, W. A. Benjamin, Reading, Massachusetts, 1973, Second priting with revisions, 1980.

[21] T. Y. Lam, *Ordering, Valuations And Quadratic Forms*. CBMS Regional Conference Series in Mathematics, 52. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the Amer. Math. Soc., Providence, Ri, 1983.

[22] T.Y. Lam, *Fields of u–invariant after Merkurjev*. Ring Theory 1989 (Ramat gan and Jerusalem, 1988/1989), 12–30, Israel Math. Conf. Proc., 1, Weizmann, Jerusalem, 1989.

[23] P. Mammone e D. Shapiro, *The Albert quadratic form for an algebra of degree four*, Proc. Amer. Math. Soc. **105** (1989), 525–530.

[24] R. Parimala, R. Sridharan e V. Suresh, *A question on the discriminants of involutions of central division algebras*, Math. Ann. **297** (1993), 575-580.

[25] A. Pfister, *Quadratische formen in beliebigen Körpern*, Invent. Math. **1** (1966), 116–132.

[26] C. Polcino Miles, *Anéis de divisão: Uma introdução través da história*, in Atas da XVIII Escola de Álgebra, Unicamp, 2004.

[27] A. Prestel, *Lectures on Formally Real Fields.* Lecture Notes in Mathematics, 1093. Springer-Verlag, Berlin, (1984).

[28] M. L. Racine, *A simple proof of a theorem of Albert*, Proc. Amer. Math. Soc. **43** (1974), 487–488.

[29] I. Reiner, *Maximal Orders*, Academic Press, London-New York, 1975, London Mathematical Society Monographs, N°5.

[30] J. Rotman, *Galois Theory*, Springer-Verlag New York Inc., 1990.

[31] L. H. Rowen, *Central Simple Algebras*, Israel J. of Math. **29** (1978), 285–301.

[32] W. Scharlau, *Quadratic and hermitian forms*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 270. Springer-Verlag, Berlin, 1985.

[33] A. Wadsworth, *Similarity of quadratic forms and isomorphism of their function fields*, Trans. Amer. Math. Soc. **208** (1975), 352–358.

[34] A. Wadsworth, *Merkurjev's elementary proof Merkurjev's theorem.* Applications of algebraic K-theory to algebraic geometry and number theory, Part I,II (Boulder, Colo., 1983), Contemp. Math. **55** Amer. Math. Soc., Providence, RI, (1986), 741–776.

[35] A. Wadsworth, *16–Dimensional Algebras with involutions*, Unpublished notes, http://math.ucsd.edu/∼wadswrth/, 1990.

Índice Remissivo