

**Universidade Estadual de Maringá**

Programa de Pós-Graduação em Matemática

Centro de Ciências Exatas

(Mestrado)

**INVOLUÇÕES POSITIVAS SOBRE UMA  
ÁLGEBRA SEMISIMPLES**

**Raquel Polizeli**

Orientadora: Rosali Brusamarello

Maringá - Pr

2007

“... A vida não está contida na escala do tempo,  
não está contida na escala da caducidade.  
O tempo, pelo contrário, está na palma das mãos da vida,  
a qual cerrada, se torna um ponto  
e aberta, se torna infinito.  
Aquele que acredita alcança...”  
(Masaharu Taniguchi)

**À minha família.**

# Agradecimentos

Agradeço à **Deus** por me conduzir sempre pelos melhores caminhos, por ouvir minhas preces, perdoar minhas falhas e por colocar em minha vida pessoas maravilhosas como essas:

Meus familiares. Em especial: Minha mãe Julia, meu avô José Luiz, minha avó Ana, estes sei que me iluminam de onde estão. Meu amado pai Orlando, minha mãe amiga Sônia, meus irmãos Celso e Carol, minha cunhada Silvia e meus padrinhos João Roberto e Maria. Todos estes sempre me apoiaram.

Meu namorado Rodrigo, meu grande companheiro.

Meus amigos, companheiras de repúblicas e os mais que amigos, Mariana, Eloisa, Priscila e Fernando, que tornaram-se quase irmãos para mim.

Minha orientadora Rosali, um exemplo de profissional e de mulher, uma pessoa muito especial, que com muita paciência me acompanhou na realização desse trabalho.

Os membros da banca: O professor Marcelo, mais um exemplo a ser seguido, um grande profissional e um ser humano louvável. O professor Osvaldo, que muito contribuiu nesse trabalho e na minha formação. O professor Vitor, que nos presenteou com valiosos conselhos na finalização desse trabalho.

Os professores do DMA, que contribuíram direta ou indiretamente para minha formação. A secretária da pós-graduação Lucia, sempre atenta e prestativa.

À todos vocês, meu sincero muito obrigada.

Finalmente, agradeço à CAPES pelo suporte financeiro.

# Resumo

Nesse trabalho iremos estender o Teorema 13.3 de Scharlau [10], que caracteriza a involução canônica sobre a álgebra de grupo  $K[G]$ , onde  $K$  é um corpo real fechado. Com isso estaremos caracterizando involuções positivas em álgebras semisimples de dimensão finita sobre um corpo real fechado.

**Palavras Chaves:** Involução, álgebras centrais simples, álgebras semisimples, corpos reais fechados, matrizes hermitianas.

# Abstract

In this work we extend Theorem 13.3 of Scharlau [10] that characterizes the canonical involution on the group algebra  $K[G]$ , where  $K$  is a real closed field. With this we give a characterization of positive involutions in semisimple algebras of finite dimension over a real closed field.

**Keywords:** Involution, central simple algebras, semisimple algebras, real closed fields, hermitian matrix.

# Sumário

<b>Introdução</b>	<b>1</b>
<b>1 Preliminares</b>	<b>3</b>
1.1 Corpos Formalmente Reais e Ordenados . . . . .	3
1.2 Corpos Reais Fechados . . . . .	10
1.3 Espaços Bilineares e Quadráticos . . . . .	15
<b>2 Anéis Simples e Semisimples</b>	<b>20</b>
2.1 Anéis e Módulos Simples . . . . .	20
2.2 Condições que definem Semisimplicidade . . . . .	29
2.3 Anéis Semisimples . . . . .	31
<b>3 Álgebras Centrais Simples</b>	<b>37</b>
3.1 Álgebras Centrais Simples . . . . .	37
3.2 Estendendo o corpo base de uma álgebra central simples . . . . .	44
3.2.1 Traço e Norma . . . . .	46
<b>4 Involuções sobre Álgebras Centrais Simples</b>	<b>50</b>
4.1 Classificação de Involuções . . . . .	50
4.2 Diagonalização de matrizes simétricas e hermitianas . . . . .	56

4.3	A Involução Canônica em uma Álgebra de Grupos. . . . .	63
5	Álgebras Semisimples com uma Involução Positiva	70
	Bibliografia	78



# Introdução

Dentro do nosso contexto, uma involução é um anti-automorfismo de ordem dois de um anel. O exemplo mais elementar de involução é a transposição de matrizes. Um exemplo mais complicado de uma álgebra sobre  $\mathbb{Q}$  que admite uma involução é a álgebra de multiplicação de uma superfície de Riemann. Albert (1934/35) determinou condições necessárias e suficientes para que uma álgebra com divisão sobre  $\mathbb{Q}$  seja uma álgebra de multiplicação. Para conseguir isto, Albert desenvolveu a teoria de álgebras centrais simples com involução, baseado na teoria de álgebras simples iniciada alguns anos antes por Brauer, Noether e também por Albert e Hasse. Esta é a origem histórica da teoria de involuções.

Seja  $G$  um grupo finito,  $K$  um corpo e  $K[G]$  a álgebra de grupo de  $G$  sobre  $K$ . Em [10], Scharlau investiga a involução canônica  $\sigma$  sobre  $K[G]$ , a qual é a aplicação  $K$ -linear definida por  $\sigma(g) = g^{-1}$ . Assumindo que  $\text{car } K = 0$ , pelo Teorema de Maschke (2.23),  $K[G]$  é uma álgebra semisimples. Sabemos ainda que cada fator simples da álgebra de grupo é uma álgebra de matrizes (Teorema de Wedderburn, 2.11). No Teorema 13.3 do Capítulo 8 de [10], Scharlau mostra que se  $K$  é um corpo real fechado, então cada fator simples  $B$  de  $K[G]$  é invariante pela involução canônica e, mais ainda, a involução sobre  $B$  é a conhecida involução conjugada transposta. O Capítulo 4 desta dissertação está dedicado a demonstração deste Teorema 13.3 do livro do Scharlau.

Como o nosso intuito é trabalhar sobre corpos reais fechados, no Capítulo 1 iremos explorar um pouco da teoria de corpos formalmente reais e corpos ordenados.

Ainda neste capítulo faremos uma breve introdução de conceitos e resultados da teoria de formas quadráticas.

Para um bom entendimento do Teorema 13.3 é necessário que se conheça bem a teoria de anéis simples e semisimples. Isto está detalhado no Capítulo 2.

No Capítulo 3 iremos estudar as álgebras centrais simples, onde toda a teoria de involuções foi inicialmente desenvolvida. Vale ainda ressaltar que toda a teoria de álgebras centrais simples se aplica a álgebra de matrizes.

Como trabalharemos a maior parte do tempo com corpos reais fechados podemos falar em involução positiva. Apesar de não ter sido comentado em [10], a involução canônica do Teorema 13.3 é uma involução positiva. Na verdade, o Teorema 13.3 é verdadeiro para qualquer involução positiva sobre  $K[G]$ . Em [2], Oukhtite e Boulagouaz estenderam este resultado para o caso de involuções positivas sobre qualquer álgebra semisimples de dimensão finita sobre um corpo real fechado. Eles mostram que se  $\sigma$  é uma involução positiva sobre uma álgebra semisimples, então  $\sigma$  restrita a cada fator simples é a involução conjugada transposta. Este resultado está detalhado no Capítulo 5 desta dissertação.

# Capítulo 1

## Preliminares

Iniciamos este capítulo com a teoria de corpos ordenados, ou seja, corpos que possuem uma ordem. O exemplo mais conhecido de corpo ordenado é o corpo dos números reais  $\mathbb{R}$ . Iremos ver que existe uma subclasse dos corpos ordenados (corpos reais fechados) que tem o mesmo comportamento de  $\mathbb{R}$  no que diz respeito às propriedades algébricas e de ordem. Iremos, inclusive, demonstrar nesse capítulo o Teorema Fundamental da Álgebra para corpos reais fechados, e no Capítulo 4 demonstraremos o Teorema de Frobenius, também para corpos reais fechados. Introduziremos ainda neste capítulo alguns conceitos e resultados da teoria de formas bilineares e quadráticas, apenas o necessário para o bom entendimento do restante do trabalho.

### 1.1 Corpos Formalmente Reais e Ordenados

Iniciaremos definindo corpos formalmente reais, pois só podemos definir ordem nesses tipos de corpos. Veremos a seguir que, na verdade, todo corpo formalmente real possui uma ordem.

**Definição 1.1.** Um corpo  $K$  é dito *formalmente real* ou simplesmente *real* se  $-1$  não pode ser representado como soma de quadrados em  $K$ .

**Observação 1.2.** Note que corpos de característica finita não são formalmente reais. Com efeito, consideremos um corpo de característica  $p$ , logo  $\underbrace{1 + \dots + 1}_{p \text{ vezes}} = 0$ , o que implica que  $\underbrace{1^2 + \dots + 1^2}_{p-1 \text{ vezes}} = -1$ . Assim corpos formalmente reais devem ter característica zero.

Se  $A$  é um anel comutativo arbitrário, denotaremos por  $\square A$  o conjunto dos elementos  $x \in A$  tais que  $x$  é a soma de quadrados de  $A$  e  $\square A^* = \square A - \{0\}$ .

**Proposição 1.3.** *Um corpo  $K$  é formalmente real se, e somente se,  $\square K \neq K$ .*

**Demonstração:** Se  $K$  é formalmente real  $-1 \notin \square K$  e portanto  $\square K \neq K$ .

Reciprocamente, suponha que  $-1 \in \square K$ , para todo  $a \in K$  temos

$$a = \left(\frac{a+1}{2}\right)^2 + (-1)\left(\frac{a-1}{2}\right)^2,$$

então  $a \in \square K$ , ou seja,  $\square K = K$ . Portanto se  $\square K \neq K$ , então  $-1 \notin \square K$ . ■

**Lema 1.4.** *Se  $K$  é um corpo, então  $\square K$  é fechado para a adição e a multiplicação e  $\square K^*$  é um grupo multiplicativo.*

**Demonstração:** Primeiramente considere  $x, x' \in \square K$ , logo

$$x+x' = \sum y_i^2 + \sum y'_i{}^2 \in \square K \text{ e } x.x' = \sum y_i^2 \cdot \sum y'_i{}^2 = \sum_{i,j} (y_i \cdot y'_j)^2 \in \square K \text{ com } y_i, y'_i \in K.$$

Para provarmos que  $\square K^*$  é um grupo multiplicativo, basta mostrarmos que para todo  $x \in \square K^*$  existe  $x^{-1} \in \square K^*$  tal que  $x.x^{-1} = 1$ , visto que as outras condições seguem trivialmente. Note que se  $x \in \square K^*$  temos  $x(x^{-1})^2 = \sum y_i^2 \cdot (x^{-1})^2 = \sum (y_i x^{-1})^2 \in \square K^*$ , ou seja,  $x^{-1} = x(x^{-1})^2 \in \square K^*$ . ■

Para aplicações posteriores, definiremos ordem de uma maneira mais geral do que a necessária para os propósitos desta seção.

**Definição 1.5.** Seja  $A$  um anel comutativo. Um subconjunto  $P \subset A$  é chamado de *pré-ordem* de  $A$  se

$$P + P \subset P, \quad P \cdot P \subset P, \quad -1 \notin P, \quad \square A \subset P.$$

Uma pré-ordem de um corpo  $K$  é uma *ordem* se também valem

$$P \cup -P = K, \quad P \cap -P = 0.$$

**Lema 1.6. (Prestel)** *Seja  $P$  uma pré-ordem de  $A$ . Se  $ab \in P$ , então  $P + aP$  ou  $P - bP$  é uma pré-ordem.*

**Demonstração:** Veja que  $(P + aP) + (P + aP) = P + P + a(P + P) \subset P + aP$  e

$$(P + aP)(P + aP) = PP + a(P + P) + a^2P \subset P + aP.$$

De modo análogo  $(P - bP) + (P - bP) \subset P - bP$ .

Como  $0 \in P$  temos que  $P \subset P + aP$  e como  $\square A \subset P$ , então  $\square A \subset P + aP$ . Analogamente se  $P \subset P - bP$ , então  $\square A \subset P - bP$ .

Suponha que  $-1 \in P + aP$  e  $-1 \in P - bP$ , logo existem  $x, y, v, w \in P$  tais que  $-1 = x + ay = v - bw$ . Dessa forma  $1 = (x + ay)(v - bw)$ , ou seja,  $1 = xv - bwx + ayv - aybw$ . Como  $ayv = -v - xv$  e  $-bwx = -x - vx$  temos  $1 = -x - vx - v - aybw$ , isto é,  $-1 = x + vx + v + aybw \in P$ , pois  $ab \in P$ . Isto é uma contradição e portanto  $-1 \notin P + aP$  ou  $-1 \notin P - bP$ . ■

**Lema 1.7.** *Seja  $P$  uma pré-ordem maximal de  $A$  (que é maximal com respeito a inclusão). Então  $P \cup -P = A$  e  $P \cap -P$  é um ideal primo de  $A$ .*

**Demonstração:** Primeiro vamos mostrar que  $P \cup -P = A$ . Para isso, tome  $x \in A$ . Como  $x^2 \in P$ , pelo lema anterior  $P + xP$  ou  $P - xP$  é uma pré-ordem. Assumiremos primeiro que  $P - xP$  seja uma pré-ordem, logo  $P \subset P - xP$  e como  $P$  é uma pré-ordem maximal devemos ter  $P = P - xP$ , assim  $-x \in P$ . Se assumirmos que  $P + xP$

é uma pré-ordem, pelo mesmo argumento acima, teremos  $x \in P$ . Portanto para todo  $x \in A$  temos que  $x \in P$  ou  $x \in -P$  e como  $P \cup -P \subset A$  temos  $P \cup -P = A$ .

Agora mostraremos que  $P \cap -P$  é um ideal de  $A$ . Tomemos  $x_1, x_2 \in P \cap -P$ , como  $P$  é uma pré-ordem,  $x_1 + x_2 \in P$ . Por outro lado,  $-x_1 - x_2 = -(x_1 + x_2) \in P$ , o que implica que  $x_1 + x_2 \in -P$ . Seja  $x \in P \cap -P$  e  $a \in A$ , como  $P \cup -P = A$  temos  $a \in P$  ou  $a \in -P$ . Se  $a \in P$  então  $ax \in P$ , pois  $x \in P$  e  $P$  é pré-ordem, mas também  $x \in -P$ , assim  $a(-x) \in P$ , o que implica que  $ax \in -P$ . Logo  $ax \in P \cap -P$ . Se  $a \in -P$ , de forma análoga, obtemos que  $ax \in P \cap -P$ . Portanto  $P \cap -P$  é um ideal de  $A$ .

Resta mostrar que  $P \cap -P$  é um ideal primo, para tanto considere  $x_1 x_2 \in P \cap -P$ . Suponha que  $x_1 \notin P \cap -P$ . Como  $x_1 x_2 \in P$ , pelo Lema 1.6 temos que  $P + x_1 P$  ou  $P - x_2 P$  é uma pré-ordem. Se  $x_1 \notin P$ ,  $P + x_1 P$  não pode ser uma pré-ordem, pois  $P$  é uma pré-ordem maximal. Logo  $P - x_2 P$  é pré-ordem e como  $P$  é maximal devemos ter  $-x_2 \in P$ , ou seja,  $x_2 \in -P$ . Por outro lado, como  $x_1 x_2 \in -P$ , então  $x_1(-x_2) \in P$ , novamente pelo Lema 1.6,  $P + x_1 P$  ou  $P + x_2 P$  é uma pré-ordem. Mas  $x_1 \notin P$  assim  $P + x_1 P$  não pode ser uma pré-ordem, logo  $P + x_2 P$  é pré-ordem, ou seja,  $x_2 \in P$ . Donde concluímos que  $x_2 \in P \cap -P$ . Se  $x_1 \notin -P$ , como  $(-x_1)(-x_2) \in P \cap -P$ , de forma análoga ao caso anterior, concluímos que  $x_2 \in P \cap -P$ . Portanto  $P \cap -P$  é um ideal primo de  $A$ . ■

**Corolário 1.8.** *Seja  $P$  uma pré-ordem de  $A$ . Então existe uma pré-ordem  $R \supset P$  tal que  $R \cup -R = A$  e  $R \cap -R$  é um ideal primo de  $A$ .*

**Demonstração:** Pelo Lema de Zorn,  $P$  está contido em uma pré-ordem maximal  $R$  e pelo Lema 1.7 temos o desejado. ■

Pelo Lema 1.7, toda pré-ordem maximal de um corpo é uma ordem, já que um corpo só possui os ideais triviais.

**Teorema 1.9.** *Sejam  $K$  um corpo formalmente real e  $P$  uma pré-ordem de  $K$ . Então  $P$  é igual a intersecção de todas as ordens  $R$  contendo  $P$ , ou seja,  $P = \bigcap_{R \supset P} R$ .*

**Demonstração:** Sendo a intersecção tomada sobre todas ordens contendo  $P$  temos que  $P \subset \bigcap R$ . Resta mostrarmos que  $\bigcap R \subset P$ , o que equivale a mostrar que se um elemento não pertence a  $P$ , então este não pertence a uma das ordens  $R$  em questão. Considere  $\alpha \notin P$ , então  $P - \alpha P$  é uma pré-ordem, pois caso contrário  $-1 = x - \alpha y$  com  $x, y \in P$ . Assim  $\alpha = (xy^{-1} + y^{-1})(yy^{-1})$  leva à contradição  $\alpha = (xy)y^{-2} + yy^{-2} \in P$ . Pelo corolário anterior existe uma ordem  $R$  com  $P - \alpha P \subset R$ , então  $-\alpha \in R$ . Portanto  $\alpha \notin R$ , pois  $R \cap -R = \{0\}$ . ■

**Corolário 1.10. (Artin-Schreier)** *Assuma que  $K$  é formalmente real. Então  $\square K$  é a intersecção de todas as ordens de  $K$ . Em particular  $K$  tem ao menos uma ordem.*

**Demonstração:** Como  $-1 \notin \square K$ , pelo Lema 1.4,  $\square K$  é uma pré-ordem de  $K$ . Pelo lema acima  $\square K$  é a intersecção de todas as ordens que contém  $\square K$  e como toda ordem de  $K$  contém  $\square K$ , concluímos que  $\square K$  é a intersecção de todas as ordens de  $K$ . Claramente  $K$  possui alguma ordem, pois caso contrário a intersecção de todas as ordens de  $K$  daria vazio. ■

**Observação 1.11.** (1) Se  $P$  é uma pré-ordem de  $K$ , os elementos de  $P^* = P \setminus \{0\}$  são ditos *positivos*, os elementos de  $-P^*$  são ditos *negativos* (com respeito a  $P$ ).

(2) Das condições  $P + P \subset P$ ,  $PP \subset P$ ,  $P \cup -P = K$  e  $P \cap -P = 0$  pode-se mostrar as outras duas:  $\square K \subset P$  e  $-1 \notin P$ . De fato, como temos  $x$  ou  $-x$  em  $P$  para todo  $x \neq 0$ ,  $x^2 = (-x)^2 \in P$  e portanto  $\square K \subset P$ . Além disso,  $1 \in \square K \subset P$  e  $P \cap -P = 0$ , então  $-1 \notin P$ .

(3) Se  $P$  é uma ordem de  $K$ , podemos definir uma relação binária  $\leq$  por

$$x \leq y \Leftrightarrow y - x \in P.$$

Esta relação satisfaz as seguintes propriedades para  $x, y, z \in K$ .

$$(i) x \leq x$$

$$(ii) x \leq y, y \leq z \Rightarrow x \leq z$$

$$(iii) x \leq y, y \leq x \Rightarrow x = y$$

$$(iv) x \leq y \text{ ou } y \leq x$$

$$(v) x \leq y \Rightarrow x + z \leq y + z$$

$$(vi) x \leq y, 0 \leq z \Rightarrow zx \leq zy$$

Para mostrarmos essas seis propriedades usaremos basicamente a definição da relação binária dada acima e o fato de  $P$  ser uma ordem. (i) segue do fato de que  $0 \in P$ , visto que  $x \leq x \Leftrightarrow x - x \in P$ . Em (ii) temos que  $y - x \in P$  e  $z - y \in P$ , logo  $(y - x) + (z - y) \in P$ , ou seja,  $z - x \in P$ . De (iii) temos  $y - x \in P$  e  $x - y \in P$ . Mas note que  $x - y = -(y - x) \in -P$  e como  $P \cap -P = \{0\}$  devemos ter  $y - x = 0$ , ou seja,  $x = y$ . A propriedade (iv) nos diz que  $x \leq y$  ou  $y \leq x$ . Suponha que  $y - x \notin P$ , dessa forma  $-(y - x) \in P$ , ou seja,  $x - y \in P$ . Supondo que  $x - y \notin P$  analogamente teremos  $y - x \in P$ . Em (v) temos  $y - x \in P$ , logo  $y - z + z - x \in P$ , ou seja,  $(y + z) - (x + z) \in P$ . Segue que  $x + z \leq y + z$ . Finalizando, em (vi) temos  $y - x \in P$  e  $z \in P$ , o que implica que  $(y - x)z \in P$ , isto é,  $yz - xz \in P$ . Portanto  $xz \leq yz$ .

Reciprocamente, se é dada uma relação binária  $\leq$  com as seis propriedades acima, então  $P := \{x \in K ; 0 \leq x\}$  é uma ordem. De fato, para todo  $x, y \in P$  temos  $0 \leq x$  e  $0 \leq y$ . Segue de (v) que  $0 + y \leq x + y$  e assim  $0 \leq y \leq x + y$ , ou seja,  $x + y \in P$ . Pelo item (vi), para todo  $x, y \in P$  temos  $0 \cdot y \leq xy$ , ou seja,  $0 \leq xy$ . Portanto  $xy \in P$ . Como  $P = \{x \in K ; 0 \leq x\}$  temos que  $-P = \{x \in K ; x \leq 0\}$ . Vamos mostrar que  $P \cup -P = K$ . Claramente  $P \cup -P \subset K$ . Considere  $x, 0 \in K$ , pelo item (iv),  $x \leq 0$  ou  $0 \leq x$ , ou seja,  $x \in P$  ou  $x \in -P$ . Logo  $x \in P \cup -P$ . Temos ainda que  $P \cap -P = \{0\}$ , já que para  $x \in P \cap -P$  temos que  $0 \leq x$  e  $x \leq 0$  e pelo item (iii) temos  $x = 0$ . Pelo item (2) da observação anterior podemos concluir que  $P$  é uma ordem.



Pelo visto acima, dada uma ordem  $P$  definimos uma relação  $\leq$  e dada a relação  $\leq$  definimos uma ordem  $P$ , ou seja, ambos conceitos são equivalentes. Assim  $\leq$  é freqüentemente chamada de *ordem* e  $P$  de *domínio positivo* ou *cone positivo* de  $\leq$ . Denotaremos  $x < y$  quando  $x \leq y$  e  $x \neq y$ .

**Definição 1.12.** Chamamos o par  $(K, P)$  formado por um corpo  $K$  e uma ordem  $P$  de  $K$  de *corpo ordenado*. Se  $F$  é um subcorpo de  $K$ , então  $P \cap F$  é uma ordem de  $F$ . Dizemos que  $(K_1, P_1)/(K, P)$  é uma *extensão de corpos ordenados* se  $K_1/K$  é uma extensão de corpos e  $P_1 \supset P$ . Então  $P = K \cap P_1$  e  $P_1$  é dita uma extensão de  $P$  para  $K_1$ .

Para extensões algébricas o seguinte resultado é fundamental.

**Teorema 1.13.** *Seja  $(K, P)$  um corpo ordenado.*

- (1) *Se  $L = K(\sqrt{d})$ , existe uma extensão de  $P$  para  $L$  se, e somente se,  $d \in P$ .*
- (2) *Se  $L/K$  é uma extensão finita de grau ímpar, existe sempre uma extensão de  $P$  para  $L$ . Em particular,  $L$  é formalmente real.*

**Demonstração:** (1) Primeiramente mostraremos que se  $d \in P$ , então existe uma extensão de  $P$  para  $L = K(\sqrt{d})$ . Consideremos o semi-anel gerado por  $P$  e  $\square L$ , que é o conjunto de todas somas  $\sum x_i y_i^2$ ,  $x_i \in P$  e  $y_i \in L$ . Se  $d \in P$ , este conjunto é uma pré-ordem de  $L$ , pois caso contrário teríamos  $-1 = \sum x_i (\alpha_i + \beta_i \sqrt{d})^2 = \sum x_i (\alpha_i^2 + \beta_i^2 d) + 2\sqrt{d} \sum x_i \alpha_i \beta_i$ , logo  $-1 = \sum x_i (\alpha_i^2 + \beta_i^2 d) \in P$ , o que é uma contradição. Pelo Teorema 1.9 esta pré-ordem está contida em uma ordem de  $L$ .

Reciprocamente, suponha que exista  $P_1$  uma extensão de  $P$ , logo  $K \cap P_1 = P$ . Como  $\square L \subset P_1$ ,  $\sqrt{d}^2 = d \in P_1$  e como  $d \in K$ , temos  $d \in K \cap P_1 = P$ .

(2) Como  $L/K$  é finita, então é algébrica. Assumimos  $L = K(x)$  e seja  $p(X)$  o polinômio minimal de  $x$ , de grau  $n$ . Consideremos o semi-anel  $R$  gerado por  $P$  e  $\square L$ . Vamos assumir que se  $M/K$  é uma extensão finita de grau ímpar tal que o grau

de  $M/K$  seja menor que  $n$ , então existe uma extensão de  $P$  para  $M$ . Para mostrar que o resultado vale para  $n$ , mostraremos que  $R$  é uma pré-ordem de  $L$ .

Supondo que  $R$  não é uma pré-ordem, então  $-1 \in R$ , ou seja,

$$-1 = \sum \alpha_i f_i(X)^2 + p(X)q(X) \quad (1.1)$$

sendo que  $\alpha_i \in P$  e  $\deg(f_i) < n = \deg(p)$ , onde “deg” denota o grau do polinômio. Calculando esta equação em  $x$  vemos que as  $f_i$  não podem ser todas constantes, senão teríamos  $-1 = \sum \alpha_i c^2 \in P$  com  $c \in K$ . Os termos de maior grau de  $\sum \alpha_i f_i(X)^2$  não podem ser cancelados, pois todos são positivos. Logo o grau de  $\sum \alpha_i f_i(X)^2$  é par. Da equação (1.1) e do fato que  $n$  é ímpar segue que o grau de  $q(X)$  tem que ser ímpar. Seja  $r(X)$  um fator irredutível de grau ímpar de  $q(X)$ . Então  $-1 \equiv \sum \alpha_i f_i(X)^2 \pmod{r(X)}$ . Como  $L' = K[X]/(r(X))$  é uma extensão finita de  $K$  de grau ímpar, e menor do que  $n$ , por indução, existe uma extensão  $R'$  de  $P$  para  $L'$ . Logo  $P \subset R'$  e  $\square L' \subset R'$ . Mas como  $-1 = \sum \alpha_i \overline{f_i(X)}^2$  com  $\alpha_i \in P$  e  $(\overline{f_i(X)})^2 \in \square L'$  obtemos que  $-1 \in R'$ . O que é uma contradição. Portanto  $R$  é uma pré-ordem de  $L$  que esta contida numa ordem de  $L$ . ■

## 1.2 Corpos Reais Fechados

Iniciamos esta seção considerando extensões algébricas maximais de corpos formalmente reais e de corpos ordenados.

**Definição 1.14.** Um corpo formalmente real  $K$  é *real fechado* se nenhuma extensão algébrica própria de  $K$  é formalmente real. Uma extensão algébrica  $L$  de  $K$  é chamada *fecho real* de  $K$  se  $L$  é real fechado.

**Definição 1.15.** Um corpo ordenado  $(K, P)$  é chamado *real fechado* se não existe extensão algébrica própria  $(L, R)$  de  $(K, P)$ . Uma extensão algébrica  $(L, R)$  de  $(K, P)$  é dita *fecho real* de  $(K, P)$  se  $(L, R)$  é real fechado.

**Teorema 1.16.** *Todo corpo formalmente real tem um fecho real. Todo corpo ordenado tem um fecho real.*

**Demonstração:** Seja  $K$  um corpo formalmente real. Tome um fecho algébrico  $\overline{K}$  de  $K$ . Aplicando o Lema de Zorn para a família de todos corpos intermediários formalmente reais  $\overline{K} \supset L \supset K$ , obteremos um fecho real de  $K$ .

Analogamente, para todo corpo ordenado  $(K, P)$ , consideremos  $\overline{K}$  um fecho algébrico de  $K$ . Aplicando o Lema de Zorn para todos corpos intermediários ordenados  $\overline{K} \supset (L, R) \supset (K, P)$ , teremos um fecho real de  $(K, P)$ . ■

O teorema seguinte mostra que existe somente uma noção de real fechado.

**Teorema 1.17.** *Se  $(K, P)$  é real fechado, então  $K$  é real fechado e  $P = \square K = K^2$ .*

**Demonstração:** Como  $(K, P)$  é real fechado, então não há extensão algébrica própria ordenada  $(L, R)$  de  $(K, P)$ . Se  $d \in P$ , pelo item (1) do Teorema 1.13, existe uma extensão  $(L = K(\sqrt{d}), P_1)$  com  $P_1$  estendendo  $P$ . Então  $(L, P_1) = (K, P)$  o que implica que  $d \in K^2$ . Portanto  $P = K^2$ . Como  $K^2 \subset \square K \subset P$ , obtemos o desejado. Em particular existe uma única ordem em  $K$ .

Vamos mostrar agora que  $K$  é real fechado, para isto suponha que exista uma extensão formalmente real própria  $L/K$ . Segue do Corolário 1.10 que  $L$  tem pelo menos uma ordem. Como toda ordem contém  $K^2$ , esta necessariamente é uma extensão de  $P$ . Isto é uma contradição, pois  $(K, P)$  é real fechado. ■

Este teorema revela que  $R$  é unicamente determinado se  $(L, R)$  é um fecho real de  $(K, P)$ , a saber,  $R = L^2$ . Assim dizemos simplesmente que  $L$  é um fecho real de  $(K, P)$ .

Dos teoremas anteriores temos o seguinte corolário.

**Corolário 1.18.** *Se  $K$  é formalmente real, então toda ordem de  $K$  pode ser escrita como  $K \cap L^2$ , onde  $L$  é um fecho real de  $K$  para a ordem dada.*

**Demonstração:** Seja  $K$  formalmente real e  $P$  uma ordem de  $K$ . Pelos teoremas anteriores existe um fecho real  $(L, R)$  de  $(K, P)$  com  $R = L^2$ . Como  $R$  estende  $P$  devemos ter que  $P = K \cap L^2$ . ■

**Observação 1.19.** Um corpo  $K$  é chamado *euclidiano* se  $K^2$  é uma ordem de  $K$ . Na verdade, esta é a única ordem de  $K$ . De fato, caso haja uma outra ordem  $P$ , devemos ter que  $K^2 \subset P$ . Considere  $x \in P$  tal que  $x \notin K^2$ , então  $x \in -K^2 \subset -P$ . Logo  $x \in P \cap -P$  o que implica que  $x = 0$ . Portanto  $K^2 = P$ .

É fácil ver que todo corpo euclidiano é formalmente real e que corpos reais fechados são euclidianos.

Veremos em seguida o Teorema Fundamental da Álgebra, que caracteriza corpos reais fechados. Mas antes precisamos de um lema. Na demonstração deste lema denotaremos o grau de uma extensão  $L$  de  $K$  por  $[L : K]$ .

**Lema 1.20.** *Seja  $K$  um corpo que não é algebricamente fechado. Suponha que  $K(\sqrt{-1})$  é uma extensão algebricamente fechada de  $K$ . Então toda extensão algébrica de  $K$  é isomorfa a  $K(\sqrt{-1})$ .*

**Demonstração:** Seja  $F$  uma extensão algébrica de  $K$  e seja  $u \in F - K$  com polinômio minimal  $f \in K[x]$  de grau superior a um. Como  $K(\sqrt{-1})$  é algebricamente fechado,  $f$  se decompõe em  $K(\sqrt{-1})$ . Se  $v \in K(\sqrt{-1})$  é uma raiz de  $f$ , então as extensões  $K(u)$  e  $K(v)$  são isomorfas, visto que  $u$  e  $v$  são raízes do mesmo polinômio minimal de ambas extensões. Assim  $K(u) \simeq K(v) \subset K(\sqrt{-1})$ . Como  $[K(v) : K] = [K(u) : K] > 1$  e  $[K(\sqrt{-1}) : K] = 2$  temos que  $[K(v) : K] = 2$  e  $K(v) = K(\sqrt{-1})$ , logo  $F$  é uma extensão algébrica de um corpo algebricamente fechado  $K(u) \simeq K(\sqrt{-1})$ . Como um corpo algebricamente fechado não possui extensão algébrica, a não ser o próprio, devemos ter  $F = K(u) \simeq K(\sqrt{-1})$ . ■

**Teorema 1.21. (Teorema Fundamental da Álgebra)** *As seguintes afirmações são equivalentes:*

- (1)  $K$  é real fechado.
- (2)  $K$  é euclidiano e todo polinômio de grau ímpar sobre  $K$  tem uma raiz em  $K$ .
- (3)  $K$  não é algebricamente fechado, mas  $K(\sqrt{-1})$  o é.

**Demonstração:** (1)  $\Rightarrow$  (2) Como  $K$  é real fechado, pelo Teorema 1.17,  $P = K^2$ . Assuma agora que existe um polinômio  $p(X)$  de grau ímpar que não tenha raízes em  $K$ . Assim cada um de seus fatores também não tem raízes em  $K$ . Como a decomposição de polinômios de grau ímpar em fatores irredutíveis deve conter ao menos um fator de grau ímpar, podemos assumir que  $p(X)$  é irredutível. Como  $L = K/(p(X))$  é uma extensão de grau ímpar, pelo Teorema 1.13 (2) temos que  $K/(p(X))$  é formalmente real. O que é um absurdo, pois  $K$  é real fechado. Portanto  $p(X)$  possui ao menos uma raiz em  $K$ .

(2)  $\Rightarrow$  (3) Como  $K$  é euclidiano, os quadrados em  $K$  são positivos, logo o polinômio  $X^2 + 1$  não tem raiz em  $K$ . Assim  $K$  não é algebricamente fechado.

Passaremos a mostrar agora que  $L = K(\sqrt{-1})$  é algebricamente fechado. O primeiro fato a notar é que  $L^* = L^{*2}$ . Para tanto basta mostrar que  $L^* \subset L^{*2}$ . Dado  $\alpha + \beta\sqrt{-1}$  queremos encontrar  $x, y$  tais que  $(x + y\sqrt{-1})^2 = \alpha + \beta\sqrt{-1}$ . Se tomarmos  $x = 0$ , basta considerarmos  $y^2 = -\alpha$ . Se  $x \neq 0$ , da igualdade  $x^2 + 2xy\sqrt{-1} - y^2 = \alpha + \beta\sqrt{-1}$  temos que  $x^2 - y^2 = \alpha$  e  $2xy = \beta$ , ou seja,  $y = \beta/2x$  e  $x^2 - \beta^2/2x^2 = \alpha$ . Assim temos  $2x^4 - 2\alpha x^2 - \beta^2 = 0$ . Portanto basta tomarmos  $x = \sqrt{1/2(\alpha + \sqrt{\alpha^2 + 2\beta^2})}$  e  $y = \frac{\beta}{2x}$ .

Pelo provado acima,  $L$  não pode ter extensão quadrática. Assumimos agora que  $L$  tem uma extensão algébrica  $M$  de grau  $2^n m > 1$ , com  $m$  ímpar. Seja  $N$  o fecho normal de  $M$  sobre  $K$ , logo  $[N : K] = 2^{n'} m'$ , com  $m'$  ímpar. Como  $K$  é euclidiano,  $\text{car } K = 0$  e todo polinômio irredutível é separável. Assim  $N/K$  é uma extensão finita normal e separável. Considerando o grupo de Galois  $\text{Gal}(N/K)$ , temos que

$o(\text{Gal}(N/K)) = [N : K] = 2^{n'} m'$ . Este grupo possui um 2-subgrupo de Sylow  $H$  de ordem  $2^{n'}$ . Se  $F$  é o corpo fixo de  $H$ , temos que  $[F : K] = \frac{o(\text{Gal}(N/K))}{o(H)} = \frac{2^{n'} m'}{2^{n'}} = m'$ , que é ímpar. Note que  $K$  não tem extensão de grau ímpar, pois todo polinômio de grau ímpar sobre  $K$  tem uma raiz em  $K$ . Logo  $F = K$  e assim  $m' = 1$ . Como  $[N : K] = [N : L].[L : K]$  temos que  $[N : L] = 2^{n'-1}$ . Suponhamos que  $n' > 1$ . O grupo de Galois de  $N$  sobre  $L$  tem ordem  $2^{n'-1}$  e pelo Teorema de Cauchy temos um subgrupo  $H_1$  de  $\text{Gal}(N/L)$  tal que  $o(H_1) = 2$ . Considerando  $F_1$  o corpo fixo de  $H_1$  temos que  $[F_1 : L] = 2$ , o que é um absurdo, pois  $L$  não tem extensão quadrática. Dessa forma concluímos que  $n' = 1$ , assim  $N = L$ . Portanto  $L$  é algebricamente fechado.

(3)  $\Rightarrow$  (1) Note que  $K(\sqrt{-1})$  não é formalmente real, pois  $-1 = (\sqrt{-1})^2$ . Pelo Lema 1.20, temos que  $K(\sqrt{-1})$  é a única extensão algébrica própria de  $K$  (a menos de isomorfismo). Assim para mostrarmos que  $K$  é real fechado, basta mostrarmos que  $K$  é formalmente real. Com efeito, como  $K$  não é algebricamente fechado e  $K(\sqrt{-1})$  o é devemos ter  $K \neq K(\sqrt{-1})$ , o que implica que  $-1$  não é um quadrado de  $K$ . Assim é suficiente mostrarmos que toda soma de quadrados de  $K$  é um quadrado, isto é,  $K^2 + K^2 \subset K^2$ . Isso nos garante que  $-1$  não é soma de quadrados de  $K$ . Como  $K(\sqrt{-1})$  é algebricamente fechado, para todo  $a, b \in K$  existe  $c, d \in K$  tal que  $a + b\sqrt{-1} = (c + d\sqrt{-1})^2$ . Logo  $a = c^2 - d^2$  e  $b = 2cd$ . Assim  $a^2 + b^2 = (c^2 + d^2)^2 \in K^2$ . Portanto  $K$  é formalmente real. ■

Encerraremos essa seção com um corolário que segue diretamente do Lema 1.20 e do Teorema Fundamental da Álgebra 1.21.

**Corolário 1.22.** *Toda extensão algébrica de um corpo real fechado  $K$  é isomorfa ao corpo  $K(\sqrt{-1})$ .*

### 1.3 Espaços Bilineares e Quadráticos

Iniciamos recordando os conceitos de forma bilinear e forma quadrática vistos nos cursos de Álgebra Linear. Nesta seção,  $K$  sempre denotará um corpo de característica distinta de 2.

**Definição 1.23.** Seja  $V$  um espaço vetorial sobre  $K$ . Uma *forma bilinear simétrica* sobre  $K$  é uma aplicação  $B : V \times V \rightarrow K$  que satisfaz as propriedades:

- (1)  $B(x + y, z) = B(x, z) + B(y, z)$ , para todo  $x, y, z \in V$ ;
- (2)  $B(\alpha x, y) = \alpha B(x, y) = B(x, \alpha y)$ , para todo  $x, y \in V$  e  $\alpha \in K$ ;
- (3)  $B(x, y) = B(y, x)$ , para todo  $x, y \in V$ .

**Definição 1.24.** Seja  $V$  um espaço vetorial sobre  $K$ . A aplicação  $q : V \rightarrow K$  é chamada de *forma quadrática de  $V$*  se satisfaz as seguintes propriedades:

- (1)  $q(\alpha x) = \alpha^2 q(x)$ , para todo  $x \in V, \alpha \in K$ ;
- (2)  $B_q : V \times V \rightarrow K$  definida por  $B_q(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$ , para todo  $x, y \in V$ , é uma forma bilinear simétrica.

A função  $B_q$  definida acima é dita a *forma bilinear associada à  $q$* .

Dada uma forma bilinear simétrica  $B$  sobre um espaço vetorial  $V$ , podemos definir  $q_B : V \rightarrow K$  por  $q_B(x) = B(x, x)$ . A função  $q_B$  definida é uma forma quadrática e é chamada *forma quadrática associada à  $B$* . Quando não houver perigo de confusão usaremos apenas  $q$  para denotar  $q_B$  e apenas  $B$  para denotar  $B_q$ .

**Observação 1.25.** Sejam  $\mathcal{B} = \{e_1, \dots, e_n\}$  uma base do espaço vetorial  $V$  e  $x = \sum_{i=1}^n x_i e_i, y = \sum_{j=1}^n y_j e_j$  elementos de  $V$ . Se  $B$  é uma forma bilinear sobre  $K$ , então

$$B(x, y) = B\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j\right) = \sum_{i=1}^n x_i B(e_i, \sum_{j=1}^n y_j e_j) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j B(e_i, e_j).$$

**Definição 1.26.** A matriz  $M_B = (B(e_i, e_j))$  é chamada *matriz da forma bilinear*  $B$  em relação à base  $\mathcal{B}$ .

Deste modo, temos

$$B(x, y) = (x_1 \ x_2 \ \dots \ x_n) \begin{pmatrix} B(e_1, e_1) & \dots & B(e_1, e_n) \\ \vdots & \ddots & \vdots \\ B(e_n, e_1) & \dots & B(e_n, e_n) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = [x]_{\mathcal{B}}^t M_B [y]_{\mathcal{B}}.$$

A *matriz de uma forma quadrática*  $q$  é definida como sendo a matriz da forma bilinear associada a  $q$ . Assim,

$$M_q = M_{B_q} \text{ e } q(x) = B_q(x, x) = [x]_{\mathcal{B}}^t M_{B_q} [x]_{\mathcal{B}}.$$

**Definição 1.27.** Um *espaço bilinear* é um par  $(V, B)$ , onde  $V$  é um espaço vetorial sobre  $K$  e  $B$  é uma forma bilinear simétrica sobre  $V$ . Chamamos  $(V, q)$  de *espaço quadrático*, onde  $q$  é uma forma quadrática sobre  $V$ .

A verificação de que as correspondências  $q \rightarrow B_q$  e  $B \rightarrow q_B$  (ou  $(V, q) \rightarrow (V, B_q)$  e  $(V, B) \rightarrow (V, q_B)$ ) são inversas uma da outra é imediata desde que  $q_{B_q} = q$  e  $B_{q_B} = B$ . Ou seja, podemos identificar formas quadráticas com formas bilineares. Assim, conceitos e propriedades de espaços quadráticos (ou formas quadráticas) podem ser transmitidos para espaços bilineares (ou formas bilineares) e vice-versa.

Vale ressaltar que esta correspondência biunívoca não ocorre se o corpo  $K$  for de característica 2 ou se estivermos trabalhando com formas bilineares sobre anéis em que 2 não é inversível.

**Definição 1.28.** Sejam  $(V, B), (V', B')$  dois espaços bilineares. Dizemos que eles são *isométricos* se existe um isomorfismo linear  $\tau : V \rightarrow V'$  tal que  $B'(\tau(u), \tau(v)) = B(u, v)$ , para todo  $u, v \in V$  (ou  $q_{B'}(\tau(u)) = q_B(u)$ , para todo  $u \in V$ ).

Notação  $(V, B) \cong (V', B')$ .

Ser isométrico é uma relação de equivalência. A classe de equivalência  $(q) = \{q' \mid q' \cong q\}$  é chamada *classe de isometria*.



**Proposição 1.29.** *Sejam  $(V, B)$ ,  $(V', B')$  espaços bilineares. Então  $(V, B) \cong (V', B')$  se, e somente se,  $M_B$  é congruente a  $M_{B'}$ .*

**Demonstração:** [5], pg 4.■

**Definição 1.30.** Seja  $(V, B)$  um espaço bilinear. Dois vetores  $x, y \in V$  são *ortogonais* se  $B(x, y) = 0$ . Denotamos por  $x \perp y$ .

Se  $X$  e  $Y$  são subconjuntos de  $V$ , dizemos que  $X$  é *ortogonal* a  $Y$  se  $B(x, y) = 0$ , para todo  $x \in X$  e para todo  $y \in Y$ . Denotamos por  $X \perp Y$ .

**Definição 1.31.** Dizemos que  $(V, B)$  é um *espaço bilinear regular* (ou, *não degenerado*, ou equivalentemente, que  $q_B$  é uma *forma quadrática regular* (ou, *não degenerada*) se para todo  $x \in V$ ,  $B(x, y) = 0$  para todo  $y \in V$  implica que  $x = 0$ .

**Definição 1.32.** Se  $(V, B)$  e  $(V', B')$  são dois espaços bilineares, então escrevemos  $(V, B) \perp (V', B')$  para o espaço bilinear  $(V \oplus V', B \perp B')$ , onde

$$(B \perp B')((x, x'), (y, y')) = B(x, y) + B'(x', y').$$

O espaço  $(V, B) \perp (V', B')$  é chamado de *soma ortogonal de  $(V, B)$  e  $(V', B')$* . A soma ortogonal de espaços bilineares induz naturalmente uma soma ortogonal de espaços quadráticos  $(V, q_B) \perp (V', q'_B) = (V \oplus V', q_B \perp q'_B)$ , onde

$$(q_B \perp q'_B)(x, x') = q_B(x) + q'_B(x').$$

**Observação 1.33.** De modo análogo, definimos soma ortogonal para  $n$  espaços quadráticos. Dados os espaços quadráticos  $(V_i, q_i)$ ,  $i = 1, \dots, n$  ( $n \geq 2$ ). Seja  $V = V_1 \oplus \dots \oplus V_n$  e  $q : V \rightarrow K$  definida por  $q(x_1, \dots, x_n) = \sum_{i=1}^n q_i(x_i)$ . O par  $(V, q)$  é um espaço quadrático denotado por  $(V, q) = (V_1, q_1) \perp \dots \perp (V_n, q_n)$ , chamado soma ortogonal dos espaços  $(V_1, q_1), \dots, (V_n, q_n)$ . Observe que a forma bilinear associada a  $q$  é dada pela aplicação  $B : V \times V \rightarrow K$  definida por

$$B((x_1, \dots, x_n), (y_1, \dots, y_n)) = B_1(x_1, y_1) + \dots + B_n(x_n, y_n).$$

Quando o contexto for claro usaremos também a notação,  $V_1 \perp \dots \perp V_n$  ou  $q_1 \perp \dots \perp q_n$ .

**Definição 1.34.** Sejam  $(V, q)$  um espaço quadrático sobre  $K$  e  $d \in \dot{K}$ . Dizemos que  $q$  representa  $d$  se existe  $v \in V$  tal que  $q(v) = d$ . Note que  $v$  é automaticamente um vetor não nulo. Denotaremos por  $D_K(q)$  o conjunto formado pelos elementos de  $\dot{K}$  que são representados por  $q$ , ou seja,

$$D_K(q) = \{d \in \dot{K} \mid \exists v \in V \text{ tal que } q(v) = d\}.$$

Quando não houver perigo de confusão usaremos  $D(V)$  para denotar  $D_K(q)$ .

Nosso objetivo agora é mostrar que todo espaço quadrático é isométrico a uma soma ortogonal de espaços unidimensionais. A classe de isometria de um espaço quadrático unidimensional  $(Kv, q)$ , com  $q(v) = d \in \dot{K}$ , será denotada por  $\langle d \rangle$ . Claramente,  $\langle d \rangle$  é regular se, e somente se,  $d \in \dot{K}$ .

**Teorema 1.35. (Critério da Representação)** *Seja  $(V, q)$  um espaço quadrático e  $d \in \dot{K}$ . Então  $d \in D(V)$  se, e somente se,  $V \cong \langle d \rangle \perp V'$ , onde  $(V', q')$  é outro espaço quadrático.*

**Demonstração:** [5], Representation Criterion 2.3 pg 7.■

A primeira consequência do Critério da Representação é a existência de uma base ortogonal em qualquer espaço quadrático. Em outras palavras, todo espaço quadrático é isométrico a uma soma ortogonal de espaços unidimensionais.

**Corolário 1.36.** *Se  $(V, q)$  é um espaço quadrático sobre  $K$ , então existem escalares  $d_1, \dots, d_n \in \dot{K}$  tais que  $V \cong \langle d_1 \rangle \perp \dots \perp \langle d_n \rangle$ .*

**Demonstração:** Se  $D(V) = \emptyset$ , então  $B \equiv 0$  e  $V$  é isométrico a soma de  $\langle 0 \rangle$ 's.

Se existe algum  $d_1 \in D(V)$ , pelo teorema anterior  $V \cong \langle d_1 \rangle \perp V'$ , para algum subespaço  $(V', B')$ . Aplicando o teorema anterior novamente com  $(V', B')$ , obtemos  $V \cong \langle d_1 \rangle \perp \langle d_2 \rangle \perp V''$ , para algum subespaço  $(V'', B'')$  e  $d_2 \in \dot{K}$ . Como  $V$  é de dimensão finita, após um número finito de passos obtemos o resultado.■

**Notação:** Representaremos  $\langle d_1 \rangle \perp \dots \perp \langle d_n \rangle$  por  $\langle d_1, \dots, d_n \rangle$ . O caso especial da forma  $\langle d \rangle \perp \dots \perp \langle d \rangle$  representaremos por  $n\langle d \rangle$ .

Encerramos esta seção com os conceitos de espaço isotrópico e de espaço anisotrópico, que serão utilizados no capítulo 4.

**Definição 1.37.** Seja  $(V, B)$  um espaço bilinear. Um vetor não nulo  $v \in V$  é chamado *isotrópico* se  $B(v, v) = 0$  ( $q(v) = 0$ ). Se  $B(v, v) \neq 0$  diz-se que  $v$  é *anisotrópico*. Dizemos que  $(V, B)$  é um *espaço isotrópico* se existe um vetor isotrópico em  $V$ . Caso contrário, se diz que  $(V, B)$  é um *espaço anisotrópico*. Finalmente, dizemos que  $(V, B)$  é um espaço *totalmente isotrópico* se todo vetor  $v$  não nulo de  $V$  é isotrópico, isto é,  $B \equiv 0$ .

# Capítulo 2

## Anéis Simples e Semisimples

O objetivo principal deste capítulo é mostrar o Teorema de Wedderburn, o qual afirma que um anel simples nada mais é que um anel de matrizes. Iremos ainda caracterizar os anéis e módulos semisimples e mostrar o Teorema de Maschke, que estabelece condições para que um anel de grupo seja semisimples.

No decorrer deste capítulo,  $R$  denota um anel com unidade 1 e, a menos se diga o contrário, os  $R$ -módulos serão considerados como módulos unitários à esquerda.

### 2.1 Anéis e Módulos Simples

**Definição 2.1.** Seja  $R$  um anel. Um  $R$ -módulo  $M \neq 0$  é *simples* se este só possui os submódulos triviais, ou seja, 0 e  $M$ . O anel  $R$  é *simples* se este só possui como ideais bilaterais o ideal nulo e o próprio  $R$ .

**Exemplo 2.2.** Um ideal à esquerda  $L \neq 0$  de  $R$  é um  $R$ -módulo simples se, e somente, se  $L$  é minimal. De fato, se  $L$  é simples, para todo ideal à esquerda  $J \subset L$  temos que  $J = 0$  ou  $J = L$ , pois  $J$  é um submódulo de  $L$ . Assim não existe  $J$  tal que  $L \supsetneq J \neq 0$ , ou seja,  $L$  é minimal.

Reciprocamente, se  $L$  é minimal, para todo ideal à esquerda  $J$  tal que  $0 \subset J \subset L$  temos que  $J = 0$  ou  $J = L$ . Assim os únicos submódulos à esquerda de  $L$  são os triviais. Portanto  $L$  é simples.

Como todo anel possui um ideal à esquerda maximal, pelo exemplo a seguir, todo anel possui um módulo simples.

**Exemplo 2.3.** Se  $M \neq R$  é um ideal à esquerda,  $R/M$  é simples se, e somente, se  $M$  é maximal.

Com efeito, seja  $M \neq R$  um ideal à esquerda. Temos que  $R/M$  é um  $R$ -módulo à esquerda. Se  $R/M$  é simples, os únicos submódulos de  $R/M$  são os triviais. Suponha que  $M$  não seja maximal, isto é, existe um ideal à esquerda  $J$  tal que  $M \subsetneq J \subsetneq R$ . Pelo Teorema da Correspondência  $J/M$  é ideal de  $R/M$  e  $0 \neq J/M \subsetneq R/M$ . Absurdo! Portanto  $M$  é maximal.

Reciprocamente, considere  $I$  um ideal de  $R/M$  e novamente pelo Teorema da Correspondência  $I = J/M$  para algum ideal à esquerda  $J$  de  $R$  com  $M \subset J$ . Mas como  $M$  é maximal, devemos ter  $J = M$  ou  $J = R$  e portanto  $J/M$  é um ideal trivial de  $R/M$ .

**Teorema 2.4. (Lema de Schur)** *Se  $M$  é um  $R$ -módulo simples, então o anel de endomorfismos  $A = \text{End}_R(M)$  é um anel com divisão.*

**Demonstração:** Sabemos que  $A = \text{End}_R(M)$  é um anel com as operações de soma e composição usuais. Resta mostrarmos que todo elemento não-nulo de  $A$  é inversível. Se  $f \in A$  é um endomorfismo não-nulo,  $\ker(f) \neq M$  e  $\text{im}(f) \neq 0$ . Sabemos que  $\ker(f)$  é um submódulo de  $M$ , assim como  $\text{im}(f)$ , mas como  $M$  é simples  $\ker(f) = 0$  e  $\text{im}(f) = M$ , ou seja,  $f$  é um isomorfismo. Portanto  $f$  é inversível. ■

O teorema a seguir nos traz um exemplo de anel simples.

**Teorema 2.5.** *Seja  $D$  um anel com divisão com centro  $K$ . O anel  $M(n, D)$  de todas as matrizes  $n \times n$  com coeficientes em  $D$  é um anel simples. O centro deste anel é canonicamente isomorfo a  $K$ .*

**Demonstração:** Vamos mostrar que o anel  $M(n, D)$  é simples, ou seja, só possui como ideais bilaterais os triviais. Seja  $e_{ij}$  a matriz com coeficiente 1 no lugar  $(i, j)$

e coeficientes nulos no restante. Então  $e_{ij}e_{kl} = 0$  se  $j \neq k$  e  $e_{ij}e_{jk} = e_{ik}$ . Seja  $J$  um ideal bilateral não-nulo de  $M(n, D)$ . Tomemos  $A \in J$  tal que  $A$  é uma matriz não-nula com pelo menos algum coeficiente  $\alpha_{ij} \neq 0$ . Assim para todo  $k$ ,  $(\alpha_{ij})^{-1}(e_{ki}Ae_{jk}) = e_{kk} \in J$ . Logo o ideal  $J$  contém a matriz identidade  $I = e_{11} + \dots + e_{nn}$  e portanto  $J = M(n, D)$ . Agora vamos mostrar que o centro de  $M(n, D)$  é isomorfo a  $K$ . Note que se  $A = (\alpha_{ij})$  está no centro de  $M(n, D)$  a equação  $e_{ij}A = Ae_{ij}$  nos mostra que  $\alpha_{ii} = \alpha_{jj}$ , para todo  $i, j$ , e  $\alpha_{ij} = 0$ , para todo  $i \neq j$ . Logo as matrizes do centro de  $M(n, D)$  são matrizes escalares. Se  $A = \text{diag}(\alpha, \alpha, \dots, \alpha)$ , então  $(g.e_{ij})A = A(g.e_{ij})$  para todo  $g \in D$ , o que implica  $g\alpha = \alpha g$ . Denotando o centro de  $D$  por  $C(D)$  segue que  $\alpha \in C(D) = K$ . Assim o centro  $C(M(n, D))$  de  $M(n, D)$  é isomorfo a  $K$ , basta considerar a aplicação canônica  $\varphi : C(M(n, D)) \rightarrow K$  tal que  $\varphi(\text{diag}(\alpha, \alpha, \dots, \alpha)) = \alpha$ , que é claramente um isomorfismo. ■

**Teorema 2.6. (Wedderburn, Rieffel)** *Sejam  $R$  um anel simples e  $M$  um ideal não nulo à esquerda de  $R$ . Então existe um isomorfismo canônico  $R \simeq \text{End}_D(M)$  com  $D = \text{End}_R(M)$ .*

**Demonstração:** Seja  $A = \text{End}_D(M)$ . Consideremos a aplicação canônica

$$i : R \rightarrow A, \quad \text{com } (i\alpha)x = \alpha x, \quad \text{para todo } \alpha \in R \text{ e } x \in M.$$

Vamos mostrar que  $i$  é um isomorfismo de anéis. Primeiro vamos checar que  $i\alpha \in \text{End}_D(M)$  para todo  $\alpha \in R$ . Para todo  $x_1, x_2 \in M$  e  $\lambda \in D$  temos que

$$(i\alpha)(x_1 + x_2) = \alpha(x_1 + x_2) = \alpha x_1 + \alpha x_2 = (i\alpha)(x_1) + (i\alpha)(x_2),$$

assim como

$$(i\alpha)(\lambda x) = \alpha(\lambda x) = \lambda(\alpha x) = \lambda((i\alpha)x).$$

Logo  $i$  está bem definida.

Temos que  $i$  é um homomorfismo de anéis, visto que

$$i(\alpha_1 + \alpha_2)x = (\alpha_1 + \alpha_2)x = \alpha_1 x + \alpha_2 x = (i\alpha_1)x + (i\alpha_2)x$$

$$\text{e } i(\alpha_1\alpha_2)x = (\alpha_1\alpha_2)x = \alpha_1(\alpha_2x) = (i\alpha_1)(i\alpha_2)x.$$

Particularmente  $i(1_R)x = 1_Rx = x$  para todo  $x \in M$ , ou seja,  $i(1_R) = \text{id}_M = 1_A$ . Sendo o  $\ker(i)$  um submódulo de  $R$  e sendo  $R$  simples temos que  $\ker(i) = 0$ , assim  $i$  é injetora. Para mostrar que  $i$  é sobrejetora, basta mostrarmos que  $i(R)$  é um ideal à esquerda de  $A$ , visto que  $i(R)$  contém o elemento unidade de  $A$ .

Para  $y \in M$  a multiplicação à direita por  $y$ ,  $r_y : M \rightarrow M$  dada por  $r_y(x) = xy$  para todo  $x \in M$ , é um elemento de  $D$ . Assim para  $f \in A$  temos  $f(xy) = f(x)y$  o que implica

$$(f(ix))y = f((ix)y) = f(xy) = f(x)y = (i(fx))y, \text{ ou seja, } f(ix) = i(fx), \forall x \in M.$$

Dessa forma temos que  $i(M)$  é um ideal à esquerda de  $A$ . Agora veja que o ideal bilateral  $MR$  de  $R$  gerado por  $M$  é igual a  $R$ , pois  $R$  é simples. Como  $i(R) = i(MR) = i(M)i(R)$ , e para todo  $x \in M$  temos  $i(R)x = Rx \in M$ , logo para todo  $f \in A$  e  $x \in M$ ,  $f(i(R))x = f(i(M)i(R))x = f(i(M)i(R)x) = (f(i(M)))i(R)x = i(M)i(R)x = i(R)x$ , ou seja,  $f(i(R)) = i(R)$ , portanto  $i(R)$  é um ideal à esquerda de  $A$ . ■

É importante salientarmos que o teorema acima difere do teorema clássico de Wedderburn, pois nele nenhuma condição de finitude é assumida.

Provaremos agora, afirmações relativas ao anel  $M(n, D)$ , com  $D$  um anel com divisão. Estas serão úteis na seção 1.3, onde definiremos anéis semisimples.

**Teorema 2.7.** *Sejam  $D$  um anel com divisão e  $R = M(n, D)$ . Então seguem as seguintes afirmações:*

(1) *Os ideais de matrizes coluna*

$$L_i = \left\{ \sum_{j=1}^n e_{ji}\alpha_j; \alpha_j \in D \right\}, i = 1, \dots, n$$

*são ideais minimais à esquerda de  $R$ . Além disso  $R = L_1 \oplus \dots \oplus L_n$ .*

(2) Todos  $R$ -módulos simples, em particular todos os ideais minimais à esquerda, são isomorfos.

(3) Todo  $R$ -módulo  $M$  não-nulo finitamente gerado é soma direta de  $R$ -módulos simples.

**Demonstração:** (1) Para mostrarmos que os ideais de matrizes coluna são ideais minimais à esquerda, basta mostrarmos que estes são simples. Seja  $A \in L_i$  tal que  $A \neq 0$ , logo  $A = \sum e_{ji}\alpha_j$  com  $\alpha_k \neq 0$  para algum  $k$ , então

$$(\alpha_k^{-1}e_{kk})A = e_{ki}.$$

Logo o ideal à esquerda gerado por  $A(\neq 0)$  é igual a  $L_i$ , pois se  $B = \sum e_{ji}\beta_j$  é um elemento qualquer de  $L_i$ , basta tomarmos  $C = \sum e_{jk}\beta_j$  e teremos que  $C.e_{ki} = B$ . Portanto  $L_i$  é simples.

Claramente  $M(n, D)$  é a soma dos ideais  $L_i$ ,  $i = 1, \dots, n$  e como  $L_i$  e  $L_j$  para  $i \neq j$  não tem elementos não-nulos em comum, temos que  $M(n, D) = L_1 \oplus \dots \oplus L_n$ .

(2) Seja  $N$  um  $R$ -módulo simples. Como  $R = \sum L_i$  e  $RN = N$ , existe um  $i$  tal que  $L_i N \neq 0$ . Assim existe um  $\alpha \in L_i$  e  $x \in N$  tal que  $\alpha x \neq 0$ . Definimos então

$$f : L_i \rightarrow N ; f(\alpha) = \alpha x \text{ para todo } \alpha \in L_i,$$

que é uma aplicação não-nula. Note que  $f$  é um homomorfismo de módulos, visto que para  $\alpha_1, \alpha_2 \in L_i$  e  $r \in R$

$$f(\alpha_1 + \alpha_2) = (\alpha_1 + \alpha_2)x = \alpha_1 x + \alpha_2 x = f(\alpha_1) + f(\alpha_2) \text{ e}$$

$$f(r\alpha_1) = r\alpha_1 x = rf(\alpha_1).$$

Como  $L_i$  e  $N$  são simples podemos concluir que  $f$  é um isomorfismo de módulos. É claro que todos os  $L_i$ 's são isomorfos entre si como  $R$ -módulos à esquerda. Portanto todos módulos simples são isomorfos.

(3) Para mostrar que todo  $R$ -módulo finitamente gerado  $M \neq 0$  é soma direta de  $R$ -módulos simples, considere  $N$  um submódulo maximal próprio de  $M$ , e  $x \in M \setminus N$ .



Como  $M/N$  é simples temos  $M = N + Rx = N + \sum L_i x$ , com cada  $L_i x$  nulo ou um  $R$ -módulo simples. Como  $N \neq M$  existe um  $i$  tal que  $L_i x \not\subseteq N$ . Sendo  $N$  maximal,  $M = N + L_i x$  e como  $L_i x$  é simples,  $N \cap L_i x = \{0\}$ . Portanto  $M = N \oplus L_i x$ . Como  $M$  é finitamente gerado, ou seja, um  $D$ -módulo de dimensão finita, basta usarmos indução sobre  $\dim_D(M)$ . ■

Para a demonstração do resultado a seguir, particularmente, trabalharemos com os homomorfismos à direita de seus argumentos.

**Teorema 2.8.** *Sejam  $D$  e  $D'$  anéis com divisão tais que  $M(m, D') \simeq M(n, D)$ , então  $D' \simeq D$  e  $m = n$ .*

**Demonstração:** Se  $N$  é um  $M(m, D)$ -módulo simples, iremos mostrar que existe um isomorfismo,  $\text{End}_{M(m, D)}(N) \simeq D$ . Analogamente prova-se que  $\text{End}_{M(n, D')}(N) \simeq D'$ , assim, como  $M(m, D) \simeq M(n, D')$  temos  $\text{End}_{M(n, D')}(N) \simeq \text{End}_{M(m, D)}(N)$  e portanto  $D' \simeq D$ . A igualdade  $m = n$  é devido ao fato de que  $m^2 = \dim_D M(m, D) = \dim_{D'} M(n, D') = n^2$ .

Agora, finalmente mostraremos que existe o isomorfismo desejado. Observe que o espaço  $D^m$  de vetores coluna é um  $M(m, D)$ -módulo simples, que é isomorfo aos ideais  $L_i$  do teorema anterior. É suficiente portanto mostrarmos que  $\text{End}_{M(m, D)}(D^m)$  é isomorfo a  $D$ . Consideremos também  $D^m$  como  $D$ -módulo à direita. Então consideremos a função  $\varphi : D \rightarrow \text{End}_{M(m, D)}(D^m)$  definida por:

$$x(\varphi\delta) = x\delta \quad \text{para } \delta \in D, x \in D^m.$$

É fácil mostrar que  $\varphi\delta$  é um  $M(m, D)$ -endomorfismo.

Temos que  $\varphi$  é um homomorfismo de anéis, pois se  $\delta_1, \delta_2 \in D$  e  $x \in D^m$

$$x(\varphi(\delta_1 + \delta_2)) = x(\delta_1 + \delta_2) = x\delta_1 + x\delta_2 = x(\varphi\delta_1) + x(\varphi\delta_2)$$

$$x(\varphi(\delta_1\delta_2)) = x(\delta_1\delta_2) = (x\delta_1)\delta_2 = (x(\varphi\delta_1))\delta_2 = (x(\varphi\delta_1))(\varphi\delta_2).$$

E mais,  $\varphi$  é sobrejetor. Com efeito, tome  $\lambda \in \text{End}_{M(m,D)}(D^m)$  qualquer e escreva

$$e_1\lambda = e_1\delta_1 + \cdots + e_m\delta_m, \text{ com } e_i, i = 1, \dots, m \text{ base de } D^m \text{ sobre } D \text{ e } \delta_j \in D.$$

Então  $\lambda = \varphi\delta_1$ , pois

$$e_1\lambda = (e_{11}e_1)\lambda = e_{11}(e_1\lambda) = e_{11}e_1\delta_1 + \cdots + e_{11}e_m\delta_m = e_1\delta_1 = e_1(\varphi\delta_1)$$

visto que,  $e_{11}e_1 = e_1$ ,  $e_{11}e_k = 0$  com  $k \neq 1$ . Analogamente,  $e_j\lambda = (e_{j1}e_1)\lambda = e_{j1}(e_1\lambda) = e_{j1}e_1\delta_1 + \cdots + e_{j1}e_m\delta_m = e_j\delta_1 = e_j(\varphi\delta_1)$  para todo  $j = 2, \dots, m$ . Donde concluímos que  $\varphi$  é sobrejetor.

Note que se  $\varphi(\delta) = 0$ , então  $x(\varphi\delta) = x\delta = 0$  para todo  $x \in D^m$ . Logo  $\delta \equiv 0$ , portanto  $\varphi$  é um isomorfismo. ■

Poderíamos demonstrar o teorema acima utilizando os homomorfismos à esquerda de seus argumentos, mas para isso teríamos que considerar os homomorfismos sobre o anel oposto de  $D$  (que definiremos no Capítulo 4), pois a multiplicação à direita em  $D$  corresponde à multiplicação à esquerda no anel oposto de  $D$ .

Antes de finalizamos esta seção com o Teorema de Wedderburn, precisamos dos seguintes resultados.

**Lema 2.9.** *Seja  $R$  um anel. Se  $R$  é considerado como um  $R$ -módulo à direita, então existe um isomorfismo canônico  $R \simeq \text{End}_R(R)$ .*

**Demonstração:** Considere a aplicação canônica  $\alpha : R \rightarrow \text{End}_R(R)$  definida por  $\alpha(a) = l_a$ , onde  $l_a$  é a multiplicação à esquerda por  $a$ , com  $a \in R$ . Claramente  $l_a$  é um  $R$ -endomorfismo, sendo  $R$  visto como  $R$ -módulo à direita. Veja também que  $\alpha$  é um homomorfismo de anéis, pois para  $a_1, a_2, b \in R$  temos

$$\alpha(a_1 + a_2)(b) = l_{(a_1+a_2)}(b) = (a_1 + a_2)b = a_1b + a_2b = (\alpha a_1 + \alpha a_2)b \text{ e}$$

$$\alpha(a_1 a_2)(b) = l_{(a_1 a_2)}(b) = (a_1 a_2)b = a_1(a_2 b) = a_1(l_{a_2} b) = l_{a_1}(l_{a_2} b) = (\alpha a_1)(\alpha a_2)(b).$$

Temos ainda que  $\alpha$  é injetor, pois  $l_a x = 0$  para todo  $x$  implica que  $ax = 0$  para todo  $x$ , ou seja,  $a = 0$ .

A aplicação  $\alpha$  é sobrejetora, visto que, se  $f \in \text{End}_R(R)$ , então  $f(x) = f(1x) = f(1)x$ , logo  $f = l_{f(1)}$ . Portanto  $\alpha$  é um isomorfismo. ■

Sejam  $R$  um anel,  $M = M_1 \oplus \cdots \oplus M_m$  e  $N = N_1 \oplus \cdots \oplus N_n$   $R$ -módulos, sendo  $M_i$  e  $N_j$   $R$ -submódulos. O conjunto formado por matrizes,

$$G = \{(\varphi_{ji}) ; \varphi_{ji} \in \text{Hom}_R(M_i, N_j)\},$$

com o produto usual de matrizes e o produto em  $\text{Hom}_R(M_i, N_j)$  sendo a composição, é um grupo de matrizes  $n \times m$ .

**Lema 2.10.** *Seja  $R$  um anel. Considere os  $R$ -módulos  $M, N$  e o grupo  $G$  como dados acima. Então existe um isomorfismo de grupos entre  $\text{Hom}_R(M, N)$  e  $G$ . Em particular,  $\text{End}_R(M^n) \simeq M(n, \text{End}_R(M))$ .*

**Demonstração:** Considerando  $M$  e  $N$  como acima, primeiro suponha que  $N = N_1$ . Sejam  $\varphi : M_1 \oplus \cdots \oplus M_m \rightarrow N$  um homomorfismo e  $\varphi_i : M_i \rightarrow M$  a restrição de  $\varphi$  ao fator  $M_i$ . Temos que todo elemento  $x \in M$  é representado de forma única como  $x = x_1 + \cdots + x_m$ , com  $x_i \in M_i$ . Associamos a  $x$  o vetor coluna  $X = (x_1, \dots, x_m)^t$ , com cada  $x_i \in M_i$ . Agora, associamos a  $\varphi$  o vetor linha  $(\varphi_1, \dots, \varphi_m)$ , com  $\varphi_i \in \text{Hom}_R(M_i, N)$  e a atuação de  $\varphi$  no elemento  $x \in M$  é descrita pela matriz da multiplicação do vetor linha pelo vetor coluna.

Para o caso geral, agora com  $\varphi : M_1 \oplus \cdots \oplus M_m \rightarrow N_1 \oplus \cdots \oplus N_n$ . Seja  $\pi_j : N_1 \oplus \cdots \oplus N_n \rightarrow N_j$  a projeção no  $j$ -ésimo fator. Assim podemos aplicar o procedimento feito para o primeiro caso para  $\pi_j \circ \varphi_i = \varphi_{ji}$ , para cada  $j$ . Dessa forma os elementos  $\varphi_{ji} \in \text{Hom}_R(M_i, N_j)$  são unicamente determinados, logo  $\varphi$  tem

como matriz de representação

$$\begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1m} \\ \varphi_{21} & \varphi_{22} & \cdots & \varphi_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{n1} & \varphi_{n2} & \cdots & \varphi_{nm} \end{pmatrix}$$

Aplicando esta no elemento  $X$  obtemos  $\varphi(X)$ .

Reciprocamente, dada a matriz  $(\varphi_{ji})$  com  $\varphi_{ji} \in \text{Hom}_R(M_i, N_j)$ , podemos definir um elemento de  $\text{Hom}_R(M, N)$  com esta matriz de representação. Assim temos um isomorfismo de grupos entre  $\text{Hom}_R(M, N)$  e este grupo de matrizes.

Em particular, se tomarmos  $M = N$  e  $M_i = M$ , temos um isomorfismo de anéis entre  $\text{End}_R(M^n)$  e  $M(n, \text{End}_R(M))$ . ■

**Teorema 2.11. (Wedderburn)** *Seja  $R$  um anel simples que tem um ideal minimal à direita  $M$ . Então  $R \simeq M(n, D)$  para um conveniente anel com divisão  $D$ .*

**Demonstração:** Como  $M$  é um módulo à direita temos que  $RM$  é um ideal bilateral de  $R$ , mas  $R$  é simples, logo  $RM = R$ . Assim podemos escrever

$$1 = a_1x_1 + \cdots + a_nx_n \quad \text{para convenientes } a_i \in R, x_i \in M.$$

Entre essas equações escolhemos uma com um número mínimo de parcelas, digamos  $n$ .

Afirmamos que  $R = a_1M \oplus \cdots \oplus a_nM$ . De fato, como  $a = a_1(x_1a) + \cdots + a_n(x_na)$  para todo  $a \in R$  temos que  $R = a_1M + \cdots + a_nM$ . Suponha por absurdo que  $0 = a_1y_1 + \cdots + a_ny_n$  com  $y_i \in M$  e que estes somandos não são todos nulos, digamos  $a_ny_n \neq 0$ . Então  $y_nR = M$ , porque  $M$  é minimal. Assim

$$a_nM = a_ny_nR = (-a_1y_1 - \cdots - a_{n-1}y_{n-1})R \subset a_1M + \cdots + a_{n-1}M.$$

O que produz uma representação com menos de  $n$  elementos para 1, pois se  $a_nx_n = a_1x'_1 + \cdots + a_{n-1}x'_{n-1}$  para  $x'_i \in M$ , teríamos  $1 = a_1(x_1 - x'_1) + \cdots + a_{n-1}(x_{n-1} - x'_{n-1})$ . Isso mostra que a soma  $R = \sum a_iM$  é direta.

Como a aplicação  $\psi : M \rightarrow a_i M$  é claramente um isomorfismo de  $R$ -módulos, temos que  $R \simeq M^n = M \oplus \cdots \oplus M$ .

Usando os Lemas 2.9 e 2.10 obtemos

$$R \simeq \text{End}_R(R) \simeq \text{End}_R(M^n) \simeq M(n, \text{End}_R(M)).$$

Como  $M$  é simples pelo Lema de Schur 2.4  $\text{End}_R(M)$  é um anel com divisão, considerando  $D = \text{End}_R(M)$  temos o desejado. ■

## 2.2 Condições que definem Semisimplicidade

Seja  $R$  um anel. Nesta seção todos os módulos e homomorfismos serão  $R$ -módulos e  $R$ -homomorfismos, a menos que se especifique o contrário.

**Teorema 2.12.** *As seguintes condições sobre um módulo  $E$  são equivalentes.*

- (1)  $E$  é a soma de uma família de submódulos simples.
- (2)  $E$  é a soma direta de uma família de submódulos simples.
- (3) Todo submódulo  $F$  de  $E$  é um somando direto, isto é, existe um submódulo  $F'$  tal que  $E = F \oplus F'$ .

**Demonstração:** Vamos mostrar que (1) implica em (2). Para isso considere  $E = \sum_{i \in I} E_i$  uma soma, não necessariamente direta, de submódulos simples. Vamos

mostrar que existe um subconjunto  $J \subset I$  tal que  $E = \bigoplus_{j \in J} E_j$ . Seja  $J$  um conjunto maximal de  $I$  tal que a soma  $\sum_{j \in J} E_j$  é direta. Afirmamos que essa soma é igual a  $E$ .

É suficiente provar que cada  $E_i \subset \sum_{j \in J} E_j$ . Note que a interseção de  $\sum_{j \in J} E_j$  com  $E_i$  é um submódulo de  $E_i$ , como  $E_i$  é simples, essa interseção é zero ou  $E_i$ . Caso seja zero, então  $J$  não será maximal, pois teremos um elemento a mais na soma direta, o que é falso. Logo  $E_i$  está contido na soma  $\sum_{j \in J} E_j$  para todo  $i$ , assim  $E \subset \sum_{j \in J} E_j$ .

Portanto  $E = \bigoplus_{j \in J} E_j$ .

Vamos mostrar agora que (2) implica em (3). Considere  $F$  um submódulo de  $E$ . Seja  $J$  um conjunto maximal de  $I$  tal que a soma  $F + \bigoplus_{j \in J} E_j$  é direta.

Temos que  $F + \bigoplus_{j \in J} E_j = E$ . De fato, como anteriormente para cada  $E_i$  temos que  $(F + \bigoplus_{j \in J} E_j) \cap E_i$  é um submódulo de  $E_i$ , que é simples, ou seja, a interseção é zero ou  $E_i$ , caso seja zero contraria o fato de  $J$  ser maximal. Logo  $E_i \subset (F + \bigoplus_{j \in J} E_j)$ .

Portanto  $E = (F + \bigoplus_{j \in J} E_j)$ .

Finalmente, assumamos (3). Para mostrar (1), primeiro vamos mostrar que todo submódulo não nulo de  $E$  contém um submódulo simples. Como todo módulo não nulo de  $E$  contém um submódulo principal, basta mostrarmos para esse caso.

Seja  $v \in E$  com  $v \neq 0$ , então por definição,  $Rv$  é um submódulo principal de  $E$  e o núcleo de homomorfismo  $R \rightarrow Rv$  é um ideal à esquerda  $L \neq R$ . Assim  $L$  está contido em um ideal maximal à esquerda  $M \neq R$  (que existe pelo Lema de Zorn), então  $M/L$  é um submódulo maximal de  $R/L$  com  $M/L \neq R/L$  e portanto  $Mv$  é um submódulo maximal de  $Rv$ , e  $Mv \neq Rv$ . Claramente  $Mv$  corresponde a  $M/L$  sob o isomorfismo  $R/L \rightarrow Rv$ .

Por (3), podemos escrever  $E = Mv \oplus M'$  para algum submódulo  $M'$ . Então  $Rv = Mv \oplus (M' \cap Rv)$  pois todo elemento  $x \in Rv$  pode ser escrito de forma única como uma soma  $x = \alpha v + x'$  com  $\alpha \in M$ ,  $x' \in M'$  e  $x' = x - \alpha v \in Rv$ . Como  $Mv$  é maximal em  $Rv$  temos que  $(M' \cap Rv)$  é simples, caso contrário se existisse um submódulo  $I$  não-nulo  $I \subset (M' \cap Rv)$  com  $I \neq (M' \cap Rv)$  sendo  $Rv = Mv \oplus (M' \cap Rv)$  teríamos um submódulo  $Mv + I$  de  $Rv$ , contrariando a maximalidade de  $Mv$ . Logo todo submódulo  $Rv$  de  $E$  possui submódulo simples.

Seja  $E_0$  o submódulo de  $E$  que é soma de todos submódulos simples de  $E$ . Se  $E_0 \neq E$ , então por (3)  $E = E_0 + F$  com  $F \neq 0$  e existe um submódulo de  $F$  que é simples, contradizendo a definição de  $E_0$ . Portanto  $E = E_0$ . O que finaliza a demonstração. ■

**Definição 2.13.** Seja  $E$  um módulo satisfazendo uma das três condições vistas no teorema anterior ( e portanto, as três), então  $E$  é chamado de *módulo semisimples*.

**Proposição 2.14.** *Se  $E$  é um módulo semisimples, então todo submódulo e todo módulo quociente de  $E$  é também semisimples.*

**Demonstração:** Sejam  $F$  um submódulo de  $E$  e  $F_0$  a soma de todos submódulos simples de  $F$ . Como  $E$  é semisimples e  $F_0$  é submódulo de  $E$  pelo item (3) do Teorema 2.12, temos  $E = F_0 \oplus F'_0$ . Todo elemento  $x \in F$  tem uma única representação  $x = x_0 + x'_0$  com  $x_0 \in F_0$  e  $x'_0 \in F'_0$ . Mas  $x'_0 = x - x_0 \in F$ . Logo  $F = F_0 \oplus (F \cap F'_0)$ , mas  $(F \cap F'_0) = 0$ , caso contrário teríamos  $F_1 \subset (F \cap F'_0)$  simples em  $F$ , o que não ocorre pois  $F_0$  contém todos os submódulos simples de  $F$  e  $F_0 \cap F'_0 = 0$ . Portanto  $F = F_0$ , que é semisimples.

Agora mostraremos que todo módulo quociente de  $E$  é semisimples. Podemos escrever  $E = F \oplus F'$ , com  $F'$  uma soma de submódulos simples. Considerando a aplicação canônica  $E \rightarrow E/F$ , como o núcleo desse homomorfismo é  $F$  pelo Teorema do Isomorfismo temos  $F' \simeq E/F$ . Portanto  $E/F$  é semisimples. ■

## 2.3 Anéis Semisimples

**Definição 2.15.** Um anel  $R$  é chamado *semisimples* se  $1 \neq 0$ , e se  $R$  é um  $R$ -módulo à esquerda semisimples.

**Proposição 2.16.** *Se  $R$  é semisimples, então todo  $R$ -módulo é semisimples.*

**Demonstração:** Como um  $R$ -módulo  $M$  é um módulo quociente de um módulo livre  $L$ , isto é,  $M \simeq L/N$ . Como  $L$  é soma direta de cópias de  $R$  e  $R$  é semisimples, temos que  $L$  é semisimples. Dessa forma  $M$  é um módulo quociente de um módulo semisimples, e pela Proposição 2.14,  $M$  é semisimples. ■

**Exemplo 2.17.** Sabemos que  $R = M(n, K)$ , o anel de matrizes  $n \times n$  sobre o corpo  $K$ , é semisimples, conforme visto no item (1) do Teorema 2.7. Na verdade  $R$  é simples, como provamos no Teorema 2.5.

Nosso objetivo agora é decompor um anel semisimples  $R$  como uma soma de ideais à esquerda e com isto obter um teorema de estrutura para  $R$ .

**Definição 2.18.** Um ideal à esquerda de  $R$  é chamado *simples* se este é simples como um  $R$ -módulo. Dois ideais  $L$  e  $L'$  de  $R$  são *isomorfos* se eles são isomorfos como  $R$ -módulos.

**Lema 2.19.** *Sejam  $R$  um anel e  $L$  um ideal simples à esquerda de  $R$ , e seja  $E$  um  $R$ -módulo simples. Se  $L$  não é isomorfo a  $E$ , então  $LE = 0$ .*

**Demonstração:** Como  $L$  é um ideal à esquerda de  $R$  temos  $RLE = LE$ , assim  $LE$  é um módulo e em particular um submódulo de  $E$ , como  $E$  é simples  $LE = 0$  ou  $LE = E$ . Suponhamos que  $LE = E$ . Seja  $y \in E$  tal que  $Ly \neq 0$ . Como  $Ly$  é um submódulo de  $E$ , segue que  $Ly = E$ . A aplicação  $\psi : L \rightarrow E$  dada por  $\psi(\alpha) = \alpha y$ ,  $\alpha \in L$  é um homomorfismo sobrejetivo, pois  $\text{im } \psi = Ly = E$ , e portanto não nulo. Como  $\ker \psi$  é um submódulo de  $L$ , sendo  $L$  simples e  $\psi$  não nula, temos que  $\ker \psi = 0$ . Assim  $L$  é isomorfo a  $E$ , o que é absurdo. Portanto  $LE = 0$ . ■

Seja  $\{L_i\}_{i \in I}$  uma família de ideais simples à esquerda que não sejam isomorfos entre si e tal que todo ideal simples à esquerda de  $R$  seja isomorfo a um  $L_i$ . Podemos dizer que esta família é uma família de representantes para as classes de isomorfismos de ideais simples à esquerda.

Podemos definir anel simples como sendo um anel semisimples que possui uma única classe de isomorfismos de ideais simples à esquerda.

**Teorema 2.20.** *Seja  $R$  um anel semisimples. Então existe somente um número finito de ideais simples à esquerda não isomorfos, digamos  $L_1, \dots, L_s$ . Se  $R_i =$*



$\sum_{L \simeq L_i} L$  é a soma de todos ideais simples à esquerda isomorfos a  $L_i$ , então  $R_i$  é um ideal bilateral que também é um anel (com as operações induzidas por  $R$ ). E  $R$  é um anel isomorfo ao produto direto  $R = \prod_{i=1}^s R_i$ . Cada  $R_i$  é um anel simples. Se  $e_i$  é o elemento unidade de  $R_i$ , então  $1 = e_1 + \cdots + e_s$  e  $R_i = Re_i$ . Temos  $e_i e_j = 0$  se  $i \neq j$ .

**Demonstração:** Seja  $R_i = \sum_{L \simeq L_i} L$  a soma de todos ideais simples à esquerda isomorfos a  $L_i$ . Pelo Lema 2.19 se  $i \neq j$  temos  $R_i R_j = 0$ . De fato, sejam  $R_i = \sum_{L \simeq L_i} L$  e  $R_j = \sum_{L' \simeq L_j} L'$  sendo que para  $i \neq j$   $L_i \not\simeq L_j$ , logo  $L \not\simeq L'$ . Assim  $R_i \not\simeq R_j$ , o que implica que  $R_i R_j = 0$ .

Notamos que  $R_i$ , como dado acima, é um ideal à esquerda e que  $R$  é a soma  $R = \sum_{i \in I} R_i$ , pois  $R$  é uma soma de ideais simples à esquerda.

Temos para todo  $j \in I$ ,  $R_j \subset R_j R = R_j R_j \subset R_j$ . De fato, a primeira inclusão vale pois  $R$  contém o elemento unidade, a igualdade deve-se a

$$R_j R = R_j \sum R_i = R_j R_1 + \cdots + R_j R_j + \cdots$$

e como  $R_i R_j = 0$  se  $i \neq j$  temos  $R_j R = R_j R_j$  e a segunda inclusão é clara já que  $R_j$  é um ideal à esquerda. Assim concluímos que  $R_j$  é também um ideal à direita, logo um ideal bilateral para todo  $j \in I$ .

Podemos expressar o elemento unidade de  $R$  como uma soma  $1 = \sum_{i \in I} e_i$  tal que  $e_i \in R_i$ , com um número finito de  $e_i \neq 0$ . Como  $R$  é semisimples essa soma é única. Digamos que  $e_i \neq 0$  para  $i = 1, \dots, s$  e escrevemos  $1 = e_1 + \cdots + e_s$ .

Para todo  $x \in R$  podemos escrever  $x = \sum_{i \in I} x_i$  com  $x_i \in R_i$ . Para  $j = 1, \dots, s$  temos  $e_j x = e_j x_j$ , pois  $e_j \in R_j$  e  $R_i R_j = 0$  para todo  $i \neq j$ , e também  $x_j = 1x_j = e_1 x_j + \cdots + e_s x_j = e_j x_j$ . Além disso  $x = e_1 x + \cdots + e_s x = e_1 x_1 + \cdots + e_s x_s = x_1 + \cdots + x_s$ , isso prova que não existe outro índice  $i$  além dos  $i = 1, \dots, s$  e que a  $i$ -ésima componente  $x_i$  de  $x$  é unicamente determinada, pois depende apenas de

$e_j$  que é único. Assim todo  $x \in R$  é representado de forma única como soma dos  $x_i \in R_i$  com  $i = 1, \dots, s$ , ou seja,  $R = R_1 + \dots + R_s$  é uma soma direta. Como para o caso de  $I$  ser finito, a soma direta coincide com o produto direto, temos que  $R = \prod_{i=1}^s R_i$ . Além disso,  $e_i$  é um elemento unidade de  $R_i$ , visto que  $x_i e_i = x_i$  para todo  $x_i \in R_i$ , e portanto este é um anel. Portanto  $R = \prod_{i=1}^s R_i$  é um produto direto de anéis simples. ■

Um fato importante, que será de grande valia no Capítulo V, é o de que os elementos  $e_i$  do teorema anterior satisfazem  $e_i^2 = e_i$  (*idempotente*). Isso é válido, pois como  $e_i e_j = 0$  para  $i \neq j$ , temos  $e_i = 1 \cdot e_i = (e_1 + \dots + e_s) e_i = e_1 e_i + \dots + e_i^2 + \dots + e_s e_i = e_i^2$ . Segue ainda da demonstração do teorema que  $e_i \in C(R)$  (*central*) para todo  $i = 1, \dots, s$ .

**Definição 2.21.** Seja  $R$  um anel. Um conjunto  $B = \{e_1, \dots, e_n\} \subset R$ , é um conjunto ortogonal se  $e_i e_j = 0$  quando  $i \neq j$ , para todo  $i, j = 1, \dots, n$ .

Um elemento  $e_i \in B$  é dito *idempotente central primitivo* se este é idempotente central e se não pode ser escrito como soma de dois idempotentes centrais ortogonais não nulos.

Os elementos  $e_i$ , vistos no teorema anterior, são idempotentes centrais primitivos. Sendo que a primitividade desses elementos vem do fato de que  $R = \bigoplus_{i=1}^s R_i$ .

Como conseqüência do Teorema 2.20 temos o seguinte resultado.

**Corolário 2.22.** Se  $I$  é um ideal em um anel semisimples  $R$ , então  $I = Re$ , onde  $e$  é um idempotente central de  $R$ .

**Demonstração:** Como  $R$  é semisimples,  $R$  é produto direto de ideais à esquerda simples, digamos  $R = I_1 \times \dots \times I_n$ . Para cada  $j$  temos que  $I \cap I_j = 0$  ou  $I \cap I_j = I_j$ , devido à simplicidade de  $I_j$ . Reordenando se necessário podemos assumir que  $I \cap I_j = I_j$  para  $j = 1, \dots, t$  e  $I \cap I_j = 0$  para  $t < j \leq n$ . Como  $R$  tem identidade

1, existem  $e_j \in I_j$  tais que  $1 = e_1 + \cdots + e_n$ . Como  $I_j I_k = 0$  para  $j \neq k$  temos que  $e_1 + e_2 + \cdots + e_n = 1 = 1^2 = e_1^2 + e_2^2 + \cdots + e_n^2$ , pela unicidade da representação de 1, temos  $e_j^2 = e_j$  para cada  $j$ . É fácil mostrar que  $e_i$  está no centro de  $R$  e que  $e = e_1 + \cdots + e_t \in I$  é um idempotente central de  $R$ . Como  $I$  é um ideal,  $Re \subset I$ . Reciprocamente se  $u \in I$ , então  $u = u1 = ue_1 + \cdots + ue_n$ . Mas para  $j > t$   $ue_j \in I \cap I_j = 0$ . Então  $u = ue_1 + \cdots + ue_t = ue$ . Portanto  $I \subset Re$ . ■

Na seqüência vamos definir o anel de grupo. E depois veremos, no Teorema da Maschke, sob quais condições o anel de grupo é semisimples.

Sejam  $R$  um anel comutativo e  $G$  um grupo. Construimos o anel de grupo  $R[G]$  da seguinte forma, consideramos  $R[G]$  como sendo o grupo abeliano aditivo  $\sum_{\sigma \in G} R$ , que representa uma cópia de  $R$  para cada  $\sigma \in G$ . Um elemento  $\alpha = \{a_\sigma\}_{\sigma \in G}$  de  $R[G]$  tem somente um número finito de coordenadas não nulas, digamos  $a_{\sigma_1}, \dots, a_{\sigma_n}$  com  $\sigma_i \in G$ , também denotamos  $\alpha \in R[G]$  pela *soma formal*  $a_{\sigma_1}\sigma_1 + \cdots + a_{\sigma_n}\sigma_n$  ou  $\sum_{i=1}^n a_{\sigma_i}\sigma_i$ . Estamos mantendo a possibilidade de que alguns  $a_{\sigma_i}$  sejam nulos ou que alguns  $\sigma_i$  sejam repetidos, para que os elementos de  $R[G]$  possam ser representados de diferentes formas, por exemplo,  $a_{\sigma_1}\sigma_1 + 0\sigma_2 = a_{\sigma_1}\sigma_1$  ou  $a_{\sigma_1}\sigma_1 + b_{\sigma_1}\sigma_1 = (a_{\sigma_1} + b_{\sigma_1})\sigma_1$ .

Nessa notação a adição em  $R[G]$  é dada por

$$\sum_{i=1}^n a_{\sigma_i}\sigma_i + \sum_{j=1}^m b_{\sigma_j}\sigma_j = \sum_{i=1}^n (a_{\sigma_i} + b_{\sigma_i})\sigma_i \quad \text{se } n \geq m, \quad \text{tome } b_{\sigma_j} = 0 \text{ para } m < j \leq n.$$

A multiplicação é dada por

$$\left(\sum_{i=1}^n a_{\sigma_i}\sigma_i\right) \cdot \left(\sum_{j=1}^m b_{\tau_j}\tau_j\right) = \sum_{i,j} (a_{\sigma_i}b_{\tau_j})(\sigma_i\tau_j).$$

Com essas operações  $R[G]$  é um anel, chamado *anel do grupo  $G$  sobre  $R$* .

**Teorema 2.23. (Maschke)** *Sejam  $G$  um grupo finito de ordem  $n$  e  $K$  um corpo cuja característica não divide  $n$ . Então o anel de grupo  $K[G]$  é semisimples.*

**Demonstração:** Considere  $E$  um espaço vetorial sobre  $K$  que também é um  $K[G]$ -módulo. Seja  $F$  um  $K[G]$ -submódulo de  $E$ . Como  $K$  é corpo,  $E$  e  $F$  são  $K$ -espaços vetoriais e existe um  $K$ -espaço  $F'$  tal que  $E = F \oplus F'$  sobre  $K$ .

Vamos mostrar que  $F$  é um somando direto de  $E$  sobre  $K[G]$ . Para isso, considere a aplicação  $K$ -linear  $\pi : E \rightarrow F$  como a projeção sobre  $F$ . Então  $\pi(x) = x$  para todo  $x \in F$ . Considere também a aplicação  $\varphi : E \rightarrow F$  tal que  $\varphi(x) = \frac{1}{n} \sum_{\sigma \in G} (\sigma\pi)(\sigma^{-1}x)$ , e a inclusão  $j : F \rightarrow E$ . Então  $\varphi \circ j : F \rightarrow F$  é a identidade, visto que para todo  $x \in F$ ,

$$\varphi \circ j(x) = \varphi(x) = \frac{1}{n} \sum_{\sigma \in G} (\sigma\pi)(\sigma^{-1}x) = \frac{1}{n} \sum_{\sigma \in G} \sigma\sigma^{-1}x = \frac{1}{n} \sum_{\sigma \in G} x = x.$$

Note que a aplicação  $\varphi$  é um  $K[G]$ -homomorfismo, pois para todo  $\tau \in G$

$$\tau \sum_{\sigma \in G} \sigma\pi\sigma^{-1}(x) = \sum_{\sigma \in G} \tau\sigma\pi\sigma^{-1}\tau^{-1}\tau(x) = \sum_{\sigma \in G} \tau\sigma\pi\sigma^{-1}\tau^{-1}\tau(x) = \sum_{\sigma \in G} \sigma\pi\sigma^{-1}(\tau x),$$

visto que  $\tau\sigma$  percorre  $G$ . Logo temos que  $E = F \oplus \ker \varphi$  (lembrando que  $\ker \varphi$  é um  $K[G]$ -submódulo de  $E$ ). Pelo Teorema 2.12,  $E$  é um  $K[G]$ -módulo semisimples. Portanto todo  $K[G]$ -módulo é semisimples, em particular,  $K[G]$  também o é. ■

# Capítulo 3

## Álgebras Centrais Simples

Como foi observado na introdução, Albert desenvolveu sua teoria de involuções sobre álgebras centrais simples. Precisamos, portanto conhecer bem a teoria de álgebras centrais simples, para que no Capítulo 4 possamos classificar involuções. Vale ainda salientar que uma álgebra de matrizes é o exemplo mais elementar de álgebras centrais simples, sendo esta a mais usada neste trabalho.

### 3.1 Álgebras Centrais Simples

Juntando as estruturas de anel e de módulo em um mesmo conjunto, obtemos uma nova estrutura um pouco mais complexa, a qual definimos a seguir.

**Definição 3.1.** Seja  $K$  um anel comutativo com unidade. Um anel  $A$  é chamado de  $K$ -álgebra (ou álgebra sobre  $K$ ) se

- (1)  $(A, +)$  é um  $K$ -módulo unitário à esquerda;
- (2)  $k(ab) = (ka)b = a(kb)$  para todo  $k \in K$  e  $a, b \in A$ .

Os exemplos mais simples de  $K$ -álgebras são as extensões de corpos  $L \supset K$ . Veremos agora outros exemplos que serão importantes no decorrer do trabalho.

**Exemplo 3.2.** Dado um corpo  $K$  podemos definir uma  $K$ -álgebra de dimensão

quatro com base  $\{1, i, j, k\}$  e multiplicação dada pelas regras:

$$i^2 = j^2 = -1; \quad i.j = -j.i = k;$$

Os elementos desta álgebra são da forma  $a + bi + cj + dk$  com  $a, b, c, d \in K$ . Esta  $K$ -álgebra é conhecida como *álgebra dos Hamiltonianos* (ou *quatérnios*) e denotaremos por  $H$ .

**Exemplo 3.3.** No Capítulo 1, definimos o anel de grupo  $K[G]$ . Este é uma  $K$ -álgebra com a estrutura de  $K$ -módulo dada por

$$k\left(\sum_{\sigma \in G} a_{\sigma}\sigma\right) = \sum_{\sigma \in G} (ka_{\sigma})\sigma \quad \text{com } k, a_{\sigma} \in K; \quad \sigma \in G.$$

E assim  $K[G]$  é também chamado de *álgebra de grupo* de  $G$  sobre  $K$ .

No que segue, fixamos  $K$  como um corpo. Se  $A$  é uma  $K$ -álgebra, temos que  $K$  está contido em  $A$ , pois  $K \simeq K.1 \subset A$ . Iremos considerar somente espaços vetoriais e álgebras de dimensão finita.

**Definição 3.4.** Seja  $A$  uma  $K$ -álgebra. O *centralizador* de um conjunto  $B \subset A$  é dado por

$$C_A(B) = \{x \in A ; \quad xb = bx \quad \forall b \in B\}.$$

Se  $B = A$ ,  $C_A(A)$  é também conhecido por *centro* de  $A$ , que denotaremos simplesmente por  $C(A)$ . Uma  $K$ -álgebra  $A$  é dita *central* se  $K$  é o centro de  $A$ . Se  $A$  é uma  $K$ -álgebra simples e central dizemos que  $A$  é uma *álgebra central simples*.

**Exemplo 3.5.** Tomando  $A = M(n, K)$  temos que  $A$  é uma álgebra sobre  $K$ . E mais, os únicos ideais bilaterais de  $A$  são os triviais e o centro de  $A$  é  $K$ . Portanto  $A = M(n, K)$  é uma álgebra central simples.

Para a próxima proposição e no que segue, assumiremos conhecido o conceito de produto tensorial, bem como algumas de suas propriedades. Para maiores detalhes sobre esse assunto, ver [4], capítulo IV, pg. 207.

**Observação 3.6.** Sejam  $A$  e  $B$   $K$ -álgebras de dimensão finita. Se  $\{a_1, \dots, a_m\}$  e  $\{b_1, \dots, b_n\}$  são bases de  $A$  e  $B$ , respectivamente, então um fato conhecido é que o conjunto  $\{a_i \otimes b_j ; i = 1, \dots, m \text{ e } j = 1, \dots, n\}$  forma uma base de  $A \otimes B$ . Assim todo elemento  $x \in A \otimes B$  pode ser representado por

$$x = \sum_{i,j} \lambda_{ij} (a_i \otimes b_j),$$

com os coeficientes  $\lambda_{ij} \in K$  unicamente determinados. Podemos reescrever  $x$  da seguinte forma

$$x = \sum_j^n \left( \sum_i^m a_i \lambda_{ij} \right) \otimes b_j = \sum_j^n x_j \otimes b_j$$

onde  $x_j = \sum_i a_i \lambda_{ij} \in A$ , e estes são unicamente determinados. Analogamente podemos escrever  $x = \sum_i^m \left( a_i \otimes \left( \sum_j^n b_j \lambda_{ij} \right) \right) = \sum_i^m a_i \otimes y_i$  com  $y_i = \sum_j^n b_j \lambda_{ij}$  também unicamente determinados.

Em particular, se  $\sum_j^n x_j \otimes b_j = 0 = \sum_j^n 0 \otimes b_j$ , então  $x_j = 0$  para todo  $j = 1, \dots, n$ .

Do mesmo modo se  $\sum_i^m a_i \otimes y_i = 0$ ,  $y_i = 0$  para todo  $i = 1, \dots, m$ .

É importante salientarmos que o teorema abaixo é válido não só para álgebras finitamente geradas. Mas como em nosso trabalho estamos considerando somente álgebras de dimensão finita, faremos a demonstração somente para esse caso. A demonstração geral segue análoga à apresentada aqui.

**Teorema 3.7.** (1) Se  $A$  e  $B$  são  $K$ -álgebras e  $A' \subset A$ ,  $B' \subset B$  são subálgebras, então  $C_{A \otimes B}(A' \otimes B') = C_A(A') \otimes C_B(B')$ . Em particular, se  $A$  e  $B$  são centrais, então  $A \otimes B$  é central.

(2) Se  $A$  é uma álgebra central simples e  $B$  é simples, então  $A \otimes B$  é simples.

(3) Se  $A$  e  $B$  são álgebras centrais simples, então  $A \otimes B$  também o é.

**Demonstração:** Como  $A$  e  $B$  são  $K$ -álgebras finitamente geradas, nessa demonstração fixamos  $\alpha = \{a_1, \dots, a_m\}$ ,  $\beta = \{b_1, \dots, b_n\}$  bases de  $A$  e  $B$  respectivamente.

(1) Note que  $C_A(A') \otimes C_B(B') \subset C_{A \otimes B}(A' \otimes B')$ , pois se  $x \otimes y \in C_A(A') \otimes C_B(B')$ , então  $ax \otimes by = xa \otimes yb$ , para todo  $a \in A'$  e  $b \in B'$ . Pelas propriedades de produto tensorial temos que

$$(a \otimes b)(x \otimes y) = (ax \otimes by) = (xa \otimes yb) = (x \otimes y)(a \otimes b).$$

Assim  $x \otimes y \in C_{A \otimes B}(A' \otimes B')$ . Reciprocamente, tome  $x \in C_{A \otimes B}(A' \otimes B')$  e considere a base  $\beta$  de  $B$ . Logo  $x = (x_1 \otimes b_1) + \cdots + (x_n \otimes b_n)$  e, pela observação anterior, os  $x_i$  são unicamente determinados. Para todo  $a \in A'$  temos que  $(a \otimes 1)x = x(a \otimes 1)$ , pois  $x \in C_{A \otimes B}(A' \otimes B')$  e assim

$$(ax_1 \otimes b_1) + \cdots + (ax_n \otimes b_n) = (x_1a \otimes b_1) + \cdots + (x_na \otimes b_n).$$

Pela unicidade da representação, temos que  $x_i \in C_A(A')$ . Considere agora,  $\{a_1, \dots, a_k\}$  uma base de  $C_A(A')$  sobre  $K$ . Logo  $x$  pode ser representado por  $x = a_1 \otimes y_1 + \cdots + a_k \otimes y_k$ , sendo  $y_i \in B$  unicamente determinados. Assim para todo  $b \in B'$  temos que  $(1 \otimes b)x = x(1 \otimes b)$ , ou seja,

$$(a_1 \otimes by_1) + \cdots + (a_k \otimes by_k) = (a_1 \otimes y_1b) + \cdots + (a_k \otimes y_kb).$$

Dessa forma  $y_i \in C_B(B')$ , pela unicidade da representação. Portanto  $x \in C_A(A') \otimes C_B(B')$ . Em particular se  $C_A(A) = C_B(B) = K$ , então  $C_{A \otimes B}(A \otimes B) = K \otimes K = K$ , ou seja, se  $A$  e  $B$  são centrais  $A \otimes B$  também o é.

(2) Vamos mostrar que  $A \otimes B$  só possui como ideais bilaterais os triviais. Considere  $I$  um ideal bilateral não nulo de  $A \otimes B$ . Primeiro assumimos que  $I$  contém um elemento  $a \otimes b \neq 0$ . Os ideais bilaterais de  $A$  e  $B$  gerados por  $a$  e  $b$  respectivamente, são os próprios  $A$  e  $B$ , visto que  $A$  e  $B$  são simples. Logo existem  $\alpha_i, \alpha'_i \in A$  e  $\beta_i, \beta'_i \in B$  tais que  $\sum \alpha_i a \alpha'_i = 1 = \sum \beta_i b \beta'_i$ , o que implica  $\sum (\alpha_i \otimes \beta_i)(a \otimes b)(\alpha'_i \otimes \beta'_i) = 1 \otimes 1 \in I$ , sendo que  $1 \otimes 1$  é a unidade em  $A \otimes B$ . Portanto, nesse caso,  $A \otimes B$  é simples.

Para o caso geral, escolha  $x \in I$  não-nulo com a representação

$$x = (c_1 \otimes b_1) + \cdots + (c_k \otimes b_k) \text{ com } c_i \in A, b_i \in B \text{ e } k \text{ o menor possível,}$$



ou seja, não há um elemento não nulo em  $I$  que possa ser representado com menos que  $k$  parcelas. Podemos assumir, sem perda de generalidade, que  $c_k = 1$ . De fato, como  $c_k \neq 0$  temos que existem  $\alpha_i, \alpha'_i \in A$  tais que  $\sum \alpha_i c_k \alpha'_i = 1$ , pois  $A$  é simples. Assim se  $c_k \neq 1$ , podemos trocar  $x$  por  $x' = \sum (\alpha_i \otimes 1)x(\alpha'_i \otimes 1)$  que continua em  $I$ , ainda tem  $k$  parcelas e

$$\begin{aligned} x' &= \left( \sum \alpha_i c_1 \alpha'_i \right) \otimes b_1 + \left( \sum \alpha_i c_2 \alpha'_i \right) \otimes b_2 + \cdots + \left( \sum \alpha_i c_k \alpha'_i \right) \otimes b_k = \\ &= c'_1 \otimes b_1 + c'_2 \otimes b_2 + \cdots + 1 \otimes b_k \quad \text{com } c'_j = \sum \alpha_i c_j \alpha'_i \in A. \end{aligned}$$

Vamos mostrar que  $k = 1$ . Agora suponha por absurdo que  $k > 1$ . Então  $c_{k-1}$  e  $c_k$  são linearmente independentes, senão teríamos  $c_{k-1} = \lambda c_k$  e  $(c_{k-1} \otimes b_{k-1}) + (c_k \otimes b_k) = c_k \otimes (\lambda b_{k-1} + b_k)$  o que acarreta uma representação para  $x$  com um número menor que  $k$  parcelas. Como  $c_k = 1 \in K = C(A)$ , temos que  $c_{k-1} \notin C(A)$ , pois em um corpo todos os elementos são linearmente dependentes. Assim existe  $a \in A$  tal que  $ac_{k-1} - c_{k-1}a \neq 0$ . Consideremos o comutador  $y = (a \otimes 1)x - x(a \otimes 1) \in I$ , ou seja,  $y = (ac_1 - c_1a) \otimes b_1 + \cdots + (ac_{k-1} - c_{k-1}a) \otimes b_{k-1}$ . Como os elementos  $b_i$  são linearmente independentes e um dos somandos acima é não nulo, temos que a soma total é não nula, isto é,  $y \neq 0$ . Dessa forma construímos um elemento  $y \in I$ ,  $y \neq 0$  representado com um número menor que  $k$  parcelas, o que é absurdo. Portanto  $k = 1$  e voltamos ao primeiro caso.

(3) Se  $A$  e  $B$  são álgebras centrais simples, pelos itens (1) e (2), temos que  $A \otimes B$  é uma álgebra central simples. ■

**Definição 3.8.** Se  $A$  é um anel definimos  $A^\circ$  por  $A = A^\circ$  como grupo abeliano aditivo, mas com produto  $\circ$  em  $A^\circ$  definido por  $a \circ b = ba$ . O anel  $A^\circ$  é chamado de *anel oposto de  $A$* .

É obvio que  $A^\circ$  é também um anel. Os elementos neutro e unidade de  $A$  e  $A^\circ$  coincidem. Todo ideal à esquerda (direita) de  $A$  é um ideal à direita (esquerda) de  $A^\circ$ . Portanto  $A$  e  $A^\circ$  “tem os mesmos” ideais bilaterais. Se  $A$  é central, simples ou

um anel com divisão, então  $A^\circ$  também o é. Claramente  $A = A^{\circ\circ}$  e  $A = A^\circ$  se, e somente, se  $A$  é comutativo. Em geral  $A$  e  $A^\circ$  não são isomorfos. Se a  $K$ -álgebra  $A$  é uma álgebra central simples, então  $A^\circ$  também é uma álgebra central simples.

**Teorema 3.9.** *Seja  $A$  uma álgebra central simples sobre  $K$ . Então  $A \otimes A^\circ \simeq M(n, K)$ , onde  $n = \dim_K A$ .*

**Demonstração:** Como  $A$  é um espaço vetorial sobre  $K$ , sabemos da Álgebra Linear que  $M(n, K) \simeq \text{End}_K(A)$ , basta portanto mostrar que  $A \otimes A^\circ \simeq \text{End}_K(A)$ . Para isso definimos  $\psi : A \times A^\circ \rightarrow \text{End}_K(A)$  tal que para  $a \in A$  e  $b \in A^\circ$  temos  $\psi(a, b)(x) = axb$  para todo  $x \in A$ . Dessa forma  $\psi(a, b) \in \text{End}_K(A)$ , já que para  $x_1, x_2 \in A$  e  $\lambda \in K$ ,

$$\psi(a, b)(x_1 + x_2) = a(x_1 + x_2)b = ax_1b + ax_2b = \psi(a, b)(x_1) + \psi(a, b)(x_2) \quad \text{e}$$

$$\psi(a, b)(\lambda x_1) = a(\lambda x_1)b = \lambda(ax_1b) = \lambda\psi(a, b)(x_1).$$

Observe que  $\psi(a + b, c)(x) = (a + b)xc = axc + bxc = \psi(a, c)(x) + \psi(b, c)(x)$ , para todo  $x \in A$ . Analogamente  $\psi(a, b + c)(x) = \psi(a, b)(x) + \psi(a, c)(x)$ , para todo  $x \in A$ . Lembrando que  $K$  é o centro de  $A$ , temos  $\psi(\lambda a, b)(x) = \lambda axb = ax\lambda b = \psi(a, \lambda b)(x)$ , para todo  $x \in A$  e  $\lambda \in K$ . Portanto  $\psi$  é bilinear. Também temos que  $\psi$  é multiplicativa. De fato,  $\psi(ac, b \circ d)(x) = acxdb = a(cx)d b = \psi(a, b)(cx d) = \psi(a, b)\psi(c, d)(x)$ . Assim pela Propriedade Universal do Produto Tensorial existe um homomorfismo de álgebras  $\varphi : A \otimes A^\circ \rightarrow \text{End}_K(A)$ . Como  $\ker \psi$  é um ideal de  $A \otimes A^\circ$  e como  $A \otimes A^\circ$  é uma álgebra central simples temos que  $\psi$  é injetor. Como as dimensões de  $A \otimes A^\circ$  e  $\text{End}_K(A)$  coincidem temos que  $\psi$  é sobrejetor. Donde concluímos que  $A \otimes A^\circ \simeq \text{End}_K(A)$ . ■

**Observação 3.10.** Seja  $A$  um álgebra central simples sobre  $K$  e seja  $E = \text{End}_K(A) \simeq A \otimes A^\circ$ .  $A$  e  $A^\circ$  podem ser consideradas como subálgebras de  $E$  pelas identificações  $a \leftrightarrow a \otimes 1$  e  $b \leftrightarrow 1 \otimes b$ , ou ainda, os elementos de  $A$  correspondem às multiplicações à esquerda e os elementos de  $A^\circ$  às multiplicações à direita. Assim  $A$  pode ser

visto não só como um  $K$ -módulo mas também como um  $A$ -módulo, um  $A^\circ$ -módulo e um  $E$ -módulo. Pelo Teorema 3.7 existem os seguintes isomorfismos canônicos  $\text{End}_A(A) \simeq C_E(A) \simeq A^\circ$  e  $\text{End}_A(A) \simeq C_E(A^\circ) \simeq A$ . Sendo que o isomorfismo  $\text{End}_A(A) \simeq C_E(A)$  segue da definição de centralizador.

Recordemos que se  $A$  é uma  $K$ -álgebra e  $\alpha$  um elemento inversível de  $A$ , então  $x \rightarrow \alpha x \alpha^{-1}$  é um *automorfismo interno* de  $A$ , que denotaremos por  $\text{int}(\alpha)$ . Na seqüência vamos provar um resultado básico, que será muito usado de agora em diante.

**Teorema 3.11. (Skolem-Noether)** *Sejam  $A$  uma álgebra central simples sobre  $K$  e  $B$  uma  $K$ -álgebra simples. Sejam  $\sigma, \tau : B \rightarrow A$  homomorfismos de álgebras. Então existe um automorfismo interno  $\varphi$  de  $A$  tal que  $\tau = \varphi\sigma$ .*

**Demonstração:** Consideremos primeiro o caso em que  $A = \text{End}_K(V)$ , sendo  $V$  um  $K$ -espaço vetorial. Então  $V$  é também um  $A$ -módulo. Usando as aplicações  $\sigma$  e  $\tau$  podemos ver  $V$  como  $B$ -módulo por dois caminhos diferentes. Estes  $B$ -módulos serão denotados por  $V_\sigma$  e  $V_\tau$ . Pelo Teorema 2.7  $V_\sigma$  e  $V_\tau$  são isomorfos como  $B$ -módulos. Seja  $f : V_\tau \rightarrow V_\sigma$  um  $B$ -isomorfismo. Então para todo  $b \in B$  e  $x \in V$

$$f((\tau b)x) = (\sigma b)(f(x)).$$

Logo  $\tau(b) = f^{-1}(\sigma b)f$ . Como  $f \in A$ , a afirmação está provada nesse caso.

No caso geral, consideremos as aplicações

$$\sigma \otimes \text{id}, \tau \otimes \text{id} : B \otimes A^\circ \rightarrow A \otimes A^\circ \simeq \text{End}_K(A).$$

Como  $A$  é uma álgebra central simples temos que  $A^\circ$  também o é, e como  $B$  é simples pelo Teorema 3.7 temos que  $B \otimes A^\circ$  é simples. Pelo caso anterior, existe um  $f \in A \otimes A^\circ$ , com  $f$  inversível, tal que  $(\tau b) \otimes a = f^{-1}((\sigma b) \otimes a)f$ , para todo  $b \in B$  e  $a \in A^\circ$ .

Fazendo  $b = 1$  primeiro vemos que  $f$  comuta com todos elementos de  $1 \otimes A^\circ$ , visto que  $(\tau(1)) \otimes a = f^{-1}((\sigma 1) \otimes a)f$ , e como  $\tau(1) = \sigma(1) = 1$  temos  $f(1 \otimes a) =$

$(1 \otimes a)f$ . Pela Observação 3.10  $f = g \otimes 1$  para algum  $g \in A$ . Fazendo  $a = 1$ , como  $(\tau b) \otimes a = f^{-1}((\sigma b) \otimes a)f$ , temos  $(\tau b) \otimes 1 = (g \otimes 1)^{-1}((\sigma b) \otimes 1)(g \otimes 1)$ . Portanto  $\tau b = g^{-1}(\sigma b)g$ , para todo  $b \in B$ . ■

**Corolário 3.12.** *Seja  $A$  uma álgebra central simples. Todo automorfismo  $\varphi$  de  $A$  é um automorfismo interno.*

**Demonstração:** Basta tomar  $A = B$ ,  $\sigma = \text{id}$  e  $\tau = \varphi$  no teorema anterior. ■

## 3.2 Estendendo o corpo base de uma álgebra central simples

Seja  $A$  uma  $K$ -álgebra e  $L$  uma extensão de corpos de  $K$ . Definimos  $A_L = A \otimes_K L$  e temos que  $A_L$  é uma  $L$ -álgebra. De fato, claramente  $A_L$  é um anel. Resta mostrarmos que  $A_L$  é um  $L$ -espaço vetorial. Como  $A_L$  é grupo comutativo com a soma, são verificadas as propriedades relacionados à soma.

O produto por escalar de  $L$  é definido nos elementos básicos por  $\lambda(a \otimes l) = a \otimes \lambda l$  para todo  $\lambda \in L$  e estendido por linearidade.

Assim para  $a, a_1, a_2 \in A$  e  $\alpha, \lambda, l, l_1, l_2 \in L$

- $\alpha\lambda(a \otimes l) = a \otimes \alpha\lambda l = \alpha(a \otimes \lambda l) = \alpha(\lambda(a \otimes l))$
- $1(a \otimes l) = (a \otimes l)$
- $\lambda((a_1 \otimes l_1) + (a_2 \otimes l_2)) = \lambda(a_1 \otimes l_1) + \lambda(a_2 \otimes l_2)$  (por definição)
- $(\alpha + \lambda)(a \otimes l) = a \otimes (\alpha + \lambda)l = a \otimes (\alpha l + \lambda l) = (a \otimes \alpha l) + (a \otimes \lambda l) = \alpha(a \otimes l) + \lambda(a \otimes l)$ .

Portanto  $A_L$  é um  $L$ -espaço vetorial.

Para concluirmos o fato de que  $A_L$  é uma  $L$ -álgebra, resta checarmos que para todo  $\lambda \in L$  e  $x, y \in A_L$  vale que  $\lambda(x \cdot y) = (\lambda x)y = x(\lambda y)$ . De fato, se  $x = a_1 \otimes l_1$

e  $y = a_2 \otimes l_2$ , então  $\lambda(x.y) = \lambda(a_1 a_2 \otimes l_1 l_2) = a_1 a_2 \otimes \lambda l_1 l_2 = (a_1 \otimes \lambda l_1).(a_2 \otimes l_2) = (\lambda(a_1 \otimes l_1)).(a_2 \otimes l_2) = (\lambda x)y$ . Analogamente  $\lambda(x.y) = a_1 a_2 \otimes l_1 \lambda l_2 = (a_1 \otimes l_1).(a_2 \otimes \lambda l_2) = (a_1 \otimes l_1).\lambda(a_2 \otimes l_2) = x(\lambda y)$ . Como queríamos.

Se  $(a_\alpha)$  é uma base de  $A$  sobre  $K$  (que existe pois todo espaço vetorial possui base),  $(a_\alpha \otimes 1)$  é uma base de  $A_L$  sobre  $L$ . De fato, dado um elemento básico  $a \otimes x$ , com  $a \in A$  e  $x \in L$ , temos que  $a = \alpha_1 a_{\alpha_1} + \cdots + \alpha_n a_{\alpha_n}$ , com  $\alpha_i \in K$ . E assim

$$a \otimes x = (\alpha_1 a_{\alpha_1} + \cdots + \alpha_n a_{\alpha_n}) \otimes x = (\alpha_1 (a_{\alpha_1} \otimes x) + \cdots + \alpha_n (a_{\alpha_n} \otimes x)) = \alpha_1 x (a_{\alpha_1} \otimes 1) + \cdots + \alpha_n x (a_{\alpha_n} \otimes 1) \text{ com } \alpha_i x \in L \text{ para todo } i = 1, \dots, n.$$

Segue que  $(a_\alpha \otimes 1)$  gera  $A_L$ . Agora, se  $\alpha_1 (a_{\alpha_1} \otimes 1) + \cdots + \alpha_n (a_{\alpha_n} \otimes 1) = 0$ , então  $(a_{\alpha_1} \otimes \alpha_1) + \cdots + (a_{\alpha_n} \otimes \alpha_n) = 0$ . Portanto  $a_{\alpha_i} \otimes \alpha_i = 0$ , para  $i = 1, \dots, n$ . Como  $a_{\alpha_i} \neq 0$  devemos ter que  $\alpha_i = 0$ , para  $i = 1, \dots, n$ , o que implica que  $(a_\alpha \otimes 1)$  é linearmente independente.

Dessa forma podemos concluir que  $\dim_K A = \dim_L A_L$ .

**Proposição 3.13.** *Se  $A$  é uma álgebra central simples sobre  $K$  e  $L \supset K$  é uma extensão de corpos, então  $A_L$  é uma álgebra central simples sobre  $L$ .*

**Demonstração:** Como  $A_L = A \otimes_K L$ , temos pelo Teorema 3.7 que  $C(A_L) = C(A) \otimes C(L) = K \otimes_K L \simeq L$ . Novamente pelo Teorema 3.7, como  $A$  é álgebra central simples e  $L$  é simples,  $A \otimes_K L$  é simples. Portanto  $A_L$  é uma  $L$ -álgebra central simples. ■

**Lema 3.14.** *Se  $K$  é um corpo algebricamente fechado, então a única álgebra de dimensão finita sobre  $K$  é o próprio  $K$ .*

**Demonstração:** Considere  $A$  uma  $K$ -álgebra de dimensão finita. Dado  $a \in A$  temos que  $K[a] = \{f(a) : f(X) \in K[X]\} \subset A$  é um espaço vetorial sobre  $K$ . Logo  $\dim_K K[a] < \dim_K A < \infty$ . Digamos  $\dim_K K[a] = n$ . Assim  $1, a, a^2, \dots, a^n \in K[a]$

são linearmente dependentes, ou seja, existem  $\alpha_0, \dots, \alpha_n \in K$  tais que  $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \dots + \alpha_n a^n = 0$ , segue que  $a$  é raiz do polinômio  $\alpha_0 + \alpha_1 X + \alpha_2 X^2 + \dots + \alpha_n X^n \in K[X]$ . Como  $K$  é algebricamente fechado,  $a \in K$ . Portanto  $A = K$ . ■

**Definição 3.15.** Se  $A$  é uma álgebra central simples de dimensão finita sobre  $K$ , então qualquer extensão de corpos  $L$  de  $K$  tal que  $A \otimes_K L = M(n, L)$  é chamada de *corpo de decomposição de  $A$* .

O lema anterior mostra que todo fecho algébrico  $\bar{K}$  de  $K$  é um corpo de decomposição para qualquer álgebra central simples de dimensão finita sobre  $K$ . De fato, pelo Teorema de Wedderburn  $A_{\bar{K}} \simeq M(n, D)$ , para alguma  $\bar{K}$ -álgebra com divisão  $D$ . Mas como  $\bar{K}$  é algebricamente fechado, pelo lema anterior,  $D = \bar{K}$ . Portanto  $A_{\bar{K}} \simeq M(n, \bar{K})$ .

**Observação 3.16.** Pode-se ainda mostrar que toda álgebra central simples possui um corpo de decomposição de dimensão finita. E também que existem corpos de decomposição separáveis. (Ver [10], Cap. 8, Teoremas 5.4 e 5.5).

**Corolário 3.17.** *Se  $A$  é uma álgebra central simples de dimensão finita, então  $\dim_K A$  é um quadrado.*

**Demonstração:** Segue de  $\dim_K A = \dim_{\bar{K}} A_{\bar{K}} = \dim M(n, \bar{K}) = n^2$ . ■

### 3.2.1 Traço e Norma

Recordemos da Álgebra Linear que dado um operador linear  $T : V \rightarrow V$ , onde  $V$  é um espaço vetorial sobre um corpo  $K$ , podemos definir traço e determinante de  $T$  como sendo o traço e o determinante da matriz do operador em relação a uma base de  $V$  sobre  $K$ .

Seja  $A$  uma  $K$ -álgebra, então podemos definir o operador  $l_a : A \rightarrow A$  por  $l_a(x) = ax$ . O traço e o determinante de  $l_a$  são também chamados *traço* e *norma*

do elemento  $a$  e denotamos por  $\text{Tr}_{A/K}(a)$  e  $N_{A/K}(a)$ , respectivamente. Logo

$$\text{Tr}_{A/K}(a) = \text{tr}(l_a) \quad \text{e} \quad N_{A/K}(a) = \det(l_a).$$

Em particular, se  $L \supset K$  é uma extensão finita de corpos e  $u \in L$ , então  $\text{Tr}_{L/K}(u) = \text{tr}(l_u)$  e  $N_{L/K}(u) = \det(l_u)$ . Se  $L \supset K$  é uma extensão galoisiana finita e  $G = \{\sigma_1, \dots, \sigma_n\}$  é o grupo de Galois de  $L$  sobre  $K$ , também definimos

$$\text{Tr}_{L/K}(u) = \sum_{i=1}^n \sigma_i(u) \quad \text{e} \quad N_{L/K}(u) = \prod_{i=1}^n \sigma_i(u).$$

Esta definição coincide com a definição anterior para o caso em que  $L \supset K$  é uma extensão galoisiana finita.

**Observação 3.18.** Para o caso de álgebras de matrizes é importante observar que o traço usual de uma matriz não coincide com o traço da multiplicação à esquerda por esta matriz. Considere  $A = M(n, L)$  uma álgebra de matrizes sobre  $L$ . Dado  $a \in A$ , temos que  $\text{Tr}_{A/K}(a)$  é o traço da multiplicação à esquerda pela matriz  $a = (a_{ij}) \in M(n, L)$ . Uma conta simples nos dá que a matriz de  $l_a$  em relação a base canônica  $\{e_{11}, e_{12}, \dots, e_{nn}\}$  é uma matriz em blocos:

$$\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix}, \text{ com } A_{ij} = \begin{pmatrix} a_{ji} & 0 & \cdots & 0 \\ 0 & a_{ji} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{ji} \end{pmatrix}$$

$$\begin{aligned} \text{Portanto } \text{Tr}_{A/K}(a) &= \text{tr}(l_a) = na_{11} + na_{22} + \dots + na_{nn} = \\ &= n(a_{11} + a_{22} + \dots + a_{nn}) = n \cdot \text{tr}(a). \end{aligned}$$

**Observação 3.19.** Sejam  $A$  e  $B$   $K$ -álgebras. Se  $i : A \rightarrow B$  é um isomorfismo, temos que  $\text{Tr}_{A/K}(x) = \text{Tr}_{B/K}(i(x))$ . De fato, basta notar que a matriz de  $l_x$  na base  $\{e_1, \dots, e_m\}$  de  $A$ , coincide com a matriz de  $l_{i(x)}$  na base  $\{i(e_1), \dots, i(e_m)\}$  de  $B$ . Logo  $\text{tr}(l_{i(x)}) = \text{tr}(l_x)$ , donde segue o resultado.

No Capítulo 4 iremos utilizar o Teorema Hilbert 90. Devido à sua importância, decidimos fazer a demonstração, apesar de fugir um pouco do assunto.

**Teorema 3.20. (Hilbert 90)** *Seja  $L/K$  uma extensão de corpos normal e finita, digamos de grau  $n$ , com grupo de Galois  $G$  cíclico gerado por um elemento  $\sigma$ . Então  $\lambda \in L$  tem norma  $N(\lambda) = \lambda \sigma(\lambda) \sigma^2(\lambda) \dots \sigma^{n-1}(\lambda) = 1$  se, e somente, se  $\lambda = \mu \sigma(\mu^{-1})$  para algum  $\mu \in L - \{0\}$ .*

**Demonstração:** Começemos assumindo que  $\lambda = \mu \sigma(\mu^{-1})$ . Como  $\sigma$  tem ordem  $n$ , temos  $N(\lambda) = \lambda \sigma(\lambda) \sigma^2(\lambda) \dots \sigma^{n-1}(\lambda) = (\mu \sigma(\mu^{-1})) (\sigma(\mu \sigma(\mu^{-1}))) \dots (\sigma^{n-1}(\mu \sigma(\mu^{-1})))$

$$= \mu \sigma(\mu^{-1}) \sigma(\mu) \sigma^2(\mu^{-1}) \dots \sigma^{n-1}(\mu) \sigma^n(\mu^{-1}) = \mu \sigma^n(\mu^{-1}) = 1.$$

Reciprocamente, suponha  $N(\lambda) = 1$  e para  $c \in L$  definimos

$$d_0 = \lambda c$$

$$d_1 = (\lambda \sigma(\lambda)) \sigma(c)$$

$\vdots$

$$d_i = (\lambda \sigma(\lambda) \dots \sigma^i(\lambda)) \sigma^i(c) \quad \text{para } 0 \leq i \leq n-1.$$

Assim  $d_{n-1} = N(\lambda) \sigma^{n-1}(c) = \sigma^{n-1}(c)$ . Além disso, como

$$\sigma(d_i) = (\sigma(\lambda) \sigma^2(\lambda) \dots \sigma^{i+1}(\lambda)) \sigma^{i+1}(c) \quad \text{temos}$$

$$d_{i+1} = (\lambda \sigma(\lambda) \dots \sigma^i(\lambda) \sigma^i(c) \sigma^{i+1}(\lambda)) \sigma^{i+1}(c) = \lambda \sigma(d_i) \quad \text{para } 0 \leq i \leq n-2.$$

Definimos  $\mu = d_0 + d_1 + \dots + d_{n-1}$ . Podemos escolher  $c$  de modo que  $\mu \neq 0$ . De fato, suponha que  $\mu = 0$  para todo  $c \in L$ . Logo para cada  $c \in L$  temos

$$\alpha_0 \sigma^0(c) + \alpha_1 \sigma(c) + \alpha_2 \sigma^2(c) + \dots + \alpha_{n-1} \sigma^{n-1}(c) = 0,$$

onde  $\alpha_i = \lambda \sigma(\lambda) \dots \sigma^i(\lambda)$  com  $\alpha_i \in L$  para todo  $i = 1, \dots, n-1$  e pelo menos  $\alpha_{n-1} \neq 0$ . Dessa forma os automorfismos distintos  $\sigma^i$  são linearmente dependentes



sobre  $L$ , o que é falso. Assim podemos escolher  $c$  tal que  $\mu \neq 0$ . Mas agora

$$\begin{aligned}
 \sigma(\mu) &= \sigma(d_0) + \cdots + \sigma(d_{n-1}) \\
 &= (\sigma(\lambda)\sigma(c)) + (\sigma(\lambda)\sigma^2(\lambda)\sigma^2(c)) \cdots + (\sigma^n(c)) \\
 &= (\lambda^{-1}\lambda)((\sigma(\lambda)\sigma(c)) + (\sigma(\lambda)\sigma^2(\lambda)\sigma^2(c)) \cdots + (c)) \\
 &= \lambda^{-1}(d_1 + \cdots + d_{n-1}) + \lambda c \\
 &= \lambda^{-1}(d_1 + \cdots + d_{n-1} + d_0) \\
 &= \lambda^{-1}\mu.
 \end{aligned}$$

Portanto  $\lambda = \mu\sigma(\mu^{-1})$ . ■

# Capítulo 4

## Involuções sobre Álgebras Centrais Simples

Iniciaremos este capítulo introduzindo a teoria de involuções sobre álgebras centrais simples. A segunda seção envolve apenas teoria de matrizes, mas apresenta um resultado crucial que será usado na seção seguinte, quando iremos estudar a involução sobre uma álgebra de grupo.

### 4.1 Classificação de Involuções

Primeiramente vejamos o que é uma involução.

**Definição 4.1.** Seja  $R$  um anel. Uma aplicação  $\sigma : R \rightarrow R$  é chamada *involução* sobre  $R$ , se para todo  $x, y \in R$  tivermos:

$$\sigma(x + y) = \sigma(x) + \sigma(y), \quad \sigma(xy) = \sigma(y)\sigma(x), \quad \sigma(\sigma(x)) = \sigma^2(x) = x.$$

O par  $(R, \sigma)$  é chamado de *anel com involução*.

Os homomorfismos de anéis que nos interessam são os que preservam a involução.

**Definição 4.2.** Chamamos de *homomorfismo de anéis com involução* ao homomorfismo de anéis  $f : (R, \sigma) \rightarrow (S, \tau)$  em que  $\tau(f(x)) = f(\sigma(x))$ .

Veremos agora alguns exemplos bem conhecidos de involuções:

**Exemplo 4.3.** A conjugação complexa  $\bar{\phantom{x}}$  sobre  $\mathbb{C}$  dada por  $\overline{(a + bi)} = (a - bi)$  é uma involução. Podemos definir uma involução em  $K(\sqrt{-1})$  por  $\overline{(a + b\sqrt{-1})} = (a - b\sqrt{-1})$ . Chamaremos esta involução também de *conjugação complexa*.

**Exemplo 4.4.** Considere a álgebra dos Hamiltonianos  $H$ , definida no Exemplo 3.2. A aplicação  $\bar{\phantom{x}} : H \rightarrow H$  definida por  $\overline{a + bi + cj + dk} = a - bi - cj - dk$  é uma involução, conhecida como involução canônica sobre  $H$ .

**Exemplo 4.5.** A transposição de matrizes  $M(n, D)$ , onde  $D$  é um anel comutativo qualquer, é uma involução. Visto que para todo  $A, B \in M(n, D)$ ,  $(A + B)^t = A^t + B^t$ ,  $(AB)^t = B^t A^t$  e  $(A^t)^t = A$ .

**Exemplo 4.6.** A conjugada transposta  $^{-t}$  sob o anel de matrizes  $M(n, D)$ , definida por  $(a_{ij})^{-t} = (\overline{a_{ij}})^t$  é uma involução.

Note que a involução do exemplo anterior não é uma composição de involuções, pois a conjugação dos elementos das matrizes não é uma involução em  $M(n, D)$ . Vale observar que a composta de duas involuções em um anel  $A$  será uma involução se, e somente, se  $A$  for um anel comutativo.

**Exemplo 4.7.** Considere  $G$  um grupo finito e  $K$  um corpo. A aplicação  $\sigma : K[G] \rightarrow K[G]$  definida por  $\sigma(\sum_g a_g g) = \sum_g a_g g^{-1}$ , é uma involução conhecida como *involução canônica* sobre a álgebra de grupos  $K[G]$ .

**Observação 4.8.** Se  $A$  é uma  $K$ -álgebra, uma involução  $\sigma : A \rightarrow A$  não é necessariamente  $K$ -linear. Se  $L$  é o centro de  $A$ , toda involução  $\sigma$  leva o centro  $L$  nele próprio. De fato, seja  $y \in L$  e  $x \in A$ . Vamos mostrar que  $\sigma(y)x = x\sigma(y)$ . Como  $y\sigma(x) = \sigma(x)y$ , temos  $\sigma(y)x = \sigma(y)\sigma(\sigma(x)) = \sigma(\sigma(x)y) = \sigma(y\sigma(x)) = \sigma(\sigma(x))\sigma(y) = x\sigma(y)$ .

Para o caso de  $A$  ser uma álgebra central simples, teremos que  $\sigma(K) = K$ . Assim temos duas opções:

(i)  $\sigma|_K$  é a identidade. Neste caso,  $\sigma$  é  $K$ -linear e dizemos que  $\sigma$  é de *primeira espécie*.

(ii)  $\sigma|_K$  não é a identidade, ou seja,  $\sigma|_K$  é um automorfismo não-trivial de  $K$ . Dizemos nesse caso que a involução  $\sigma$  é de *segunda espécie*. Se  $k$  denota o corpo fixado por  $\sigma|_K$ , então a extensão  $K/k$  é uma extensão quadrática separável. No caso das involuções de primeira espécie definimos  $K = k$  e dizemos em ambos os casos que  $\sigma$  é uma  $K/k$ -involução. Frequentemente a extensão  $K/k$  (trivial ou quadrática separável) será fixada e consideramos a categoria de  $K$ -álgebras com  $K/k$ -involuções.

**Exemplo 4.9.** Nos exemplos acima, temos que os exemplos 4.3 e 4.6 (onde a conjugação é a complexa) são exemplos de involuções de segunda espécie, as demais são involuções de primeira espécie.

Na seqüência faremos a classificação de involuções em álgebras centrais simples. Um fato decisivo na classificação de involuções é o de que a composição de duas  $K/k$ -involuções é um automorfismo. O que é verdadeiro, pois para  $\sigma, \tau$   $K/k$ -involuções sobre uma álgebra  $A$  e  $x, y \in A$ ,

$$\begin{aligned}\sigma\tau(x+y) &= \sigma(\tau(x) + \tau(y)) = \sigma\tau(x) + \sigma\tau(y) \quad \text{e} \\ \sigma\tau(x.y) &= \sigma(\tau(y).\tau(x)) = \sigma\tau(x) + \sigma\tau(y).\end{aligned}$$

Agora note que  $\ker(\sigma\tau) = \{0\}$ , pois se  $\sigma\tau(x) = 0$  temos  $\sigma\sigma\tau(x) = \sigma(0)$ , ou seja,  $\tau(x) = 0$ . Mas  $x = \tau\tau(x) = \tau(0) = 0$ . Usaremos fortemente o fato que sendo  $\sigma\tau$  um automorfismo, pelo Teorema de Skolem-Noether 3.11 e seu corolário,  $\sigma\tau$  é um automorfismo interno.

O próximo teorema classifica involuções sobre álgebras centrais simples.

**Teorema 4.10.** *Sejam  $A$  uma álgebra central simples sobre  $K$  e  $\sigma$  uma  $K/k$ -involução sobre  $A$ . Então valem as afirmações.*

(1) *Se  $\lambda \in K$  é tal que  $\lambda\sigma(\lambda) = 1$  e  $a$  é um elemento  $\lambda$ -hermitiano inversível de*

$A$ , isto é,  $a = \lambda\sigma(a)$ , então a aplicação  $\sigma_a : A \rightarrow A$ , dada por  $\sigma_a(x) = a\sigma(x)a^{-1}$  com  $x \in A$ , é uma  $K/k$ -involução sobre  $A$ .

(2) Se reciprocamente  $\tau$  é uma  $K/k$ -involução arbitrária sobre  $A$ . Então existe um elemento inversível  $a = \pm\sigma(a)$  em  $A$  tal que  $\tau = \sigma_a$ .

(3) Para o caso de involuções de primeira espécie,  $a$  é unicamente determinado a menos de um fator escalar  $\alpha \in K^*$ . No caso das involuções de segunda espécie, inclusive podemos encontrar um  $a$  satisfazendo  $a = \sigma(a)$ , este  $a$  é unicamente determinado a menos de um escalar  $\alpha \in K^*$ .

(4) Sejam  $\sigma_a, \sigma_b$  duas  $K/k$ -involuções sobre  $A$ . Então  $(A, \sigma_a) \simeq (A, \sigma_b)$  se, e somente, se existe um  $c \in A$  e  $\alpha \in K$  tais que  $b = \alpha c a \sigma(c)$ .

**Demonstração:** (1) Se  $x, y \in A$  temos que  $\sigma_a(x + y) = a\sigma(x + y)a^{-1} = a(\sigma(x) + \sigma(y))a^{-1} = a(\sigma(x))a^{-1} + a(\sigma(y))a^{-1} = \sigma_a(x) + \sigma_a(y)$ ;

$$\sigma_a(x.y) = a\sigma(x.y)a^{-1} = a(\sigma(y).\sigma(x))a^{-1} = a(\sigma(y))a^{-1}.a(\sigma(x))a^{-1} = \sigma_a(y).\sigma_a(x),$$

$$\sigma_a(\sigma_a(x)) = \sigma(a\sigma(x)a^{-1}) = a\sigma(a\sigma(x)a^{-1})a^{-1} = a\sigma(a^{-1})\sigma(\sigma(x))\sigma(a)a^{-1} =$$

$$= \lambda\sigma(a)\sigma(a^{-1})x\lambda^{-1}aa^{-1} = \lambda x \lambda^{-1} = x, \text{ visto que } \lambda \in K. \text{ Portanto}$$

$\sigma_a$  é uma  $K/k$ -involução.

(2) Dada  $\tau$  uma  $K/k$ -involução arbitrária sobre  $A$ , como já observamos,  $\sigma\tau$  é um automorfismo interno, logo existe um elemento inversível  $b \in A^*$  tal que  $\sigma\tau(x) = b^{-1}xb$ . Como  $\sigma$  é sobrejetor, existe  $a \in A^*$  tal que  $b = \sigma(a)$ , assim  $\sigma\tau(x) = \sigma(a^{-1})x\sigma(a)$ . Aplicando  $\sigma$  a última igualdade temos

$$\tau(x) = \sigma\sigma\tau(x) = \sigma(\sigma(a^{-1})x\sigma(a)) = a\sigma(x)a^{-1}.$$

$$\text{Aplicando } \tau \text{ na igualdade acima, obtemos } x = \tau\tau(x) = \tau(a\sigma(x)a^{-1}) =$$

$$= \tau(a^{-1})\tau\sigma(x)\tau(a) = a\sigma(a^{-1})a^{-1}a\sigma\sigma(x)a^{-1}a\sigma(a)a^{-1} = a\sigma(a^{-1})x\sigma(a)a^{-1}.$$

Logo  $a\sigma(a^{-1}) = \alpha \in K^*$  (lembrando que  $K = C(A)$ ), o que implica que  $a = \alpha\sigma(a)$ . Usando o fato que os elementos de  $K$  comutam com os elementos de  $A$  obtemos que  $\sigma(a) = \sigma(\alpha\sigma(a)) = \sigma(\sigma(a)\alpha) = \sigma(\alpha)a$ , e assim  $a = \alpha\sigma(a) = \alpha\sigma(\alpha)a$ .

Isto nos leva a concluir que  $\alpha\sigma(\alpha) = 1$ . Se  $\sigma$  é de primeira espécie, então  $\alpha^2 = 1$  e assim  $\alpha = \pm 1$  e obtemos o desejado.

Caso  $\sigma$  seja uma involução de segunda espécie, considere a extensão de corpos  $K/k$ , onde  $k$  é o corpo fixo por  $\sigma$ . A extensão  $K/k$  é normal, tem grau dois e o grupo de Galois  $G(K, k)$  é cíclico gerado por  $\sigma$ . Como  $N(\alpha) = \alpha\sigma(\alpha) = 1$ , podemos usar o Teorema 3.20 (Teorema de Hilbert 90) e escolher um  $\mu \in K^*$  tal que  $\mu\sigma(\mu^{-1}) = \alpha$ . Substituindo  $a$  por  $c = \mu^{-1}a$  temos que

$$\tau(x) = a\sigma(x)a^{-1} = \mu c\sigma(x)c^{-1}\mu^{-1} = \mu\sigma_c(x)\mu^{-1} = \sigma_c(x), \quad \text{pois } \mu \in K.$$

Agora, como  $\sigma(\mu^{-1}) = \mu^{-1}\alpha$  e  $\sigma(a) = \sigma(\alpha)a$  obtemos

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

Portanto nesse caso encontramos  $c \in K^*$  tal que  $\tau = \sigma_c$  e  $\sigma(c) = c$ .

(3) Para o caso de primeira espécie, se tomarmos  $b = \alpha a$ , com  $\alpha \in K^*$ , temos que  $\sigma_b = \sigma_a$  e  $\sigma(b) = \pm b$ . Já para o caso de segunda espécie temos que tomar  $\alpha \in k^*$ , pois precisamos que  $\sigma(\alpha) = \alpha$  para satisfazer  $\sigma(b) = b$ .

(4) Por definição  $(A, \sigma_a)$  e  $(A, \sigma_b)$  são isomorfos somente se existe um automorfismo  $f$  em que  $\sigma_b f(x) = f \sigma_a(x)$ . Por Skolen-Noether,  $f$  é um automorfismo interno, ou seja, existe um elemento  $c \in A^*$  tal que  $f(x) = c x c^{-1}$ . De  $\sigma_b(x) = f \sigma_a f^{-1}(x)$  temos

$$\begin{aligned} b\sigma(x)b^{-1} &= f\sigma_a f^{-1}(x) = f\sigma_a(c^{-1}xc) = f(a\sigma(c^{-1}xc)a^{-1}) = \\ &= ca\sigma(c^{-1}xc)a^{-1}c^{-1} = ca\sigma(c)\sigma(x)\sigma(c^{-1})a^{-1}c^{-1} \text{ para todo } x \in A. \end{aligned}$$

O que implica que  $b$  e  $ca\sigma(c)$  devem ser iguais a menos de um fator escalar de  $K$ , ou seja,  $b = \alpha ca\sigma(c)$  tal que  $\alpha \in K$ . ■

Para qualquer  $K/k$ -involução  $\sigma$  definimos

$$\begin{aligned} A^+ &= \{x \in A ; \sigma(x) = x\} && \text{(elementos simétricos)} \\ A^- &= \{x \in A ; \sigma(x) = -x\} && \text{(elementos anti-simétricos)}. \end{aligned}$$

Ambos são  $k$ -subespaços de  $A$ .

Se a característica de  $K$  é diferente de dois ( $\text{car } K \neq 2$ ), as involuções de primeira espécie podem ser separadas em duas classes distintas.

**Teorema 4.11.** *Seja  $A$  uma álgebra central simples de dimensão  $n^2$  sobre  $K$  e  $\sigma$  uma involução.*

(1) *Se  $\text{car } K \neq 2$ , então  $A = A^+ \oplus A^-$ .*

(2) *Se  $\sigma$  é de primeira espécie, então  $\dim_K(A^+) = \frac{1}{2}n(n+1)$  ou  $\dim_K(A^+) = \frac{1}{2}n(n-1)$ . Se  $\text{car } K = 2$  sempre temos  $\dim_K(A^+) = \frac{1}{2}n(n+1)$ .*

**Demonstração:** (1) Se  $\text{car } K \neq 2$ , para todo elemento  $x \in A$  podemos escrever  $x = \frac{1}{2}(x + \sigma(x)) + \frac{1}{2}(x - \sigma(x))$ , onde  $(x + \sigma(x)) \in A^+$ , pois  $\sigma(x + \sigma(x)) = \sigma(x) + x = x + \sigma(x)$ . Analogamente  $(x - \sigma(x)) \in A^-$ , já que  $\sigma(x - \sigma(x)) = \sigma(x) - x = -(x - \sigma(x))$ . Temos também que  $A^+ \cap A^- = 0$ , pois se  $x \in A^+ \cap A^-$  temos  $x = \sigma(x) = -x$ , o que implica que  $x = 0$ . Portanto  $A = A^+ \oplus A^-$ .

(2) Seja  $L$  um corpo de decomposição de  $A$ . Estendendo  $A$  a  $A_L = A \otimes_K L \cong M(n, L)$ . A involução  $\sigma$  é estendida à uma aplicação  $K$ -linear  $\sigma(a \otimes \alpha) = \sigma(a) \otimes \alpha$  para todo  $a \in A$  e  $\alpha \in L$ . Assim é equivalente provarmos a afirmação sobre  $M(n, L)$ . Em  $M(n, L)$  a involução canônica é a transposição. Assim os elementos simétricos formam um subespaço  $S$  de dimensão  $\frac{1}{2}n(n+1) = \frac{n^2+n}{2}$ . Pelo teorema anterior, qualquer outra involução  $\tau$  é obtida pela conjugação da transposição por um elemento inversível  $a \in M(n, L)$  com  $a = \pm a^t$ . Logo  $\tau(x) = ax^t a^{-1}$ .

Se  $a$  é simétrico,  $aS$  é o subespaço formado pelos elementos simétricos em relação a  $\tau$ , ou seja,  $\tau(ax) = ax$  para todo  $x \in S$ . Assim  $\dim_K(A^+) = \frac{1}{2}n(n+1)$ .

Se  $a$  é anti-simétrico,  $aS$  é o subespaço dos elementos anti-simétricos em relação a  $\tau$  e nesse caso temos  $\dim_K(A^-) = \frac{1}{2}n(n+1)$ . Como  $A = A^+ \oplus A^-$ , temos  $\dim_K(A) = \dim_K(A^+) + \dim_K(A^-)$ , isto é,  $n^2 = \dim_K(A^+) + \frac{1}{2}n(n+1)$ . Portanto,  $\dim_K(A^+) = \frac{1}{2}n(n-1)$ .

Para o caso em que  $\text{car}K = 2$ , temos que os elementos anti-simétricos são simétricos, logo a segunda situação nunca ocorre e teremos sempre  $\dim_K(A^+) = \frac{1}{2}n(n+1)$ . ■

**Definição 4.12.** Seja  $\sigma$  uma involução de primeira espécie sob uma álgebra central simples  $A$  de dimensão  $n^2$ . Se  $\dim_K(A^+) = \frac{1}{2}n(n+1)$  a involução  $\sigma$  é dita do *tipo ortogonal* ou *tipo + (positivo)*. Já se  $\dim_K(A^+) = \frac{1}{2}n(n-1)$  a involução é dita do *tipo simplético* ou *tipo - (negativo)*. Involuções de segunda espécie são chamadas de *unitárias*.

**Observação 4.13.** (i) Pela definição acima e pelo visto na demonstração do item (2) do Teorema 4.11 segue que, se  $\sigma$  é de primeira espécie e  $a \in A^+$ , então  $\sigma$  e  $\sigma_a$  são do mesmo tipo. Caso  $a \in A^-$ , então  $\sigma$  e  $\sigma_a$  são de tipos distintos.

(ii) Consideremos a involução canônica sobre a álgebra dos hamiltonianos  $H$  definida no Exemplo 3.2. Claramente  $\bar{\phantom{x}}|_K = \text{id}$ . Neste caso temos que  $\overline{(a+bi+cj+dk)} = (a-bi-cj-dk)$  se, e somente se,  $b=c=d=0$ . Logo  $\dim_K(A^+) = 1 = \frac{2^2-2}{2}$ . Portanto a involução canônica sobre  $H$  é da primeira espécie e do tipo simplético.

## 4.2 Diagonalização de matrizes simétricas e hermitianas

Um fato bem conhecido da Álgebra Linear é que uma matriz simétrica com valores complexos é congruente a uma matriz diagonal real. Nesta seção iremos generalizar este resultado para matrizes hermitianas com valores na álgebra  $H$  dos Hamiltonianos sobre um corpo real fechado  $K$ . Esta generalização será feita seguindo os passos da seção 5-7 do livro [8], que mostra que uma matriz hermitiana com valores complexos é congruente a uma matriz diagonal real. A diagonalização de matrizes hermitianas com valores em  $H$  é crucial para demonstrarmos o Teorema 13.3 de [10].



Nesta seção vamos fixar  $K$  como um corpo real fechado e

$$H = \{a + bi + cj + dk; a, b, c, d \in K\}$$

a álgebra dos Hamiltonianos sobre  $K$ . Imitando o caso real, dado  $x = a + bi + cj + dk$  denotaremos  $a = \operatorname{Re}(x)$  e se  $a = 0$ ,  $x$  é chamado *imaginário puro*. Observamos que a conjugação definida por  $\overline{a + bi + cj + dk} = a - bi - cj - dk$  tem algumas das propriedades da conjugação complexa, a saber: se  $x = a + bi + cj + dk$ , então

$$x + \bar{x} = 2a, \quad x\bar{x} = a^2 + b^2 + c^2 + d^2 \in K \quad \text{e } x = \bar{x} \Leftrightarrow x \in K.$$

**Definição 4.14.** Uma matriz  $A$  com valores em  $H$  é chamada *hermitiana* se  $\bar{A}^t = A$ . Duas matrizes hermitianas  $A$  e  $B$  sobre  $H$  são *hermitianamente congruentes* se e somente se  $B = \bar{P}^t A P$  para alguma matriz inversível  $P$ .

As matrizes hermitianas sobre  $H$  tem conexão com as *formas hermitianas* sobre  $H$ ,

$$h(x_1, \dots, x_n) = \sum_{i,j=1}^n \bar{x}_i a_{ij} x_j \quad \text{com } a_{ji} = \bar{a}_{ij} \text{ para } x_i, a_{ij} \in H.$$

Onde os coeficientes  $a_{ij}$  determinam uma matriz hermitiana.

Duas matrizes hermitianamente congruentes representam a mesma forma hermitiana.

**Teorema 4.15.** *Os valores de uma forma hermitiana sobre  $H$  estão em  $K$ .*

**Demonstração:** Inicialmente observamos que cada elemento diagonal  $a_{hh}$  está em  $K$ , pois  $a_{hh} = \bar{a}_{hh}$ . Agora como os elementos de  $K$  comutam com os elementos de  $H$  temos que  $\bar{x}_h \bar{a}_{hh} x_h = \bar{a}_{hh} \bar{x}_h x_h \in K$ . Os demais termos podem ser agrupados aos pares

$$\bar{x}_h a_{hj} x_j + \bar{x}_j a_{jh} x_h = \bar{x}_h a_{hj} x_j + \overline{(\bar{x}_h a_{hj} x_j)}.$$

Logo cada par pertence a  $K$ , pois é a soma de um elemento de  $H$  com seu conjugado. Isto completa a demonstração. ■

Devido ao teorema anterior e o fato de  $K$  ser um corpo ordenado, podemos falar em formas hermitianas definidas.

**Definição 4.16.** Uma forma hermitiana  $h$  sobre  $H$  é chamada *definida* se  $h$  é não nula para toda  $n$ -upla  $(x_1, \dots, x_n)$ , sendo  $x_i \in H$  e  $x_i \neq 0$  para todo  $i = 1, \dots, n$ . Se  $h(x_1, \dots, x_n) > 0$  para toda  $n$ -upla não nula,  $h$  é dita *definida positiva*; se  $h(x_1, \dots, x_n) < 0$  para toda  $n$ -upla não nula,  $h$  é dita *definida negativa*.

**Definição 4.17.** Uma matriz hermitiana  $A$  sobre  $H$  é *definida positiva* se a forma hermitiana definida por  $A$  é definida positiva. Analogamente uma matriz hermitiana sobre  $H$  é *definida negativa* se a forma hermitiana definida por ela é definida negativa.

Nosso objetivo agora é diagonalizar uma matriz hermitiana sobre  $H$ . Iremos diagonalizar a matriz da forma usual, usando operações elementares. Mas para que a cada passo obtenhamos uma matriz hermitianamente congruente a anterior, iremos realizar operações nas linhas e colunas. Lembramos que realizar uma operação numa linha é equivalente a multiplicar a matriz à esquerda pela matriz elementar correspondente e realizar uma operação numa coluna é equivalente a multiplicar a matriz à direita pela matriz elementar correspondente.

Ao final do processo queremos obter uma matriz diagonal  $D$  tal que  $D = \overline{E}_k^t [\dots (\overline{E}_1^t A E_1) \dots] E_k$ , sendo que cada par  $E_h, \overline{E}_h^t$  representa cada operação elementar realizada nas colunas e a operação elementar conjugada realizada nas linhas. Por exemplo, se multiplicarmos a  $j$ -ésima coluna por  $c$  devemos multiplicar a  $j$ -ésima linha por  $\bar{c}$ ; se adicionarmos  $c$  vezes a coluna  $j$  à coluna  $k$ , devemos adicionar  $\bar{c}$  vezes a linha  $j$  à linha  $k$ .

Devemos ainda estar atentos para o fato que  $H$  não é comutativo, logo ao multiplicarmos uma linha por um elemento de  $H$  devemos efetuar a multiplicação à esquerda dos elementos da linha. Analogamente, ao multiplicarmos uma coluna devemos efetuar a multiplicação à direita.

**Teorema 4.18.** *Toda matriz hermitiana  $A$  sobre  $H$  de posto  $r$  é hermitianamente congruente a matriz  $B = \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_{r-p} & 0 \\ 0 & 0 & 0 \end{pmatrix}$ . O inteiro  $p$  é unicamente determinado por  $A$ .*

**Demonstração:** Se  $A = 0$  não há o que fazer. Seja  $A$  uma matriz hermitiana não nula de posto  $r$ . Logo  $A = (a_{ts})$ , tal que  $a_{tt} \in K$  e  $a_{st} = \bar{a}_{ts} \in H$ .

Primeiro vamos mostrar que  $A$  hermitianamente congruente a uma matriz com um elemento da diagonal não nulo. Caso  $A$  tenha um elemento da diagonal não nulo, ela própria é a matriz procurada. Assim, assumiremos que todo elemento  $a_{tt} = 0$  e algum  $a_{ts} \neq 0$ , para  $t \neq s$ . Então  $a_{st} = \bar{a}_{ts} \neq 0$  e  $a_{ss} = a_{tt} = 0$ . Somamos a coluna  $s$  à coluna  $t$  e a linha  $s$  à linha  $t$ . Assim na nova matriz  $B$  temos  $b_{tt} = a_{st} + a_{ts} = \bar{a}_{ts} + a_{ts} = 2\text{Re}(a_{ts})$ . Se  $\text{Re}(a_{ts}) \neq 0$ , obtemos  $b_{tt} \neq 0$  como desejado. Se  $\text{Re}(a_{ts}) = 0$ , então  $a_{ts}$  é um “imaginário puro”. Neste caso,  $a_{ts} = a_1i + a_2j + a_3k$ , sendo  $a_l \in K$ , para todo  $l = 1, 2, 3$ , com  $a_l \neq 0$  pelo menos para algum  $l$ . Escolhemos um dos elementos  $i, j, k$  para o qual seu coeficiente  $a_l \neq 0$  e adicionamos a coluna  $s$  multiplicada à direita pelo elemento escolhido à coluna  $t$ . Por exemplo, se  $a_3 \neq 0$  podemos escolher o elemento  $k$ , multiplicamos a coluna  $s$  à direita pelo elemento  $k$  e somamos à coluna  $t$ . Agora realizando a operação equivalente para a linha, multiplicamos à esquerda a linha  $s$  pelo conjugado do elemento escolhido e somamos à linha  $t$ . Seguindo o exemplo em que escolhemos o elemento  $k$ , multiplicamos a linha  $s$  à esquerda por  $-k$  e somamos à coluna  $t$ . Assim obteremos o elemento  $b_{tt} \neq 0$ , sendo que, se o elemento escolhido foi  $k$  teremos  $b_{tt} = -2a_3 \neq 0$ . Observando que se o elemento escolhido fosse  $i$  teríamos  $b_{tt} = -2a_1 \neq 0$ , e caso o elemento escolhido fosse  $j$  teríamos  $b_{tt} = -2a_2 \neq 0$ . Logo  $A$  é hermitianamente congruente a matriz  $B$  com um elemento da diagonal não nulo e pertencente a  $K$ . Se  $t \neq 1$ , trocando a coluna  $t$  pela coluna 1 e a linha  $t$  pela linha 1, obtemos uma matriz  $C = (c_{ls})$  com  $c_{11} = b_{tt} \neq 0$ . Em  $C$  multiplicamos a primeira coluna à direita por  $-\frac{c_{1s}}{c_{11}}$  e adicionamos à coluna  $s$ , multiplicamos a primeira linha à esquerda por  $-\left(\frac{c_{1s}}{c_{11}}\right)$  e

somamos à linha  $s$ . Como  $c_{s1} = \overline{c_{1s}}$  teremos zeros nas posições  $(1, s)$  e  $(s, 1)$ .

Repetindo o processo para todo  $s$ , obtemos a matriz  $D_0 = \begin{pmatrix} c_{11} & 0 \\ 0 & D_1 \end{pmatrix}$ , onde  $D_1$  tem ordem  $(n - 1)$  e é hermitiana. Aplicando a  $D_1$  o mesmo processo aplicado a  $C$ , de forma que as operações não afetem a 1ª coluna ou a 1ª linha, teremos após um número finito de passos uma matriz diagonal  $D$  hermitianamente congruente a  $A$ . Note que  $D = \text{diag}(d_1, \dots, d_r, 0, \dots, 0)$ , com  $d_h \in K$ , onde cada  $d_h$  é não nulo. Seja  $p$  o número de elementos  $d_h$  que são positivos. Fazendo convenientes trocas de linhas, seguidas por respectivas trocas de coluna, obtemos os  $p$  elementos positivos nas primeiras posições. Como  $D$  é congruente a essa “nova” matriz, podemos assumir que  $D$  tem a seguinte propriedade  $d_h > 0$  para  $h = 1, \dots, p$  e  $d_h < 0$  para  $s > p$ . Então existem números  $c_l$  pertencentes ao corpo  $K$  tais que

$$c_h^2 = d_h^{-1}, \quad c_s^2 = -d_s^{-1}, \quad c_{r+1} = \dots = c_n = 1, \quad \text{com } h = 1, \dots, p \text{ e } s = p + 1, \dots, r.$$

A matriz  $P = \text{diag}(c_1, \dots, c_n)$  é não singular e  $P^t D P$  é a matriz  $B$  procurada.

Para mostrarmos a unicidade de  $p$ , suponha que  $A$  é também congruente a  $C = \begin{pmatrix} I_q & 0 & 0 \\ 0 & -I_{r-q} & 0 \\ 0 & 0 & 0 \end{pmatrix}$ . Sendo  $C = Q^t D' Q$  tal que  $Q = \text{diag}(c'_1, \dots, c'_n)$  e  $D'$  é uma matriz diagonal hermitianamente congruente a  $A$ . Então a forma  $f = X^t A X$  é convertida pela substituição linear não singular:  $X = P Y$ ,  $X = Q Z$  em

$$y_1^2 + \dots + y_p^2 - y_{p+1}^2 - \dots - y_r^2 \quad \text{e} \quad (4.1)$$

$$z_1^2 + \dots + z_q^2 - z_{q+1}^2 - \dots - z_r^2. \quad (4.2)$$

Se  $p \neq q$ , assumimos sem perda de generalidade  $q < p$ . Expressando as novas variáveis em termos das antigas, temos  $Y = P^{-1} X$ ,  $Z = Q^{-1} X$ . Assim cada  $y_l$  e cada  $z_h$  pode ser visto como uma combinação linear única de  $x_1, \dots, x_n$ . As equações

$$z_h = 0, \quad y_l = 0 \quad \text{com } h = 1, \dots, q \text{ e } l = p + 1, \dots, n \quad (4.3)$$

podem ser consideradas equações lineares homogêneas em  $x_1, \dots, x_n$ .

Sendo  $q + n - p < n$ , essas equações homogêneas tem uma solução não trivial,

digamos

$$X_0 = \text{col}(x_1, \dots, x_n) \neq (0, \dots, 0). \quad (4.4)$$

Temos que  $f(X_0) = X_0^t A X_0$ , mas usando  $Y_0 = P^{-1} X_0$  este valor também pode ser calculado em (4.1), ou calculado em (4.2) usando  $Z_0 = Q^{-1} X_0$ . Por (4.3) e pelo valor calculado em cada caso temos  $f(X_0) \geq 0$  em (4.1), e  $f(X_0) \leq 0$  em (4.2), assim  $f(X_0) = 0$ . Mas pelo visto em (4.3),  $f(X_0) = y_1^2 + \dots + y_p^2 = 0$ , assim  $y_1 = \dots = y_p = 0$  e  $y_{p+1} = \dots = y_n = 0$ , então  $Y_0 = 0$ , ou seja,  $X_0 = P Y_0 = 0$ , o que contradiz (4.4). Portanto  $p = q$ , o que prova a unicidade e finaliza a demonstração. ■

O inteiro  $p$  do teorema acima é chamado *índice de simetria* de  $A$ .

**Corolário 4.19.** *Toda matriz simétrica  $A$  sobre  $K$  de posto  $r$  é congruente a matriz  $B = \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_{r-p} & 0 \\ 0 & 0 & 0 \end{pmatrix}$ . O inteiro  $p$  é unicamente determinado por  $A$ .*

**Corolário 4.20.** *Toda matriz hermitiana  $A$  sobre  $K(\sqrt{-1})$  de posto  $r$  é hermitianamente congruente a matriz  $B = \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_{r-p} & 0 \\ 0 & 0 & 0 \end{pmatrix}$ . O inteiro  $p$  é unicamente determinado por  $A$ .*

**Observação 4.21.** Uma matriz hermitiana  $A$ , sobre  $K, K(\sqrt{-1})$  ou  $H$ , de posto  $r$  e índice  $p$  é definida positiva se, e somente se,  $p = r = n$ , ou seja,  $A = \pm I$ .

**Exemplo 4.22.** Para ilustramos o Teorema 4.18, considere a matriz não nula

$$A = \begin{pmatrix} 0 & i + j + k & 2i \\ -i - j - k & 0 & 2 + j \\ -2i & 2 - j & 0 \end{pmatrix}.$$

Seguindo os passos da demonstração do Teorema 4.18, vamos mostrar inicialmente que  $A$  é hermitianamente congruente a uma matriz com um elemento da diagonal não-nulo. Consideremos o elemento  $a_{ts} = a_{12} = i + j + k$  para desenvolver nosso procedimento. Note que  $\text{Re}(a_{12}) = 0$ , então devemos aplicar o procedimento descrito

quando  $a_{ts}$  é um “imaginário puro”. Como o coeficiente de  $i$  é não-nulo em  $a_{12}$ , vamos escolher o termo  $i$ . Adicionamos a coluna 2 multiplicada à direita por  $i$  à coluna 1, respectivamente adicionamos a linha 2 multiplicada à esquerda por  $-i$  à linha 1.

Obtendo a matriz  $C = \begin{pmatrix} -2 & i+j+k & -k \\ -i-j-k & 0 & 2+j \\ k & 2-j & 0 \end{pmatrix}$ . Na seqüência vamos continuar a diagonalização da matriz  $D$ . Adicionamos a coluna 1 multiplicada à direita por  $-\frac{c_{12}}{c_{11}} = \frac{i+j+k}{2}$  à coluna 2, e adicionamos a linha 1 multiplicada à esquerda por  $-\frac{c_{12}}{c_{11}} = \frac{i+j+k}{2}$  à linha 2. Obtendo  $M = \begin{pmatrix} -2 & 0 & -k \\ 0 & \frac{3}{2} & \frac{3+j+i}{2} \\ k & \frac{3-j-i}{2} & 0 \end{pmatrix}$ .

Somando a coluna 1 multiplicada à direita por  $-\frac{m_{13}}{m_{11}} = -\frac{-k}{-2}$  à coluna 3, e somamos a linha 1 multiplicada à esquerda por  $-\frac{m_{13}}{m_{11}} = -\frac{-k}{-2}$  à linha 3 assim

temos  $N = \begin{pmatrix} -2 & 0 & 0 \\ 0 & \frac{3}{2} & \frac{3+j+i}{2} \\ 0 & \frac{3-j-i}{2} & \frac{1}{2} \end{pmatrix}$ . Para concluirmos a diagonalização somamos a

coluna 2 multiplicada à direita por  $-\frac{n_{23}}{n_{22}} = -\frac{\frac{3+j+i}{2}}{\frac{3}{2}}$  à coluna 3, e somamos a linha 2 multiplicada à esquerda por  $-\frac{n_{23}}{n_{22}} = -\frac{\frac{3+j+i}{2}}{\frac{3}{2}}$  à linha 3 e finalmente temos a matriz diagonal

$$D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 3/2 & 0 \\ 0 & 0 & -8/6 \end{pmatrix}.$$

Agora fazendo trocas convenientes de colunas seguidas pelas respectivas trocas de linhas, obtemos uma matriz  $S$  na qual o elemento positivo ocupa a primeira posição,

$$\text{ou seja, } S = \begin{pmatrix} 3/2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -8/6 \end{pmatrix}.$$

Como na demonstração do Teorema 4.18, consideremos a matriz  $P = \text{diag}(c_1, c_2, c_3)$  em que  $c_1^2 = \frac{1}{3/2}$ ,  $c_2^2 = -\frac{1}{-2}$  e  $c_3^2 = -\frac{1}{-8/6}$ . Assim

$$P^t D P = \begin{pmatrix} 3/2c_1^2 & 0 & 0 \\ 0 & -2c_2^2 & 0 \\ 0 & 0 & -8/6c_3^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = B.$$

Finalmente podemos concluir que a matriz  $A$  é congruente a matriz  $B = \begin{pmatrix} I_1 & 0 \\ 0 & -I_2 \end{pmatrix}$ .

### 4.3 A Involução Canônica em uma Álgebra de Grupos.

Sejam  $G$  um grupo finito,  $K$  um corpo e  $K[G]$  a álgebra de grupo conforme definida no Exemplo 3.3 do Capítulo 2. Nosso objetivo nesta seção é mostrar que a involução canônica sobre a álgebra de grupo  $K[G]$  é uma involução bem conhecida para o caso em que  $K$  é um corpo real fechado.

Recordemos que se a característica,  $\text{car}K$ , não divide a ordem do grupo, então  $K[G]$  é uma álgebra semisimples (ver Teorema de Maschke 2.23). Sempre que assumirmos  $K$  real fechado, teremos que  $\text{car}K = 0$  e portanto  $K[G]$  é semisimples.

Precisamos de um fato trivial sobre involuções sobre uma álgebra semisimples arbitrária  $A = A_1 \times \cdots \times A_m$ . Aplicando a involução  $\sigma : A \rightarrow A$  temos  $A = \sigma(A_1) \times \cdots \times \sigma(A_m)$ . Como a decomposição de  $A$  em produto de fatores simples é única (a menos de isomorfismo), temos que  $\sigma(A_i) = A_j$  para algum  $j$ . Se  $i \neq j$ , a restrição de  $\sigma$  a  $A_i$  não é interessante, pois a involução é determinada a menos de isomorfismo por  $A_i$ . De fato, como  $\sigma(A_i) = A_j$ , temos que  $A_i = \sigma(\sigma(A_i)) = \sigma(A_j)$ . Assim podemos considerar  $\bar{\sigma}$  a involução definida em  $A_i \times A_j$  por  $\bar{\sigma}(a_i, a_j) = (\sigma(a_j), \sigma(a_i))$ . Denotando por  $A_i^o$  o anel oposto de  $A_i$  e por  $\tau$  a involução definida em  $A_i \times A_i^o$  por  $\tau(x, y) = (y, x)$ , podemos definir  $\Psi : (A_i \times A_j, \bar{\sigma}) \rightarrow (A_i \times A_i^o, \tau)$  por  $\Psi(a_i, a_j) = (a_i, \sigma(a_j))$ . Logo  $\tau(\Psi(a_i, a_j)) = \Psi(\bar{\sigma}(a_i, a_j))$  e portanto  $\Psi$  é um isomorfismo de anéis com involução. Se  $i = j$ , temos que os fatores simples são invariantes por involução e podemos tentar determinar  $\sigma|_{A_i}$ . Por exemplo podemos tentar determinar quando  $\sigma|_{A_i}$  é ortogonal, simplética ou unitária.

A mais importante ferramenta usada no estudo da involução canônica sobre  $K[G]$  é a forma traço canônica, que iremos introduzir na observação abaixo.

**Observação 4.23.** Assim como no Capítulo 2 estaremos usando aqui a notação  $\text{tr}$  para traço de matriz ou traço de operador linear e  $\text{Tr}$  para o traço de um elemento. Recordemos que  $\text{Tr}(a) = \text{tr}(l_a)$  para  $a \in A$ .

(1) Seja  $G = \{e, g_2, \dots, g_n\}$  um grupo finito com  $n$  elementos e  $A = K[G]$ . Se  $e$  é o elemento neutro de  $G$ , então  $\text{Tr}(e) = n$  e  $\text{Tr}(g) = 0$  para todo  $g \neq e$ . De fato, seja  $\{e, g_2, \dots, g_n\}$  uma base de  $K[G]$ . Temos que a matriz de  $l_e$  é dada por

$$\begin{aligned} ee &= e = 1e + 0g_2 + \dots + 0g_n \\ eg_2 &= g_2 = 0e + 1g_2 + \dots + 0g_n \\ &\vdots \\ eg_n &= g_n = 0e + 0g_2 + \dots + 1g_n. \end{aligned}$$

Assim  $\text{Tr}(e) = \text{tr}(l_e) = n$ . Para  $e \neq g \in G$  temos que a matriz de  $l_g$  terá a diagonal principal toda nula, pois  $gg_i = g_j$  com  $i \neq j$ . Logo  $\text{Tr}(g) = \text{tr}(l_g) = 0$  para todo  $g \neq e$ .

(2) A forma bilinear simétrica  $t : K[G] \times K[G] \rightarrow K$  dada por  $t(x, y) = \text{Tr}(x\sigma(y))$  é chamada *forma traço canônica* em  $K[G]$ , onde  $\sigma$  é a involução canônica em  $K[G]$ . Calculando a matriz de  $t$  na base  $G = \{e, g_2, \dots, g_n\}$  de  $K[G]$  obtemos

$$\begin{pmatrix} n & 0 & \dots & 0 \\ 0 & n & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & n \end{pmatrix}_{n \times n},$$

pois para todo  $x \in G$ ,  $t(x, x) = \text{Tr}(e) = n$  e  $t(x, y) = \text{Tr}(xy^{-1}) = 0$  para todo  $x \neq y$ . Portanto  $t \cong n \cdot \langle 1, \dots, 1 \rangle_n$ .

(3) Substituindo a multiplicação à esquerda  $l_x$  pela multiplicação à direita  $r_x$  na definição de traço, em geral temos  $\text{tr}(l_x) \neq \text{tr}(r_x)$ . Entretanto para álgebras centrais simples  $\text{tr}(l_x) = \text{tr}(r_x)$  para todo  $x$ . Isto é claro para o caso de álgebras de matrizes, visto que  $\text{tr}(AB) = \text{tr}(BA)$ . O caso geral é reduzido a este último tensorizando com um corpo de decomposição.

(4) Seja  $A$  uma  $K$ -álgebra simples com centro  $L$  e com uma involução  $\sigma$   $K$ -linear. Então  $\text{Tr}(x) = \text{Tr}(\sigma(x))$  para todo  $x \in A$ .

Demonstração: Considere primeiro o caso  $K = L$  e  $A = M(r, K)$ . Neste caso  $A$



é central simples e pelo teorema de Classificação das Involuções 4.10, existe  $y \in A$  tal que  $\sigma(x) = yx^ty^{-1}$ . Pela Observação 3.18 temos  $\text{Tr}(\sigma(x)) = r\text{tr}(\sigma(x)) = r\text{tr}(yx^ty^{-1}) = r\text{tr}(y^{-1}yx^t) = r\text{tr}(x) = \text{Tr}(x)$ . O caso geral se reduz ao primeiro caso tensorizando com o fecho algébrico  $\bar{K}$  de  $K$ . Donde temos  $A_{\bar{K}} = M(r, \bar{K}) \times \cdots \times M(r, \bar{K}) = A_1 \times \cdots \times A_m$ . Se  $x$  está em algum fator simples invariante, então  $\text{Tr}(x) = \text{Tr}(\sigma(x))$  como no caso anterior. Se  $x \in A_i \neq \sigma(A_i)$ , como  $A_i$  é uma álgebra central simples temos que  $\text{tr}(r_x) = \text{tr}(l_x)$  por (3). Mais ainda, a multiplicação à esquerda por  $\sigma(x)$  em  $\sigma(A_i) = A_i^o$  corresponde à multiplicação à direita por  $x$  em  $A_i$ . Assim,  $\text{Tr}(\sigma(x)) = \text{tr}(l_{\sigma(x)}) = \text{tr}(r_x) = \text{tr}(l_x) = \text{Tr}(x)$ .

(5) Com as hipóteses de (4) podemos definir a forma traço canônica de  $(A, \sigma)$  por

$$t_A = t : A \times A \rightarrow K, \quad t(x, y) = \text{Tr}(x\sigma(y)).$$

Claramente  $t_A$  é bilinear. É simétrica, visto que,

$$t(x, y) = \text{Tr}(x\sigma(y)) = \text{Tr}(\sigma(x\sigma(y))) = \text{Tr}(y\sigma(x)) = t(y, x).$$

Dentro do contexto das observações acima temos o seguinte resultado.

**Proposição 4.24.** *Assuma que  $\langle 1, 1, \dots, 1 \rangle_n$  é anisotrópica sobre  $K$  e  $\text{car}K \neq 0$ . Então todos fatores simples da álgebra de grupo são invariantes pela involução canônica. Assuma que  $K$  é ordenado. Então a forma traço canônica de todo fator simples é definida positiva com respeito a ordem de  $K$ .*

**Demonstração:** Suponha que  $\sigma(A_i) \neq A_i$ , então para todo  $x, y \in A_i$  temos  $t(x, y) = \text{Tr}(x\sigma(y)) = \text{Tr}(0) = 0$ , pois  $A_iA_j = 0$  se  $i \neq j$ . Portanto  $A_i$  é totalmente isotrópico, contrariando o fato que  $t$  é anisotrópica.

Notemos que  $t : K[G] \times K[G] \rightarrow K$  é definida positiva, pois

$$x\sigma(x) = \sum_g a_g g \cdot \sum_h a_h h^{-1} = \sum_g a_g^2 g g^{-1} + \sum_{g \neq h} a_g a_h g h^{-1} = \sum_g a_g^2 + \sum_{g \neq h} a_g a_h g h^{-1},$$

para todo  $x = \sum_g a_g g \in K[G]$ . Assim para todo  $x \neq 0 \in K[G]$ , temos

$$t(x, x) = \text{Tr}(x\sigma(x)) = \text{Tr}\left(\sum_g a_g^2\right) + \text{Tr}\left(\sum_{g \neq h} a_g a_h g h^{-1}\right) = n \cdot \sum_g a_g^2 > 0,$$

já que  $n$  é a ordem de  $G$  e  $a_g \in K$  logo  $a_g^2 > 0$ , para todo  $g \in G$ . Como para todo fator simples  $B$  temos que  $t_B$  é um fator ortogonal de  $t$  devemos ter que  $t_B$  é definida positiva. ■

Seja  $K$  é um corpo real fechado. Considere a álgebra de grupo  $K[G]$ , pelo Teorema de Maschke 2.23,  $K[G]$  é semisimples. Pelo Teorema de Wedderburn 2.11, cada fator simples de  $K[G]$  é isomorfo a álgebra de matrizes  $M(n, D)$ , onde  $D$  é uma  $K$ -álgebra com divisão. Veremos, no teorema a seguir, que existem poucas possibilidades para as álgebras com divisão sobre um corpo real fechado. Mas antes veremos um lema que nos será útil, a sua demonstração é um tanto técnica, e será omitida.

**Lema 4.25.** *Sejam  $D$  uma álgebra com divisão sobre um corpo  $K$  com centro  $Z$ , e subcorpo maximal  $F$  de  $K$ . Então  $\dim_Z D$  é finita se, e somente se,  $\dim_Z F$  é finita. Nesse caso  $\dim_F D = \dim_Z F$  e  $\dim_Z D = (\dim_Z F)^2$ .*

**Demonstração:** [4], Teorema 6.6 pg 459. ■

Agora, podemos enunciar e demonstrar o Teorema de Frobenius. Este nos diz que há três possibilidades para álgebras com divisão sobre um corpo real fechado, que são as já bem conhecidas.

**Teorema 4.26. (Frobenius)** *Seja  $D$  uma álgebra com divisão de dimensão finita sobre um corpo real fechado  $K$ . Então  $D$  é isomorfo a  $K$  ou ao corpo  $K(\sqrt{-1})$  ou ainda a álgebra com divisão  $H$ , dos Hamiltonianos.*

**Demonstração:** Seja  $Z$  o centro de  $D$  e  $F$  um subcorpo maximal de  $K$ . Temos  $D \supset F \supset Z \supset K$ , com  $F$  uma extensão algébrica do corpo  $K$ . Conseqüentemente, sendo  $K$  real fechado, pelo Corolário 1.22,

$$\dim_Z(F) \leq \dim_K(F) \leq 2 \tag{4.5}$$

donde temos que a  $\dim_Z(F)$  é finita. Logo pelo lema anterior

$$\dim_F(D) = \dim_Z(F) \quad \text{e} \quad \dim_Z(D) = (\dim_Z(F))^2. \quad (4.6)$$

Analisando (4.5) e (4.6), as únicas possibilidades são  $\dim_Z(D) = 1$  ou  $\dim_Z(D) = 4$ . Se  $\dim_Z(D) = 1$ , por (4.6) temos que  $D = F$  e, pelo Corolário 1.22,  $D$  é isomorfo a  $K$  ou a  $K(\sqrt{-1})$ .

Se  $\dim_Z(D) = 4$ , por (4.6) temos  $\dim_Z(F) = 2 = \dim_F(D)$ . Conseqüentemente, como  $F$  é uma extensão algébrica de  $K$  e  $\dim_Z(F) = 2$ , por (1.1) devemos ter  $Z = K$ . Como  $K$  é real fechado, novamente pelo Corolário 1.22,  $F$  é isomorfo à  $K(\sqrt{-1})$ . Além disso,  $D$  não é comutativo, caso contrário  $D$  seria uma extensão algébrica própria de  $K(\sqrt{-1})$ , contrariando o fato de  $K(\sqrt{-1})$  ser algebricamente fechado. Como  $F$  é isomorfo a  $K(\sqrt{-1})$  podemos representar  $F = K(i)$  para algum  $i \in F$  tal que  $i^2 = -1$ . A aplicação  $\varphi : F \rightarrow F$  dada por  $\varphi(a + bi) = a - bi$ , que fixa os elementos de  $K$ , é um automorfismo diferente da identidade sobre  $F$ . Como  $D$  é uma álgebra central simples, pelo Teorema de Skolem-Noether,  $\varphi$  pode ser estendido para um automorfismo interno  $\beta$  de  $D$ , dado por  $\beta(x) = dx d^{-1}$  para  $d \neq 0$ ,  $d \in D$ . Como  $-i = \beta(i) = di d^{-1}$ , temos  $-id = di$ , e  $\beta(\beta(i))$  nos dá  $id^2 = d^2 i$ . Conseqüentemente  $d^2 \in D$  comuta com todo elemento de  $F = K(i)$ . Assim  $d^2 \in F$ , caso contrário  $d^2$  e  $F$  poderiam gerar um subcorpo de  $D$  contendo propriamente o subcorpo maximal  $F$ . Como os únicos elementos de  $F$  que são fixados por  $\beta$  são os elementos de  $K$  e  $\beta(d^2) = dd^2 d^{-1} = d^2$ , temos que  $d^2 \in K$ . Se  $d^2 > 0$ , então  $d \in K$ . O que é impossível pois se  $d \in K$  temos que  $\beta$  é a identidade. Então  $d^2 = -r^2$  para  $r \neq 0$ ,  $r \in K$ . Logo  $\left(\frac{d}{r}\right)^2 = -1$ . Seja  $j = \frac{d}{r}$  e  $k = ij$ . Não é difícil (apesar de trabalhoso) mostrar que  $\{1, i, j, k\}$  é uma base de  $D$  sobre  $K$  e que existe um isomorfismo de  $K$ -álgebras tal que  $D \simeq H$ . ■

Considere agora, a involução canônica sobre a álgebra de grupo  $K[G]$ , onde  $K$  é um corpo real fechado. O teorema a seguir identifica a involução canônica sobre um fator simples de  $K[G]$  com a involução conjugada transposta sobre a álgebra de

matrizes.

**Teorema 4.27.** *Seja  $K$  um corpo real fechado e  $G$  um grupo finito. Então todo fator simples  $B$  da álgebra de grupo  $K[G]$  é invariante pela involução canônica. Se  $\sigma$  é a involução canônica em  $K[G]$  temos que  $(B, \sigma) \simeq (M(r, D), t \circ -)$ , onde  $D = K, K(\sqrt{-1})$  ou  $H$  e  $-$  é a identidade em  $K$ , a conjugação complexa em  $K(\sqrt{-1})$  e a involução canônica em  $H$ .*

**Demonstração:** Como  $K$  é real fechado,  $-1$  não é uma soma de quadrados em  $K$ . Logo a forma  $\langle 1, 1, \dots, 1 \rangle$  é anisotrópica. Pela Proposição 4.24 todo fator simples  $B$  de  $K[G]$  é invariante por involução e  $t_B$ , a forma traço canônica restrita a  $B$ , é definida positiva. Pelo Teorema de Wedderburn 2.11 existe um isomorfismo  $i : B \rightarrow M(r, D)$ , onde  $D$  é uma álgebra com divisão sobre  $K$ . Pelo Teorema de Frobenius 4.26 devemos ter  $D = K, K(\sqrt{-1})$  ou  $H$ . A involução canônica  $\sigma|_B$  induz uma involução  $\tau$  em  $M(r, D)$  via o isomorfismo  $i$ , como segue:

$$\begin{array}{ccc} B & \xrightarrow{\sigma} & B \\ i \downarrow & & \downarrow i \\ M(r, D) & \xrightarrow{\tau} & M(r, D) \end{array} \quad \tau = i \circ \sigma \circ i^{-1}$$

O isomorfismo  $i$  é uma isometria entre  $t_B$  e  $b = t_{M(r, D)}$ . De fato, temos que mostrar que  $t_B(x, y) = b(i(x), i(y))$ , ou seja,  $t_B(x\sigma(y)) = t_{M(r, D)}(i(x)\tau(i(y)))$ . Mas  $\tau(i(y)) = i\sigma i^{-1}(i(y)) = i\sigma(y)$ , logo  $t_{M(r, D)}(i(x)\tau(i(y))) = t_{M(r, D)}(i(x)i\sigma(y)) = t_{M(r, D)}(i(x\sigma(y)))$ . Tomando uma base  $\{e_1, e_2, \dots, e_{r^2}\}$  para  $B$  e  $\{i(e_1), i(e_2), \dots, i(e_{r^2})\}$  para  $M(r, D)$  e calculando as matrizes de  $l_{x\sigma(y)} : B \rightarrow B$  e  $l_{i(x\sigma(y))} : M(r, D) \rightarrow M(r, D)$  nas respectivas bases, obtemos a mesma matriz. De fato, como  $i(x\sigma(y))i(e_j) = i(x\sigma(y)e_j)$ , se  $x\sigma(y)e_j = a_{1j}e_1 + \dots + a_{rj}e_r$  com  $a_{ij} \in K$ , temos  $i(x\sigma(y))i(e_j) = a_{1j}i(e_1) + \dots + a_{rj}i(e_r)$ . Logo  $t_B(x\sigma(y)) = t_{M(r, D)}(i(x)\tau(i(y)))$ . Agora, como  $t_B$  é definida positiva, temos que  $b$  é definida positiva. Vamos mostrar que  $b$  só pode ser positiva se  $(M(r, D), \tau) \simeq (M(r, D), t \circ -)$ . Pelo Teorema da Classificação de Involuções 4.10 existe uma matriz inversível  $U$  tal que  $\tau(\alpha_{ij}) = U(\overline{\alpha_{ij}})^t U^{-1}$ , onde

$\bar{\phantom{x}}$  é a involução em  $D$  e  $U = \pm \bar{U}^t$ . Podemos trocar  $U$  por qualquer matriz hermiticamente congruente a ela, com isso estaremos trocando o isomorfismo  $i$ . Mais especificamente, trocar  $U$  por uma matriz  $\bar{P}^t U P$  (com  $P$  inversível) significa trocar o isomorfismo  $i$  pelo isomorfismo  $j : B \rightarrow M(r, D)$  definido por  $j(b) = V i(b) V^{-1}$ , onde  $V = \bar{P}^t$ .

Vamos analisar cada uma das três possibilidades para  $D$  separadamente.

Se  $D = K$  então  $\bar{\phantom{x}}$  é a identidade e temos que  $U$  é simétrica e definida. Caso contrário a forma definida por  $U$  não seria definida, ou seja, existiria um vetor  $x \neq 0$  tal que  $x^t U x = 0$ . Considerando esse vetor como uma matriz coluna  $X \in M(r, D)$  teremos  $X^t U X = 0$ , logo  $b(X^t, X^t) = t_{M(r, D)}(X^t \tau(X^t)) = t_{M(r, D)}(X^t U X U^{-1}) = 0$ . Isto contradiz o fato de que  $b$  é definida positiva. Assim, sendo  $U$  definida, positiva ou negativa, pelo Corolário 4.19 temos que  $U$  é congruente a matriz  $\pm I$ . Dessa forma basta trocar  $U$  por  $I$  ou  $-I$  e obtemos  $\tau(\alpha_{ij}) = (\bar{\alpha}_{ij})^t$ .

Se  $D = K(\sqrt{-1})$ , a involução  $\bar{\phantom{x}}$  é a conjugação complexa, temos que  $t \circ \bar{\phantom{x}}$  é uma involução de segunda espécie. Pelo item (3) do Teorema 4.10, podemos encontrar  $U$  tal que  $U = \bar{U}^t$ . Usando o mesmo argumento do caso  $D = K$  mostramos que  $U$  é definida. Agora, pelo Corolário 4.20, temos que  $U$  é congruente a matriz  $\pm I$  donde segue o resultado.

Se  $D = H$ , temos que  $\bar{\phantom{x}}$  é a involução canônica. A matriz  $U$  não pode ser anti-hermitiana, pois assim  $b$  seria isotrópica. (Para  $B = H$  podemos mostrar que  $b \cong \langle 1, -1, -1, 1 \rangle$ . O caso geral pode ser reduzido a este, escrevendo  $U$  na forma diagonal e considerando o subespaço  $e_{11}H$  de  $M(r, H)$ .) Logo  $U$  é hermitiana. Para concluir que  $U$  é definida usamos novamente o argumento do caso  $D = K$ . Pelo Teorema 4.18  $U$  é congruente a matriz  $\pm I$ , o que finaliza a demonstração. ■

## Capítulo 5

# Álgebras Semisimples com uma Involução Positiva

Nosso objetivo agora é demonstrar um teorema de Boulagouaz, M., Oukhtite, L., [2] que estende o Teorema 4.27 para uma álgebra semisimples de dimensão finita com involução positiva. Neste capítulo  $K$  será sempre um corpo real fechado e  $A$  uma álgebra semisimples.

Como  $A$  é semisimples, pelo Teorema 2.20,  $A$  tem decomposição única em soma direta de componentes simples  $A_i$ , ou seja,  $A = \bigoplus_{i=1}^l A_i$ . Mais ainda, cada  $A_i$  é gerado por um único elemento  $e_i$  idempotente central primitivo, e  $1 = e_1 + \dots + e_l$ .

Lembremos que se  $\sigma$  é uma involução sobre  $A$ , então  $\sigma$  restrita a uma componente simples  $A_i$  não é necessariamente uma involução. Pela unicidade da decomposição de  $A$  temos que  $\sigma(A_i) = A_j$ . Portanto  $\sigma$  induz uma involução em  $A_i$  se, e somente, se  $\sigma(A_i) = A_i$ , que equivale a  $\sigma(e_i) = e_i$ . Consideremos agora o traço como definido anteriormente, onde para cada  $a \in A$ ,  $Tr(a) = tr(l_a)$ . A involução  $\sigma$  sobre  $A$  é dita *positiva* se esta é  $K$ -linear e  $Tr(\sigma(a)a) > 0$ , para todo  $a \neq 0$ ,  $a \in A$ .

A involução utilizada no Teorema 4.27 é uma involução positiva, como veremos no exemplo a seguir.

**Exemplo 5.1.** Considere  $G$  um grupo finito e seja  $\sigma$  a involução canônica da álgebra de grupos  $K[G]$ , definida por  $\sigma(\sum_g a_g g) = \sum_g a_g g^{-1}$ . Por definição,  $\sigma$  é uma in-

volução  $K$ -linear. Mais ainda, se  $x = \sum_g a_g g \in K[G]$ , vimos na demonstração da Proposição 4.24 (pg.65) que  $Tr(\sigma(x)x) = n \cdot \sum_g a_g^2$ , onde  $n$  é a ordem de  $G$ . Se  $x \neq 0$ , existe  $g_0 \in G$  tal que  $a_{g_0} \neq 0$ . Portanto  $Tr(\sigma(x)x) \geq n \cdot a_{g_0}^2 > 0$ . Donde segue que  $\sigma$  é uma involução positiva.

Observe que uma involução positiva deve deixar invariante cada componente simples  $A_i$  de  $A$ . De fato, suponha que  $\sigma(A_i) = A_j$  com  $i \neq j$ . De  $A_i A_j = 0$  para  $i \neq j$ , temos que  $\sigma(x)x = 0$  para todo  $x \in A_i$ , que contradiz o fato de que  $\sigma$  é positiva. Então  $\sigma(A_i) = A_i$  e assim a restrição de  $\sigma$  a  $A_i$  é claramente uma involução positiva.

A próxima proposição nos dá o comportamento dos ideais de  $A$  em relação a uma involução. Para sua demonstração necessitamos do seguinte lema.

**Lema 5.2.** *Seja  $(B, \sigma)$  uma álgebra central simples com involução. As seguintes afirmações são equivalentes.*

- (1) *Para todo  $x \in B$ , se  $\sigma(x)x = 0$ , então  $x = 0$ .*
- (2) *Todo ideal à direita de  $B$  é gerado por um elemento idempotente simétrico.*

**Demonstração:** [1], Corolário 1.8 pg 465. ■

**Proposição 5.3.** *Seja  $\sigma$  uma involução positiva sobre  $A$ . Então seguem as afirmações.*

- (1) *Todo ideal bilateral de  $A$  é invariante sob  $\sigma$ .*
- (2) *Todo ideal à direita  $I$  de  $A$  é gerado por um único idempotente simétrico.*

**Demonstração:** (1) Seja  $I$  um ideal bilateral de  $A$ . A semisimplicidade de  $A$  e o Corolário 2.22 asseguram a existência de um elemento  $e$  idempotente central em  $A$  tal que  $I = Ae$ . Para cada idempotente central primitivo  $e_i$ , temos que  $ee_i$  e  $(1-e)e_i$  são idempotentes centrais ortogonais. Claramente ambos são idempotentes centrais e, como  $(ee_i) \cdot ((1-e)e_i) = (ee_i) \cdot (e_i - ee_i) = ee_i - ee_i = 0$ , segue a ortogonalidade.

Note que  $e_i = ee_i + (1 - e)e_i$  e como  $e_i$  é primitivo, temos que  $ee_i = 0$  ou  $ee_i = e_i$ . O fato de que  $e = e1 = \sum_{i=1}^l ee_i$ , nos leva a concluir que  $e = \sum_{i \in S} e_i$ , tal que  $S$  é subconjunto de  $\{1, 2, \dots, l\}$ . Conseqüentemente,  $\sigma(e) = e$ , pois  $\sigma$  é positiva e  $\sigma(e_i) = e_i$ . Portanto  $\sigma(I) = A\sigma(e) = I$ .

(2) Seja  $I$  um ideal à direita de  $A = \bigoplus_{i=1}^l A_i$ , então  $I = eA = eA_1 + \dots + eA_l$ . Como  $e \in A$  temos que  $e = \beta_1 + \dots + \beta_l$ , com  $\beta_i \in A_i$ . Sabemos que  $e^2 = e$ , logo  $\beta_i^2 = \beta_i$ , para todo  $i = 1, \dots, l$ . Assim

$$eA_i = \beta_1 A_i + \dots + \beta_i A_i + \dots + \beta_l A_i = \beta_i A_i \text{ para todo } i = 1, \dots, l.$$

Dessa forma  $I = \beta_1 A_1 + \dots + \beta_l A_l$  com  $\beta_i$  idempotente em  $A_i$ . Podemos escrever  $I = I_1 + \dots + I_l$ , onde  $I_i$  é o ideal à direita de  $A_i$  gerado por  $\beta_i$ . Como  $\sigma$  é positiva, para todo  $x \in A_i$ , se  $\sigma(x)x = 0$ , então  $x = 0$ . De acordo com o Lema 5.2, cada ideal  $I_i$  é gerado por um  $\alpha_i \in A_i$ , tal que  $\alpha_i$  é idempotente simétrico, ou seja,  $I_i = \alpha_i A_i$  e  $\sigma(\alpha_i) = \alpha_i$ . Fixemos  $f = \alpha_1 + \dots + \alpha_l$ . Como  $\alpha_i, \alpha_j$  são idempotentes ortogonais para todo  $i \neq j$ ,  $f$  também é idempotente e  $\sigma(f) = f$ , portanto  $I = fA$ . Suponha agora que  $f$  e  $f'$  são idempotentes simétricos tais que  $I = fA = f'A$ . Tendo em vista que  $f \in f'A$  temos que  $f = f'x$ , com  $x \in A$ . Aplicando  $f'$  à igualdade anterior temos  $f'f = f'x$ , logo  $f = f'f$ . Analogamente  $f' = ff'$ . Como  $f'$  e  $f$  são invariantes sobre  $\sigma$ , segue que  $f' = \sigma(f') = \sigma(ff') = \sigma(f')\sigma(f) = f'f = f$ . ■

**Lema 5.4.** *A admite uma involução positiva se, e somente se, toda componente simples  $A_i$  de  $A$  admite uma involução positiva.*

**Demonstração:** Se  $A$  admite uma involução positiva  $\sigma$  temos que  $\sigma(A_i) = A_i$  e portanto  $\sigma|_{A_i}$  é uma involução que é claramente positiva em  $A_i$ . Reciprocamente seja  $\sigma_i$  uma involução positiva em  $A_i$ , e seja  $\sigma : A \rightarrow A$  definida por  $\sigma(x_1 + \dots + x_r) = \sigma_1 x_1 + \dots + \sigma_r x_r$ , com  $x_i \in A_i$ . Vamos mostrar que  $\sigma$  é uma involução. Sejam



$x_1 + \cdots + x_r, y_1 + \cdots + y_r \in A$  temos que

$$\begin{aligned} \sigma((x_1 + \cdots + x_r) + (y_1 + \cdots + y_r)) &= \sigma((x_1 + y_1) + \cdots + (x_r + y_r)) = \\ \sigma_1(x_1 + y_1) + \cdots + \sigma_r(x_r + y_r) &= \sigma_1(x_1) + \sigma_1(y_1) + \cdots + \sigma_r(x_r) + \sigma_r(y_r) = \\ \sigma_1(x_1) + \cdots + \sigma_r(x_r) + \sigma_1(y_1) + \cdots + \sigma_r(y_r) &= \sigma(x_1 + \cdots + x_r) + \sigma(y_1 + \cdots + y_r). \end{aligned}$$

Como  $A_i A_j = 0$  para  $i \neq j$  segue que  $((x_1 + \cdots + x_r).(y_1 + \cdots + y_r)) = ((x_1.y_1) + \cdots + (x_r.y_r))$ . Assim

$$\begin{aligned} \sigma((x_1 + \cdots + x_r).(y_1 + \cdots + y_r)) &= \sigma((x_1.y_1) + \cdots + (x_r.y_r)) = \\ \sigma_1(x_1.y_1) + \cdots + \sigma_r(x_r.y_r) &= \sigma_1(y_1).\sigma_1(x_1) + \cdots + \sigma_r(y_r).\sigma_r(x_r) = \\ (\sigma_1(y_1) + \cdots + \sigma_r(y_r)).(\sigma_1(x_1) + \cdots + \sigma_r(x_r)) &= \sigma(y_1 + \cdots + y_r).\sigma(x_1 + \cdots + x_r). \end{aligned}$$

Para finalizar,  $\sigma(\sigma(x_1 + \cdots + x_r)) = \sigma(\sigma_1(x_1) + \cdots + \sigma_r(x_r)) = \sigma_1\sigma_1(x_1) + \cdots + \sigma_r\sigma_r(x_r) = x_1 + \cdots + x_r$ .

Agora mostraremos que  $\sigma$  é positiva. Como  $A_i A_j = 0$  para  $i \neq j$ , segue também que  $Tr(\sigma(x)x) = Tr(\sum_i (\sigma_i(x_i)x_i) \cdot \sum_i x_i) = \sum_i Tr(\sigma_i(x_i)x_i)$ . Como  $x \neq 0$  existe algum  $1 \leq j \leq r$  tal que  $x_j \neq 0$ . Como  $\sigma_j$  é positiva, temos  $Tr(\sigma_j(x_j)x_j) > 0$  e portanto  $Tr(\sigma(x)x) = \sum_i Tr(\sigma_i(x_i)x_i) \geq Tr(\sigma_j(x_j)x_j) > 0$ . ■

Pelo Teorema de Wedderburn cada  $A_i$  é isomorfo a  $M(n_i, D_i)$ , onde  $D_i$  é um anel com divisão sobre  $K$ . Sendo  $K$  real fechado, pelo Teorema de Frobenius 4.26,  $D_i = K$  ou  $D_i = K(\sqrt{-1})$  ou  $D_i = H$ . Denotemos por  $\sigma$  o endomorfismo de  $A$  definido em cada componente simples  $M(n, D)$  por  $\sigma(x_{ij}) = (\overline{x_{ji}})$ , onde  $\overline{x} = x$  se  $D = K$ , se  $D = K(\sqrt{-1})$  temos que  $\overline{x}$  é a conjugação complexa e se  $D = H$  teremos que  $\overline{x}$  é a involução canônica. Então  $\sigma$  é uma involução positiva bem definida. De fato, como vimos no exemplo 4.6 do Capítulo 4, nos três casos  $\sigma$  é uma involução. Mais ainda, para todo  $x \in D$ ,  $\sigma(x)x = \overline{xx} = \mu \in K$ , e  $\mu$  é uma soma de quadrados. Portanto  $Tr(\sigma(x)x) = \mu.n > 0$ .

**Proposição 5.5.** *Toda involução positiva  $\tau$  sobre uma componente simples  $A_i$  de  $A$  pode ser estendida a uma involução positiva sobre  $A$ .*

**Demonstração:** Pelo visto acima,  $A$  possui uma involução positiva  $\sigma$ . Além disso, a restrição de  $\sigma$  a  $A_i$  é uma involução. Consideremos a aplicação  $\theta : A \rightarrow A$  definida por  $\theta(x) = \tau(x_i) + \sum_{i \neq j} \sigma(x_j)$ , para todo  $x = x_i + \sum_{i \neq j} x_j$ , com  $x_i \in A_i$ ,  $x_j \in A_j$  para  $i \neq j$ . É fácil ver que  $\theta$  é uma involução sobre  $A$  estendendo  $\tau$ . Afirmamos que  $\theta$  é uma involução positiva sobre  $A$ . De fato, seja  $x = x_i + \sum_{i \neq j} x_j$  um elemento não nulo de  $A$ , logo  $\theta(x)x = \tau(x_i)x_i + \sum_{i \neq j} \sigma(x_j)x_j$ . Sendo  $x \neq 0$  deve existir algum  $1 \leq l \leq r$  tal que  $x_l \neq 0$ . Se  $l = i$ , como  $Tr(\sigma(x_j)x_j) \geq 0$  para todo  $i \neq j$ , então

$$Tr(\theta(x)x) = Tr(\tau(x_i)x_i) + \sum_{i \neq j} Tr(\sigma(x_j)x_j) \geq Tr(\tau(x_i)x_i) > 0.$$

Se  $l \neq i$  então

$$Tr(\theta(x)x) = Tr(\sigma(x_l)x_l) + Tr(\tau(x_i)x_i) + \sum_{j \neq i, l} Tr(\sigma(x_j)x_j) \geq Tr(\sigma(x_l)x_l) > 0.$$

■

**Observação 5.6.** Seja  $M(n, D)$  uma componente de  $A$  e seja  $\sigma$  uma involução positiva sobre  $A$ . Se  $D = K$  ou  $H$ , então  $C(D) = K$ , como  $\sigma$  é  $K$ -linear, concluímos nesse caso que  $\sigma$  é a identidade em  $C(D)$ . Se  $D = K(\sqrt{-1})$  temos que  $C(D) = D$ , então  $\sigma(\sqrt{-1}) = \pm\sqrt{-1}$ , mas pela positividade de  $\sigma$  segue que  $\sigma(\sqrt{-1}) = -\sqrt{-1}$ . Dessa forma  $\sigma(x) = \bar{x}$  para todo  $x \in C(D)$ .

Logo involuções positivas sobre  $A$  induzem a mesma restrição sobre o centro de cada componente simples  $A_i$  de  $A$ , ou seja, essa restrição só depende da positividade e não da ação da involução.

**Lema 5.7.** Para  $a, b \in A$ , as seguintes condições são equivalentes.

- (1)  $h(x, y) = Tr(a\sigma(x)by)$  é uma forma bilinear simétrica não-degenerada.
- (2)  $a$  e  $b$  são inversíveis e  $\sigma(b) = \lambda b$ ,  $\sigma(a) = \lambda^{-1}a$ , onde  $\lambda \in C(A)$  e  $\sigma(\lambda)\lambda = 1$ .

**Demonstração:** Assumiremos (1) e vamos mostrar a validade de (2). Primeiramente afirmamos que  $a$  é inversível. Caso contrário,  $a$  seria um divisor de zero, ou seja, existe  $c \in A$  tal que  $ac = 0$ . Como  $\sigma$  é sobrejetora existiria  $z \in A$  tal que

$\sigma(z) = c$  e assim  $h(z, y) = 0$  para todo  $y$ . Isto contradiz o fato de que  $h$  é não-degenerada. Analogamente prova-se que  $b$  é inversível. Pela simetria da aplicação  $Tr$  obtemos  $h(x, y) = Tr(a(\sigma(x)by)) = Tr((\sigma(x)by)a)$  e como  $\sigma$  é  $K$ -linear segue que  $h(y, x) = Tr(a\sigma(y)bx) = Tr(\sigma(a\sigma(y)bx)) = Tr(\sigma(x)\sigma(b)y\sigma(a))$ . Pela simetria de  $h$  temos  $Tr(\sigma(x)bya) = Tr(\sigma(x)\sigma(b)y\sigma(a))$ , para todo  $x, y \in A$ . Como  $h$  é não-degenerada  $bya = \sigma(b)y\sigma(a)$ , para todo  $y \in A$ . Fazendo  $y = 1$  temos  $b^{-1}\sigma(b) = a\sigma(a^{-1})$ . Assim  $b^{-1}\sigma(b)y = yb^{-1}\sigma(b)$ , para todo  $y \in A$ . Logo existe  $\lambda \in C(A)$  tal que  $b^{-1}\sigma(b) = \lambda$ , dessa forma temos que  $\sigma(b) = \lambda b$  e  $a = \lambda\sigma(a)$ . Como  $b$  é inversível temos  $1 = \sigma(1) = \sigma(bb^{-1}) = \sigma(b^{-1})\sigma(b)$ , agora note que  $\sigma(\lambda) = \sigma(b^{-1})b$  e  $\sigma(b) = b\lambda$ , pois  $\lambda \in C(A)$ . Assim fazendo as devidas substituições concluímos que  $\lambda$  é inversível e  $\sigma(\lambda)\lambda = 1$ .

Agora assumindo (2) provaremos (1). Pela  $K$ -linearidade de  $\sigma$  e a simetria da forma traço, segue que

$$\begin{aligned} h(x, y) &= Tr(a\sigma(x)by) = Tr(\sigma(a\sigma(x)by)) = Tr(\sigma(y)\sigma(b)x\sigma(a)) = \\ &= Tr(\sigma(y)\lambda bx\lambda^{-1}a) = Tr(\sigma(y)bx\lambda a) = Tr(a\sigma(y)bx) = h(y, x). \end{aligned}$$

Logo  $h$  é simétrica. Seja  $x \in A$  tal que  $h(x, y) = 0$ , para todo  $y \in A$ . Então  $Tr(a\sigma(x)by) = 0 = t(a\sigma(x)b, y)$ , para todo  $y \in A$ . Como  $t$  é não-degenerada obtemos que  $a\sigma(x)b = 0$ . Como  $a$  e  $b$  são inversíveis teremos  $\sigma(x) = 0$ , logo  $x = 0$ , pois  $\sigma$  é injetora. Portanto  $h$  é não-degenerada. ■

O teorema a seguir estende o Teorema 4.27 para uma álgebra semisimples de dimensão finita com uma involução positiva.

**Teorema 5.8.** *Sejam  $A$  uma álgebra semisimples de dimensão finita sobre  $K$  e  $\sigma$  uma involução positiva sobre  $A$ . Para cada componente simples  $B$  de  $A$*

- (1)  $(B, \sigma) \simeq (M(n, K), t)$  e  $\sigma$  é ortogonal ou
- (2)  $(B, \sigma) \simeq (M(n, H), t \circ^-)$  e  $\sigma$  é simplética ou
- (3)  $(B, \sigma) \simeq (M(n, K(\sqrt{-1})), t \circ^-)$  e  $\sigma$  é do segundo tipo.

**Demonstração:** Seja  $B$  uma  $K$ -álgebra simples de dimensão finita, pelo Teorema de Wedderburn existe uma álgebra com divisão  $D$  sobre  $K$  tal que  $B \simeq M(n, D)$ . Seja  $\Phi : B \rightarrow M(n, D)$  um isomorfismo. Então  $\Phi$  induz uma involução  $\gamma_\Phi$  sobre  $M(n, D)$  definida por  $\gamma_\Phi = \Phi \circ \sigma \circ \Phi^{-1}$ . Como  $\gamma_\Phi \circ \Phi = \Phi \circ \sigma$  temos que  $\Phi : (B, \sigma) \rightarrow (M(n, D), \gamma_\Phi)$  é um isomorfismo de álgebras com involução. A involução  $\gamma_\Phi$  é positiva. De fato, se  $Y \in M(n, D)$  tal que  $Y \neq 0$ , então existe um elemento  $0 \neq b \in B$  tal que  $Y = \Phi(b)$ . Assim

$$\text{Tr}(\gamma_\Phi(Y)Y) = \text{Tr}(\Phi\sigma\Phi^{-1}(\Phi(b))\Phi(b)) = \text{Tr}(\Phi\sigma(b)\Phi(b)) = \text{Tr}(\Phi(\sigma(b)b)) = \text{Tr}(\sigma(b)b) > 0,$$

sendo que a última igualdade segue da Observação 3.19. Sabemos que as involuções positivas  $\gamma_\Phi$  e  $t \circ \bar{\phantom{x}}$  da  $K$ -álgebra simples  $M(n, D)$  induzem a mesma restrição sobre o centro  $C(D)$  de  $D$ , ou seja, ambas possuem o mesmo corpo fixo. Assim pelo Teorema da Classificação das Involuções 4.10, existe  $U \in GL(n, D)$  satisfazendo  $U = \pm \bar{U}^t$ , tal que  $\gamma_\Phi(X) = U\bar{X}^tU^{-1}$  para todo  $X \in M(n, D)$ . Como  $\gamma_\Phi$  é positiva, então  $\text{Tr}(U\bar{X}^tU^{-1}X) > 0$  para todo  $X \in M(n, D)$  tal que  $X \neq 0$ . Portanto  $U = \bar{U}^t$ . Agora, usando o Lema 5.7, concluímos que  $h(X, Y) = \text{Tr}(U\bar{X}^tU^{-1}Y)$  é uma forma bilinear simétrica não-degenerada sobre a álgebra simples  $M(n, D)$ . Como  $h$  é definida positiva, temos que  $U$  é definida positiva. Pelo Exercício 17 da seção 9.3 de [3], existe algum elemento  $V \in GL(n, D)$  satisfazendo  $\bar{V}^t = V$  tal que  $V^2 = U$ . Então a aplicação  $\psi : B \rightarrow M(n, D)$  definida por  $\psi(b) = V^{-1}\Phi(b)V$ , é um isomorfismo de  $K$ -álgebras. Além disso,  $\psi$  induz uma involução  $\gamma_\psi$  sobre  $M(n, D)$  definida por  $\gamma_\psi = \psi \circ \sigma \circ \psi^{-1}$ . Para finalizarmos a demonstração, é suficiente mostrarmos que  $\gamma_\psi = t \circ \bar{\phantom{x}}$ . Seja  $X \in M(n, D)$ , usando que  $\psi^{-1}(X) = \Phi^{-1}(VXV^{-1})$ , obtemos

$$\begin{aligned} \gamma_\psi(X) &= \psi \circ \sigma \circ \psi^{-1}(X) = \psi(\sigma(\Phi^{-1}(VXV^{-1}))) = \psi(\Phi^{-1}\gamma_\Phi(VXV^{-1})) = \\ &= \psi(\Phi^{-1}(U\bar{VXV^{-1}}^tU^{-1})) = V^{-1}\Phi(\Phi^{-1}(U\bar{VXV^{-1}}^tU^{-1}))V = V^{-1}(U\bar{VXV^{-1}}^tU^{-1})V. \end{aligned}$$

Como  $V^2 = U$  e  $\bar{V}^t = V$  concluímos que  $\gamma_\psi(X) = \bar{X}^t$ , para todo  $X \in M(n, D)$ . Conseqüentemente  $(B, \sigma) \xrightarrow{\psi} (M(n, D), t \circ \bar{\phantom{x}})$  é um isomorfismo de álgebras com involução. ■

Sejam  $\sigma$  e  $\tau$  duas involuções da primeira espécie sobre uma álgebra central simples (sobre um corpo de característica diferente de dois) e  $\text{int}(u)$  o automorfismo interno da conjugação por  $u$ . Sabemos que  $\sigma$  e  $\tau$  tem o mesmo tipo se, e somente se,  $\tau = \text{int}(u) \circ \sigma$  sendo que  $u$  é um elemento inversível tal que  $\sigma(u) = u$ . Analogamente  $\sigma$  e  $\tau$  tem tipos diferentes se, e somente se,  $\sigma(u) = -u$ . Se  $\sigma$  e  $\tau$  são da segunda espécie e possuem o mesmo corpo fixo, então podemos escolher  $\tau = \text{int}(u) \circ \sigma$ , onde  $\sigma(u) = u$ . Deste comentário junto com o Teorema 5.8 temos o seguinte corolário.

**Corolário 5.9.** *Seja  $\sigma$  uma involução positiva sobre  $A$ . Se  $\tau$  é uma outra involução positiva sobre  $A$ , então  $\tau = \text{int}(u) \circ \sigma$  para algum elemento inversível  $u \in A$  satisfazendo  $\sigma(u) = u$ .*

A recíproca do corolário acima não é verdadeira. Vejamos um contra-exemplo. Seja  $K$  um corpo real fechado e seja  $D_3$  o grupo diedral de ordem 6. Considere a álgebra de grupos  $A = K[D_3]$ , com a involução canônica positiva  $\sigma$  definida por  $\sigma(\sum_g a_g g) = \sum_g a_g g^{-1}$ . Como  $D_3 = \{1, \alpha, r, r^{-1}, \alpha r, \alpha r^{-1}\}$ , onde  $\alpha^2 = 1$ ,  $r^3 = 1$  e  $\alpha r \alpha = r^{-1}$ , então  $\alpha$  é inversível e  $\sigma(\alpha) = \alpha$ . Conseqüentemente,  $\tau = \text{int}(u) \circ \sigma$  é uma involução sobre  $A$ . Fixando  $x = r - r^{-1}$ , temos  $\tau(x)x = -2 + r + r^{-1}$ . Como  $\text{Tr}(r + r^{-1}) = 0$ , pois  $r + r^{-1} \in G$ , segue que  $\text{Tr}(\tau(x)x) = -12 < 0$ . O que prova que  $\tau$  não é uma involução positiva sobre  $A$ .

Para finalizarmos este trabalho, seja  $\sigma$  uma involução positiva sobre  $A$  definida sobre cada componente simples  $M(n, D)$ , como acima, por  $\sigma((x_{ij})) = (\overline{x_{ij}})^t$ . Seja  $U(A)$  o conjunto dos elementos inversíveis de  $A$ . Fixando

$$\mathcal{C}(\sigma) = \{a \in U(A); \text{ existe } b \in A \text{ com } \sigma(b) = b \text{ e } b^2 = a\}.$$

**Teorema 5.10.** *As involuções positivas de  $A$  são  $\{\text{int}(u) \circ \sigma, u \in \mathcal{C}(\sigma)\}$ .*

**Demonstração:** Como  $\sigma$  é positiva, claramente  $\text{int}(u) \circ \sigma$  é uma involução positiva. Reciprocamente, seja  $\tau$  uma involução positiva sobre  $A$ . Pelo Corolário 5.9, existe um elemento inversível  $u \in A$  tal que  $\sigma(u) = u$  e  $\tau = \text{int}(u) \circ \sigma$ . Como  $\text{Tr}(u^{-1} \sigma(x) u y)$

é uma forma bilinear simétrica não-degenerada definida positiva, pelo Exercício 17 da seção 9.3 de [3], existe um elemento  $v \in A$  tal que  $\sigma(v) = v$  e  $v^2 = \lambda u$ , onde  $\lambda$  é um elemento do centro de  $A$ . Tomando  $u' = \lambda u$ , é fácil mostrar que  $\tau = \text{int}(u') \circ \sigma$ , com  $\sigma(u') = u'$  e  $u' = v^2$ . Portanto  $u' \in \mathcal{C}(\sigma)$ , e obtemos o desejado. ■

# Bibliografia

- [1] BAYER-FLUCKIGER,E.;SHAPIRO,D. B. e TIGNOL,J.-P., *Hyperbolic Involutions*, Math. Z. **214**, n°3, 461-476, (1993).
- [2] OUKHTITE, L. e BOULAGOUAZ, M., *Semisimples algebra with a positive involution*, Algebras Groups and Geometries **22**, n°2, 233-240, (2005).
- [3] HOFFMAN,K. e KUNZE,R., *Álgebra Linear*, 2ªedição, Livros Técnicos e Científicos Editora, Rio de Janeiro, 1979.
- [4] HUNGERFORD, T.W., *Algebra*, Springer-Verlag, New York, 1974.
- [5] LAM, T.Y., *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics **67**, American Mathematical Society, Providence, 2004.
- [6] LANG, SERGE, *Algebra*, 3ªed., Addison-Wesley Publishing Company Inc., Reading, 1995.
- [7] LEWIS, D., *Involutions and anti-automorphisms of algebras*, Bull. London Math. Soc. **38**, n°4, 529-545, (2006).
- [8] PERLIS, SAM, *Theory of Matrices*, Dover, New York, 1952.
- [9] PRESTEL, A., *Lectures on Formally Real Fields*, Monografias de Matemática, IMPA, Rio de Janeiro, 1975.
- [10] SCHARLAU, W., *Quadratic and Hermitian Forms*, Springer-Verlag, Berlin-Heidekberg, 1985.