Universidade Estadual de Maringá

Programa de Pós-Graduação em Matemática

Centro de Ciências Exatas

(Mestrado)

INVOLUÇÕES SOBRE ÁLGEBRAS DE GRUPO SEMISIMPLES

Robson Willians Vinciguerra

Orientadora: Rosali Brusamarello

Maringá - Pr

2009

"...É muito melhor arriscar coisas grandiosas,
alcançar triunfo e glória, mesmo expondo-se à derrota,
do que formar fila com os pobres de espírito,
que não gozam muito e nem sofrem muito,
porque vivem na penumbra cinzenta,
que não conhece nem vitória nem derrota..."
(Theodore Roosevelt)

Dedico este trabalho a Deus.

Á toda minha família.

Á minha namorada.

Agradecimentos

Agradeço à Deus que sempre esteve ao meu lado, atendendo minhas orações e me dando força para superar todos os obstáculos que encontrei.

À minha família, pelo apoio, incentivo e por me acolher nas horas mais difíceis.

À minha namorada, por ter sido companheira em todos os momentos e ter respeitado todas minhas decisões.

À prof[a]. Rosali Brusamarelo, pela dedicação, compreensão, incentivo e principalmente pelos valiosos ensinamentos durante a minha orientação.

Aos professores da banca: Francisco Cesar Polcino Milies e Irene Naomi Nakaoka, por terem lido o meu trabalho e pelas preciosas correções e sugestões.

Aos professores do DMA-UEM que contribuíram com a minha formação.

Aos meus colegas, pela amizade sincera e pelo companheirismo durante o curso.

À Lucia, por sua eficiência, paciência e amizade.

À Silvana, pela gentileza em preparar nossos cafezinhos.

Finalmente, à CAPES pelo apoio financeiro.

Resumo

Neste trabalho apresentamos condições necessárias e suficientes para que a involução canônica de uma álgebra de grupo semisimples $K[G]$ induza, em cada uma de suas componentes simples, uma involução de primeira espécie. Quando tal propriedade ocorre e K for um corpo real fechado teremos uma versão melhorada para o Teorema 13.3 de Scharlau [12].

Palavras Chaves: involuções sobre álgebras, anéis semisimples, álgebras de grupo, involuções de primeira espécie.

Abstract

In this work we present necessary and sufficient conditions for which the canonical involution of the group algebra $K[G]$ induces an involution of the first kind on each simple component of $K[G]$. If the conditions are satisfied and K is a real closed field, then we give an improved version of Theorem 13.3 of Scharlau [12].

Keywords: involutions of algebras, semisimple ring, group algebras, involution of the first kind.

Sumário

Introdução

Uma involução sobre um anel é um anti-automorfismo de ordem dois. A conjugação nos números complexos e a transposição de matrizes são dois exemplos elementares, e bem conhecidos, de involuções.

A teoria de álgebras com involução surgiu, por volta de 1930, quando Albert [1] tentava resolver um problema de geometria algébrica, o qual envolvia a determinação de uma álgebra de multiplicação de uma matriz de Riemann. Na tentativa de resolver o citado problema, Albert precisou desenvolver a teoria de álgebras centrais simples com involução, que teve como base a teoria de álgebras simples iniciada alguns anos antes por Brauer, Noether e também por Albert e Hasse. Ressaltamos que, apesar da motivação geométrica, o trabalho de Albert foi puramente algébrico.

Neste trabalho estudaremos involuções definidas sobre uma álgebra semisimples de dimensão finita. Uma álgebra semisimples A pode ser representada de modo único como soma direta de anéis simples, ou seja, $A = \bigoplus_{i=1}^{l} A_i$, onde cada A_i é um anel simples. Dada uma involução σ sobre A, temos que $A = \sigma(A) = \bigoplus_{i=1}^{l} \sigma(A_i)$. Pela unicidade da decomposição, temos que $\sigma(A_i) = A_j$, para algum j. Um dos objetivos deste trabalho é determinar condições necessárias e suficientes para que $\sigma(A_i) = A_i$, para todo $1 \leq i \leq l$, ou seja, a restrição de σ a cada componente simples A_i é uma involução sobre A_i.

Para o caso em que a álgebra de grupo $K[G]$ é semisimples, faremos um estudo da involução canônica $g \mapsto g^{-1}$. Neste caso iremos determinar ainda condições para

que a involução canônica restrita às componentes simples seja uma involução de primeira espécie.

Dividimos este trabalho em 4 capítulos, sendo que os capítulos 1, 2 e 3 contém essencialmente os pré-requisitos necessários para o desenvolvimento dessa dissertação e no Capítulo 4 realizaremos a maior parte do que foi descrito no parágrafo acima.

Iniciamos o Capítulo 1 fazendo um estudo dos corpos reais fechados, pois as álgebras de grupo sobre esses corpos serão objeto de estudo no Capítulo 4. Ainda, nesse capítulo, estudaremos, de forma detalhada, a teoria de anéis simples e semisimples já que na maior parte desse trabalho as involuções que utilizaremos estão definidas sobre tais anéis.

Já no Capítulo 2, descreveremos cada elemento de uma família de idempotentes primitivos centrais de $K[G]$ utilizando os caracteres de G, quando K for algebricamente fechado. Para isso, faremos nesse capítulo uma breve introdução de conceitos e resultados da teoria de representações de grupos.

No Capítulo 3, definiremos álgebras centrais simples e obteremos alguns resultados envolvendo essas álgebras. Dentre eles, o Teorema de Skolem-Noether 3.9, que diz que todo automorfismo sobre álgebras centrais simples é um automorfismo interno. Também, nesse capítulo, daremos o conceito de involuções, bem como algumas de suas propriedades. Finalizaremos o terceiro capítulo estabelecendo condições necessárias e suficientes para que qualquer involução sobre álgebras semisimples de dimensão finita seja invariante em cada uma de suas componente simples.

Por fim, no capítulo 4, mostraremos algumas condições necessárias e suficientes para que a involução canônica de $K[G]$ induza em cada uma de suas componentes simples uma involução de primeira espécie. Este resultado funciona como uma ferramenta importante para caracterizarmos as componentes simples de $K[G]$, quando K for real fechado. Veremos que estas condições são dadas em termos dos caracteres de G sobre K e das classes de conjugação de G. Em particular, mostraremos que

a involução canônica de $K[G]$ restrita à cada componente simples é uma involução de primeira espécie sempre que G for um (c)-grupo e, por isso, finalizaremos esse trabalho dedicando a última seção desse capítulo para o estudo dessa classe especial de grupos.

Capítulo 1

Preliminares

Iniciaremos este capítulo com a noção de corpos formalmente reais e ordenados e, com base nesse estudo, definiremos corpos reais fechados e mostraremos o Teorema Fundamental da Álgebra, o qual caracteriza os corpos reais fechados. Tal teorema será importante para a demonstração do Teorema de Frobenius no Capítulo 4. Introduziremos ainda a teoria de módulos e anéis semisimples visando mostrar o Teorema de Wedderburn-Artin, que nos dá uma decomposição para um anel semisimples como soma direta de anéis de matrizes. Na seqüência, veremos o Teorema de Maschke, o qual estabelece condições para que um anel de grupo seja semisimples. Encerraremos este capítulo determinando uma base para o centro do anel de grupo $K[G]$ sobre K.

1.1 Corpos Formalmente Reais e Ordenados

Começamos definindo corpos formalmente reais, em seguida, definiremos ordem e corpos ordenados. Veremos mais adiante que 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 uma soma de quadrados em K. Caso contrário, dizemos que K é *não real*.

Outra caracterização para corpos formalmente reais é a seguinte:

Proposição 1.2. *As seguintes condições são equivalentes:*

(1) *K é formalmente real.*

(2) *Para qualquer $n \in \mathbb{N}$ a equação $x_1^2 + \ldots + x_n^2 = 0$ admite somente a solução trivial em K.*

Demonstração: Suponhamos que $(a_1, \ldots, a_n) \neq 0$ seja solução para $x_1^2 + \ldots + x_n^2 = 0$ em K, logo $a_1^2 + \ldots + a_i^2 + \ldots + a_n^2 = 0$, onde $a_i \neq 0$ para algum $1 \leq i \leq n$. Como $a_i \in K$ temos

$$a_1^2(a_i^{-1})^2 + \ldots + a_i^2(a_i^{-1})^2 + \ldots + a_n^2(a_i^{-1})^2 = 0.$$

Disso segue que $(a_1 a_i^{-1})^2 + \ldots + (a_{i-1}a_i^{-1})^2 + (a_{i+1}a_i^{-1})^2 + \ldots + (a_n a_i^{-1})^2 = -1$, contradizendo o fato que K é formalmente real. Reciprocamente, assumimos que $-1 = a_1^2 + \ldots + a_k^2$, então $0 = 1 + (-1) = 1^2 + a_1^2 + \ldots + a_k^2$, logo $(1, a_1, \ldots, a_k)$ é uma solução não trivial para $x_1^2 + \ldots + x_k^2 = 0$, contradizendo (2). ■

Observação 1.3. Se K é formalmente real, então a característica de K deve ser 0. De fato, suponhamos que $char(K) \neq 0$, assim devemos ter $char(K) = p$, sendo p primo. Isso implica que $\underbrace{1 + \ldots + 1}_{p \text{ vezes}} = 0$ e, conseqüentemente, $\underbrace{1^2 + \ldots + 1^2}_{p-1 \text{ vezes}} = -1$, contradizendo o fato que K é formalmente real. Portanto, $char(K) = 0$.

Dado um corpo K, denotamos $Q(K)$ o conjunto de todos elementos de K que podem ser expresso como uma soma de quadrados em K. Também, escrevemos $Q(K)^*$ para $Q(K) \setminus \{0\}$.

Proposição 1.4. *Seja K um corpo, então*

(1) *$Q(K)^*$ é um subgrupo multiplicativo de K^*.*

(2) *K é formalmente real se, e somente se, $Q(K) \neq K$ e $char(K) \neq 2$.*

Demonstração: (1) Primeiramente, notemos que $1 \in Q(K)^*$, assim $Q(K)^* \neq \emptyset$. Também, $Q(K)^*$ é fechado para multiplicação. De fato, consideremos $a, b \in$

$Q(K)^*$, assim podemos escrever $a = \sum x_i^2$ e $b = \sum y_j^2$, logo $a.b = \sum x_i^2 . \sum y_j^2 = \sum_{i,j}(x_i.y_j)^2 \in Q(K)^*$. Agora, como $a^{-1} = a(a^{-1})^2 = \sum x_i^2(a^{-1})^2 = \sum(x_i.a^{-1})^2 \in Q(K)^*$, obtemos que todo elemento de $Q(K)^*$ possui inverso em $Q(K)^*$. Disso, segue que $Q(K)^*$ é um subgrupo multiplicativo.

(2) Suponhamos que K é formalmente real, então pela observação anterior, temos que $char(K) = 0 \neq 2$. Usando o fato que K é formalmente real implica que $-1 \notin Q(K)$, e portanto, $Q(K) \neq K$. Reciprocamente, assumimos que $char(K) \neq 2$ e K é não real, ou seja, $-1 \in Q(K)$, assim para todo $a \in K$ temos

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

ou seja, $Q(K) = K$, contradizendo o fato que $Q(K) \neq K$. ■

Definição 1.5. Uma *ordem* sobre um corpo K é um conjunto $P \subsetneq K$ que satisfaz as seguintes propriedades:

$(P1)$ $P + P \subseteq P$

$(P2)$ $P.P \subseteq P$

$(P3)$ $P \cup (-P) = K$.

Dado tal conjunto P, dizemos que (K, P) é um *corpo ordenado*.

A proposição seguinte nos fornece algumas propriedades básicas de um corpo ordenado.

Proposição 1.6. *Seja (K, P) um corpo ordenado qualquer. Então*

(1) *$Q(K) \subseteq P$. Em particular, $0, 1 \in P$.*

(2) *$-1 \notin P$ e $P \cap (-P) = \{0\}$.*

(3) *K é formalmente real, e assim $char(K) = 0$.*

(4) *$P^* = P \setminus \{0\}$ é um subgrupo de índice 2 em K^*.*

(5) *Se $P' \subsetneq K$ denota uma ordem em K, então $P \subseteq P' \Rightarrow P = P'$.*

Demonstração: (1) Sabemos que $P + P \subseteq P$, logo, é suficiente mostrarmos que $K^2 \subseteq P$. Para isso, tomemos $x \in K$, por (P3) temos que $x \in P$ ou $-x \in P$. Se $x \in P$, então $x^2 \in P.P \subseteq P$. Por outro lado, se $-x \in P$, então $x^2 = (-x)(-x) \in P.P \subseteq P$.

(2) Primeiramente, observemos que $char(K) \neq 2$. De fato, suponhamos que $char(K) = 2$, logo $1+1 = 0$, assim obtemos que $1 = -1$. Disso segue que $P = -P$ e por (P3) temos $P = K$, o que não pode ocorrer. Portanto, devemos ter $char(K) \neq 2$. Agora, suponhamos que $-1 \in P$, assim para todo $a \in K$ temos

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

contradizendo novamente o fato que $P \subsetneq K$. Logo, $-1 \notin P$.

Mostremos que $P \cap (-P) = \{0\}$. Seja $x \in P \cap (-P)$, se $x \neq 0$ teremos $-1 = (x^{-1})^2 x(-x) \in P$, que é uma contradição. Portanto, $P \cap (-P) = \{0\}$.

(3) O fato que $-1 \notin P$ e $Q(K) \subseteq P$ implica que $-1 \notin Q(K)$. Logo, K é formalmente real.

(4) Primeiro mostremos que P^* é um subgrupo multiplicativo de K^*. Já vimos em (1) que $P^* \neq \emptyset$. Dados $a, b \in P^*$, segue que $a.b \in P.P \subseteq P$, logo P^* é fechado para a multiplicação. Também, para $a \in P^*$ temos $a^{-1} = (a^{-1})^2 a \in P^*$. Portanto, P^* é um subgrupo de K^*. Agora notemos que $1.P^*$ e $-1.P^*$ são classes laterais distintas, visto que $-1 \notin P^*$. Uma vez que $K^* = P^* \cup (-P^*)$, segue que $\dfrac{|K^*|}{|P^*|} = 2$, como queríamos.

(5) Suponhamos que P' é uma ordem em K e $P \subseteq P'$, então por (4) devemos ter $\dfrac{|K^*|}{|P^*|} = \dfrac{|K^*|}{|P'^*|} = 2$, o que implica $|P^*| = |P'^*|$. Como $P \subseteq P'$, concluímos que $P = P'$. ■

Observação 1.7. Se (K, P) é um corpo ordenado, então devemos ter $K = P \cup (-P)$ e $P \cap (-P) = \{0\}$, ou seja, K é união disjunta de $\{0\}$, P^* e $-P^*$. Assim podemos introduzir a notação $x \leq_P y$ para dizer que $y - x \in P$ e $x <_P y$ quando tivermos

$y - x \in P^*$. Observemos que, dados $x, y \in K$ temos uma das três possibilidades:

$$x = y\,, \quad x <_P y \quad \text{ou} \quad y <_P x\,.$$

Dizemos que $\leq_P$ é uma *ordem total* sobre os elementos de K. Se P é dado e fixado, então escrevemos $\leq$ e $<$ ao invés de $\leq_P$ e $<_P$.

Observação 1.8. Sejam (K, P) um corpo ordenado e K_0 um subcorpo de K, então $P_0 = P \cap K_0$ é uma ordem sobre K_0. Claramente P_0 satisfaz os axiomas de ordem sobre K_0, dizemos que esta ordem é induzida pela ordem P sobre K.

Exemplo 1.9. Um exemplo de corpo ordenado é $K = \mathbb{R}$, o corpo dos números reais, que possui uma única ordem dada por $P = \mathbb{R}^2$. Pelo que observamos acima, temos que o subcorpo dos números racionais $\mathbb{Q}$ de $\mathbb{R}$ também é ordenado por $P_0 = \mathbb{R}^2 \cap \mathbb{Q}$.

Lema 1.10. *Sejam K um corpo formalmente real e $L = K(\sqrt{a})$ uma extensão quadrática de K. Então L é não real se, e somente se, $-a \in Q(K)^*$.*

Demonstração: Suponhamos que L é não real, assim podemos escrever

$$-1 = \sum (b_i + c_i\sqrt{a})^2 = \sum b_i^2 + \sum 2b_ic_i\sqrt{a} + a\sum c_i^2\,,$$

para $b_i, c_i \in K$. O fato que $-1 \in K$ e $\sqrt{a} \notin K$ implica que $\sum 2b_ic_i\sqrt{a} = 0$. Disso resulta

$$-1 = \sum b_i^2 + a\sum c_i^2\,.$$

Notemos que, se $\sum c_i^2 = 0$, obtemos $-1 = \sum b_i^2 \in Q(K)$, o que não pode ocorrer, pois K é formalmente real. Por outro lado, se $\sum c_i^2 \neq 0$ segue que

$$-a = \left(1 + \sum b_i^2\right)\left(\sum c_i^2\right)^{-1}\,.$$

Como $Q(K)^*$ é um grupo, concluímos que $-a \in Q(K)^*$. Reciprocamente, assumimos que $-a \in Q(K)^*$, assim temos que $(\sqrt{a})^2 + (-a) = 0$, ou seja, 0 é uma soma de quadrados em L. Portanto, L é não real. ■

Definição 1.11. Um corpo K é chamado *euclidiano* se K é formalmente real e $|K^*/K^{2*}| = 2$.

Observação 1.12. Seja K euclidiano. O fato que K é formalmente real implica que $-1 \notin K^{2*}$, assim $1.K^{2*}$ e $-1.K^{2*}$ são classes laterais distintas. Uma vez que $|K^*/K^{2*}| = 2$, segue que $K^* = K^{2*} \cup (-K^{2*})$.

Definição 1.13. Um corpo K é chamado *pitagórico* se a soma de dois quadrados em K é sempre um quadrado.

Observação 1.14. Um corpo K é pitagórico se, e somente se, $1+y^2$ é um quadrado, para todo $y \in K$. De fato, suponhamos que $x^2+y^2 = \lambda^2$, para todo $x, y \in K$ e para algum $\lambda \in K$. Em particular, fazendo $x = 1$ segue que $1+y^2 = \lambda^2$, para todo $y \in K$ e para algum $\lambda \in K$. Reciprocamente, assumimos que $1 + y^2$ é um quadrado para todo $y \in K$. Temos $a^2 + b^2 = a^2(1 + (a^{-1}b)^2)$ e por hipótese $1 + (a^{-1}b)^2 = \lambda^2$ para algum $\lambda \in K$. Logo, $a^2 + b^2 = a^2\lambda^2 = (a\lambda)^2$, para todo $a, b \in K$, como queríamos.

Proposição 1.15. *Se K é euclidiano, então K é pitagórico com uma única ordem.*

Demonstração: Suponhamos que K é euclidiano, se mostrarmos que a soma $1+y^2$ é um quadrado em K, para todo $y \in K$, então pela observação acima teremos que K é pitagórico. Sabemos por hipótese que $K = K^2 \cup (-K^2)$. Seja $y \in K$, assim $1 + y^2 \in K^2$ ou $1 + y^2 \in -K^2$, se $1 + y^2 \in -K^2$, logo $1 + y^2 = -x^2$, para algum $x \in K$, mas isso implica $-1 = x^2+y^2$, ou seja, K é não real, o que é absurdo, pois F é euclidiano. Portanto, devemos ter $1+y^2 \in K^2$, para todo $y \in K$, como queríamos.

Agora, notemos que $P = K^2$ é uma ordem em K. De fato,

- $P \neq K$, pois se $P = K$, então $|K^*/K^{2*}| = 1$, contrariando o fato que K é euclidiano.
- $P.P \subseteq P$, dados $a^2.b^2 \in P.P$ temos $a^2.b^2 = (a.b)^2 \in K^2 = P$.
- $P \cup (-P) = K$, segue do fato que K é euclidiano.

- $P + P \subseteq P$, como já vimos, K é pitagórico, e o resultado segue.

Vamos mostrar que $P = K^2$ é a única ordem em K. Para isso, suponhamos que P' também determina uma ordem em K. Pelo ítem (1) da Proposição 1.6 temos que $Q(K) \subseteq P'$, como $P = K^2 \subseteq Q(K)$, segue que $P \subseteq P'$. Aplicando novamente 1.6, ítem (5), concluímos $P = P'$. Portanto, $P = K^2$ é a única ordem em K. ■

Nosso objetivo agora é caracterizar os corpos euclidianos, para isso, mostraremos dois resultados que nos serão úteis.

Proposição 1.16. *Se K é um corpo tal que $char(K) \neq 2$ e $\overline{K}$ é o fecho algébrico de K, então $L \supset K$ é uma extensão quadrática sobre K, isto é, $dim_K L = 2$ se, e somente se, $L = K(\alpha)$ para algum $\alpha \in \overline{K} \setminus K$ tal que $\alpha^2 \in K$.*

Demonstração: Suponhamos que $dim_K L = 2$ e consideremos $\{1, \beta\}$ uma base para o espaço vetorial L sobre K. Como $\beta^2 \in L$, podemos escrever $\beta^2 = r + s\beta$, para $r, s \in K$. Agora, coloquemos $\alpha = \beta - \frac{s}{2}$ e notemos que $\alpha^2 = r + \frac{s^2}{4} \in K$. Além disso, $\alpha \in L \setminus K$, pois se $\alpha \in K$, teríamos que $\beta = \alpha + \frac{s}{2} \in K$, uma contradição. Dessa forma, devemos ter $[K(\alpha) : K] > 1$ e, usando o fato que $2 = [L : K] = [L : K(\alpha)] \, . \, [K(\alpha) : K]$ obtemos $[K(\alpha) : K] = 2$ e $[L : K(\alpha)] = 1$. Portanto, $L = K(\alpha)$. Reciprocamente, observemos que $dim_K L > 1$, pois $\alpha \in L$ e $\alpha \notin K$. Além disso, temos que α é raiz do polinômio $p(x) = x^2 - \alpha^2 \in K[x]$, e portanto, α é algébrico sobre K. Consideremos $m_\alpha(x)$ o polinômio minimal de α sobre K, assim se $\partial m_\alpha = n$, sabemos que todo elemento de L é representado unicamente na forma $k_0 + k_1\alpha + \ldots + k_n\alpha^n$, com $k_0, \ldots, k_n \in K$. Uma vez que $\alpha^2 \in K$, esta expressão se reduz para $a + b\alpha$, com $a, b \in K$. Logo, $\{1, \alpha\}$ é uma base para L sobre K, e portanto, $dim_K L = 2$. ■

Definição 1.17. Dado um elemento $c = x + y\sqrt{a} \in L = K(\sqrt{a})$, dizemos que $\bar{c} = x - y\sqrt{a}$ é o *conjugado* de c em L. A *norma* de um elemento $c \in L = K(\sqrt{a})$ é definida por $N_{L/K}(c) = c\,\bar{c}$. É fácil mostrar que $N_{L/K}(c) \in K$.

Lema 1.18. *Sejam K um corpo tal que $char(K) \neq 2$ e $L = K(\sqrt{a})$, onde $a \notin K^{*2}$, uma extensão quadrática de K. Definamos $r^* : K^*/K^{*2} \to L^*/L^{*2}$ por $r^*(cK^{*2}) = cL^{*2}$ e $N : L^*/L^{*2} \to K^*/K^{*2}$ por $N(cL^{*2}) = N_{L/K}(c)K^{*2}$. Consideremos i o homomorfismo inclusão. Então a seqüência*

$$\{1\} \to \{K^{*2}, aK^{*2}\} \xrightarrow{i} K^*/K^{*2} \xrightarrow{r^*} L^*/L^{*2} \xrightarrow{N} K^*/K^{*2} \text{ é exata.}$$

Demonstração: Primeiramente, mostraremos que $\mathrm{Ker}\,(r^*) = \mathrm{Im}(i)$, ou seja, $\mathrm{Ker}\,(r^*) = \{K^{*2}, aK^{*2}\}$, visto que $\mathrm{Im}(i) = \{K^{*2}, aK^{*2}\}$. Claramente $\{K^{*2}, aK^{*2}\} \subset \mathrm{Ker}\,(r^*)$, pois $a = \sqrt{a}\sqrt{a} \in L^{*2}$ e assim $r^*(aK^{*2}) = aL^{*2} = L^{*2}$ e $r^*(K^{*2}) = L^{*2}$. Com isso, provamos que $\mathrm{Im}(i) \subset \mathrm{Ker}\,(r^*)$.

Por outro lado, tomemos $cK^{*2} \in \mathrm{Ker}\,(r^*)$, isso implica que $r^*(cK^{*2}) = L^{*2}$, ou seja, $cL^{*2} = L^{*2}$. Assim, obtemos que $c \in K^* \cap L^{*2}$. Do fato que $c \in L^{*2}$ segue que $c = (r + s\sqrt{a})^2 = r^2 + 2rs\sqrt{a} + s^2a$, para $r, s \in K$. Como $c \in K^*$, devemos ter $2rs = 0$, uma vez que $char(K) \neq 2$ segue que $rs = 0$, e portanto, $r = 0$ ou $s = 0$. Se $s = 0$ então $c = r^2 \in K^{*2}$, isso nos diz que $cK^{*2} = K^{*2}$. Caso $r = 0$, então $c = as^2 \in aK^{*2}$, logo $cK^{*2} = aK^{*2}$. Portanto, $\mathrm{Ker}\,(r^*) \subset \mathrm{Im}(i)$ e concluímos que $\mathrm{Ker}\,(r^*) = \mathrm{Im}(i)$.

Agora, mostraremos que $\mathrm{Ker}\,(N) = \mathrm{Im}(r^*)$. Para isso, tomemos $xL^{*2} \in \mathrm{Ker}\,(N)$, assim devemos ter $N(xL^{*2}) = N_{L/K}(x)K^{*2} = K^{*2}$, logo $N_{L/K}(x) = x\bar{x} = b^2$, para algum $b \in K^*$. Definamos $z = b - \bar{x} \in L$, assim $xz^2 = x(b^2 - 2b\bar{x} + \bar{x}^2) = x(x\bar{x} - 2b\bar{x} + \bar{x}^2) = x\bar{x}(x + \bar{x} - 2b) \in K$. Suponhamos que $z \neq 0$, como $xL^{*2} = xz^2L^{*2}$ e $xz^2 \in K$ segue que $r^*(xz^2K^{*2}) = xz^2L^{*2} = xL^{*2}$, e portanto, $xL^{*2} \in \mathrm{Im}(r^*)$. Por outro lado, se $z = 0$ então $\bar{x} = b$, sendo $b \in K$ segue que $x = \bar{b} = b \in K$ e assim $r^*(xK^{*2}) = xL^{*2}$. Disso concluímos que $xL^{*2} \in \mathrm{Im}(r^*)$. Logo, $\mathrm{Ker}\,(N) \subset \mathrm{Im}(r^*)$.

Reciprocamente, seja $xL^{*2} \in \mathrm{Im}(r^*)$, isso implica que existe $c \in K^*$ tal que $r^*(cK^{*2}) = xL^{*2}$, ou seja, $cL^{*2} = xL^{*2}$. Como $c \in K^*$ temos que $N_{L/K}(c) = c.c = c^2 \in K^{*2}$, e portanto, $N(xL^{*2}) = N(cL^{*2}) = N_{L/K}(c)K^{*2} = c^2K^{*2} = K^{*2}$, isto é, $xL^{*2} \in \mathrm{Ker}\,(N)$ provando que $\mathrm{Im}(r^*) \subset \mathrm{Ker}\,(N)$. Portanto, $\mathrm{Ker}\,(N) = \mathrm{Im}(r^*)$. ■

O próximo resultado fornece uma caracterização importante para os corpos euclidianos.

Teorema 1.19. *Seja K um corpo, então as seguintes condições são equivalentes:*

(1) *K é euclidiano.*

(2) *K é formalmente real, mas toda extensão quadrática de K é não real.*

(3) *$i = \sqrt{-1} \notin K$, e $L = K(i)$ é quadraticamente fechado, ou seja, $L^2 = L$.*

(4) *$char(K) \neq 2$ e existe uma extensão quadrática $M \supseteq K$ que é quadraticamente fechada.*

Demonstração: (1) $\Rightarrow$ (3) Suponhamos que K é euclidiano, logo, K é formalmente real. Se $i = \sqrt{-1} \in K$, então $-1 = \sqrt{-1}.\sqrt{-1} \in K^2$, contradizendo o fato que K é formalmente real. Portanto, $i \notin K$.

Definamos $L = K(i)$, assim o homomorfismo $N : L^*/L^{*2} \to K^*/K^{*2}$ é trivial. Com efeito, dado $cL^{*2} \in L^*/L^{*2}$, c pode ser representando na forma $r + s\sqrt{-1}$ para $r, s \in K$, assim $N(cL^{*2}) = N((r+s\sqrt{-1})L^{*2}) = N_{L/K}(r+s\sqrt{-1})K^{*2} = (r^2+s^2)K^{*2}$. Pela Proposição 1.15, temos que K é pitagórico, com isso $r^2 + s^2 \in K^{*2}$. Portanto, $N(cL^{*2}) = K^{*2}$, para todo $c \in L^*$. Sendo N trivial, do lema anterior obtemos a seguinte seqüência exata:

$$\{1\} \to \{K^{*2}, -K^{*2}\} \xrightarrow{i} K^*/K^{*2} \xrightarrow{r^*} L^*/L^{*2} \to \{1\}.$$

Assim r^* é sobrejetora e $\text{Ker}\,(r^*) = \{K^{*2}, -K^{*2}\}$. Pelo Teorema do Isomorfismo, L^*/L^{*2} é isomorfo a $\dfrac{K^*/K^{*2}}{\{K^{*2}, -K^{*2}\}}$. Pela Observação 1.12 temos $K^* = K^{*2} \cup (-K^{*2})$ e assim $\dfrac{K^*/K^{*2}}{\{K^{*2}, -K^{*2}\}} = \{1\}$. Portanto $L = L^2$, ou seja, L é quadraticamente fechado.

(3) $\Rightarrow$ (4) Já temos que $K(i)$ é uma extensão de K que é quadraticamente fechada. Agora, suponhamos que $char(K) = 2$, isso implica que $1 = -1$. Assim $i = \sqrt{-1} = \sqrt{1} = 1 \in K$, o que não pode ocorrer. Portanto, necessariamente $char(K) \neq 2$.

(4) $\Rightarrow$ (2) Suponhamos que $char(K) \neq 2$ e $M \supseteq K$ é uma extensão quadraticamente fechada. Pela Proposição 1.16 podemos tomar $M = K(\sqrt{a})$ com $a \notin K^{*2}$. A função norma $M^*/M^{*2} \to K^*/K^{*2}$ tem imagem $\{x^2 - ay^2 : x, y \in K\}/K^{*2}$. Uma vez que $M^* = M^{*2}$, devemos ter $\{x^2 - ay^2 : x, y \in K\} = K^{*2}$. Em particular, $-a \in K^{*2}$, o que implica $a \in -K^{*2}$. Podemos assumir $a = -1$, logo $\{x^2 + y^2 : x, y \in K\} = K^{*2}$ e isso nos diz que K é pitagórico. Suponhamos que K não é formalmente real, então $-1 \in Q(K) = K^{*2}$, contradizendo o fato que $-1 = a \notin K^{*2}$. Logo, K é formalmente real.

Na seqüência exata do lema anterior temos

$$\{1\} \to \{K^{*2}, -K^{*2}\} \xrightarrow{i} K^*/K^{*2} \xrightarrow{r^*} M^*/M^{*2} = \{1\},$$

assim $K^*/K^{*2} = \{K^{*2}, -K^{*2}\}$. Agora, seja L uma extensão quadrática de K. Já vimos que $L = K(\sqrt{b})$, para $b \notin K^{*2}$. Como $K^*/K^{*2} = \{K^{*2}, -K^{*2}\}$ e $b \notin K^{*2}$, devemos ter $bK^{*2} = -K^{*2}$, isso nos diz que $b = -x^2$ para algum $x \in K^*$. Dessa forma, $L = K(\sqrt{b}) = K(\sqrt{-x^2}) = K(x\sqrt{-1}) = K(\sqrt{-1})$. Portanto, $K(\sqrt{-1})$ é a única extensão quadrática de K, que claramente não é formalmente real.

(2) $\Rightarrow$ (1) Como K é formalmente real, $-1 \notin K^{*2}$, assim K^{*2} e $-K^{*2}$ são classes laterais distintas de K^*/K^{*2}. Basta provarmos que $K^* = K^{*2} \cup (-K^{*2})$ para obtermos $|K^*/K^{*2}| = 2$. Com efeito, consideremos $a \in K^*$ tal que $a \notin K^{*2}$. Assim $K(\sqrt{a})$ é uma extensão quadrática de K, e por hipótese temos que $K(\sqrt{a})$ é não real. Aplicando o Lema 1.10 obtemos

$$-a = a_1^2 + \ldots + a_n^2,$$

para $a_i \in K$, $1 \leq i \leq n$. Podemos assumir esta equação com n minimal. Em particular, cada $a_i \neq 0$. Com isso, se $n \geq 2$, então $a_1^2 + a_2^2 \notin K^{*2}$, pois se $a_1^2 + a_2^2 = x^2$ para algum $x \in K$, teríamos $-a = \underbrace{x^2 + a_3^2 + \ldots + a_n^2}_{n-1 \text{ parcelas}}$ o que não pode ocorrer, visto que n é minimal. Portanto, $a_1^2 + a_2^2 \notin K^{*2}$ e, novamente podemos escrever

$$-(a_1^2 + a_2^2) = b_1^2 + \ldots + b_m^2,$$

para $b_i \in K$, $1 \leq i \leq m$. Disso segue que $0 = b_1^2 + \ldots + b_m^2 + a_1^2 + a_2^2$, contradizendo o fato que K é formalmente real. Logo $n = 1$ e assim $a = -a_1^2 \in -K^{*2}$. Com isso, concluímos que $K^* = K^{*2} \cup (-K^{*2})$. Como desejávamos. ■

1.2 Corpos Reais Fechados

Nesta seção, veremos que todo corpo formalmente real possui uma ordem. Além disso, demonstraremos o Teorema Fundamental da Álgebra, o qual estabelece uma caracterização para os corpos reais fechados. Iniciamos com a noção de corpo real fechado.

Definição 1.20. Um corpo K é chamado *real fechado* se K é formalmente real, mas toda extensão algébrica de K é não real.

Exemplo 1.21. Um exemplo simples de corpo real fechado é o conjunto dos números reais $\mathbb{R}$, visto que $\mathbb{R}$ é formalmente real e a única extensão algébrica própria de $\mathbb{R}$ é o conjunto dos números complexos $\mathbb{C}$, que claramente é não real.

Corolário 1.22. *Seja K um corpo real fechado. Então K é euclidiano e $K(\sqrt{-1})$ é quadraticamente fechado.*

Demonstração: Suponhamos que K é real fechado, assim, por definição, temos que K é formalmente real e toda extensão algébrica de K é não real. Como toda extensão quadrática é algébrica, segue que toda extensão quadrática é não real. Logo, a condição (2) do Teorema 1.19 é satisfeita. Portanto, K é euclidiano e $K(\sqrt{-1})$ é quadraticamente fechado. ■

Proposição 1.23. *Sejam K um corpo formalmente real e $\overline{K}$ seu fecho algébrico. Então existe um corpo real fechado R tal que $K \subset R \subset \overline{K}$.*

Demonstração: Consideremos S a coleção de todos subcorpos formalmente reais de $\overline{K}$ contendo K. Notemos que $S \neq \emptyset$, pois $K \in S$. Além disso, toda subcoleção

$\{K_\alpha\}$ de S totalmente ordenada, com relação a inclusão, possui um limitante superior, a saber $\cup K_\alpha$, que por sua vez, pertence a S. Pelo Lema de Zorn, existe um elemento $R \in S$ tal que R é maximal. O tal corpo R claramente é real fechado.■

Teorema 1.24. *Um corpo K é formalmente real se, e somente se, K possui pelo menos uma ordem.*

Demonstração: Suponhamos que K é formalmente real. Pela proposição anterior, existe um corpo real fechado R tal que $R \supset K$. Usando o Corolário 1.22, obtemos que R é euclidiano, assim, pela Proposição 1.15 segue que R possui uma única ordem. Uma vez que R possui uma ordem e K é um subcorpo de R, então K possui uma ordem que é induzida pela ordem de R. Reciprocamente, se K possui uma ordem, então pela Proposição 1.6 segue que K é formalmente real. ■

Observação 1.25. Seja K um corpo ordenado, então, pelo teorema acima, temos que K é formalmente real e, portanto, para todo $n \in \mathbb{N}$, a equação $x_1^2 + \ldots + x_n^2 = 0$ admite somente a solução trivial em K. Usaremos esse fato no Capítulo 4 desse trabalho.

Nosso objetivo, agora, é demonstrar o Teorema Fundamental da Álgebra, mas antes precisamos de alguns resultados.

Proposição 1.26. *Seja K um corpo, então as seguintes condições são equivalentes:*

(1) *Qualquer polinômio $f \in K[x]$ de grau ímpar tem raiz em K.*

(2) *K não tem extensão própria de grau ímpar.*

Demonstração: Suponhamos que L é uma extensão própria de K de grau ímpar. Conseqüentemente, $[L : K] > 1$. Desde que $[L : K] < \infty$, decorre que L é uma extensão algébrica de K. Então, seja $\alpha \in L \setminus K$ e $f \in K[x]$ o polinômio minimal de α sobre K. Como $[K(\alpha) : K]$ divide $[L : K]$ que é ímpar, segue que $\partial f = [K(\alpha) : K]$

é um inteiro ímpar > 1. Como f é irredutível em $K[x]$ segue que f não tem raiz em K, contradizendo (1).

Reciprocamente, suponhamos que (2) ocorre. Para provarmos (1), vamos usar indução sobre $n = \partial f$. Se $n = 1$, claramente f tem uma raiz em K. Assumimos $n > 1$. Se f for irredutível sobre K, então $\frac{K[x]}{(f)}$ é uma extensão própria de grau ímpar, contradizendo (2). Assim devemos ter $f = f_1 f_2$, onde $\partial f_1 < \partial f$ e $\partial f_2 < \partial f$. O fato que $\partial f = \partial f_1 + \partial f_2$ e ∂f é ímpar, implica que ∂f_1 ou ∂f_2 é ímpar. Digamos que ∂f_1 é ímpar, então usando a hipótese de indução segue que f_1 tem uma raiz em K, assim f também tem uma raiz em K. ■

A demonstração da próxima proposição será omitida, uma vez que envolve alguns resultados técnicos, que fogem de nossos interesses.

Proposição 1.27. *Se K é formalmente real, então toda extensão L de K de grau ímpar também é formalmente real.*

Demonstração: Ver [7], Proposição 2.1, pg 241. ■

Corolário 1.28. *Se K é um corpo real fechado, então todo polinômio de grau ímpar sobre K tem raiz em K.*

Demonstração: Como K é real fechado, por definição, K é formalmente real. Logo, a Proposição 1.27 implica que toda extensão de grau ímpar é formalmente real. Agora, usando novamente o fato que K é real fechado segue que K não tem extensão algébrica própria formalmente real, isso implica que K não tem extensão própria de grau ímpar. Logo, o resultado segue da Proposição 1.26. ■

Lema 1.29. *Seja K um corpo que não é algebricamente fechado. Suponhamos que $K(\sqrt{-1})$ é uma extensão algebricamente fechada de K. Então toda extensão algébrica própria de K é isomorfa a $K(\sqrt{-1})$.*

Demonstração: Seja L uma extensão algébrica própria de K e seja $u \in L \setminus K$ 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 raíz de f, então as extensões $K(u)$ e $K(v)$ são isomorfas, visto que u e v são raízes do mesmo polinômio minimal. 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, $K(u) \simeq K(\sqrt{-1})$ e, assim, L é uma extensão algébrica de um corpo algebricamente fechado. Como um corpo algebricamente fechado não possui extensão algébrica, a não ser ele próprio, devemos ter $L = K(u) \simeq K(\sqrt{-1})$. ■

Teorema 1.30. (Fundamental da Álgebra) *As seguintes condições são equivalentes:*

(1) *K é real fechado.*

(2) *K é euclidiano e todo polinômio de grau ímpar sobre K tem raiz em K.*

(3) *$i := \sqrt{-1} \notin K$ e $L = K(i)$ é algebricamente fechado.*

Demonstração: (1) $\Rightarrow$ (2) Segue do Corolário 1.22 e Corolário 1.28.

(2) $\Rightarrow$ (3) Primeiramente, usando o fato que K é euclidiano, pelo Teorema 1.19 temos $i := \sqrt{-1} \notin K$ e $L = K(i)$ é quadraticamente fechado. Resta mostrar que todo polinômio não constante sobre L tem uma raiz em L. Para tanto, tomemos $f(x) \in L[x] \setminus L$ e consideremos $\alpha \mapsto \overline{\alpha}$ a conjugação complexa sobre L. Então $h(x) = f(x)\overline{f}(x) \in K[x]$, pois $h(x) = f(x)\overline{f}(x) = \overline{f}(x)f(x) = \overline{f}(x)\overline{\overline{f}}(x) = \overline{f(x)\overline{f}(x)} = \overline{h}(x)$. Agora veremos que se $h(x)$ tem uma raiz em L, então $f(x)$ também tem uma raiz em L. De fato, seja $a \in L$ uma raiz de $h(x)$, assim $f(a)\overline{f}(a) = 0$. Como L é corpo devemos ter $f(a) = 0$ ou $\overline{f}(a) = 0$. Se $f(a) = 0$, então $a \in L$ é uma raiz de $f(x)$. Caso ocorra $\overline{f}(a) = 0$, então $\overline{\overline{f}}(a) = \overline{0}$, e isto nos dá $f(\overline{a}) = 0$. Logo, $\overline{a} \in L$ é raiz de $f(x)$. Portanto, $f(x)$ tem uma raiz em L.

Por conta disso, é suficiente mostrarmos que todo polinômio $g(x) \in K[x] \setminus K$

tem uma raiz em L. Para isso, consideremos E um corpo de decomposição para $(x^2+1)g(x)$ sobre K. Dessa forma, temos que E é uma extensão normal e finita sobre K que contém L. Mais ainda, como $char(K) = 0$, E é uma extensão separável sobre K, e portanto, $E : K$ é uma extensão galoisiana.

Por hipótese temos que todo polinômio de grau ímpar em $K[x]$ tem raiz em K. Logo, pela Proposição 1.26, segue que K não tem extensão própria de grau ímpar. Isto nos diz que $[E : K]$ é um múltiplo de 2. Suponhamos que $[E : K] = 2^n m$ com $m > 1$ um inteiro ímpar. Pelo Teorema da Correspondência de Galois temos $|\mathrm{Gal}(E/K)| = 2^n m$, assim temos um 2-subgrupo de Sylow H de ordem 2^n. Se $H^\dagger$ é o corpo fixo de H então

$$[H^\dagger : K] = \frac{|\mathrm{Gal}(E/K)|}{|H|} = \frac{2^n m}{2^n} = m,$$

que é ímpar, e isto não ocorre. Logo, devemos ter $[E : K] = 2^n$ para algum $n \in \mathbb{N}^*$.

Agora usando o fato que $2^n = [E : K] = [E : L].[L : K]$, e $[L : K] = 2$ vem $[E : L] = 2^{n-1}$. Suponhamos que $n > 1$ e observemos que $[E : L]$ é uma extensão galoisiana. Assim $|\mathrm{Gal}(E/L)| = 2^{n-1}$, e portanto, existe um 2-subgrupo de Sylow $H_1 = 2^{n-2}$. Novamente, considerando $H_1^\dagger$ o corpo fixo de H_1, obtemos

$$[H_1^\dagger : L] = \frac{|\mathrm{Gal}(E/L)|}{|H_1|} = \frac{2^{n-1}}{2^{n-2}} = 2,$$

que é uma contradição, pois L não tem extensão quadrática. Portanto, $n = 1$, o que implica $[E : L] = 1$, ou seja, $E = L$. Sendo L o corpo de decomposição de $(x^2+1)g(x)$ sobre K, segue que $g(x)$ tem uma raiz em L, como desejávamos.

(3) $\Rightarrow$ (1) Por hipótese temos que $i := \sqrt{-1} \notin K$. Mostremos que $L = K(i)$ é quadraticamente fechado. Com efeito, claramente $L^2 \subset L$. Por outro lado, tomemos $\alpha \in L$. Vamos mostrar que $\alpha \in L^2$, ou seja, $\alpha = \lambda^2$ para algum $\lambda \in L$. Como $x^2 - \alpha \in L[x] \setminus L$ e L é algebricamente fechado, existe $\lambda \in L$ tal que $\lambda^2 - \alpha = 0$, ou seja, $\alpha = \lambda^2$. Logo, L é quadraticamente fechado.

Com isso, temos que a condição (3) do Teorema 1.19 é satisfeita, e portanto,

K é formalmente real. Agora pelo Lema 1.29, a única extensão algébrica própria de K é L que claramente é não real. Portanto, K é real fechado. ■

Encerraremos essa seção com um corolário que segue diretamente do Lema 1.29 e do Teorema Fundamental da Álgebra.

Corolário 1.31. *Toda extensão algébrica própria de um corpo real fechado K é isomorfa ao corpo $K(\sqrt{-1})$.*

1.3 Semisimplicidade

Iniciamos esta seção definindo módulos simples e semisimples e, também, apresentando alguns resultados básicos envolvendo esses módulos. Em seguida, daremos outra caracterização para os módulos semisimples.

Definição 1.32. Seja R um anel. Um R-módulo $M \neq 0$ é *simples* se este só possui os submódulos triviais, ou seja, (0) e M.

Definição 1.33. Um R-módulo M é chamado *semisimples* se todo submódulo N de M é um somando direto, isto é, existe um submódulo N' tal que $M = N \oplus N'$.

Veremos agora que submódulo de módulo semisimples é semisimples, mais adiante, mostraremos que o quociente também o é (ver Corolário 1.37).

Proposição 1.34. *Seja $N \neq (0)$ um submódulo de um R-módulo semisimples M. Então, N é semisimples e contém um submódulo simples.*

Demonstração: Para mostrarmos que N é semisimples, consideremos S um submódulo arbitrário de N. Então S também é submódulo de M, sendo M semisimples, segue que existe outro submódulo S' tal que $M = S \oplus S'$. Mostraremos que $N = S \oplus (S' \cap N)$ e, com isso, teremos que N é semisimples.

Observemos que $S \cap (S' \cap N) \subset S \cap S'$. O fato que $M = S \oplus S'$ implica que $S \cap S' = (0)$. Logo, devemos ter $S \cap (S' \cap N) = (0)$. Por outro lado, dado

um elemento $n \in N$, como N é submódulo de M, temos que $n \in M$, e portanto, podemos escrever $n = x + y$ com $x \in S$ e $y \in S'$. Assim $y = n - x \in N$, pois $x \in S \subset N$, logo, $y \in N \cap S'$, provando que $N = S + (S' \cap N)$.

Para mostrarmos que N contém um submódulo simples, escolha um elemento $x \in N$ tal que $x \neq 0$. Consideremos $\mathcal{F}$ a coleção de todos submódulos de N que não contém x. Notemos que $(0) \in \mathcal{F}$, e portanto, $\mathcal{F} \neq \emptyset$. Além disso, toda subcoleção totalmente ordenada $\{N_\alpha\}$ de $\mathcal{F}$ tem um limitante superior, a saber $\cup N_\alpha$. Então, pelo Lema de Zorn, $\mathcal{F}$ possui um elemento maximal N_1. Uma vez que N é semisimples, existe outro submódulo N_2 de N tal que $N = N_1 \oplus N_2$. Vamos mostrar que N_2 é simples. De fato, se N_2 não fosse simples, então N_2 conteria um submódulo próprio W e assim existiria W' tal que $N_2 = W \oplus W'$. Notemos que $N = N_1 \oplus W \oplus W'$ e $N_1 = (N_1 + W) \cap (N_1 + W')$. Como $x \notin N_1$, devemos ter que $x \notin N_1 + W$ ou $x \notin N_1 + W'$. Contradizendo a maximalidade de N_1. ■

O próximo teorema nos fornece outras maneiras de definirmos módulos semisimples.

Teorema 1.35. *Seja M um R-módulo. Então as seguintes condições são equivalentes:*

(1) *M é semisimples.*

(2) *M é uma soma direta de submódulos simples.*

(3) *M é uma soma (não necessária direta) de submódulos simples.*

Demonstração: (1) $\Rightarrow$ (2) Consideremos a coleção $\mathcal{F}$ de todos submódulos de M que podem ser escritos como soma direta de submódulos simples. Como M é semisimples, temos, pela proposição anterior, que M contém um submódulo simples. Assim $\mathcal{F} \neq \emptyset$, pois contém, pelo menos, somas diretas com um único somando.

Vamos definir uma ordem em $\mathcal{F}$. Dados $\bigoplus_{i \in I} M_i$ e $\bigoplus_{i \in J} M_i$ em $\mathcal{F}$, dizemos que

$\bigoplus_{i\in I} M_i < \bigoplus_{i\in J} M_i$ se, e somente se, $I \subset J$. Agora, é fácil verificarmos que $(\mathcal{F}, <)$ satisfaz as condições do Lema de Zorn, assim existe um elemento M_0 maximal em $\mathcal{F}$, o qual podemos escrever na forma $M_0 = \bigoplus_{i\in I} M_i$, com M_i simples, para todo $i \in I$. Basta mostrarmos que $M_0 = M$. Suponhamos que $M_0 \neq M$. Como M é semisimples existe N submódulo de M tal que $M = M_0 \oplus N$. Pela Proposição 1.34, segue que N contém um submódulo simples S, mas então $M_0 \oplus S = \bigoplus_{i\in I} M_i \oplus S \supset M_0$. Contradizendo a maximalidade de M_0. Portanto, devemos ter $M = M_0 = \bigoplus_{i\in I} M_i$.

(2) $\Rightarrow$ (3) Trivial.

(3) $\Rightarrow$ (1) Por hipótese podemos escrever $M = \sum_{i\in I} M_i$, onde M_i é simples, para todo $i \in I$. Tomemos N um submódulo próprio arbitrário de M e mostremos que N é um somando direto.

Consideremos a família $\mathcal{F} = \left\{ \sum_{i\in J} M_i \ : \ J \subset I, \ \left(\sum_{i\in J} M_i \right) \cap N = (0) \right\}$. Notemos que M_i é simples e $M_i \cap N$ é submódulo de M_i, assim se $M_i \cap N \neq (0)$ então $M_i \cap N = M_i$, o que implica $M_i \subset N$. Uma vez que $N \neq M$ segue que existe pelo menos um submódulo M_i tal que $M_i \cap N = (0)$, assim $\mathcal{F}$ é não vazia. Pelo Lema de Zorn, existe um submódulo maximal em $\mathcal{F}$, digamos $M_0 = \sum_{i\in J_0} M_i$.

Mostremos que $M = M_0 \oplus N$. Com efeito, claramente $M_0 \cap N = (0)$, pois $M_0 \in \mathcal{F}$. Resta-nos mostrarmos que $M = M_0 + N$. Se, para todo $i \in I$, tivermos $M_i \subset M_0 + N$, então $M = M_0 + N$. Suponhamos, por absurdo, que exista um índice i_0 tal que $M_{i_0} \not\subset M_0 + N$. Como M_{i_0} é simples e $M_{i_0} \cap (M_0 + N)$ é submódulo de M_{i_0}, devemos ter $M_{i_0} \cap (M_0 + N) = (0)$ ou $M_{i_0} \cap (M_0 + N) = M_{i_0}$, o fato que $M_{i_0} \not\subset M_0 + N$ implica que a última igualdade não pode ocorrer. Logo, $M_{i_0} \cap (M_0 + N) = (0)$.

Afirmamos que $(M_{i_0} + M_0) \cap N = (0)$. De fato, se $x \in (M_{i_0} + M_0) \cap N$, então $x = m_{i_0} + m_0 = n$. Logo, $m_{i_0} = -m_0 + n \in M_0 + N$ e, como $M_{i_0} \cap (M_0 + N) = (0)$, devemos ter $m_{i_0} = 0$. Segue assim que $x = m_0 = n$, ou seja, $x \in M_0 \cap N$. Mas $M_0 \in \mathcal{F}$, logo, $M_0 \cap N = (0)$ e, portanto, $x = 0$. Com isso mostramos que

$M_{i_0} + M_0 \in \mathcal{F}$, contradizendo a maximalidade de M_0. ■

Já sabemos que todo submódulo N de um módulo semisimples M é semisimples. O próximo teorema nos mostra que os somandos diretos simples de N são também somandos diretos simples de M.

Corolário 1.36. *Sejam $M = \bigoplus_{i\in I} M_i$ uma decomposição de um R-módulo semisimples M como soma direta de submódulos simples e N um submódulo de M. Então, existe um subconjunto de índices $J \subset I$ tal que $N \simeq \bigoplus_{i\in J} M_i$.*

Demonstração: Dado um submódulo N de M, temos, pela demonstração de (3) $\Rightarrow$ (1) do teorema anterior, que sempre podemos encontrar um subconjunto de índices $J_0 \subset I$ tal que $M = N \oplus M_0$, onde $M_0 = \bigoplus_{i\in J_0} M_i$. Então

$$N \simeq \frac{M}{M_0} \simeq \frac{\bigoplus_{i\in I} M_i}{\bigoplus_{i\in J_0} M_i} \simeq \bigoplus_{i\in I\setminus J_0} M_i,$$

assim $J = I \setminus J_0$ é o subconjunto de índices procurado. ■

Corolário 1.37. *Um módulo quociente de um R-módulo semisimples M é isomorfo a um submódulo de M, assim também é semisimples.*

Demonstração: Seja L um módulo quociente de M, consideremos $\pi : M \to L$ o homomorfismo canônico e $N = \mathrm{Ker}\,(\pi)$. Uma vez que M é semisimples, segue que existe um submódulo N' de M tal que $M = N \oplus N'$, o que implica $N' \simeq \frac{M}{N}$. Agora, pelo Teorema do Isomorfismo temos que $\frac{M}{N} \simeq L$. Logo, $N' \simeq \frac{M}{N} \simeq L$. ■

Definição 1.38. Um anel R é chamado *semisimples* se R, visto como um R-módulo à esquerda, é semisimples.

Como os submódulos do R-módulo R são os ideais à esquerda do anel R, temos que R é semisimples se, e somente se, todo ideal à esquerda é um somando direto.

Podemos caracterizar anéis semisimples da seguinte forma:

Teorema 1.39. *Seja R um anel. Então as seguintes condições são equivalentes:*

(1) *Todo R-módulo é semisimples.*

(2) *R é um anel semisimples.*

(3) *R é uma soma direta de um número finito de ideais minimais à esquerda.*

Demonstração: (1) $\Rightarrow$ (2) Se todo R-módulo é semisimples então, em particular, R visto como um R-módulo à esquerda será semisimples.

(2) $\Rightarrow$ (1) Suponhamos que R é um anel semisimples e seja M um R-módulo arbitrário. Sabemos que M é imagem por um homomorfismo sobrejetor de um R-módulo livre F, assim existe $f : F \to M$ tal que $f(F) = M$. Como F é livre, F pode ser escrito na forma $F = \bigoplus_{i \in I} Ra_i$ com $Ra_i \simeq R$ semisimples. Assim, F é semisimples, e portanto, usando o Teorema do Isomorfismo e o Corolário 1.37 vem que $\dfrac{F}{\mathrm{Ker}\,(f)} \simeq f(F) = M$ é semisimples.

(2) $\Rightarrow$ (3) Uma vez que os submódulos simples de R são exatamente os ideais minimais à esquerda de R, segue do Teorema 1.35, que R pode ser escrito na forma $R = \bigoplus_{i \in I} L_i$ em que cada L_i é um ideal minimal à esquerda. Resta-nos mostrar que esta soma é finita.

Com efeito, como $1 \in R$ podemos escrever $1 = x_{i_1} + x_{i_2} + \ldots + x_{i_n}$ com $x_{i_j} \in L_{i_j}$. Então, dado um elemento arbitrário $r \in R$, temos que $r = r.1 = rx_{i_1} + rx_{i_2} + \ldots + rx_{i_n}$ e $rx_{i_j} \in L_{i_j}$, $1 \leq j \leq n$. Isso mostra que $R \subset L_{i_1} \oplus L_{i_2} \oplus \ldots \oplus L_{i_n}$, e portanto, $R = L_{i_1} \oplus L_{i_2} \oplus \ldots \oplus L_{i_n}$.

(3) $\Rightarrow$ (2) Segue do Teorema 1.35. ■

Exemplo 1.40. Consideremos o anel de matrizes $n \times n$ sobre um anel com divisão D, denotado por $M_n(D)$. Vamos mostrar que este anel é semisimples. Definamos:

$$L_1 = \begin{pmatrix} D & 0 & \dots & 0 \\ D & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ D & 0 & \dots & 0 \end{pmatrix}, L_2 = \begin{pmatrix} 0 & D & \dots & 0 \\ 0 & D & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & D & \dots & 0 \end{pmatrix}, \dots, L_n = \begin{pmatrix} 0 & 0 & \dots & D \\ 0 & 0 & \dots & D \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & D \end{pmatrix}.$$

Claramente cada L_i é um ideal à esquerda de $M_n(D)$. Outro ideal de $M_n(D)$ contido em L_i seria da forma:

$$I_i = \begin{pmatrix} 0 & \dots & I & \dots & 0 \\ 0 & \dots & I & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & I & \dots & 0 \end{pmatrix},$$

onde I é um ideal à esquerda de D. Mas como D é um anel com divisão, devemos ter $I = (0)$ ou $I = D$. Portanto, L_i é minimal para todo $1 \leq i \leq n$. Além disso, é fácil ver que $M_n(D) = L_1 \oplus L_2 \oplus \ldots \oplus L_n$. Logo, pelo Teorema 1.39 obtemos que $M_n(D)$ é semisimples.

Definição 1.41. Um elemento e em um anel R é chamado *idempotente*, se $e^2 = e$. Claramente, 0 e 1 são elementos idempotentes, os quais são chamados *idempotentes triviais*.

A seguir, mostraremos que todo ideal à esquerda de um anel semisimples é gerado por um idempotente.

Teorema 1.42. *Seja R um anel. Então, R é semisimples se, e somente se, todo ideal à esquerda de R é da forma $L = Re$, onde $e \in R$ é idempotente.*

Demonstração: Suponhamos que R é semisimples e seja L um ideal à esquerda de R. O fato que R é semisimples implica que L é um somando direto, ou seja, existe L' ideal à esquerda de R tal que $R = L \oplus L'$. Como $1 \in R$ temos que $1 = x + y$ com $x \in L$ e $y \in L'$, disso segue que $x = x.1 = x^2 + xy$. Assim $xy = x - x^2 \in L$ e, como

L' é um ideal à esquerda, temos também que $xy \in L'$. Em virtude de $L \cap L' = (0)$ vem $xy = 0$ e, conseqüentemente, $x = x^2$ é idempotente. Agora vamos mostrar que $Rx = L$. Como L é um ideal à esquerda e $x \in L$ concluímos de imediato que $Rx \subset L$. Para mostrarmos que $L \subset Rx$ tomemos $a \in L$ e vejamos que $a = a.1 = ax + ay$, assim $a - ax = ay \in L \cap L' = (0)$. Isso implica $a = ax \in Rx$ e, concluímos que $L \subset Rx$, como queríamos.

Reciprocamente, assumimos que todos ideais à esquerda de R são como na hipótese. Temos que mostrar que R visto como um R-módulo é semisimples, ou seja, que todo ideal à esquerda L de R é um somando direto. Por hipótese, um ideal L é da forma $L = Re$, com $e \in R$ idempotente. Definimos $L' = R(1 - e)$ e afirmamos que $R = L \oplus L'$. Com efeito, dado um elemento $x \in R$ sempre podemos escrever $x = xe + x(1 - e)$, isso implica que $R = Re + R(1 - e)$. Além disso, se $x \in Re \cap R(1 - e)$, segue que $x = re = s(1 - e)$, para $r, s \in R$. Então $xe = re.e = re^2 = re = x$, por outro lado temos que $xe = s(1 - e)e = se - se^2 = se - se = 0$, disso vem $x = 0$. Logo, $Re \cap R(1 - e) = (0)$ e, portanto, $R = L \oplus L'$. ■

Mostraremos agora que os idempotentes que geram os ideais minimais à esquerda da decomposição de R têm algumas propriedades.

Teorema 1.43. *Seja* $R = \bigoplus_{i=1}^{t} L_i$ *uma decomposição de um anel semisimples* R *como soma direta de ideais minimais à esquerda. Então, existe uma família* $\{e_1, e_2, \ldots, e_t\}$ *de elementos de* R *tal que:*

(i) $e_i \neq 0$ *é um elemento idempotente,* $1 \leq i \leq t$.

(ii) Se $i \neq j$ *então* $e_i e_j = 0$.

(iii) $1 = e_1 + e_2 + \ldots + e_t$.

(iv) e_i *não pode ser escrito como* $e_i = e_i' + e_i''$, *com* e_i', e_i'' *idempotentes tais que* $e_i', e_i'' \neq 0$ *e* $e_i'.e_i'' = 0$, $1 \leq i \leq t$.

Reciprocamente, se existir uma família de idempotentes $\{e_1, e_2, \ldots, e_t\}$ *satisfazendo as condições acima, então os ideais à esquerda* $L_i = Re_i$ *são minimais e* $R = \bigoplus_{i=1}^{t} L_i$.

Demonstração: Consideremos $R = \bigoplus_{i=1}^{t} L_i$ uma decomposição do anel semisimples R como soma direta de ideais minimais à esquerda e escrevemos $1 = e_1 + e_2 + \ldots + e_t$ com $e_i \in L_i$. Então, de maneira análoga à demonstração do Teorema 1.42 podemos concluir que cada e_i é idempotente, $L_i = Re_i$, $1 \leq i \leq t$, e que $i \neq j$ implica $e_i.e_j = 0$. Finalmente, se para algum índice i pudermos escrever $e_i = e_i^{'} + e_i^{''}$, onde $e_i^{'}, e_i^{''}$ são idempotentes tais que $e_i^{'}, e_i^{''} \neq 0$ e $e_i^{'}.e_i^{''} = 0$, então teremos $L_i = Re_i^{'} \oplus Re_i^{''}$ com $Re_i^{'}, Re_i^{''} \neq 0$, contradizendo a minimalidade de L_i.

Reciprocamente, suponhamos que existe uma família de idempotentes $\{e_1, e_2, \ldots, e_t\}$ satisfazendo as condições acima. Primeiramente, provemos que cada ideal $L_i = Re_i$ é minimal, $1 \leq i \leq t$. De fato, se L_i não fosse minimal, existiria um submódulo próprio J contido em L_i. Como R é um R-módulo semisimples, L_i também seria semisimples, assim existiria outro submódulo $J^{'}$ de L_i tal que $L_i = J \oplus J^{'}$. Com isso poderíamos escrever $e_i = e_i^{'} + e_i^{''}$, com $e_i^{'}, e_i^{''}$ idempotentes tais que $e_i^{'}, e_i^{''} \neq 0$ e $e_i^{'}.e_i^{''} = 0$, que contradiria o item (iv). Logo, L_i é minimal. O fato que $R = L_1 + L_2 + \ldots + L_t$ segue imediatamente da condição (iii). Para provarmos que esta soma é direta tomemos $x \in L_j \cap \left(\sum_{i \neq j} L_i \right)$, logo, $x = r_j e_j = \sum_{i \neq j} r_i e_i$. Multiplicando a última igualdade à direita por e_j obtemos $r_j e_j^2 = r_j e_j = x = \sum_{i \neq j} r_i e_i e_j = 0$, ou seja, $L_j \cap \left(\sum_{i \neq j} L_i \right) = (0)$, como queríamos. ■

Definição 1.44. Dois idempotentes satisfazendo a condição (ii) são chamados *ortogonais*, e um idempotente satisfazendo a condição (iv) é dito *primitivo*. Também, se para um idempotente $e \in R$ ocorre $e.a = a.e$, para todo $a \in R$, dizemos que e é um idempotente *central*.

Pelo que já estudamos, percebemos que é importante saber se um anel R é semisimples, pois se isso ocorre, temos pelo Teorema 1.39, que todo R-módulo é semisimples e, portanto, é uma soma direta de R-módulos simples. Concluiremos esta seção mostrando que todo R-módulo simples é determinado, a menos de isomorfismo, pelos ideais minimais à esquerda dados na decomposição de R. Antes disso, mostraremos um resultado auxiliar.

Lema 1.45. *Sejam L um ideal minimal à esquerda de um anel semisimples R e M um R-módulo simples. Então, $LM \neq (0)$ se, e somente se, $L \simeq M$ como R-módulos, neste caso $LM = M$.*

Demonstração: Suponhamos que $LM \neq (0)$. Assim existem $x \in L$ e $m \in M$ tais que $xm \neq 0$, conseqüentemente, $Lm \neq (0)$. Como Lm é um submódulo de M que é simples e $Lm \subset LM \subset M$, obtemos $Lm = LM = M$. Agora consideremos a aplicação $f : L \to M$ dada por $a \mapsto am$. Claramente f é um homomorfismo sobrejetor de R-módulos, como $x \in L$ e $f(x) = xm \neq 0$ devemos ter $x \notin \mathrm{Ker}\,(f)$, e portanto, $\mathrm{Ker}\,(f) \neq L$. Agora, o fato que $\mathrm{Ker}\,(f) \neq L$ é um submódulo de L, que é minimal, implica que $\mathrm{Ker}\,(f) = (0)$, mostrando que f também é injetora. Logo, $L \simeq M$.

Reciprocamente, assumimos que $L \simeq M$ como R-módulos e seja $f : L \to M$ um isomorfismo. Como R é semisimples, existe um elemento idempotente $e \in R$ tal que $L = Re$. Uma vez que f é um isomorfismo e $0 \neq e \in L$, existe $m_0 \in M$ tal que $m_0 \neq 0$ e $f(e) = m_0$. Assim obtemos $m_0 = f(e) = f(e^2) = ef(e) = em_0 \neq 0$, o que implica $LM \neq (0)$, como queríamos. ■

Proposição 1.46. *Seja $R = \bigoplus_{i=1}^{t} L_i$ uma decomposição de um anel semisimples R como soma direta de ideais minimais à esquerda. Então, todo R-módulo simples é isomorfo a um ideal L_i dado na decomposição de R.*

Demonstração: Consideremos $R = \bigoplus_{i=1}^{t} L_i$ uma decomposição de R como soma direta de ideais minimais à esquerda e seja M um R-módulo simples. Uma vez que M é simples, temos que $M \neq (0)$, logo, existe $m \in M$ tal que $m \neq 0$. Disso segue que $0 \neq m = 1.m \in RM$, e portanto, $RM \neq 0$. Agora, como $RM \neq (0)$ é um submódulo de M que é simples, segue que $RM = M$. Mas $RM = \bigoplus_{i=1}^{t} L_i M$, assim, deve existir algum índice j tal que $L_j M \neq (0)$. Portanto, usando o lema anterior, concluímos que $L_j \simeq M$. ■

1.4 O Teorema de Wedderburn-Artin

Nesta seção, vamos descrever a estrutura de um anel semisimples. Para tanto, precisamos de mais informações sobre seus ideais bilaterais.

Lema 1.47. *Seja L um ideal minimal à esquerda de um anel semisimples R. Então, a soma de todos ideais à esquerda de R isomorfos a L é um ideal bilateral de R.*

Demonstração: Definamos $A = \sum_{J \simeq L} J$. Temos que A é um ideal à esquerda, pois toda soma de ideais à esquerda é um ideal à esquerda. Vamos mostrar que A também é ideal à direita. Como R é um anel semisimples, podemos decompor R da forma $R = \bigoplus_{i=1}^{t} L_i$, sendo cada L_i um ideal minimal à esquerda. Assim temos que $AR = \sum_{J \simeq L} JR = \sum_{J \simeq L} \sum_{i=1}^{t} JL_i$. Como $JL_i \subset L_i$, que é minimal, segue que $JL_i = (0)$ ou $JL_i = L_i$. Mas, pelo Lema 1.45, a última alternativa acontece quando $J \simeq L_i$, isto é, quando $L_i \simeq L$ e, conseqüentemente, $L_i \subset A$. Logo, devemos ter $AR \subset A$, como queríamos. ■

Lema 1.48. *Seja I um ideal bilateral de um anel semisimples R contendo um ideal minimal à esquerda L. Então, I contém todos ideais à esquerda isomorfos a L.*

Demonstração: Tomemos $L \subset I$ um ideal minimal à esquerda de R e seja J um ideal à esquerda isomorfo a L. Mostremos que $J \subset I$. O fato que $J \simeq L$ implica que J também é minimal. Mais ainda, pelo Lema 1.45 temos que $LJ \neq (0)$. Agora, sendo $LJ \neq (0)$ ideal de J que é minimal, segue que $LJ = J$. Como $L \subset I$ e I é um ideal bilateral de R devemos ter $LJ \subset I$. Com isso concluímos que $J = LJ \subset I$. ■

Proposição 1.49. *Sejam L um ideal minimal à esquerda de um anel semisimples R e B a soma de todos ideais à esquerda de R isomorfos a L. Então, B é um ideal minimal bilateral de R.*

Demonstração: Pelo Lema 1.47 já temos que B é um ideal bilateral. Resta-nos mostrar que B é minimal.

Consideremos $B^{'} \neq (0)$ um ideal bilateral de R contido em B. Vamos mostrar que $B^{'} = B$. Primeiramente observemos que esse ideal existe, na pior das hipóteses poderia ser B. Agora, se $L^{'}$ é um ideal minimal à esquerda de R contido em $B^{'}$, vamos mostrar que $L^{'} \simeq L$. Suponhamos que $L^{'} \not\simeq L$, então para todo ideal $J \simeq L$ devemos ter $J \not\simeq L^{'}$ e, pela contrapositiva do Lema 1.45, obtemos $L^{'}J = (0)$. Uma vez que B é constituído da soma desses ideais $J \simeq L$ e $L^{'}J = (0)$, então $L^{'}B = (0)$. Em particular, $L^{'}L^{'} = (0)$, visto que $L^{'} \subset B$. Mas isso não pode ocorrer, pois, como R é semisimples, temos $L^{'} = Re$, e portanto, $0 \neq e = e^2 \in L^{'}L^{'}$. Assim, necessariamente $L^{'} \simeq L$. Notemos que $B^{'}$ é um ideal bilateral do anel semisimples R e $L^{'}$ é um ideal minimal à esquerda de $B^{'}$, assim pelo Lema 1.48 temos que $B^{'}$ contém todos ideais à esquerda isomorfos a $L^{'}$. Como $L^{'} \simeq L$, segue que $B^{'}$ contém todos ideais à esquerda isomorfos a L. Dessa forma, temos $B = \sum_{J \simeq L} J \subset B^{'} \subset B$. Portanto, $B^{'} = B$. ■

Observação 1.50. Dada uma decomposição de um anel semisimples R como soma direta de ideais minimais à esquerda, reordenando se necessário, podemos agrupar os ideais isomorfos:

$$R = \underbrace{L_{11} \oplus L_{12} \oplus \ldots \oplus L_{1r_1}} \oplus \underbrace{L_{21} \oplus L_{22} \oplus \ldots \oplus L_{2r_2}} \oplus \ldots \oplus \underbrace{L_{s1} \oplus L_{s2} \oplus \ldots \oplus L_{sr_s}}.$$

Com essa notação $L_{ij} \simeq L_{ih}$. Além disso, se $i \neq k$ então $L_{ij} \not\simeq L_{kh}$. Usando a contrapositiva do Lema 1.45 obtemos $L_{ij}L_{kh} = (0)$, para $i \neq k$. Ainda, segue da Proposição 1.46, que todos ideais minimais à esquerda são isomorfos a um dos ideais de R dado na decomposição acima.

Teorema 1.51. *Mantendo a notação acima, denotamos por A_i a soma de todos ideais à esquerda de R isomorfos a L_{i1}, $1 \leq i \leq s$. Então:*

(i) Cada A_i é um ideal minimal bilateral de R.

(ii) $A_iA_j = (0)$ se $i \neq j$.

(iii) $R = \bigoplus_{i=1}^{s} A_i$ como anéis, onde s é o número de classes de isomorfismo de ideais minimais à esquerda de R.

Demonstração: *(i)* Uma vez que L_{i1} é um ideal minimal à esquerda e A_i é a soma de todos ideais isomorfos L_{i1}, segue da Proposição 1.49 que A_i é um ideal minimal bilateral de R.

(ii) Temos que $A_iA_j = \sum_{k=1}^{r_i} \sum_{h=1}^{r_j} L_{ik}L_{jh}$ e se $i \neq j$, então $L_{ik}L_{jh} = (0)$ para todo $1 \leq k \leq r_i$ e $1 \leq h \leq r_j$. Portanto, $A_iA_j = (0)$.

(iii) Primeiramente, vamos mostrar que $R = \sum_{i=1}^{s} A_i$. Observemos que R pode ser escrito como:

$$R = \underbrace{L_{11} \oplus L_{12} \oplus \ldots \oplus L_{1r_1}} \oplus \underbrace{L_{21} \oplus L_{22} \oplus \ldots \oplus L_{2r_2}} \oplus \ldots \oplus \underbrace{L_{s1} \oplus L_{s2} \oplus \ldots \oplus L_{sr_s}}.$$

Disso segue que se $x \in R$, então podemos escrever x da seguinte forma:

$$x = \underbrace{x_{11} + x_{12} + \ldots + x_{1r_1}} + \underbrace{x_{21} + x_{22} + \ldots + x_{2r_2}} + \ldots + \underbrace{x_{s1} + x_{s2} + \ldots + x_{sr_s}},$$

com $x_{ij} \in L_{ij}$. Definamos $y_i = x_{i1} + x_{i2} + \ldots + x_{ir_i}$, $1 \leq i \leq s$. Então $y_i \in A_i$, $1 \leq i \leq s$ e $x = y_1 + y_2 + \ldots + y_s$. Portanto, $R = \sum_{i=1}^{s} A_i$. Que esta soma é direta segue do fato que $R = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{r_i} L_{ij}$. ■

Definição 1.52. Um anel R é chamado *simples* se (0) e R são os únicos ideais bilaterais de R.

Exemplo 1.53. Se D é um anel com divisão, então $M_n(D)$ é um anel simples.

De fato, tomemos I um ideal bilateral de $M_n(D)$ tal que $I \neq (0)$, vamos mostrar que $I = M_n(D)$. O fato que $I \neq (0)$ implica que existe uma matriz $A \in I$ tal que $A \neq 0$, ou seja, pelo menos uma entrada da matriz A deve ser diferente de zero, digamos a_{hk}. Consideremos as matrizes elementares $E_{ij} \in M_n(D)$ com 1 na entrada (i, j) e 0 nas demais. Coloquemos $B_i = E_{ih}AE_{ki}$ e vejamos que B_i possui o elemento 0 em todas entradas exceto a entrada (i, i) que possui o elemento a_{hk}, isto é, $B_i = a_{hk}E_{ii}$.

Como I é um ideal bilateral e $A \in I$ devemos ter que $B_i = E_{ih}AE_{ki} \in I$ para todo $1 \leq i \leq n$. Logo, $B = B_1 + \ldots + B_n \in I$. Notemos que B é uma matriz diagonal e todos elementos da diagonal são iguais a $a_{hk} \neq 0$. Logo, B é inversível, e portando, $I = M_n(D)$, como desejávamos.

Corolário 1.54. *Os ideais A_i, do Teorema 1.51, são anéis simples.*

Demonstração: Como cada A_i é um ideal minimal bilateral de R, basta mostrarmos que qualquer ideal bilateral B_i de A_i também é um ideal bilateral de R, e assim, teremos $B_i = (0)$ ou $B_i = A_i$.

Para isso tomemos $b \in B_i$ e $r \in R$. Podemos escrever $r = x_1 + x_2 + \ldots + x_s$ com $x_j \in A_j$, para todo $1 \leq j \leq s$. Então, $r.b = \sum_{j=1}^{s} x_j b$. Observemos que $x_j b = 0$ se $j \neq i$, pois $x_j \in A_j$, $b \in A_i$ e $A_j A_i = (0)$ se $i \neq j$. Disso segue que $rb = x_i b \in B_i$.

Portanto, $RB_i \subset B_i$. Analogamente, mostramos que $B_iR \subset B_i$ e concluímos que B_i é um ideal bilateral de R. ■

Podemos agora caracterizar todos os ideais bilaterais de R utilizando os ideais A_i construídos no Teorema 1.51.

Proposição 1.55. *Seja* $R = \bigoplus_{i=1}^{s} A_i$ *uma decomposição de um anel semisimples* R *como soma direta de ideais minimais bilaterais. Então*

(i) *Todo ideal bilateral* I *de* R *pode ser escrito na forma* $A_{i_1} \oplus A_{i_2} \oplus \ldots \oplus A_{i_t}$, *com* $1 \leq i_1 < \ldots < i_t \leq s$.

(ii) *Se* $R = \bigoplus_{j=1}^{r} B_i$ *é outra decomposição de* R *como soma direta de ideais minimais bilaterais, então* $s = r$, *e depois de uma possível renumeração de índices,* $A_i = B_i$, *para todo* $1 \leq i \leq s$.

Demonstração: (i) Seja I um ideal bilateral de R. Então $I = \bigoplus_{i=1}^{s}(A_i \cap I)$. Como cada A_i é um ideal minimal bilateral e $A_i \cap I$ é um ideal bilateral de A_i, segue que $A_i \cap I = (0)$ ou $A_i \cap I = A_i$. Portanto, $I = A_{i_1} \oplus A_{i_2} \oplus \ldots \oplus A_{i_t}$, com $1 \leq i_1 < \ldots < i_t \leq s$.

(ii) Como cada B_j é um ideal bilateral de R, por (i), temos que $B_j = A_{i_1} \oplus A_{i_2} \oplus \ldots \oplus A_{i_t}$, com $1 \leq i_1 < \ldots < i_t \leq s$. Além disso, temos também que B_j é minimal, assim devemos ter apenas um A_i na decomposição de B_j, e assim $A_i = B_j$. Reordenando, se necessário, podemos concluir que $A_i = B_i$, para todo $1 \leq i \leq s$. ■

Definição 1.56. Se $R = \bigoplus_{i=1}^{s} A_i$ é a decomposição de um anel semisimples como soma direta de ideais minimais bilaterais, então os anéis simples A_i são chamados *componentes simples* de R.

Veremos no próximo teorema que a decomposição de R como soma direta de ideais minimais bilaterais esta relacionada com uma família especial de idempotentes.

Teorema 1.57. *Seja* $R = \bigoplus_{i=1}^{s} A_i$ *a decomposição de um anel semisimples* R *como soma direta de ideais minimais bilaterais. Então, existe uma família* $\{e_1, e_2, \ldots, e_s\}$, *de elementos de* R *tal que:*

(i) $e_i \neq 0$ *é um elemento idempotente central,* $1 \leq i \leq s$.

(ii) *Se* $i \neq j$ *então* $e_i e_j = 0$.

(iii) $1 = e_1 + e_2 + \ldots + e_s$.

(iv) e_i *não pode ser escrito como* $e_i = e_i^{'} + e_i^{''}$, *com* $e_i^{'}, e_i^{''}$ *idempotentes centrais tais que* $e_i^{'}, e_i^{''} \neq 0$ *e* $e_i^{'}.e_i^{''} = 0$, $1 \leq i \leq s$.

Reciprocamente, se existir uma família de idempotentes $\{e_1, e_2, \ldots, e_t\}$ *satisfazendo as condições acima, então os ideais* $A_i = Re_i$ *são minimais bilaterais e* $R = \bigoplus_{i=1}^{t} A_i$.

Demonstração: A prova é análoga a do Teorema 1.43, resta-nos mostrar que cada e_i, $1 \leq i \leq s$, é central. Dado $x \in R$, temos que $1.x = x = x.1$, assim por (iii), obtemos $x = \sum_{i=1}^{s} xe_i = \sum_{i=1}^{s} e_i x$. Uma vez que cada A_i é um ideal bilateral, devemos ter $xe_i, e_i x \in A_i$. Agora, usando o fato que a soma é direta, concluímos que $xe_i = e_i x$. ■

Observação 1.58. Uma outra propriedade importante é que e_i é o elemento identidade sobre o anel A_i. De fato, dado $x_i \in A_i$, temos que $x_i = x_i.1 = x_i(e_1 + \ldots + e_l) = x_i e_1 + \ldots + x_i e_l$. Como $x_i e_j \in A_i A_j = (0)$ se $i \neq j$, segue que $x_i = x_i e_i$

Definição 1.59. Uma família de idempotentes $\{e_1, \ldots, e_s\}$ satisfazendo as condições do teorema acima é chamada *família completa de idempotentes primitivos centrais.*

Teorema 1.60. *Se* I *é um ideal bilateral de um anel semisimples* R, *então* $I = Re$, *onde* e *é um idempotente central de* R.

Demonstração: Suponhamos que R é semisimples e seja $R = \bigoplus_{i=1}^{s} A_i$ a decomposição de R como no Teorema 1.51. Para cada j temos que $I \cap A_j = (0)$ ou

$I \cap A_j = A_j$, visto que A_j é simples. Reordenando, se necessário, podemos assumir que $I \cap A_j = A_j$ para $1 \leq j \leq t$ e $I \cap A_j = (0)$ para $j = t+1, \ldots, s$. Notemos que, dessa forma $A_j \subset I$ para $j = 1, 2, \ldots, t$. Consideremos $\{e_1, \ldots, e_s\}$ a família de idempotentes primitivos centrais de R e definamos $e = e_1 + \ldots + e_t \in I$. É fácil verificarmos que $e^2 = e$. Uma vez que cada e_i é central, segue que $xe = xe_1 + \ldots + xe_t = e_1x + \ldots + e_tx = ex$, para todo $x \in R$. Logo, e é um idempotente central de R.

Agora mostremos que $I = Re$. Com efeito, como I é um ideal e $e \in I$ temos que $Re \subset I$. Por outro lado, se $u \in I$, então $u = u.1 = u(e_1 + \ldots + e_s) = ue_1 + \ldots + ue_s$. Mas para $j > t$, temos que $ue_j \in I \cap A_j = (0)$. Disso segue que $u = ue_1 + \ldots + ue_t = ue \in Re$. Portanto, $I = Re$. ■

Vimos que R tem uma decomposição como soma direta de componentes simples, quando R for um anel semisimples. Mostraremos adiante que cada componente simples é isomorfa a um anel de matrizes sobre um anel de divisão. Para tanto, precisamos de alguns resultados auxiliares.

Lema 1.61. *Seja R um anel e seja $M = M_1 \oplus \ldots \oplus M_r$ e $N = N_1 \oplus \ldots \oplus N_s$ dois R-módulos escrito como soma direta de submódulos. Sejam $\varepsilon_j : M_j \to M$ a inclusão de cada M_j em M e $\pi_i : N \to N_i$ o homomorfismo natural de N sobre seus componentes.*

(i) Suponhamos que, para cada par de índices i, j temos um homomorfismo $\phi_{ij} \in Hom_R(M_j, N_i)$. Então, a aplicação $\phi : M \to N$ definida por:

$$\phi(m_1 + m_2 + \ldots + m_r) = \begin{pmatrix} \phi_{11} & \phi_{12} & \ldots & \phi_{1r} \\ \phi_{21} & \phi_{22} & \ldots & \phi_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{s1} & \phi_{s2} & \ldots & \phi_{sr} \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix}$$

$$= \underbrace{\phi_{11}(m_1) + \ldots + \phi_{1r}(m_r)}_{\in N_1} + \underbrace{\phi_{21}(m_1) + \ldots + \phi_{2r}(m_r)}_{\in N_2} + \ldots + \underbrace{\phi_{s1}(m_1) + \ldots + \phi_{sr}(m_r)}_{\in N_s},$$

é um homomorfismo. Para indicar que ϕ é dada como na forma acima denotamos $\phi = (\phi_{ij})$.

(ii) Se $\phi \in Hom_R(M,N)$*, então* $\phi_{ij} = \pi_i \circ \phi \circ \varepsilon_j \in Hom_R(M_j, N_i)$ *e* $\phi = (\phi_{ij})$.

(iii) Para $\phi = (\phi_{ij})$ *e* $\psi = (\psi_{ij})$*, temos* $\phi + \psi = (\phi_{ij} + \psi_{ij})$.

A demonstração será omitida, por ser extensa, mas é bem simples e direta.

Corolário 1.62. *Seja* R *um anel e* M *um* R*-módulo, então* $Hom_R(M^{(n)}, M^{(n)}) \simeq M_n(Hom_R(M,M))$*, como anéis.*

Demonstração: Basta considerarmos a aplicação $\psi : M_n(Hom_R(M,M)) \to Hom_R(M^{(n)}, M^{(n)})$, que associa cada matriz $(\phi_{ij}) \in M_n(Hom_R(M,M))$ à função $\phi : M^{(n)} \to M^{(n)}$ dada por

$$\phi(m_1 + \ldots + m_n) = \underbrace{\phi_{11}(m_1) + \ldots + \phi_{1n}(m_n)}_{\in M} + \ldots + \underbrace{\phi_{n1}(m_1) + \ldots + \phi_{nn}(m_n)}_{\in M}.$$

Não é difícil, apesar de trabalhoso, mostrar que ψ é um isomorfismo de anéis. ■

Lema 1.63. *Seja* R *um anel,* M *um* R*-módulo semisimples e* $B = Hom_R(M,M)$*. Então,* M *admite uma estrutura de* B*-módulo dada por* $\phi.m = \phi(m)$*, para todo* $\phi \in B$*, e todo* $m \in M$*. Além disso, para cada* $m \in M$ *e* $f \in Hom_B(M,M)$*, existe um elemento* $a \in R$ *tal que* $f(m) = am$.

Demonstração: Sabemos que M é um R-módulo, assim, já temos que M é um grupo abeliano para soma. Também, é fácil verificarmos que M satisfaz as demais propriedades de B-módulo.

Mostraremos que para cada $m \in M$ e $f \in Hom_B(M,M)$, existe um elemento $a \in R$ tal que $f(m) = am$. De fato, seja $m \in M$. Notemos que Rm é um submódulo de M, como M é semisimples, existe um submódulo W de M tal que $M = Rm \oplus W$. Se denotarmos por $\pi : M \to M$ a projeção sobre Rm, temos que $\pi \in Hom_R(M,M) = B$. Dado um elemento $f \in Hom_B(M,M)$ obtemos

$$f(m) = f(\pi(m)) = f(\pi.m) = \pi(f(m)) \in Rm.$$

Logo, existe um elemento $a \in R$ tal que $f(m) = am$. ■

Teorema 1.64. (Densidade de Jacobson) *Sejam M um R-módulo semisimples e $B = Hom_R(M, M)$. Se $f \in Hom_B(M, M)$ e $\{m_1, \ldots, m_n\}$ é um conjunto arbitrário de elementos de M, então existe um elemento $b \in R$ tal que $f(m_i) = bm_i$ para todo $1 \leq i \leq n$.*

Demonstração: Dado $f \in Hom_B(M, M)$, definimos $f^{(n)} : M^{(n)} \to M^{(n)}$ por

$$f^{(n)}(x_1 + \ldots + x_n) = f(x_1) + \ldots + f(x_n), \quad x_1, \ldots, x_n \in M.$$

Seja $B' = Hom_R(M^{(n)}, M^{(n)})$. Vamos mostrar que $f^{(n)} \in Hom_{B'}(M^{(n)}, M^{(n)})$.

De fato, se $a, b \in M^{(n)}$, é claro que $f^{(n)}(a+b) = f^{(n)}(a) + f^{(n)}(b)$. Agora, dado $\phi \in B'$, pelo Corolário 1.62, podemos escrever $\phi = (\phi_{ij})$ com $\phi_{ij} \in Hom_R(M, M)$. Logo,

$$\begin{aligned}
&(f^{(n)} \circ \phi)(m_1 + \ldots + m_n) = f^{(n)}(\phi(m_1 + \ldots + m_n)) \\
&= f^{(n)}(\underbrace{\phi_{11}(m_1) + ... + \phi_{1n}(m_n)}_{\in M} + ... + \underbrace{\phi_{n1}(m_1) + ... + \phi_{nn}(m_n)}_{\in M}) \\
&= f(\phi_{11}(m_1) + ... + \phi_{1n}(m_n)) + ... + f(\phi_{n1}(m_1) + ... + \phi_{nn}(m_n)) \\
&= f(\phi_{11}(m_1)) + \ldots + f(\phi_{1n}(m_n)) + \ldots + f(\phi_{n1}(m_1)) + \ldots + f(\phi_{nn}(m_n)) \\
&= \phi_{11}(f(m_1)) + \ldots + \phi_{1n}(f(m_n)) + \ldots + \phi_{n1}(f(m_1)) + \ldots + \phi_{nn}(f(m_n)) \\
&= \phi(f(m_1) + \ldots + f(m_n)) = (\phi \circ f^{(n)})(m_1 + \ldots + m_n).
\end{aligned}$$

E podemos concluir que $f^{(n)} \in Hom_{B'}(M^{(n)}, M^{(n)})$. Pelo lema anterior, existe um elemento $b \in R$ tal que

$$f^{(n)}(m_1 + \ldots + m_n) = b(m_1 + \ldots + m_n).$$

Portanto, $f(m_i) = bm_i$ para todo $1 \leq i \leq n$. ■

Lema 1.65. (Schur) *Sejam R um anel e M, N R-módulos simples. Se $f : M \to N$ é um homomorfismo não-nulo, então f é um isomorfismo.*

Demonstração: Suponhamos que $f : M \to N$ é um homomorfismo não-nulo, assim $\mathrm{Im}(f) \neq (0)$, uma vez que $\mathrm{Im}(f)$ é um submódulo de N que é simples, devemos

ter $\mathrm{Im}(f) = N$, isso implica que f é sobrejetora. Analogamente, $\mathrm{Ker}\,(f) \neq M$ é um submódulo de M que também é simples. Logo, $\mathrm{Ker}\,(f) = (0)$, ou seja, f é injetora, e portanto, um isomorfismo. ■

Corolário 1.66. *Sejam R um anel e M, N R-módulos simples. Então*

(i) Se $M \ncong N$, então $Hom_R(M, N) = (0)$.

(ii) $Hom_R(M, M)$ é um anel de divisão.

Demonstração: (*i*) Sejam M, N R-módulos simples, dado $f \in Hom_R(M, N)$, como $M \ncong N$, temos que f não pode ser um isomorfismo. Logo, pela contrapositiva do Lema de Schur 1.65, f é o homomorfismo nulo, e portanto, $Hom_R(M, N) = (0)$.

(*ii*) Tomemos $f \in Hom_R(M, M)$ com $f \neq 0$, então pelo Lema de Schur 1.65, f é um isomorfismo, e portanto, f é inversível. ■

Proposição 1.67. *Seja M um R-módulo livre com base $\{m_i : i \in I\}$. Seja N um R-módulo e para cada $i \in I$ considere n_i um elemento de N. Então existe um único homomorfismo $f : M \to N$ de R-módulos tal que $f(m_i) = n_i$, para todo $i \in I$.*

Demonstração: Dado $m \in M$, existem únicos $a_1, \ldots, a_n \in A$ tais que $m = \sum_{i=1}^{n} a_i m_i$. Definamos $f : M \to N$ por $f(m) = \sum_{i=1}^{n} a_i n_i$. Logo, $f(m_i) = n_i$ para todo $i \in I$. Como os a_i's são únicos, f está bem definida e é fácil verificarmos que f é um homomorfismo.

Para mostrar a unicidade, suponha que exista $g : M \to N$ homomorfismo tal que $g(m_i) = n_i$. Assim, dado $m = \sum_{i=1}^{n} a_i m_i \in M$ temos que

$$g(m) = g(\sum_{i=1}^{n} a_i m_i) = \sum_{i=1}^{n} a_i g(m_i) = \sum_{i=1}^{n} a_i n_i = f(m).$$

Portanto, $f = g$, e assim, f é única. ■

Nos próximos resultados iremos utilizar o conceito de anel Artiniano à esquerda. Recordemos que um anel R é dito Artiniano à esquerda se qualquer cadeia decrescente de ideais à esquerda

$$I_1 \supset I_2 \supset \ldots \supset I_i \supset \ldots$$

estaciona, ou seja, existe um índice t tal que $I_t = I_{t+i}$ para $i \geq 1$.

Lema 1.68. *Sejam R um anel Artiniano à esquerda semisimples e M um R-módulo simples. Consideremos o anel com divisão $D = Hom_R(M, M)$. Então, M visto como um D-módulo é de dimensão finita.*

Demonstração: Seja M um D-módulo e $\{m_1, \ldots, m_n, \ldots\}$ uma base infinita de M sobre D. Para cada índice t, definamos:

$$A_t = \{a \in R : am_i = 0, 1 \leq i \leq t\}.$$

Temos que A_t é um ideal à esquerda e que $A_t \supset A_{t+1}$, $t = 1, 2, \ldots, n, \ldots$

Vamos mostrar que esta inclusão é estrita. Com efeito, uma vez que M é um R-módulo simples, segue que $M \neq (0)$ e, conseqüentemente, existe $m \in M$ tal que $m \neq 0$. Agora, considerando o subconjunto $\{0, m\}$ de M, pela proposição anterior existe $f : M \to M$ homomorfismo de D-módulos tal que

$$f(m_i) = \begin{cases} 0, \text{ se } i \neq t+1 \\ m, \text{ se } i = t+1. \end{cases}$$

Sendo $\{m_1, \ldots, m_{t+1}\}$ um subconjunto de M e $f \in Hom_D(M, M)$ segue do Teorema de Jacobson 1.64 que existe $a \in R$ tal que $f(m_i) = am_i$, $1 \leq i \leq t+1$. Como $am_i = f(m) = 0$, se $1 \leq i \leq t$, e $am_{t+1} = f(m_{t+1}) = m \neq 0$, obtemos que $a \in A_t$ e $a \notin A_{t+1}$, ou seja, $A_t \supsetneq A_{t+1}$. Portanto, se $\{m_1, \ldots, m_n, \ldots\}$ for infinito, teremos uma cadeia de ideais à esquerda estritamente decrescente

$$A_1 \supset A_2 \supset \ldots \supset A_t \supset \ldots$$

contrariando o fato de R ser um anel Artiniano à esquerda. ■

Definição 1.69. Seja A um anel, denotamos por A° o *anel oposto de* A, isto é, o anel definido sobre o mesmo conjunto, usando a mesma adição de A, mas com produto em A° dado por $x \circ y = yx$, onde yx denota a multiplicação de y e x em A.

Observação 1.70. É obvio que A° é também um anel. O elemento neutro e a unidade de A e A° coincidem. Todo ideal à esquerda (direita) de A é um ideal à direita (esquerda) de A°. Portanto A e A° têm os mesmos ideais bilaterais.

Lema 1.71. *Sejam R um anel Artiniano à esquerda simples, M um R-módulo simples e $D = Hom_R(M, M)$. Então $R \simeq Hom_D(M, M) \simeq M_n(D^\circ)$, sendo n a dimensão de M como D-módulo.*

Demonstração: Definamos $\phi : R \to Hom_D(M, M)$ associando cada elemento $a \in R$ ao homomorfismo de D-módulo f_a dado por $f_a(x) = ax$ para todo $x \in M$.

Primeiramente, mostremos que ϕ é um homomorfismo de anéis. De fato, dados $a, b \in R$, temos que
$\phi(a+b)(x) = f_{a+b}(x) = (a+b)x = ax + bx = f_a(x) + f_b(x) = \phi(a)(x) + \phi(b)(x)$.
$\phi(a.b)(x) = f_{ab}(x) = (ab)x = a(bx) = a(f_b(x)) = f_a(f_b(x)) = f_a(\phi(b)(x)) = \phi(a)(\phi(b)(x)) = (\phi(a) \circ \phi(b))(x))$.

Agora, para provarmos a injetividade, notemos que $\text{Ker}\,(\phi) = \{a \in R : am = 0, \text{ para todo } m \in M\}$ é um ideal bilateral de R. Uma vez que M é simples, temos que $M \neq (0)$, assim existe $m \in M$ tal que $m \neq 0$. Como $1.m = m \neq 0$, segue que $1 \notin \text{Ker}\,(\phi)$, logo $\text{Ker}\,(\phi) \neq R$. Sendo R um anel simples, concluímos que $\text{Ker}\,(\phi) = (0)$.

Vamos mostrar que ϕ é sobrejetora. Para isso, consideremos $\{m_1, m_2, \ldots, m_n\}$ uma base de M sobre D, que é finita pelo Lema 1.68. Dado $f \in Hom_D(M, M)$, pelo Teorema de Jacobson 1.64, existe $a \in R$ tal que $f(m_i) = am_i$, para todo $1 \leq i \leq n$. Vamos mostrar que $\phi(a) = f$. Observemos que se $x \in M$, podemos escrever x da seguinte forma:

$$x = f_1(m_1) + \ldots + f_n(m_n),$$

para $f_i \in D = Hom_R(M, M)$, para todo $1 \leq i \leq n$. Assim

$$\begin{aligned} f(x) &= f(f_1(m_1) + \ldots + f_n(m_n)) = f(f_1(m_1)) + \ldots + f(f_n(m_n)) \\ &= f_1(f(m_1)) + \ldots + f_n(f(m_n)) = f_1(am_1) + \ldots + f_n(am_n) \\ &= af_1(m_1) + \ldots + af_n(m_n) = a(f_1(m_1) + \ldots + f_n(m_n)) \\ &= ax = \phi(a)(x). \end{aligned}$$

Logo, ϕ é sobrejetora, e portanto, um isomorfismo de anéis.

Agora, iremos mostrar que $Hom_D(M, M) \simeq M_n(D^\circ)$. Observemos que se n é a dimensão de M sobre D, então $M \simeq D^n$ como D-módulos. Com isso, fazendo $M = D$ no Corolário 1.62, e vendo D como um D-módulo, obtemos

$$Hom_D(M, M) \simeq M_n(Hom_D(D, D)).$$

Assim, basta mostrarmos que $Hom_D(D, D) \simeq D^\circ$. Para isso, definamos $\phi : D^\circ \to Hom_D(D, D)$ associando cada elemento $a \in D^\circ$ ao homomorfismo de D-módulo $f_a : D \to D$ dado por $f_a(x) = xa$, para todo $x \in D$. Mostremos que ϕ é um isomorfismo de anéis. De fato, para quaisquer $a, b \in D^\circ$ e $x \in D$ temos:
$\phi(a + b)(x) = f_{a+b}(x) = x(a + b) = xa + xb = f_a(x) + f_b(x) = \phi(a)(x) + \phi(b)(x)$.
$\phi(a \circ b)(x) = f_{ba}(x) = xba = f_a(xb) = f_a(f_b(x)) = f_a(\phi(b)(x)) = \phi(a)\phi(b)(x)$.
Portanto, ϕ é homomorfismo de anéis. Agora observemos que $\text{Ker}\,(\phi) \neq D^\circ$ e $\text{Ker}\,(\phi)$ é um ideal do anel com divisão D°, o qual possui somente os ideais triviais. Logo, devemos ter $\text{Ker}\,(\phi) = (0)$, e portanto, ϕ é injetora. Para verificarmos a sobrejetividade, tomemos $f \in Hom_D(D, D)$, temos que $f(x) = f(x.1) = xf(1)$, para todo $x \in D$. Fazendo $a = f(1) \in D^\circ$, segue que

$$\phi(a)(x) = \phi(f(1))(x) = xf(1) = f(x) \text{ para todo } x \in D.$$

Portanto, ϕ é um isomorfismo de anéis. ■

Teorema 1.72. (Wedderburn-Artin) *Um anel R é semisimples se, e somente se, é uma soma direta de anéis de matrizes sobre anéis com divisão:*

$$R \simeq M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s).$$

Demonstração: Suponhamos que R é um anel semisimples, assim podemos escrever

$$R = \underbrace{L_{11} \oplus L_{12} \oplus \ldots \oplus L_{1r_1}}_{A_1} \oplus \underbrace{L_{21} \oplus L_{22} \oplus \ldots \oplus L_{2r_2}}_{A_2} \oplus \ldots \oplus \underbrace{L_{s1} \oplus L_{s2} \oplus \ldots \oplus L_{sr_s}}_{A_s},$$

onde cada L_{ij} é ideal minimal à esquerda e $L_{ij} \simeq L_{ih}$. Então, $R = \bigoplus_{i=1}^{s} A_i$ é a decomposição de R como soma direta de ideais minimais bilaterais, como no Teorema 1.51.

Notemos que os ideais L_{ij}, $1 \leq j \leq r_i$, da decomposição de A_i são minimais, assim devemos ter que cada L_{ij}, $1 \leq j \leq r_i$, é um anel Artiniano à esquerda. Uma vez que A_i é soma direta de L_{ij}, $1 \leq j \leq r_i$, segue que A_i é um anel Artiniano à esquerda. Além disso, temos que L_{i1} é um submódulo simples de A_i. Assim, pelo lema anterior, $A_i \simeq Hom_{D_i}(L_{i1}, L_{i1}) \simeq M_{n_i}(D_i)$, sendo $D_i = Hom_R(L_{i1}, L_{i1})$ e n_i a dimensão de L_{i1} como D_i-módulo, para todo $1 \leq i \leq s$. Pelo Corolário 1.66, D_i é um anel com divisão.

Reciprocamente, assumimos que $R \simeq M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s)$. Como cada componente $M_{n_i}(D_i)$ é um anel semisimples, podemos escrever $M_{n_i}(D_i)$ como soma de um número finito de ideais minimais à esquerda, que também são ideais minimais à esquerda de R, ou seja, R é uma soma de um número finito de ideais minimais à esquerda. Portanto, pelo Teorema 1.39, R é um anel semisimples. ■

Finalizaremos esta seção estabelecendo a unicidade para a decomposição de um anel semisimples dada no Teorema de Wedderburn-Artin 1.72, mas antes citaremos um resultado auxiliar.

Teorema 1.73. *Sejam D e D' anéis com divisão tais que $M_m(D) \simeq M_n(D')$, então $D \simeq D'$ e $m = n$.*

Demonstração: Ver [12], Teorema 1.9, pg 283. ■

Teorema 1.74. *Seja R um anel semisimples e suponhamos que*

$$R \simeq M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s) \simeq M_{m_1}(D_1^{'}) \oplus \ldots \oplus M_{m_r}(D_r^{'}),$$

com D_i, $D_j^{'}$, $1 \leq i \leq s$, $1 \leq j \leq r$ anéis com divisão. Então, $s = r$ e, após uma permutação adequada de índices, temos que $n_i = m_i$ e $D_i \simeq D_i^{'}$.

Demonstração: Já vimos que anéis de matrizes sobre anéis com divisão são simples, logo, pela Proposição 1.55 vem $r = s$ e $M_{n_i}(D_i) \simeq M_{m_j}(D_j^{'})$. Se $i \neq j$ podemos fazer uma permutação de índices e obteremos $M_{n_i}(D_i) \simeq M_{m_i}(D_i^{'})$. Portanto, segue do teorema anterior que $n_i = m_i$ e $D_i \simeq D_i^{'}$. ■

1.5 Os Anéis de Grupo R[G]

Nesta seção, iremos mostrar que, sob certas condições, os anéis de grupo são semisimples. Em seguida, encontraremos uma base para o centro dos anéis de grupo $K[G]$, onde G é um grupo finito e K um corpo. Esta será muito útil no Capítulo 4. Começamos definindo anel de grupo.

Seja G um grupo e R um anel com identidade. Podemos construir um R-módulo livre tendo como base os elementos de G, que será denotado por $R[G]$. Assim, os elementos de $R[G]$ podem ser escritos de modo único na forma $\sum_{g \in G} a_g g$, com $a_g \in R$ e somente um número finito de coeficientes são diferentes de zero (em outras palavras, a soma é finita).

Definimos a adição em $R[G]$ por

$$\left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g,$$

e a multiplicação da seguinte forma

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{h \in G} b_h h\right) = \sum_{g,h \in G} (a_g b_h)(gh).$$

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

Teorema 1.75. (Maschke) *Seja G um grupo. Se R é um anel semisimples, G é finito e $|G|$ é inversível em R, então o anel de grupo $R[G]$ é semisimples.*

Demonstração: Suponhamos que as hipóteses são válidas e vamos mostrar que $R[G]$ é um anel semisimples, ou seja, $R[G]$ visto como um $R[G]$-módulo é semisimples. Para isso, consideremos M um $R[G]$-submódulo de $R[G]$ e mostremos que M é um somando direto de $R[G]$. Por hipótese, R é semisimples, assim, pelo Teorema 1.39, devemos ter que todo R-módulo é semisimples, em particular, $R[G]$ visto como um R-módulo é semisimples. Como M é também um R-submódulo de $R[G]$, existe um R-submódulo N de $R[G]$ tal que $R[G] = M \oplus N$.

Seja $\pi : R[G] \to M$ a projeção canônica sobre M. Definimos: $\pi^* : R[G] \to M$ dada por

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx), \quad \text{para todo } x \in R[G].$$

Observemos que π^* está bem definida, pois $\pi(gx) \in M$, para todo $x \in R[G]$ e $g \in G$. Como M é um $R[G]$-submódulo de $R[G]$, temos que $g^{-1}\pi(gx) \in M$, logo, $\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx) \in M$.

Se provarmos que π^* é um $R[G]$-homomorfismo, então $\mathrm{Ker}\,(\pi^*)$ será um $R[G]$-submódulo de $R[G]$, assim, se mostrarmos que $R[G] = M \oplus \mathrm{Ker}\,(\pi^*)$ teremos que $R[G]$ é um anel semisimples.

Inicialmente, mostremos que π^* é um $R[G]$-homomorfismo. Como π^* é um R-homomorfismo, é suficiente mostrarmos que $\pi^*(ax) = a\pi^*(x)$, para todo $x, a \in G$. De fato, temos que

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{1}{|G|} \sum_{g \in G} aa^{-1}g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Como g percorre todos elementos de G, o produto ga também percorre todos elementos de G, logo,

$$\pi^*(ax) = a\frac{1}{|G|} \sum_{h \in G} h^{-1}\pi(hx) = a\pi^*(x).$$

Assim π^* é um $R[G]$-homomorfismo e $\mathrm{Ker}\,(\pi^*)$ é um $R[G]$-submódulo de $R[G]$. Vamos mostrar agora que $\mathrm{Im}(\pi^*) = M$. Com efeito, uma vez que π é uma projeção sobre M, devemos ter $\pi(m) = m$, para todo $m \in M$. Também, como M é um $R[G]$-módulo, temos que $gm \in M$, para todo $g \in G$. Daí,

$$\pi^*(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gm) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gm = \frac{1}{|G|}(\underbrace{m+m+...+m}_{|G|\text{ vezes}}) = m.$$

Logo, $M \subset \mathrm{Im}(\pi^*)$, e portanto, $\mathrm{Im}(\pi^*) = M$.

Observemos, ainda, que $(\pi^*)^2 = \pi^*$, pois

$$\pi^*(\pi^*(x)) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(\underbrace{g\pi^*(x)}_{\in M}) = \frac{1}{|G|}\sum_{g\in G} g^{-1}(g\pi^*(x)) = \pi^*(x),$$

para todo $x \in R[G]$.

Para mostrarmos que $R[G] = M \oplus \mathrm{Ker}\,(\pi^*)$, consideremos a seqüência exata

$$0 \to \mathrm{Ker}\,(\pi^*) \xrightarrow{i} R[G] \xrightarrow{\pi^*} M \to 0.$$

Fazendo $\varphi = \pi^*_{|_M} : M \to R[G]$, podemos notar que $\mathrm{Im}(\pi^*) = M \subset R[G]$ e, assim, obtemos um homomorfismo de $R[G]$-módulos $\varphi : M \to R[G]$ tal que $\pi^* \circ \varphi = I_M$. De fato, como π^* é um homomorfismo sobrejetor, dado $m \in M$, existe $x \in R[G]$ tal que $\pi^*(x) = m$. Daí,

$$(\pi^* \circ \varphi)(m) = (\pi^* \circ \varphi)(\pi^*(x)) = \pi^*(\pi^*(\pi^*(x))) = \pi^*(x) = m.$$

Portanto, a seqüência se fatora, ou seja, $R[G] = M \oplus \mathrm{Ker}\,(\pi^*)$. ■

Observação 1.76. Se $R = K$ é um corpo, K é sempre semisimples, pois K visto como um K-módulo é um K-espaço vetorial, assim dado um K-subespaço E de K, sempre obtemos um K-subespaço F tal que $K = E \oplus F$.

Corolário 1.77. *Sejam G um grupo finito e K um corpo. Se $char(K) \nmid |G|$ então $K[G]$ é semisimples.*

Demonstração: Uma vez que K é um corpo, pela observação acima, temos que K é semisimples. Além disso, o fato que $char(K) \nmid |G|$ implica que $|G|$ é inversível em K. Logo, usando o Teorema de Maschke 1.75, segue que $K[G]$ é semisimples. ■

Como conseqüência do Teorema de Maschke 1.75, juntamente com o Teorema de Wedderburn-Artin 1.72 segue o seguinte:

Teorema 1.78. *Sejam G um grupo finito e K um corpo tal que $char(K) \nmid |G|$. Então:*

(i) $K[G]$ é uma soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$. Cada B_i é um anel simples e $\{B_i\}_{1\leq i\leq r}$ são as componentes simples de $K[G]$.

(ii) Qualquer ideal bilateral de $K[G]$ é uma soma direta de alguns membros da família $\{B_i\}_{1\leq i\leq r}$.

(iii) Cada componente simples B_i é isomorfa a um anel de matriz da forma $M_{n_i}(D_i)$, com D_i um anel com divisão contendo uma cópia isomorfa de K em seu centro, e o isomorfismo:

$$K[G] \overset{\phi}{\simeq} \bigoplus_{i=1}^{r} M_{n_i}(D_i),$$

é um isomorfismo de anéis.

(iv) Em cada anel de matriz $M_{n_i}(D_i)$, o conjunto:

$$I_i = \left\{ \begin{pmatrix} x_1 & 0 & \dots & 0 \\ x_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_i} & 0 & \dots & 0 \end{pmatrix} : x_1, x_2, \dots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i},$$

é um ideal minimal à esquerda.

Dado $x \in KG$, consideramos $\phi(x) = (\alpha_1, \dots, \alpha_r) \in \bigoplus_{i=1}^{r} M_{n_i}(D_i)$ e definimos o produto de x por um elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. Com esta definição, I_i torna-se um KG-módulo simples.

(v) $I_i \not\simeq I_j$ se $i \neq j$.

(vi) Qualquer KG-módulo simples é isomorfo a algum I_i, $1 \leq i \leq r$.

Corolário 1.79. *Sejam G um grupo finito e K um corpo algebricamente fechado tal que $char(K) \nmid |G|$. Então*

$$K[G] \simeq \bigoplus_{i=1}^{r} M_{n_i}(K),$$

e $n_1^2 + n_2^2 + \ldots + n_r^2 = |G|$.

Demonstração: Como $char(K) \nmid |G|$, pelo ítem (iii) do Teorema 1.78, temos que

$$K[G] \simeq \bigoplus_{i=1}^{r} M_{n_i}(D_i),$$

onde D_i é um anel de divisão contendo uma cópia de K em seu centro. Se calcularmos a dimensão sobre K em ambos os lados da equação acima obtemos

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : K].$$

Assim, cada anel de divisão é de dimensão finita sobre K, logo todo elemento é algébrico sobre K. O fato que K é algebricamente fechado implica $D_i = K$, para todo $1 \leq i \leq r$, e segue o resultado. ■

Definição 1.80. Sejam G um grupo finito e $C_1, \ldots, C_r$ suas classes de conjugação. Para cada $i \in \{1, \ldots, r\}$ definimos $\gamma_i = \sum_{h \in C_i} h \in K[G]$. Estes elementos são chamados *somas de classe* de G sobre K.

O próximo resultado nos fornece uma base para o centro $Z(K[G])$ do anel de grupo $K[G]$. Este resultado também pode ser obtido considerando G um grupo qualquer e R um anel comutativo. Como em nossos casos utilizaremos sempre G um grupo finito e K um corpo, faremos a prova somente para esse caso, embora, a demonstração para o caso geral seja análoga.

Teorema 1.81. *Sejam K um corpo, G um grupo finito e $C_1, \ldots, C_r$ suas classes de conjugação. Então, o conjunto $\{\gamma_i\}_{i=1}^{r}$ forma uma base de $Z(K[G])$, o centro de $K[G]$ sobre K.*

Demonstração: Mostremos primeiro que cada γ_i pertence a $Z(K[G])$. De fato, dado um elemento arbitrário $g \in G$, temos que

$$g\gamma_i g^{-1} = \sum_{x \in C_i} gxg^{-1} = \sum_{y \in C_i} y = \gamma_i.$$

Logo, $g\gamma_i = g\gamma_i$ para todo $g \in G$, isso mostra que $\gamma_i \in Z(K[G])$, $1 \leq i \leq r$.

Mostremos que estes elementos são linearmente independentes sobre K. De fato, suponhamos que $k_1\gamma_1 + \ldots + k_r\gamma_r = 0$, com $k_1, \ldots, k_r \in K$. Como as classes de conjugação são disjuntas e G é uma base de $K[G]$ sobre K, devemos ter $k_i = 0$, $1 \leq i \leq r$.

Finalmente, resta-nos mostrar que $\{\gamma_i\}_{i=1}^r$ geram $Z(K[G])$ sobre K. Para isso, tomemos $\alpha = \sum_{g \in G} a_g g \in Z(K[G])$ e observemos que dado $h \in G$ temos

$$\alpha = h^{-1}\alpha h = \sum_{g \in G} a_g(h^{-1}gh),$$

então, fazendo $\beta = h^{-1}gh$ vem $\alpha = \sum_{\beta \in G} a_{h\beta h^{-1}}\beta$, e portanto, $\alpha = \sum_{\beta \in G} a_\beta \beta = \sum_{\beta \in G} a_{h\beta h^{-1}}\beta$. Como G é um conjunto linearmente independente de $K[G]$ sobre K segue que $a_\beta = a_{h\beta h^{-1}}$, para todo $\beta, h \in G$. Assim podemos colocar os coeficientes que correspondem aos elementos da mesma classe de conjugação em evidência, isto é, $\alpha = \sum_{\beta \in G} a_\beta \beta = \sum_{i=1}^{r} a_{\beta_i}\gamma_i$, com $\beta_i \in C_i$. Como queríamos provar. ■

Encerraremos esta seção mostrando que o número de componentes simples de $K[G]$ é conhecido quando K for um corpo algebricamente fechado.

Proposição 1.82. *Seja G um grupo finito e K um corpo algebricamente fechado tal que $char(K) \nmid |G|$. Então, o número de componentes simples de $K[G]$ é igual ao número de classes de conjugação de G.*

Demonstração: Pelo teorema acima, é suficiente mostrarmos que, neste caso, o número de componentes simples de $K[G]$ é igual a dimensão de $Z(K[G])$ sobre K.

Do Corolário 1.79 segue que $K[G] \simeq \bigoplus_{i=1}^{r} M_{n_i}(K)$, e portanto, $Z(K[G]) \simeq \bigoplus_{i=1}^{r} Z(M_{n_i}(K))$. Usando o fato que $Z(M_{n_i}(K)) \simeq K$ vem $Z(K[G]) \simeq \underbrace{K \oplus \ldots \oplus K}_{r \text{ vezes}}$. Conseqüentemente, $[Z(K[G]) : K] = r$. ■

Capítulo 2

Representações de Grupos

Neste capítulo, faremos um breve resumo da teoria de representações de grupos e caracteres, com o objetivo de descrevermos, no caso em que K é algebricamente fechado, cada elemento de uma família completa de idempotentes primitivos centrais de $K[G]$. Além disso, construiremos a tábua de caracter do grupo simétrico S_3 sobre $\mathbb{C}$, visando sua utilização no Capítulo 4.

2.1 Definições e Exemplos

No decorrer desta seção, R sempre denotará um anel com identidade, a menos que se diga o contrário.

Definição 2.1. Sejam G um grupo, R um anel comutativo e V um R-módulo livre de dimensão finita. Uma *representação* de G sobre R é um homomorfismo de grupos $T : G \to GL(V)$, sendo $GL(V)$ o grupo dos R-automorfismos de V.

A dimensão de V é chamada o *grau* da representação T e será denotado por $deg(T)$. A imagem $T(g)$ de um elemento $g \in G$ em $GL(V)$ é também denotada por $T_g : V \to V$.

Observação 2.2. Consideremos V um R-módulo de dimensão n e $GL_n(R)$ o grupo das matrizes $n \times n$ inversíveis com entradas em R. Se fixarmos uma R-base de V, podemos definir um isomorfismo $\phi : GL(V) \to GL_n(R)$ associando cada automorfismo $T \in GL(V)$ à sua respectiva matriz em relação a base considerada.

Definição 2.3. Sejam G um grupo e R um anel comutativo. Uma *representação matricial* de G sobre R é um homomorfismo de grupos $T : G \to GL_n(R)$, em que o inteiro n é o *grau* da representação T.

Observemos abaixo, que dada uma representação de G sobre R, podemos obter uma representação matricial e vice-versa.

Observação 2.4. Se $T : G \to GL(V)$ é uma representação de G sobre R e considerando que $\phi : GL(V) \to GL_n(R)$ é o isomorfismo visto na observação anterior, então $\phi \circ T : G \to GL_n(R)$ é uma representação matricial de G. Analogamente, dada uma representação matricial $T : G \to GL_n(R)$, temos que $\phi^{-1} \circ T : G \to GL(V)$ é uma representação de G sobre R. Porém, como o isomorfismo ϕ depende da base fixada, dada uma representação de G, podemos obter várias representações matriciais.

Essa observação induz a próxima definição, onde daremos a noção de representações equivalentes.

Definição 2.5. Duas representações $T : G \to GL(V)$ e $\overline{T} : G \to GL(W)$ de um grupo G sobre um anel comutativo R são chamadas *equivalentes* se existir um isomorfismo $\phi : V \to W$ de R-módulos tal que $\overline{T}_g = \phi \circ T_g \circ \phi^{-1}$, para todo $g \in G$.

Em termos de matrizes, dizemos que duas representações matriciais $A : G \to GL_n(R)$ e $B : G \to GL_n(R)$ de um grupo G sobre um anel comutativo R são *equivalentes* se existir uma matrix inversível $U \in GL_n(R)$ tal que $A(g) = UB(g)U^{-1}$, para todo $g \in G$.

Agora, daremos alguns exemplos de representações.

Exemplo 2.6. (Representação Trivial) Dado um grupo G e um anel comutativo R, definamos $T : G \to GL_n(R)$ por $T(g) = I_n$, para todo $g \in G$, sendo I_n a matrix identidade de $GL_n(R)$. Obviamente T é um homomorfismo de grupos, e portanto, uma representação de G.

Exemplo 2.7. (Representação Linear) Uma *representação linear* de um grupo G sobre um corpo K é um homomorfismo $T : G \to GL_1(K) = K^*$, ou seja, T é uma representação de grau 1.

No que segue, consideremos G um grupo finito, a menos que se diga o contrário.

Exemplo 2.8. (Representação Regular) Sejam K um corpo, G um grupo e consideremos o anel de grupo $K[G]$. Sabemos que $K[G]$ é um espaço vetorial sobre K cuja a base é G. Definamos $\eta : G \to GL(K[G])$ do seguinte modo: para cada elemento $g \in G$ associamos a aplicação linear $\eta_g : K[G] \to K[G]$ dada por $\eta_g(x) = g.x$, para todo $x \in G$. Dessa forma, $\eta_{gh}(x) = (gh)x = g(h(x)) = \eta_g\eta_h(x)$, assim estendendo linearmente para $K[G]$ obtemos uma representação de G, a qual chamaremos de *representação regular* de G sobre K.

Observemos que, sendo G a base de $K[G]$ sobre K, se enumerarmos os elementos de G em alguma ordem $G = \{1 = g_1, \ldots, g_n\}$, então a correspondente representação matricial de η, com respeito a base G de $K[G]$, associa cada elemento $g \in G$ a uma *matriz permutação*, ou seja, uma matriz que tem exatamente uma entrada igual a 1 em cada linha e cada coluna, e todas as outras entradas iguais a zero.

Para exemplificar, consideremos $G = \{1, a, a^2\}$ um grupo cíclico de ordem 3 e enumeremos seus elementos da seguinte forma: $g_1 = 1$, $g_2 = a$ e $g_3 = a^2$. Calculando a imagem de a pela representação regular obtemos $\eta_a(g_1) = g_2$, $\eta_a(g_2) = g_3$ e $\eta_a(g_3) = g_1$. Conseqüentemente, a matriz associada a η_a em relação a base dada é

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

Uma classe de representações de grupos muito importante são as chamadas representações irredutíveis, que veremos a seguir.

Definição 2.9. Uma representação $T : G \to GL(V)$ de um grupo G sobre um corpo K é chamada *irredutível* se $V \neq \{0\}$ e os únicos subespaços de V invariantes pela T são os triviais. Caso contrário, a representação T é dita *redutível*.

Agora, se tivermos $T : G \to GL(V)$ uma representação de G sobre K em que V contenha um subespaço W invariante por T, ou seja, $T_g(W) \subset W$ para todo $g \in G$. Então, podemos definir uma representação $T_{|_W} : G \to GL(W)$ de G sobre K, associando cada elemento $g \in G$ à restrição de T_g ao subespaço W.

Assim, se tomarmos $\{w_1, \ldots, w_t\}$ uma base para W e estendermos para uma base $\{w_1, \ldots, w_t, v_{t+1}, \ldots, v_n\}$ de V, então a matriz associada a cada aplicação T_g, com respeito a base acima, é da forma

$$\begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix},$$

onde $A(g) \in GL_t(K)$, $C(g) \in GL_{n-t}(K)$ e $B(g)$ é uma matriz $n \times (n-t)$.

Isso nos leva a dar uma interpretação matricial para redutibilidade, que é a seguinte.

Definição 2.10. Uma representação matricial $M : G \to GL_n(K)$ é chamada *redutível*, se existe uma matriz $U \in GL_n(K)$ tal que

$$UM(g)U^{-1} = \begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix}, \text{ para todo } g \in G.$$

Caso contrário, dizemos que a representação M é *irredutível*.

2.2 Representações e Módulos

Nosso propósito, agora, é relacionar a teoria de representações de grupos com os anéis de grupos de dimensão finita. Em particular, extrairemos propriedades importantes sobre representações utilizando resultados obtidos anteriormente sobre anéis de grupos. Iniciaremos mostrando que há uma correspondência biunívoca entre o conjunto dos $R[G]$-módulos que são R-livres de dimensão finita e o conjunto das representações de G sobre R.

Proposição 2.11. *Sejam G um grupo e R um anel comutativo com identidade. Então, existe uma bijeção entre as representações de G sobre R e os $R[G]$-módulos que são R-livres de dimensão finita.*

Demonstração: Seja $T : G \to GL(V)$ uma representação de G sobre R de grau n. Assim V é um R-módulo livre de dimensão n. Definamos a ação de $R[G]$ sobre V do seguinte modo: dados $g \in G$ e $v \in V$, então $g.v = T_g(v)$. Estendendo esta definição para $\alpha = \sum_{g \in G} a_g g \in R[G]$ obtemos $\alpha.v = \sum_{g \in G} a_g T_g(v)$. Dessa forma, não é difícil verificarmos que V possui uma estrutura de $R[G]$-módulo.

Reciprocamente, se V é um $R[G]$-módulo de dimensão finita sobre R, definamos a aplicação $T : G \to GL(V)$ associando cada elemento $g \in G$ ao R-automorfismo $T_g : V \to V$ dado por $T_g(v) = g.v$, para todo $v \in V$. Claramente com esta definição T é uma representação de G sobre R. ■

Devido a correspondência biunívoca da proposição anterior, segue naturalmente o próximo resultado. Omitiremos sua demonstração por ser bem simples, mas parte dela pode ser encontrada em [5], Lema 2.6, pg. 22.

Proposição 2.12. *Sejam G um grupo e R um anel comutativo com identidade. Então:*

(1) *Duas representações T e T' de G sobre R são equivalentes se, e somente se, seus correspondentes $R[G]$-módulos são isomorfos.*

(2) *Uma representação é irredutível se, e somente se, seu correspondente $R[G]$-módulo é simples.*

Observação 2.13. Se um $R[G]$-módulo M admite uma decomposição como soma direta de seus submódulos $M = \bigoplus_{i=1}^{t} M_i$, e se T e T_i denotam as representações correspondentes a estes módulos, $1 \leq i \leq t$, então $T = \bigoplus_{i=1}^{t} T_i$.

Utilizando as proposições anteriores e alguns resultados obtidos no Capítulo 1 sobre anéis de grupo, conseguimos caracterizar toda representação de um grupo G sobre K, quando K é um corpo tal que $char(K) \nmid |G|$. Vamos ver como isso acontece.

Seja T uma representação de G sobre K. Sabemos pela Proposição 2.11, que toda representação de G sobre K esta relacionada a um $K[G]$-módulo. Pelo Teorema de Maschke e seu Corolário 1.77 temos que $K[G]$ é um anel semisimples e, usando o Teorema 1.39, juntamente com o Teorema 1.35, obtemos que todo $K[G]$-módulo pode ser representado como uma soma direta de módulos simples. Logo, se M é o $K[G]$-módulo associado a representação T, podemos representar M da seguinte forma: $M = \bigoplus_{i=1}^{t} M_i$, onde cada M_i é um módulo simples. Agora, usando a observação anterior e a Proposição 2.12 obtemos $T = \bigoplus_{i=1}^{t} T_i$, sendo T_i a representação irredutível correspondente ao módulo simples M_i da decomposição de $K[G]$.

Resumindo, obtemos que toda representação de G sobre K é uma soma de representações irredutíveis. Assim, para determinarmos qualquer representação de G sobre K, a menos de equivalentes, basta determinarmos todos os $K[G]$-módulos simples, a menos de isomorfismo.

Veremos agora que a quantidade de representações irredutíveis não equivalentes e seus graus estão relacionados às componentes simples de $K[G]$.

Pelo Teorema 1.78, temos a seguinte decomposição:

$$K[G] \simeq \bigoplus_{i=1}^{r} M_{n_i}(D_i), \tag{2.1}$$

onde D_i é um anel de divisão contendo uma cópia isomorfa de K em seu centro. Se considerarmos o módulo simples

$$I_i = \begin{pmatrix} D_i & 0 & \dots & 0 \\ D_i & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ D_i & 0 & \dots & 0 \end{pmatrix},$$

temos que cada componente simples $M_{n_i}(D_i)$ pode ser escrita como $M_{n_i}(D_i) \simeq \underbrace{I_i \oplus \ldots \oplus I_i}_{n_i \text{ vezes}}$ e, portanto, $K[G] \simeq \underbrace{I_1 \oplus \ldots \oplus I_1}_{n_1 \text{ vezes}} \oplus \ldots \oplus \underbrace{I_r \oplus \ldots \oplus I_r}_{n_r \text{ vezes}}$. Como $I_i \not\simeq I_j$ se

$i \neq j$, segue que o número de $K[G]$-módulos simples não isomorfos é exatamente o número de componentes simples de $K[G]$.

Seja T_i a representação irredutível correspondente ao módulo simples I_i. Para encontrarmos o grau da representação T_i, vamos calcular a dimensão sobre K em ambos os lados da equação (2.1). Assim obtemos

$$|G| = \sum_{i=1}^{r} n_i^2 \, [D_i : K]. \tag{2.2}$$

Observemos que o módulo simples I_i, correspondente a componente simples $M_{n_i}(D_i)$, é isomorfo a $D_i^{n_i}$ e o grau da representação T_i é dado pela dimensão desse módulo sobre K. Portanto,

$$deg(T_i) = [D_i^{n_i} : K] = n_i[D_i : K].$$

Além disso, se substituirmos $deg(T_i)$ em (2.2) obtemos $|G| = \sum_{i=1}^{r} n_i deg(T_i)$.

Finalmente, se K é um corpo algebricamente fechado, então pela Proposição 1.82 temos que o número de componentes simples é igual o número de classes de conjugação de G. Isso nos diz que a quantidade de representações irredutíveis não equivalentes é igual ao número de classes de conjugação de G. Também, vimos no Corolário 1.79, que neste caso, $D_i = K$, $1 \leq i \leq r$. Portanto, $deg(T_i) = n_i$ e isso implica que $|G| = \bigoplus_{i=1}^{r} n_i^2$, sendo r o número de classes de conjugação de G.

Observação 2.14. Seja $T : G \to GL_n(K) \subset M_n(K)$ uma representação de G em K, podemos estender a representação T para uma representação $T' : K[G] \to M_n(K)$ da seguinte forma: $T'(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g T(g)$, para todo $\sum_{g\in G} a_g g \in K[G]$.

Exemplo 2.15. Seja $\eta : G \to GL_n(K)$ representação regular de $K[G]$ com $n = |G|$, então a representação $\eta' : K[G] \to M_n(K)$ associa cada $\gamma = \sum_{g\in G} a_g g$ à matriz da aplicação $\eta'(\gamma) = \sum_{g\in G} a_g \eta(g)$. Nesse caso, $\eta'(\gamma)$ é a multiplicação por γ sobre $K[G]$, pois $\eta'(\gamma)(x) = \sum_{g\in G} a_g \eta(g)(x) = (\sum_{g\in G} a_g g)x = \gamma x$ para todo $x \in K[G]$.

2.3 Caracteres

Na seqüência estudaremos alguns tópicos da teoria de caracteres. Primeiramente, relembremos que dada uma matriz $n \times n$, $A = (a_{ij})$, o traço de A é a soma dos elementos da diagonal principal, ou seja, $tr(A) = \sum_{i=1}^{n} a_{ii}$. Não é difícil verificarmos, que dadas duas matrizes $n \times n$, A, B temos que $tr(AB) = tr(BA)$. Desse fato, obtemos que matrizes similares têm o mesmo traço. Com efeito, se U é uma matriz inversível então $tr(UAU^{-1}) = tr(U(AU^{-1})) = tr((AU^{-1})U) = tr(A)$.

Definição 2.16. Sejam G um grupo, V um espaço vetorial de dimensão finita sobre K e $T : G \to GL(V)$ uma representação de G sobre K. Então, o *caracter* χ de G admitido pela representação T é a aplicação $\chi : G \to K$ dada por $\chi(g) = tr(T_g)$, para todo $g \in G$. Se a representação T é irredutível, dizemos que χ é um *caracter irredutível*.

Os caracteres possuem as seguintes propriedades:

Lema 2.17. (1) $\chi(1_G) = deg(T)$. *Em particular, se* $T = \eta$ *é a representação regular, então* $\chi(1_G) = |G|$.

(2) *Se* T *e* T' *são representações equivalentes de* G *sobre* K*, então elas admitem o mesmo caracter.*

(3) χ *é uma função constante nas classes de conjugação de* G.

Demonstração: Bastante simples, mas pode ser obtida em [10], pg. 180. ■

Se considerarmos $T_1, T_2, \ldots, T_r$ representações de um grupo G e $\chi_1, \chi_2, \ldots, \chi_r$ seus respectivos caracteres. Então o caracter da representação $T = T_1 \oplus T_2 \oplus \ldots \oplus T_r$ é da forma $\chi = \chi_1 \oplus \chi_2 \oplus \ldots \oplus \chi_r$. Dessa forma, se $char(K) \nmid |G|$ e $\{T_1, T_2, \ldots, T_r\}$ é um conjunto completo de representações irredutíveis não equivalentes de G sobre K, então qualquer outra representação de G sobre K pode ser escrita na forma

$T = \sum_{i=1}^{r} n_i T_i$, $n_i \geq 0$, $1 \leq i \leq r$. Portanto, o caracter χ admitido por T pode ser representado por $\chi = \sum_{i=1}^{r} n_i \chi_i$.

Exemplo 2.18. Sejam G um grupo finito e K um corpo algebricamente fechado. Denotamos por $\rho : G \to K$ o *caracter regular*, que é admitido pela representação regular de G sobre K. Se $char(K) \nmid |G|$, então $K[G]$ admite a seguinte decomposição:

$$K[G] \overset{\phi}{\simeq} \bigoplus_{i=1}^{r} M_{n_i}(K) \simeq \underbrace{I_1 \oplus \ldots \oplus I_1}_{n_1 \text{ vezes}} \oplus \ldots \oplus \underbrace{I_r \oplus \ldots \oplus I_r}_{n_r \text{ vezes}},$$

onde $I_i \not\simeq I_j$ se $i \neq j$. Portanto, existem r representações irredutíveis não equivalentes, em que r, neste caso, é igual ao número de classes de conjugação de G. Se T_i é a representação irredutível de G sobre K associada ao módulo simples I_i, e χ_i seu correspondente caracter, $1 \leq i \leq r$, então podemos escrever a representação regular de G sobre K como $\eta = \sum_{i=1}^{r} n_i T_i$. Dessa forma, obtemos $\rho = \sum_{i=1}^{r} n_i \chi_i$. Uma vez que $n_i = deg(T_i) = \chi_i(1)$, a equação acima pode ser reescrita como

$$\rho = \sum_{i=1}^{r} \chi_i(1) \chi_i. \tag{2.3}$$

Sejam G um grupo finito e K um corpo algebricamente fechado tal que $char(K) \nmid |G|$, então pelo Teorema 1.78, $K[G]$ pode ser escrito da seguinte forma:

$$K[G] = \bigoplus_{i=1}^{r} e_i(K[G]) \overset{\phi}{\simeq} \bigoplus_{i=1}^{r} M_{n_i}(K),$$

sendo $\{e_1, \ldots, e_r\}$ uma família completa de idempotentes centrais primitivos de $K[G]$. Consideremos $T_1, T_2, \ldots, T_r$ um conjunto completo de representações irredutíveis não equivalentes de G sobre K e $\chi_1, \chi_2, \ldots, \chi_r$ os caracteres admitidos por estas representações.

Nosso objetivo agora é descrever cada idempotente e_i de $K[G]$ utilizando caracteres.

Primeiramente, sabemos que $1_{K[G]} = e_1 + \ldots + e_r$. Também, pelo isomorfismo ϕ temos $\phi(1_{K[G]}) = (I_{n_1}, \ldots, I_{n_i}, \ldots, I_{n_r})$, logo, devemos ter $\phi(e_i) = (0, \ldots, I_{n_i}, \ldots, 0)$, onde I_{n_i} corresponde a matriz identidade de $M_{n_i}(K)$.

Seja $T_i : G \to GL(I_i)$ a representação de G sobre K associada ao módulo simples I_i da componente simples $M_{n_i}(K)$ e χ_i seu correspondente caracter.

Agora, vejamos que $T_i(e_i)(x) = e_i.x$, para todo $x \in I_i$. Como $\phi(e_i) = (0, \ldots, I_{n_i}, \ldots, 0)$, devemos ter $e_i.x = I_{n_i}x = x$, para todo $x \in I_i$ (Ver Teorema 1.78), ou seja, $T_i(e_i)$ é a aplicação identidade sobre I_i. Dessa forma, $T_i(e_i)$ corresponde a matriz identidade de $M_{n_i}(K)$. Também, o fato que $e_i e_j = 0$ se $i \neq j$, e $T_i(e_i e_j) = T_i(e_i)T_i(e_j) = I_{n_i}T_i(e_j) = T_i(e_j)$ implica $T_i(e_j) = 0$. Portanto,

$$\begin{cases} \chi_i(e_i) = tr(I_{n_i}) = deg(T_i) \\ \chi_i(e_j) = 0, \text{ se } i \neq j. \end{cases} \tag{2.4}$$

Teorema 2.19. *Com a notação acima, temos que*

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g$$

Demonstração: Como $e_i \in K[G]$ podemos escrever e_i da forma $e_i = \sum_{g \in G} a_i(g)g$. Consideremos ρ o caracter regular sobre $K[G]$, usando o fato que $\rho(g) = 0$ se $g \neq 1$ e $\rho(g) = |G|$ se $g = 1$ obtemos

$$\rho(e_i) = \sum_{g \in G} a_i(g)\rho(g) = a_i(1)|G|.$$

Notemos que, dado um elemento $x \in G$, então $x^{-1}e_i = \sum_{g \in G} a_i(g)(x^{-1}g)$, disso segue que

$$\rho(x^{-1}e_i) = \sum_{g \in G} a_i(g)\rho(x^{-1}g) = a_i(x)|G|.$$

Também, usando (2.3) temos

$$a_i(x)|G| = \rho(x^{-1}e_i) = \sum_{j=1}^{r} \chi_j(1)\chi_j(x^{-1}e_i). \tag{2.5}$$

Mas, por (2.4) temos que $T_i(e_i) = I_{n_i}$ e $T_i(e_j) = 0$, se $i \neq j$. Isso implica que,

$$\begin{aligned} T_j(x^{-1}e_i) &= T_j(x^{-1})T_j(e_i) = 0 \\ T_i(x^{-1}e_i) &= T_i(x^{-1})T_i(e_i) = T_i(x^{-1}), \end{aligned}$$

assim obtemos $\chi_j(x^{-1}e_i) = 0$ e $\chi_i(x^{-1}e_i) = \chi_i(x^{-1})$. Conseqüentemente, reescrevendo (2.5) vem

$$a_i(x) = \frac{1}{|G|}\chi_i(1)\chi_i(x^{-1}), \text{ para todo } x \in G.$$

Substituindo a expressão acima em e_i concluímos $e_i = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})g$. ■

2.4 Tábua de Caracteres

Vimos, na seção anterior, que os caracteres são constantes nas classes de conjugação $C_1, \ldots, C_r$ de G. Dessa forma, se escolhermos elementos $x_i \in C_i$, $1 \leq i \leq r$, então os caracteres $\{\chi_1, \ldots, \chi_r\}$ são completamente determinados pelos valores $\chi_i(x_j)$, $1 \leq i, j \leq r$.

	C_1	C_2	$\ldots$	C_r
χ_1	$\chi_1(x_1)$	$\chi_1(x_2)$	$\ldots$	$\chi_1(x_r)$
χ_2	$\chi_2(x_1)$	$\chi_2(x_2)$	$\ldots$	$\chi_2(x_r)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_r	$\chi_r(x_1)$	$\chi_r(x_2)$	$\ldots$	$\chi_r(x_r)$

Definição 2.20. A matrix $(\chi_i(x_j))$ definida acima é chamada *tábua de caracteres* do grupo G.

Finalizaremos essa seção encontrando os valores para a tábua de caracteres do grupo simétrico de ordem 6.

Observação 2.21. No próximo exemplo iremos usar representações lineares. Notemos que, se $T : G \to GL_1(K) = K^*$ é tal representação, então G' (subgrupo comutador de G) está contido no Ker (T). De fato, como K^* é um grupo abeliano, para todo $a, b \in G$ temos

$$T(aba^{-1}b^{-1}) = T(a)T(b)T(a^{-1})T(b^{-1}) = T(a)T(a)^{-1}T(b)T(b)^{-1} = 1.$$

Exemplo 2.22. Sejam S_3 o grupo simétrico de ordem 6 e $\mathbb{C}$ o corpo dos números complexos. Sabemos que S_3 possui 3 classes de conjugação $C_1 = \{(1)\}$, $C_2 = \{(12), (13), (23)\}$ e $C_3 = \{(123), (132)\}$ com representantes $1 = (1)$, $t = (12)$ e $c = (123)$.

Consideremos η a representação regular de S_3 sobre $\mathbb{C}$. Então devemos ter $\eta = n_1T_1 \oplus n_2T_2 \oplus n_3T_3$. Logo, o caracter regular é da forma $\rho = \sum_{i=1}^{3} \chi_i(1)\chi_i$, com $\chi_i(1) = n_i$, $1 \leq i \leq 3$. Como $\rho(1) = |S_3| = 6$ e $\rho(g) = 0$ se $g \neq 1$ temos

$$\sum_{i=1}^{3} \chi_i(1)^2 = 6 \quad \text{e} \quad \sum_{i=1}^{3} \chi_i(1)\chi_i(g) = 0 \ \text{ para } \ g \in S_3,\ g \neq 1. \tag{2.6}$$

Notemos que, o grau das representações irredutíveis T_i é dado por $deg(T_i) = \chi_i(1)$, $1 \leq i \leq 3$. Como $\sum_{i=1}^{3} \chi_i(1)^2 = 6$, a única possibilidade para $deg(T_i)$, $1 \leq i \leq 3$, será $deg(T_1) = 1$, $deg(T_2) = 1$ e $deg(T_3) = 2$, ou seja, temos duas representações irredutíveis lineares e uma representação irredutível de grau 2.

Primeiramente vamos encontrar os valores para as representações lineares de S_3. Sabemos da observação anterior que as representações lineares de S_3 possuem o subgrupo comutador S_3' contido em seus núcleos. Como $S_3' = \{1, c, c^{-1}\}$ devemos ter $\chi_1(c) = 1$ e $\chi_2(c) = 1$.

Agora, observemos que a representação linear coincide com seu caracter, então o fato que $t^2 = 1$ implica que $\chi_i(t)^2 = \chi_i(t^2) = 1$, e portanto, $\chi_i(t) = \pm 1$, para $i = 1, 2$. Comparando os valores já encontrados das representações lineares devemos ter $\chi_1(t) \neq \chi_2(t)$, pois, caso contrário, teríamos duas representações lineares irredutíveis

iguais. Portanto, temos $\chi_1(t) = 1$ e $\chi_2(t) = -1$. Colocando os resultados obtidos na tábua temos

	1	t	c
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	α	β

.

Resta-nos encontrar os valores de α e β. Usando (2.6) para $g = t$ vem

$$\chi_1(1)\chi_1(t) + \chi_2(1)\chi_2(t) + \chi_3(1)\chi_3(t) = 0.$$

Substituindo os valores já encontrados na equação acima obtemos

$$1 + (-1) + 2\alpha = 0,$$

que nos dá $\alpha = 0$. Repetindo (2.6) para $g = c$, conseguimos $\beta = -1$, completando a tábua de caracter de S_3.

Capítulo 3

Álgebras e Involuções

O objetivo inicial deste capítulo é apresentar os principais conceitos e resultados sobre álgebras centrais simples. Além disso, vamos introduzir a noção de involuções sobre anéis, bem como algumas de suas propriedades. É importante ressaltar que o estudo de involuções tem bons resultados quando essas são definidas sobre tipos especiais de álgebras. Nosso segundo objetivo, neste capítulo, é apresentar resultados envolvendo involuções sobre álgebras semisimples.

3.1 Álgebras Centrais Simples

Iremos relacionar a estrutura de anel e de módulo em um mesmo conjunto, assim, obteremos uma nova estrutura um pouco mais complexa, a qual definiremos a seguir.

Definição 3.1. Sejam R um anel comutativo com unidade e A um anel, tal que A tem uma estrutura de R-módulo. Dizemos que A é uma *R-álgebra* (ou *álgebra sobre* R) se satisfaz a seguinte condição:

$$r(ab) = (ra)b = a(rb) \text{ para todo } r \in R \ e \ a, b \in A.$$

Veremos agora alguns exemplos importantes de álgebras. Os exemplos mais comuns são as extensões de corpos, isto é, se K é um corpo, então toda extensão L de K é uma K-álgebra. Outro exemplo, que por sinal utilizaremos bastante, é o seguinte:

Exemplo 3.2. Seja $R[G]$ o anel de grupo. Este é uma R-álgebra com a estrutura de R-módulo dada por

$$r\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G}(ra_g)g \quad \text{com } r, a_g \in R;\ \ g \in G.$$

Dizemos que $R[G]$ é a *álgebra de grupo* de G sobre R.

Notemos que a álgebra de grupo $R[G]$ tem como base o grupo G sobre R, e portanto, sua dimensão é igual a $|G|$, quando G for finito.

Exemplo 3.3. Se K é um corpo, definimos uma K-álgebra tendo como base os elementos $\{1, i, j, k\}$ em que a multiplicação satisfaz

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

Todo elemento dessa álgebra é 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 $\mathbb{H}$.

No decorrer desta seção, K denotará um corpo e A uma K-álgebra. É importante notarmos que K está contido em A, pois $K \simeq K.1 \subset A$. Vamos 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

$$Z_A(B) = \{x \in A \ ;\ xb = bx \ \text{ para todo } b \in B\}.$$

No caso em que $B = A$, então $Z_A(A)$ é denominado o *centro* de A, que denotaremos simplesmente por $Z(A)$. Uma K-álgebra A é dita *central* se $Z(A) = K$. Se A é uma K-álgebra simples e central dizemos que A é uma *álgebra central simples*.

Exemplo 3.5. O anel das matrizes $M_n(K)$ é uma álgebra central simples sobre K, pois no Capítulo 1, vimos que seus únicos ideais bilaterais são os triviais. Além disso, o centro dessa álgebra é K.

Agora iremos mostrar algumas propriedades de uma álgebra central simples que serão importante para demonstrarmos o Teorema de Skolen-Noether. Como conseqüência deste, teremos que todo automorfismo sobre uma álgebra central simples será um automorfismo interno. No que segue, assumiremos que o leitor tenha conhecimento do conceito de produto tensorial, bem como de algumas de suas propriedades. Caso necessite mais informações sobre esse assunto, recomendamos ver [10], Capítulo 2, pg. 117.

Teorema 3.6. (1) *Se A e B são K-álgebras e $A' \subset A$, $B' \subset B$ são subalgebras, então $Z_{A\otimes B}(A' \otimes B') = Z_A(A') \otimes Z_B(B')$. 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: (1) Para mostrarmos $Z_{A\otimes B}(A'\otimes B') \subset Z_A(A')\otimes Z_B(B')$, tomemos $x \in Z_{A\otimes B}(A' \otimes B')$. Como A e B são K-álgebras finitamente geradas, vamos considerar $\alpha = \{a_1, \ldots, a_m\}$, $\beta = \{b_1, \ldots, b_n\}$ bases de A e B respectivamente. Um fato conhecido é que o conjunto $\{a_i \otimes b_j \ ; \ i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ forma uma base de $A \otimes B$. Por conta disso, x pode ser escrito de modo único na forma $x = \sum_{i,j} \lambda_{ij}(a_i \otimes b_j)$, com $\lambda_{ij} \in K$. Ainda, usando propriedades do produto tensorial, podemos reescrever x do seguinte modo:

$$x = \sum_{j}^{n} \left(\sum_{i}^{m} a_i \lambda_{ij} \right) \otimes b_j = \sum_{j}^{n} x_j \otimes b_j,$$

com $x_j = \sum a_i \lambda_{ij} \in A$. Como $\alpha = \{a_1, \ldots, a_m\}$ é uma base para A sobre K, segue que todos x_j são unicamente determinados. Notemos que, dado $a \in A'$ devemos ter $(a \otimes 1)x = x(a \otimes 1)$, pois $x \in Z_{A\otimes B}(A' \otimes B')$ e $a \otimes 1 \in A' \otimes B'$, assim

$$(ax_1 \otimes b_1) + \cdots + (ax_n \otimes b_n) = (x_1 a \otimes b_1) + \cdots + (x_n a \otimes b_n).$$

Como essa representação é única, obtemos que $x_i \in Z_A(A')$. De modo análogo, con-

seguimos representar x por $x = \sum_i^m a_i \otimes \left(\sum_j^n b_j \lambda_{ij} \right) = \sum_i^m a_i \otimes y_i$, com $y_i = \sum_j^n b_j \lambda_{ij}$ também unicamente determinados. Dessa forma, se considerarmos $\{a_1, \ldots, a_k\}$ uma base de $Z_A(A')$ sobre K, teremos $x = a_1 \otimes y_1 + \cdots + a_k \otimes y_k$. Então para cada $b \in B'$ obtemos $(1 \otimes b)x = x(1 \otimes b)$. Logo,

$$(a_1 \otimes by_1) + \cdots + (a_k \otimes by_k) = (a_1 \otimes y_1 b) + \cdots + (a_k \otimes y_k b),$$

e pela unicidade da representação, temos que $y_i \in Z_B(B')$. Portanto, $x \in Z_A(A') \otimes Z_B(B')$.

Reciprocamente, se $x \otimes y \in Z_A(A') \otimes Z_B(B')$, então $ax \otimes by = xa \otimes yb$, para todo $a \in A'$ e $b \in B'$. Usando as propriedades de produto tensorial obtemos

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

Disso concluímos que $x \otimes y \in Z_{A \otimes B}(A' \otimes B')$.

Agora, se A e B são centrais, então $Z_A(A) = Z_B(B) = K$. Isso implica que $Z_{A \otimes B}(A \otimes B) = K \otimes K = K$, ou seja, $A \otimes B$ também é central.

(2) Vamos mostrar que os únicos ideais bilaterais de $A \otimes B$ são os triviais. De fato, consideremos I um ideal bilateral não nulo de $A \otimes B$. Primeiramente assumimos que I contém um elemento $a \otimes b \neq 0$. Notemos que, os ideais bilaterais de A e B gerados por a e b, respectivamente, são os próprios A e B, pois A e B são simples. Logo, existem $\alpha_i, \alpha_i' \in A$ e $\beta_i, \beta_i' \in B$ tais que $\sum \alpha_i a \alpha_i' = 1 = \sum \beta_i b \beta_i'$, isso 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.

Agora, faremos a prova do caso geral. Para isso escolhemos $x \in I$ não-nulo com a representação $x = (c_1 \otimes b_1) + \cdots + (c_k \otimes b_k)$, sendo $c_i \in A$, $b_i \in B$ e k o menor possível, no sentido que todo elemento não nulo em I deve ser representado com pelo menos k parcelas. Notemos que, sem perda de generalidade, podemos assumir $c_k = 1$. Com efeito, o fato que $c_k \neq 0$, implica que o ideal bilateral gerado por c_k

deve ser o próprio A, pois A é simples, logo existem $\alpha_i, \alpha_i' \in A$ tais que $\sum \alpha_i c_k \alpha_i' = 1$. Então, caso $c_k \neq 1$, x pode ser substituído por $x' = \sum(\alpha_i \otimes 1)x(\alpha_i' \otimes 1)$. Como I é um ideal bilateral e $x \in I$, devemos ter $x' \in I$, além disso, x' tem k parcelas e

$$\begin{aligned} x' &= (\sum \alpha_i c_1 \alpha_i') \otimes b_1 + (\sum \alpha_i c_2 \alpha_i') \otimes b_2 + \cdots + (\sum \alpha_i c_k \alpha_i') \otimes b_k \\ &= c_1' \otimes b_1 + c_2' \otimes b_2 + \cdots + 1 \otimes b_k, \end{aligned}$$

com $c_j' = \sum \alpha_i c_j \alpha_i' \in A$. Mostraremos agora que necessariamente $k = 1$, e pelo caso anterior teremos que $A \otimes B$ é simples. Suponhamos, por absurdo, que $k > 1$. Observemos que c_{k-1} e c_k são linearmente independentes, pois, caso contrário, 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 nos dá uma representação para x com um número menor que k parcelas. Desde que $c_k = 1 \in Z(A) = K$, devemos ter $c_{k-1} \notin Z(A)$, pois dois elementos de um corpo são linearmente dependentes. Como $c_{k-1} \notin Z(A)$, existe $a \in A$ tal que $ac_{k-1} - c_{k-1}a \neq 0$. Coloquemos $y = (a \otimes 1)x - x(a \otimes 1) \in I$, ou seja, $y = (ac_1 - c_1 a) \otimes b_1 + \cdots + (ac_{k-1} - c_{k-1}a) \otimes b_{k-1}$. Usando o fato que os elementos b_i são linearmente independentes e um dos somandos acima é não nulo, obtemos que a soma total é não nula, isto é, $y \neq 0$. Nesse caso, conseguimos um elemento $y \in I$, $y \neq 0$ representado com um número menor que k parcelas, o que é absurdo. Portanto $k = 1$, como desejávamos.

(3) Segue diretamente dos ítens (1) e (2). ■

No que segue, A° denotará o anel oposto de A, como já foi definido no Capítulo 1. Claramente $A = A^{\circ\circ}$ e $A = A^\circ$ se, e somente se, A é comutativo. Em geral A e A° não são isomorfos. Se a K-álgebra A é uma álgebra central simples, então A° também é uma álgebra central simples, pois A e A° possuem os mesmos ideais bilaterais e $Z(A) = Z(A^\circ)$.

Teorema 3.7. *Seja A uma álgebra central simples sobre K. Então $A \otimes A^\circ \simeq M_n(K)$, onde $n = dim_K A$.*

Demonstração: Primeiramente, notemos que A é um espaço vetorial sobre K, e um fato conhecido da teoria de álgebra linear é o de que $M_n(K) \simeq \mathrm{End}_K(A)$. Por conta disso, é suficiente mostrarmos que $A \otimes A^\circ \simeq \mathrm{End}_K(A)$. De fato, definamos $\psi : A \times A^\circ \to \mathrm{End}_K(A)$ associando cada par $(a, b) \in A \times A^\circ$ a aplicação $\psi(a, b) : A \to A$ dada por $\psi(a, b)(x) = axb$ para todo $x \in A$. Não é difícil verificarmos que $\psi(a, b)$ é um homomorfismo de K-módulos, e portanto, $\psi(a, b) \in \mathrm{End}_K(A)$.

Além disso, $\psi(a+b, c)(x) = (a+b)xc = axc+bxc = \psi(a, c)(x)+\psi(b, c)(x)$, para todo $x \in A$. Do mesmo modo, mostramos que $\psi(a, b+c)(x) = \psi(a, b)(x)+\psi(a, c)(x)$, para todo $x \in A$. Também, temos que $\psi(\lambda a, b)(x) = \lambda axb = ax\lambda b = \psi(a, \lambda b)(x)$, para todo $x \in A$ e $\lambda \in K$. Com isso, mostramos que ψ é bilinear. Ainda, como $\psi(ac, b \circ d)(x) = a\,c\;\; x\;\; d\,b = a(c\; x\; d)b = \psi(a, b)(c\,x\,d) = \psi(a, b)\psi(c, d)(x)$, obtemos que ψ é multiplicativa. Nesse caso, usando a Propriedade Universal do Produto Tensorial garantimos a existência de um homomorfismo de álgebras $\varphi : A \otimes A^\circ \to \mathrm{End}_K(A)$. Assim $\mathrm{Ker}\,(\varphi)$ é um ideal de $A \otimes A^\circ$, que é simples. Logo, $\mathrm{Ker}\,(\varphi) = (0)$, e portanto, φ é injetora. Como $A \otimes A^\circ$ e $\mathrm{End}_K(A)$ possuem as mesmas dimensões, φ é sobrejetora e segue o isomorfismo $A \otimes A^\circ \simeq \mathrm{End}_K(A)$. ■

Observação 3.8. Se A é uma álgebra central simples sobre K e $E = \mathrm{End}_K(A) \simeq A \otimes A^\circ$, então A e A° podem ser consideradas como subalgebras de E, usando as identificações $a \leftrightarrow a\otimes 1$ e $b \leftrightarrow 1\otimes b$. Dessa forma, os elementos de A correspondem às multiplicações à esquerda e os elementos de A° às multiplicações à direita. Portanto, além de A ser um K-módulo, A também pode ser visto como um A-módulo, um A°-módulo e um E-módulo. Agora, usando o Teorema 3.6, segue que existem os seguintes isomorfismos canônicos $\mathrm{End}_A(A) \simeq Z_E(A) \simeq A^\circ$ e $\mathrm{End}_A(A) \simeq Z_E(A^\circ) \simeq A$. Sendo que o isomorfismo $\mathrm{End}_A(A) \simeq Z_E(A)$ vem da definição de centralizador.

É importante ressaltarmos que se A é uma K-álgebra e α um elemento inversível de A, então $x \to \alpha x\alpha^{-1}$ é um *automorfismo interno* de A, o qual denotaremos por $int(\alpha)$.

Finalizaremos essa seção provando o Teorema de Skolem-Noether, que caracteriza os automorfismos sobre uma álgebra central simples. Um fato interessante, é que esse teorema foi publicado por Skolem em 1927 e essas publicações eram feitas em periódicos noruegueses com limitada circulação internacional. Isso fez com que Emmy Noether redescobrisse o mesmo teorema independentemente após alguns anos.

Teorema 3.9. (Skolem-Noether) *Sejam A uma álgebra central simples sobre K e B uma K-álgebra simples. Sejam $\sigma, \tau : B \to A$ homomorfismos de álgebras. Então existe um automorfismo interno φ de A tal que $\tau = \varphi\sigma$.*

Demonstração: Primeiramente, consideremos o caso em que $A = \mathrm{End}_K(V)$, com V um K-espaço vetorial. Assim, V é também um A-módulo. Usando a aplicação σ podemos ver V como B-módulo da seguinte forma: $b.x = \sigma(b).x$ para todo $x \in V$ e $b \in B$. Analogamente, usando τ podemos ver V como um B-módulo. Estes B-módulos serão denotados por V_σ e V_τ. Por [12], Teorema 1.8, pg 283, temos que V_σ e V_τ são isomorfos como B-módulos. Consideremos $f : V_\tau \to V_\sigma$ um B-isomorfismo. Assim temos

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

para todo $b \in B$ e $x \in V$. Isso nos dá $\tau(b) = f^{-1}(\sigma b)f$. Uma vez que $f \in A$, neste caso, temos o resultado.

Para a demonstração do caso geral, consideremos as aplicações

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

Por hipótese, A é uma álgebra central simples, logo A° também o é. Além disso, como B é simples, o Teorema 3.6 implica que $B \otimes A^\circ$ é simples. Pelo caso anterior, existe um $f \in A \otimes A^\circ$, inversível, tal que $(\tau b) \otimes a = f^{-1}((\sigma b) \otimes a)f$, para todo $b \in B$ e $a \in A^\circ$.

Tomando $b = 1$, obtemos $\tau(1) \otimes a = f^{-1}(\sigma(1) \otimes a)f$ e, como $\tau(1) = \sigma(1) = 1$, vem $f(1 \otimes a) = (1 \otimes a)f$, para todo $a \in A^{\circ}$. Disso concluímos que f comuta com todos elementos de $1 \otimes A^{\circ}$. Pela Observação 3.8, $f = g \otimes 1$ para algum $g \in A$. Agora, fazendo $a = 1$, como $(\tau b) \otimes a = f^{-1}((\sigma b) \otimes a)f$, temos $(\tau b) \otimes 1 = (g \otimes 1)^{-1}((\sigma b) \otimes 1)(g \otimes 1)$. Disso segue que $\tau b = g^{-1}(\sigma b)g$, para todo $b \in B$. ■

Corolário 3.10. *Se A é uma álgebra central simples, então todo automorfismo φ de A é um automorfismo interno.*

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

3.2 Involuções

Nesta seção, daremos o conceito de involuções sobre anéis, definiremos involuções de primeira e segunda espécie e, apresentaremos alguns exemplos que serão importantes no decorrer do trabalho.

Definição 3.11. Seja R um anel. Uma aplicação $\sigma : R \to R$ é chamada *involução* sobre R se satisfaz:

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

para todo $x, y \in R$. O par (R, σ) é chamado de *anel com involução.*

Neste contexto, os homomorfismos de anéis que nos interessam são aqueles que preservam a involução.

Definição 3.12. Se $f : (R, \sigma) \to (S, \tau)$ é um homomorfismo de anéis satisfazendo $\tau(f(x)) = f(\sigma(x))$, então dizemos que f é um *homomorfismo de anéis com involução.*

Observação 3.13. Se A é uma K-álgebra, uma involução $\sigma : A \to A$ não é necessariamente K-linear. Se $Z(A)$ é o centro de A, então devemos ter $\sigma(Z(A)) \subset Z(A)$.

Com efeito, tomemos $y \in Z(A)$ e mostremos que $\sigma(y)x = x\sigma(y)$, para todo $x \in A$. Uma vez que $y\sigma(x) = \sigma(x)y$, para todo $x \in A$, aplicando σ em ambos os lados da última igualdade vem $x\sigma(y) = \sigma(y)x$, para todo $x \in A$, como queríamos.

Dessa forma, $\sigma : Z(A) \to Z(A)$ é uma involução e temos duas opções:

(i) $\sigma_{|_{Z(A)}}$ é a identidade. Nesse caso, dizemos que σ é de *primeira espécie*. Como $K \subset Z(A)$, essas involuções são K-lineares.

(ii) $\sigma_{|_{Z(A)}}$ não é a identidade, ou seja, $\sigma_{|_{Z(A)}}$ é um automorfismo não-trivial de K, então σ é chamada involução σ de *segunda espécie*.

Apresentaremos agora alguns exemplos de involuções.

Exemplo 3.14. Chamamos de conjugação complexa a involução $\overline{\ }$ sobre $\mathbb{C}$ dada por $\overline{(a+bi)} = (a-bi)$. Esta é uma involução de segunda espécie, pois $Z(\mathbb{C}) = \mathbb{C}$ e a conjugação não é a identidade em $\mathbb{C}$. Se K é um corpo, 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 3.15. Se $\mathbb{H}$ é a álgebra dos Hamiltonianos sobre um corpo K, definida no Exemplo 3.3. A aplicação $\overline{\ } : \mathbb{H} \to \mathbb{H}$ definida por $\overline{a+bi+cj+dk} = a-bi-cj-dk$ é uma involução, conhecida como *involução canônica* sobre $\mathbb{H}$. Este é um exemplo de involução de primeira espécie, pois $Z(\mathbb{H}) = K$ e a involução canônica restrita a K é a identidade.

Exemplo 3.16. Consideremos o anel das matrizes $M_n(D)$, com D um anel comutativo. A transposição de matrizes é uma involução de primeira espécie sobre esse anel, visto que $Z(M_n(D)) = Z(D) = D$ e a transposta de uma matriz escalar é ela mesma.

Exemplo 3.17. Seja D um anel comutativo com uma conjugação $\overline{\ }$. A conjugada transposta $^{-t}$ sob o anel de matrizes $M_n(D)$, definida por $(a_{ij})^{-t} = (\overline{a_{ij}})^t$, é uma involução de segunda espécie.

É importante salientarmos que a involução do exemplo anterior não é uma composição de involuções, pois a conjugação dos elementos das matrizes não é uma involução em $M_n(D)$. Na verdade, a composição de involuções só será uma involução quando o anel, em que estão definidas, for comutativo.

O próximo exemplo de involução será estudado com mais detalhes no próximo capítulo.

Exemplo 3.18. Consideremos G um grupo finito e K um corpo. A aplicação $\sigma : K[G] \to K[G]$, 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 grupo $K[G]$.

Agora veremos que a composição de duas involuções é um automorfismo. De fato, sejam σ, τ involuções sobre uma álgebra A e $x, y \in A$, então temos

$\sigma\tau(x+y) = \sigma(\tau(x) + \tau(y)) = \sigma\tau(x) + \sigma\tau(y)$ e

$\sigma\tau(x.y) = \sigma(\tau(y)\tau(x)) = \sigma\tau(x) \,.\, \sigma\tau(y)$.

Assim, $\sigma\tau$ é um homomorfismo de anéis. Agora, usando o fato que σ e τ são bijeções, segue que $\sigma\tau$ é um automorfismo de A. Se A é uma álgebra central simples, então, pelo Teorema de Skolem-Noether 3.9, e seu corolário, $\sigma\tau$ é um automorfismo interno.

3.3 Involuções sobre Álgebras Semisimples

Para melhor entendimento do assunto a ser tratado nesta seção fizemos uma breve introdução aplicando os resultados obtidos anteriormente a uma álgebra semisimples com involução.

Seja A uma álgebra semisimples de dimensão finita sobre um corpo K. No Capítulo 1, vimos que A tem uma única decomposição como soma direta de componentes simples: $A = \bigoplus_{i=1}^{l} A_i$, sendo cada A_i gerado por um idempotente primitivo

central e_i. Durante este trabalho, denotaremos por S um conjunto completo de idempotentes ortogonais primitivos centrais de A: $S = \{e_1, e_2, \ldots, e_l\}$.

Agora, consideremos $\sigma : A \to A$ uma involução sobre A e observemos que $A = \sigma(A) = \bigoplus_{i=1}^{l} \sigma(A_i)$. Uma vez que a decomposição de A como soma direta de componentes simples é única (não somente única a menos de isomorfismo), devemos ter $\sigma(A_i) = A_j$, para algum j. Se $i \neq j$, a restrição de σ em 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 $A_i = \sigma(\sigma(A_i)) = \sigma(A_j)$. Então, podemos considerar $\overline{\sigma}$ a involução definida sobre $A_i \times A_j$ por $\overline{\sigma}(a_i, a_j) = (\sigma(a_j), \sigma(a_i))$. Denotemos por A_i° o anel oposto de A_i e por τ a involução sobre $A_i \times A_i^\circ$ dada por $\tau(x, y) = (y, x)$. Assim, a aplicação $\psi : (A_i \times A_j, \overline{\sigma}) \to (A_i \times A_i^\circ, \tau)$, definida por $\psi(a_i, a_j) = (a_i, \sigma(a_j))$, é um isomorfismo de anéis com involução.

Esta seção será motivada pelo seguinte problema: determinar condições necessárias e suficientes para que a restrição de σ em cada componente simples A_i de A seja uma involução sobre A_i, ou seja, que $\sigma(A_i) = A_i$, para todo $1 \leq i \leq l$. Para tanto, começaremos com alguns resultados auxiliares.

Definição 3.19. Sejam (B, τ) um anel com involução e I um ideal à direita de B, então o *ideal ortogonal* $I^\perp$ com respeito a τ é definido por

$$I^\perp = \{b \in B : \tau(y)b = 0, \text{ para todo } y \in I\},$$

ou seja, $I^\perp$ é o anulador à direita de $\tau(I)$.

Lema 3.20. *Se e é um idempotente de (B, τ), então $(eB)^\perp = (1 - \tau(e))B$.*

Demonstração: Seja $x \in (eB)^\perp$, então $\tau(eb)x = 0$, para todo $b \in B$, em particular, fazendo $b = 1$ temos $\tau(e)x = 0$. Logo, $x = x - \tau(e)x = (1 - \tau(e))x$, isso implica que $x \in (1-\tau(e))B$. Por outro lado, dado $x \in (1-\tau(e))B$, temos que $x = (1-\tau(e))a$, para algum $a \in B$. Como $\tau(eb)x = \tau(b)\tau(e)(1-\tau(e))a = \tau(b)\tau(e)a-\tau(b)\tau(e^2)a = 0$, para todo $b \in B$, concluímos que $x \in (eB)^\perp$. Portanto, $(eB)^\perp = (1 - \tau(e))B$. ■

Lema 3.21. *Para cada idempotente $e_i \in S$, existe algum $e_j \in S$ tal que $\sigma(e_i) = e_j$.*

Demonstração: Sabemos que $\sigma(A_i) = A_j$, para algum $1 \leq j \leq l$. Portanto, $\sigma(e_i) \in A_j$ e, obtemos $\sigma(e_i)e_j = \sigma(e_i)$, pois e_j é o elemento identidade de A_j (ver Observação 1.58). Aplicando σ em ambos os lados da última igualdade segue $e_i = \sigma(e_j)e_i$. Analogamente, como $\sigma(e_j) \in A_i$, temos $\sigma(e_j)e_i = \sigma(e_j)$. Logo, $e_i = \sigma(e_j)e_i = \sigma(e_j)$. Novamente aplicando σ na última igualdade obtemos $\sigma(e_i) = e_j$, como desejávamos. ■

Proposição 3.22. *As seguintes condições são equivalentes:*

(1) $\sigma(A_i) = A_i$.

(2) $\sigma(e_i) = e_i$.

(3) $A_i^{\perp} = (1 - e_i)A$.

(4) $A_i \cap A_i^{\perp} = (0)$.

(5) *Existe $x \in A_i$, tal que $\sigma(x)x \neq 0$.*

Demonstração: Vamos mostrar que (1) implica (2). Então suponhamos que $\sigma(A_i) = A_i$ e observemos que, pelo Lema 3.21, temos que $\sigma(e_i) = e_j$, para algum $1 \leq j \leq l$. Da hipótese, segue que $e_j = \sigma(e_i) \in A_i$, assim $e_j \in A_i \cap A_j$. Agora, se $i \neq j$, então $A_i \cap A_j = (0)$, isso implica que $e_j = 0$, o que não pode ocorrer, pois e_j é um idempotente não nulo. Com isso devemos ter $i = j$ e conseqüentemente $\sigma(e_i) = e_i$.

Agora, assumimos que a condição (2) vale e mostremos (3). Observemos primeiro que e_i é um idempotente tal que $A_i = e_iA$, aplicando o Lema 3.20 obtemos $A_i^{\perp} = (1-\sigma(e_i))A$. Agora, usando o fato que $\sigma(e_i) = e_i$, concluímos $A_i^{\perp} = (1-e_i)A$.

Para mostrarmos que (3) implica (4), tomemos $x \in A_i \cap A_i^{\perp}$, então $x \in A_i$ e $x \in A_i^{\perp}$. Temos por hipótese que $A_i^{\perp} = (1 - e_i)A$, assim $x = (1 - e_i)a$, para

algum $a \in A$. Sabemos também que $x = e_i x$, pois $x \in A_i$. Disso, segue que $x = e_i x = e_i(1 - e_i)a = e_i a - e_i^2 a = 0$, e portanto, $A_i \cap A_i^{\perp} = (0)$.

Na seqüência, assumiremos que $A_i \cap A_i^{\perp} = (0)$ para provarmos a condição (5). Na verdade, vamos mostrar que $e_i \in A_i$ satisfaz $\sigma(e_i)e_i = e_i \neq 0$ e assim seguirá o resultado. Com efeito, como e_i é um idempotente central de A, devemos ter $A_i = e_i A = Ae_i$, e portanto, $e_i - \sigma(e_i)e_i \in A_i$. Agora, observemos que o Lema 3.20 nos dá que $A_i^{\perp} = (1 - \sigma(e_i))A$. Disso segue que $e_i - \sigma(e_i)e_i = (1 - \sigma(e_i))e_i \in A_i^{\perp}$. Logo, $e_i - \sigma(e_i)e_i \in A_i \cap A_i^{\perp} = (0)$ e, concluímos que $\sigma(e_i)e_i = e_i \neq 0$.

Finalmente, assumimos que existe $x \in A_i$ satisfazendo $\sigma(x)x \neq 0$, queremos mostrar que $\sigma(A_i) = A_i$. Já sabemos que $\sigma(A_i) = A_j$, para algum $1 \leq j \leq l$, e portanto, $\sigma(x) \in A_j$. Se $i \neq j$, então $\sigma(x)x \in A_j A_i = (0)$, o que implica $\sigma(x)x = 0$, contrariando a escolha de x. Logo, devemos ter $i = j$ e segue $\sigma(A_i) = A_i$. ■

O lema a seguir mostra que todo idempotente central de A pode ser representado como soma de elementos de S.

Lema 3.23. *Para todo idempotente central $e \in A$, existe um subconjunto I de $\{1, 2, \ldots, l\}$ tal que $e = \sum_{i \in I} e_i$.*

Demonstração: Seja e um idempotente central de A. Usando o fato que $1 = \sum_{i=1}^{l} e_i$, obtemos $e = e.1 = \sum_{i=1}^{l} ee_i$. Veremos que $ee_i = e_i$ ou $ee_i = 0$, para cada $i \in \{1, 2, \ldots, l\}$, disso seguirá o resultado. Com efeito, temos que e_i é um idempotente central primitivo. O fato que ee_i e $(1 - e)e_i$ são idempotentes ortogonais centrais tais que $e_i = ee_i + (1 - e)e_i$, implica que $ee_i = e_i$ ou $ee_i = 0$, para todo $1 \leq i \leq l$. ■

Proposição 3.24. *As seguintes condições são equivalentes:*

(1) *Todo ideal bilateral de A é invariante por σ.*

(2) *$\sigma(e) = e$, para todo idempotente central $e \in A$.*

(3) *$\sigma(A_i) = A_i$, para toda componente simples A_i de A.*

Demonstração: Suponhamos (1) e mostremos a validade de (2). Seja e um idempotente central de A, logo $I = Ae$ é um ideal bilateral de A. Assim $\sigma(I) = I$ e, em particular, $\sigma(e) \in Ae$. Logo, podemos escrever $\sigma(e) = xe$, para algum $x \in A$, então $\sigma(e)e = xe^2 = xe = \sigma(e)$. Aplicando σ em ambos os lados da última igualdade, obtemos $\sigma(e)e = e$. Portanto, segue que $\sigma(e) = \sigma(e)e = e$.

Para provarmos que (2) implica (3), basta observarmos que $A_i = Ae_i$, com e_i um idempotente central de A. Por hipótese, $\sigma(e_i) = e_i$ e, aplicando a Proposição 3.22, segue que $\sigma(A_i) = A_i$.

Agora assumindo (3) mostraremos (1). Suponhamos que todo A_i é invariante pela σ. A Proposição 3.22 nos dá $\sigma(e_i) = e_i$, para todo $1 \leq i \leq l$. Agora, se I é um ideal bilateral de A, então, pelo Teorema 1.60, existe um idempotente central $e \in A$ tal que $I = eA = Ae$. Assim, pelo Lema 3.23, segue que existe um subconjunto J de $\{1, 2, \ldots, l\}$ tal que $e = \sum_{j \in J} e_j$. Então, $\sigma(e) = \sum_{j \in J} \sigma(e_j) = \sum_{j \in J} e_j = e$, e portanto, $\sigma(I) = \sigma(eA) = \sigma(A)\sigma(e) = Ae = I$, como desejávamos. ■

Definição 3.25. Seja (B, τ) um anel com involução, dizemos que τ é *anisotrópica* se, para todo $b \in B$ tal que $\tau(b)b = 0$, tivermos $b = 0$.

Veremos na próxima proposição algumas condições necessárias e suficientes para que σ seja anisotrópica. Para sua demonstração, necessitaremos do seguinte lema. Sua demonstração requer alguns conceitos novos e, para evitar que este trabalho fique muito extenso, daremos apenas uma referência.

Lema 3.26. *Seja (B, τ) uma álgebra simples com involução. As seguintes afirmações são equivalentes.*

(1) *τ é anisotrópica.*

(2) *Todo ideal à direita de B é gerado por um elemento idempotente simétrico, ou seja, $I = eB$, para algum $e \in B$, satisfazendo $\tau(e) = e$.*

Demonstração: Ver [2], Corolário 1.8, pg. 465. ■

Proposição 3.27. *As seguintes condições são equivalentes:*

(1) *Se e é um idempotente em A tal que $\sigma(e)e = 0$, então $e = 0$.*

(2) *σ é anisotrópica.*

(3) *Para todo ideal à direita $I \subset A$, temos $I \cap I^{\perp} = (0)$.*

(4) *Para todo ideal à direita $I \subset A$, existe um idempotente $e \in A$ tal que $I = eA$ e $\sigma(e) = e$.*

Mais ainda, se alguma destas condições é válida, então $\sigma(A_i) = A_i$ para todo $1 \leq i \leq l$.

Demonstração: (1) $\Rightarrow$ (2) Seja $a \in A$ satisfazendo $\sigma(a)a = 0$. Vamos mostrar que $a = 0$. Para isso, consideremos o ideal à direita $I = aA$ de A. Como A é semisimples, pelo Teorema 1.42, existe um idempotente e tal que $I = eA$. Desde que $e \in I$, obtemos $e = ax$, para algum $x \in A$. Logo, $\sigma(e)e = \sigma(ax)ax = \sigma(x)\sigma(a)ax = 0$. Assim, por hipótese, devemos ter $e = 0$. Disso segue que $I = (0)$, uma vez que $a \in I$, concluímos que $a = 0$, como desejávamos.

(2) $\Rightarrow$ (3) Seja I um ideal à direita de A. Dado $x \in I \cap I^{\perp}$, pela definição de $I^{\perp}$, $\sigma(u)x = 0$, para todo $u \in I$, em particular, $\sigma(x)x = 0$, pois $x \in I$. Agora, usando o fato que σ é anisotrópica, concluímos que $x = 0$, e portanto, $I \cap I^{\perp} = (0)$.

(3) $\Rightarrow$ (1) Suponhamos que e é um idempotente de A satisfazendo $\sigma(e)e = 0$. Consideremos $I = eA$, o ideal à direita de A gerado por e. Já temos que $e \in I$, se mostrarmos que $e \in I^{\perp}$, então $e \in I \cap I^{\perp} = (0)$, assim concluiremos que $e = 0$. Para isso, mostremos que $\sigma(ex)e = 0$, para todo $x \in A$. De fato, $\sigma(ex)e = \sigma(x)\sigma(e)e = 0$. Logo, $e \in I^{\perp}$, como queríamos.

(2) $\Rightarrow$ (4) Primeiramente vamos mostrar que se I é um ideal à direita de $A = \bigoplus_{i=1}^{l} A_i$, então $I = \beta_1 A_1 + \cdots + \beta_l A_l$ com β_i idempotente em A_i. Com efeito, o fato que $I = eA$, para algum idempotente e, implica que $I = eA = eA_1 + \cdots + eA_l$. Ainda, como $e \in A$ temos que $e = \beta_1 + \cdots + \beta_l$, com $\beta_i \in A_i$. Sabemos que $e^2 = e$,

logo $\beta_i^2 = \beta_i$, para todo $1 \leq i \leq l$. Assim

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

Dessa forma, $I = \beta_1 A_1 + \cdots + \beta_l A_l$, com β_i idempotente em A_i.

Podemos escrever $I = I_1 + \cdots + I_l$, sendo I_i o ideal à direita de A_i gerado por β_i. Como σ é anisotrópica, então $A_i \cap A_i^{\perp} = (0)$, daí, pela Proposição 3.22, temos $\sigma(A_i) = A_i$, e portanto, (A_i, σ) é uma álgebra simples com involução. De acordo com o Lema 3.26, cada ideal I_i é gerado por um $\alpha_i \in A_i$, tal que α_i é idempotente simétrico, ou seja, $I_i = \alpha_i A_i$ e $\sigma(\alpha_i) = \alpha_i$. Fixemos $f = \alpha_1 + \cdots + \alpha_l$. Podemos observar que α_i, α_j são idempotentes ortogonais, para todo $i \neq j$, visto que $\alpha_i \in A_i$ e $\alpha_j \in A_j$. Disso segue que f também é idempotente, pois $f^2 = (\alpha_1 + \ldots + \alpha_l)(\alpha_1 + \ldots + \alpha_l) = \alpha_1^2 + \ldots + \alpha_l^2 = \alpha_1 + \ldots + \alpha_l = f$. Mais ainda, $\sigma(f) = \sigma(\alpha_1 + \ldots + \alpha_l) = \sigma(\alpha_1) + \ldots + \sigma(\alpha_l) = \alpha_1 + \ldots + \alpha_l = f$.

Agora podemos mostrar que $I = fA$. De fato, se $x \in I$, então podemos escrever $x = \alpha_1 a_1 + \ldots + \alpha_l a_l$. Usando o fato que, $\alpha_i a_j \in A_i A_j = (0)$, se $i \neq j$, segue que

$$x = \alpha_1 a_1 + \ldots + \alpha_l a_l = (\alpha_1 + \ldots + \alpha_l)(a_1 + \ldots + a_l) = f(a_1 + \ldots + a_l) \in fA.$$

Por outro lado, tomemos $x \in fA$, então $x = f(a_1 + \ldots + a_l)$, com $a_i \in A_i$. Logo,

$$x = f(a_1 + \ldots + a_l) = (\alpha_1 + \ldots + \alpha_l)(a_1 + \ldots + a_l) = \alpha_1 a_1 + \ldots + \alpha_l a_l \in I_1 + \ldots + I_l = I.$$

(4) $\Rightarrow$ (2) Queremos mostrar que σ é anisotrópica. Então, seja a um elemento de A satisfazendo $\sigma(a)a = 0$. Consideremos o ideal à direita $I = aA$. Por hipótese, existe um idempotente simétrico $e \in A$ tal que $I = eA$. Uma vez que $e \in I = aA$, podemos escrever $e = ab$, para algum $b \in A$. Logo, $e = e.e = \sigma(e)e = \sigma(b)\sigma(a)ab = 0$, o que implica $a = 0$ e obtemos o desejado.

Finalmente, se σ é anisotrópica, então como já foi visto, $A_i \cap A_i^{\perp} = (0)$, assim, pela Proposição 3.22, obtemos $\sigma(A_i) = A_i$, para todo $1 \leq i \leq l$. ■

No próximo capítulo veremos um contra-exemplo provando que a condição "σ anisotrópica" não é necessária para termos $\sigma(A_i) = A_i$, para todo $1 \leq i \leq l$.

Corolário 3.28. *Se σ é anisotrópica, então para todo ideal à direita $I \subset A$, temos $A = I \oplus I^{\perp}$.*

Demonstração: Seja I um ideal à direita de A. A Proposição 3.27, garante que existe um único idempotente simétrico $e \in A$ tal que $I = eA$, e mais $I \cap I^{\perp} = (0)$. Assim basta mostrar que $A = I + I^{\perp}$. Usando o fato que $\sigma(e) = e$, o Lema 3.20 nos dá $I^{\perp} = (eA)^{\perp} = (1 - \sigma(e))A = (1 - e)A$. Logo, dado $a \in A$, sempre podemos escrever $a = ea + (1 - e)a \in eA + (1 - e)A = I + I^{\perp}$. ■

Vamos finalizar essa seção mostrando um resultado de extensão de involuções.

Proposição 3.29. *Sejam A uma álgebra semisimples de dimensão finita e τ uma involução sobre uma componente simples A_i de A. Se A tem uma involução, então τ pode ser estendida para uma involução sobre A.*

Demonstração: Seja σ uma involução sobre A. Já vimos que $\sigma(A_i) = A_j$, para algum $1 \leq j \leq l$.

(1) Se $i \neq j$, consideremos a aplicação $\theta : A \to A$ definida por:

$$\theta\left(\sum_{i=1}^{l} a_i\right) = \tau(a_i) + \sigma\tau\sigma(a_j) + \sum_{k \neq i,j} \sigma(a_k).$$

(2) Se $\sigma(A_i) = A_i$, seja θ o endomorfismo definido sobre A por:

$$\theta\left(\sum_{i=1}^{l} a_i\right) = \tau(a_i) + \sum_{k \neq i} \sigma(a_k).$$

Não é difícil, porém trabalhoso, verificarmos que a aplicação θ, definida acima, é uma involução sobre A. Também, claramente $\theta|_{A_i} = \tau$ em ambos os casos. ■

Capítulo 4

Involução Canônica de $K[G]$

Este capítulo é baseado no artigo [4], "Involutions of semisimple group algebras" de Boulagouaz e Oukhtite. Faremos um estudo da involução canônica de $K[G]$, mais precisamente, daremos condições necessárias e suficientes para que esta involução restrita à cada componente simples de $K[G]$ induza uma involução de primeira espécie nas componentes. Em seguida, como aplicação desses resultados, para o caso em que K é real fechado, obteremos uma versão melhorada para o Teorema 13.3 do Capítulo 8, Sharlau [12], no caso em que G for um (c)-grupo. Encerraremos nosso trabalho dedicando a última seção para o estudo dos (c)-grupos, visto que estes tiveram um papel relevante para alguns dos resultados obtidos neste capítulo.

4.1 Restrição às Componentes Simples

Primeiramente, veremos algumas propriedades da álgebra de grupo $K[G]$ e faremos algumas considerações.

Sejam G um grupo finito e K um corpo tal que $char(K) \nmid |G|$. Pelo Teorema de Maschke 1.75, temos que $K[G]$ é uma álgebra de grupo semisimples de dimensão finita. Assim $K[G] = \bigoplus_{i=1}^{l} A_i$, sendo cada componente simples A_i gerada por um idempotente primitivo central $e_i \in K[G]$. Denotaremos $l = G(K)$. Como anteriormente, S denotará o conjunto completo $\{e_1, \ldots, e_{G(K)}\}$ de idempotentes primitivos

centrais de $K[G]$ e C_g a classe de equivalência dos conjugados de g em G.

Vimos no Teorema 2.19 que se tomarmos $e_{\chi_i} = \frac{\chi_i(1)}{|G|}\sum_{g\in G}\chi_i(g^{-1})g$, onde χ_i é um caracter irredutível de G sobre $\overline{K}$ (fecho algébrico de K), então $\overline{S} = \{e_{\chi_1}, \ldots, e_{\chi_{s(G)}}\}$ é um conjunto completo de idempotentes primitivos centrais de $\overline{K}[G]$, onde $s(G)$ é o número de classes de conjugação de G. Portanto, obtemos $\overline{K}[G] = \bigoplus_{i=1}^{s(G)} \overline{K}[G]e_{\chi_i}$.

O próximo resultado nos mostra que os idempotentes centrais de $K[G]$ nada mais são do que somas de idempotentes centrais de $\overline{K}[G]$.

Lema 4.1. *Para cada idempotente central $e \in K[G]$, existem $i_1 < i_2 < \ldots < i_t \in [1, s(G)]$ tais que $e = \sum_{j=1}^{t} e_{\chi_{i_j}}$.*

Demonstração: Dado $e \in K[G]$ um idempotente central, obviamente e é um idempotente de $\overline{K}[G]$. Se mostrarmos que e é central em $\overline{K}[G]$, então aplicando o Lema 3.23 concluiremos que existem $i_1 < i_2 < \ldots < i_t \in [1, s(G)]$ tais que $e = \sum_{j=1}^{t} e_{\chi_{i_j}}$. Para isso, consideremos $g_1, \ldots, g_{s(G)}$ representantes das classes de conjugação de G. Se definirmos $\gamma_{g_i} = \sum_{h\in C_{g_i}} h$, então pelo Teorema 1.81, segue que $\{\gamma_{g_1}, \ldots, \gamma_{g_{s(G)}}\}$ é uma base para os espaços vetoriais $Z(K[G])$ e $Z(\overline{K}[G])$ sobre K e $\overline{K}$ respectivamente. Em virtude disso e do fato que $K \subset \overline{K}$ devemos ter $Z(K[G]) \subset Z(\overline{K}[G])$. Agora, notemos que $e \in Z(K[G])$, assim, a última inclusão nos mostra que e é um idempotente central de $\overline{K}[G]$. Como queríamos. ■

Lema 4.2. *Seja*

$$I = \{(i_1, \ldots, i_{t_r}) \in [1, s(G)]^{t_r} : \ i_1 < \ldots < i_{t_r} \ e \ \sum_{j=1}^{t_r} e_{\chi_{i_j}} \in K[G] \ \textit{com } t_r \ \textit{minimal}\}.$$

Então o número de componente simples de $K[G]$ é igual a cardinalidade de I, isto é, $|I| = G(K)$.

Demonstração: Primeiramente mostremos que, para $(i_1, \ldots, i_{t_r}) \in I$, o elemento $e_r = \sum_{l=1}^{t_r} e_{\chi_{i_l}}$ é um idempotente primitivo central de $K[G]$. Como os $e_{\chi_{i_l}}$ são idempotentes centrais, temos imediatamente que e_r é um idempotente central de $K[G]$. Resta-nos mostrar que e_r é primitivo. Pela definição de I, temos que $J = \{i_1, \ldots, i_{t_r}\}$ é minimal, no sentido que, para todo subconjunto $\{i_1^{'}, \ldots, i_t^{'}\} \subsetneq J$, $e = \sum_{m=1}^{t} e_{\chi_{i_m^{'}}} \notin K[G]$.

Suponhamos que e_r não é primitivo, logo existem $e_r^{'}$ e $e_r^{''}$ idempotentes centrais ortogonais não nulos de $K[G]$ tais que $e_r = e_r^{'} + e_r^{''}$. Assim, pelo lema acima, existem $j_1 < \ldots < j_{t_r^{'}} \in [1, s(G)]$ e $k_1 < \ldots < k_{t_r^{''}} \in [1, s(G)]$ tais que $e_r^{'} = \sum_{m=1}^{t_r^{'}} e_{\chi_{jm}}$ e $e_r^{''} = \sum_{n=1}^{t_r^{''}} e_{\chi_{k_n}}$. Denotemos $J^{'} = \{j_1, \ldots, j_{t_r^{'}}\}$ e $J^{''} = \{k_1, \ldots, k_{t_r^{''}}\}$.

O fato que $e_r^{'}.e_r^{''} = 0$ e $\{e_{\chi_1}, \ldots, e_{\chi_{s(G)}}\}$ é um conjunto de idempotentes ortogonais, implica que $J^{'} \cap J^{''} = \emptyset$. Além disso, como $e_r^2 = e_r$ temos

$$\left(\sum_{l=1}^{t_r} e_{\chi_{i_l}}\right)\left(\sum_{m=1}^{t_r^{'}} e_{\chi_{jm}} + \sum_{n=1}^{t_r^{''}} e_{\chi_{k_n}}\right) = \sum_{l=1}^{t_r} e_{\chi_{i_l}},$$

isso implica que todo $e_{\chi_{i_l}}$ com $i_l \in J$ deve fazer parte da soma do segundo fator, ou seja, $i_l \in J^{'} \cup J^{''}$. Logo, $J \subseteq J^{'} \cup J^{''}$. Na verdade, $J = J^{'} \cup J^{''}$. Suponhamos que exista $p \in J^{'} \cup J^{''}$ tal que $p \notin J$, então

$$e_{\chi_p}.e_r = e_{\chi_p}\left(\sum_{l=1}^{t_r} e_{\chi_{i_l}}\right) = 0,$$

pois $p \notin J$. Por outro lado,

$$e_{\chi_p}.e_r = e_{\chi_p}\left(\sum_{m=1}^{t_r^{'}} e_{\chi_{jm}} + \sum_{n=1}^{t_r^{''}} e_{\chi_{k_n}}\right) = e_{\chi_p}^2 = e_{\chi_p},$$

visto que $p \in J^{'} \cup J^{''}$. Assim, teríamos $e_{\chi_p} = 0$, o que é absurdo. Logo, $J^{'} \subset J$ e $J^{''} \subset J$. Isto contraria a minimalidade de J, pois $e_r^{'} \in K[G]$ e $e_r^{''} \in K[G]$.

Dessa forma, obtemos, para cada $(i_1, \ldots, i_{t_r}) \in I$, uma componente simples $A_r = K[G]e_r$ de $K[G]$, isso nos diz que $|I| \leq G(K)$.

Reciprocamente, o Lema 4.1 mostra que para cada $e_r \in S$, existem $i_1 < \ldots < i_{t_r} \in [1, s(G)]$ tais que $e_r = \sum_{l=1}^{t_r} e_{\chi_{i_l}}$. Vamos mostrar que t_r é minimal. Suponhamos que $J = \{i_1, \ldots, i_{t_r}\}$ não é minimal, ou seja, existe um subconjunto $J' = \{j_1, \ldots, j_{t'_r}\} \subsetneq J$ tal que $e'_r = \sum_{m=1}^{t'_r} e_{\chi_{j_m}} \in K[G]$. Tome $J'' = \{k_1, \ldots, k_{t''_r}\} = J \setminus J'$. Notemos que $e''_r = \sum_{n=1}^{t''_r} e_{\chi_{k_n}}$ é um idempotente central de $K[G]$ tal que

$$e_r = \sum_{l=1}^{t_r} e_{\chi_{i_l}} = \left(\sum_{m=1}^{t'_r} e_{\chi_{j_m}} + \sum_{n=1}^{t''_r} e_{\chi_{k_n}} \right) = e'_r + e''_r \quad \text{e} \quad e'_r . e''_r = 0,$$

contradizendo o fato que e_r é primitivo. Logo, t_r é minimal. Com isso, obtemos que $(i_1, \ldots, i_{t_r}) \in I$ e conseqüentemente $G(K) \leq |I|$. Portanto, $G(K) = |I|$. ■

No que segue σ denotará a involução canônica de $K[G]$ definida por $\sigma(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g g^{-1}$. No teorema abaixo obtemos uma condição necessária e suficiente para que σ restrita à cada componente simples de $K[G]$ seja uma involução de primeira espécie.

Teorema 4.3. *As seguintes condições são equivalentes:*

(1) $\sigma(A_i) = A_i$, *para toda componente simples* A_i *de* $K[G]$.

(2) *Se* $(i_1, \ldots, i_t) \in I$, *então* $\sum_{j=1}^{t} \chi_{i_j}(1)(\chi_{i_j}(g) - \chi_{i_j}(g^{-1})) = 0$, *para todo* $g \in G$.

Mais ainda, se estas condições são válidas, então para cada componente simples A_i *de* $K[G]$, *que não é isomorfa a* K, *a restrição de* σ *em* A_i *é uma involução de primeira espécie se, e somente se, para todo* $g \in G$ *temos* $(\gamma_g - \gamma_{g^{-1}})e_i = 0$.

Demonstração: Vamos mostrar que (1) implica (2), para isso tomemos $(i_1, \ldots, i_t) \in I$. Pelo provado acima temos que $e_t = \sum_{j=1}^{t} e_{\chi_{i_j}}$ é um idempotente primitivo central de $K[G]$. Portanto, $A_t = K[G]e_t$ é uma componente simples de $K[G]$ e, por hipótese, temos $\sigma(A_t) = A_t$. Agora, usando a Proposição 3.22 segue que $\sigma(e_t) = e_t$.

Substituindo $e_{\chi_{i_j}} = \dfrac{\chi_{i_j}(1)}{|G|}\sum_{g\in G}\chi_{i_j}(g^{-1})g$ na igualdade $e_t = \sum_{j=1}^{t} e_{\chi_{i_j}}$, obtemos

$$e_t = \frac{1}{|G|}\sum_{g\in G}\left(\sum_{j=1}^{t}\chi_{i_j}(1)\chi_{i_j}(g^{-1})\right)g.$$

Aplicando σ em e_t vem

$$\sigma(e_t) = \frac{1}{|G|}\sum_{g\in G}\left(\sum_{j=1}^{t}\chi_{i_j}(1)\chi_{i_j}(g^{-1})\right)g^{-1} = \frac{1}{|G|}\sum_{g\in G}\left(\sum_{j=1}^{t}\chi_{i_j}(1)\chi_{i_j}(g)\right)g.$$

O fato que $\sigma(e_t) = e_t$ implica que $\sum_{j=1}^{t}\chi_{i_j}(1)\chi_{i_j}(g) = \sum_{j=1}^{t}\chi_{i_j}(1)\chi_{i_j}(g^{-1})$, para todo $g \in G$, ou seja, $\sum_{j=1}^{t}\chi_{i_j}(1)(\chi_{i_j}(g) - \chi_{i_j}(g^{-1})) = 0$, para todo $g \in G$.

Suponhamos que a condição (2) valha e mostremos (1). Então, seja A_i uma componente simples de $K[G]$, sabemos que existe um idempotente central primitivo $e_i \in K[G]$ tal que $A_i = K[G]e_i$. Mais ainda, vimos anteriormente que existe $(i_1, \ldots, i_{t_i}) \in I$ tal que $e_i = \sum_{j=1}^{t_i} e_{\chi_{i_j}} = \dfrac{1}{|G|}\sum_{g\in G}\left(\sum_{j=1}^{t_i}\chi_{i_j}(1)\chi_{i_j}(g^{-1})\right)g$. Portanto,

$$\sigma(e_i) = \frac{1}{|G|}\sum_{g\in G}\left(\sum_{j=1}^{t_i}\chi_{i_j}(1)\chi_{i_j}(g)\right)g.$$

Desde que $(i_1, \ldots, i_{t_i}) \in I$, por hipótese obtemos

$$\sum_{j=1}^{t_i}\chi_{i_j}(1)\chi_{i_j}(g) = \sum_{j=1}^{t_i}\chi_{i_j}(1)\chi_{i_j}(g^{-1}),$$

para todo $g \in G$. Substituindo na equação anterior, segue que

$$\sigma(e_i) = \frac{1}{|G|}\sum_{g\in G}\left(\sum_{j=1}^{t_i}\chi_{i_j}(1)\chi_{i_j}(g^{-1})\right)g = e_i.$$

Com isso, mostramos que a condição (2) da Proposição 3.22 ocorre, e portanto, $\sigma(A_i) = A_i$, como desejávamos.

Finalmente, assumimos que alguma dessas condições é satisfeita e que A_i é uma componente simples de $K[G]$, que não é isomorfa a K. Primeiramente, mostremos

que $Z(A_i)$ é gerado por $\{\gamma_{g_1}e_i, \ldots, \gamma_{g_{s(G)}}e_i\}$. Para tanto, basta mostrarmos que $Z(A_i) = Z(K[G])e_i$. Claramente $Z(K[G])e_i \subset Z(A_i)$, por outro lado, dado $x \in Z(A_i)$, temos que $xa_i = a_ix$, para todo $a_i \in A_i$. Uma vez que $x \in A_i$ segue que $x = e_ix = xe_i$, assim, tomando um elemento arbitrário $a \in K[G]$, vem $xa = xe_ia = xae_i = ae_ix = ax$, pois $ae_i \in A_i$, e portanto, $x \in Z(K[G])$.

Disso, decorre que a restrição de σ sobre A_i é de primeira espécie se, e somente se, $\sigma(\gamma_{g_i}e_i) = \gamma_{g_i}e_i$, isto é, $\gamma_{g_i^{-1}}e_i = \gamma_{g_i}e_i$, ou ainda, $(\gamma_{g_i} - \gamma_{g_i^{-1}})e_i = 0$, para $i \in \{1, \ldots, s(G)\}$. Agora, dado $g \in G$, temos que $g \in C_{g_i}$ para algum i, e assim $\gamma_g = \gamma_{g_i}$. Portanto, σ restrita a A_i é de primeira espécie se, e somente se, $(\gamma_g - \gamma_{g^{-1}})e_i = 0$ para todo $g \in G$. ■

Proposição 4.4. *Para cada caracter irredutível χ_i de G sobre $\overline{K}$ consideremos $K(\chi_i) = K\{\chi_i(g) : g \in G\}$ a extensão de K gerada por $\{\chi_i(g) : g \in G\}$ e K, e $Gal(K(\chi_i)/K)$ o seu grupo de Galois. Então cada componente simples A_i de $K[G]$ é da forma $A_i = K[G]e_{\chi_i}$, onde $e_{\chi_i} = \dfrac{\chi_i(1)}{|G|}\displaystyle\sum_{g\in G} Tr_{K(\chi_i)/K}(\chi_i(g^{-1}))g$.*

Demonstração: Ver [13], Proposição 1.1, pg. 4. ■

Proposição 4.5. *Se K é um corpo com característica zero, então as seguintes condições são equivalentes:*

(1) *$\sigma(A_i) = A_i$, para toda componente simples A_i de $K[G]$.*

(2) *Para todo caracter irredutível χ_i de G sobre $\overline{K}$:*

$$Tr_{K(\chi_i)/K}(\chi_i(g) - \chi_i(g^{-1})) = 0, \quad \textit{para todo } g \in G.$$

Demonstração: Suponhamos que (1) é válido e vamos provar (2). Primeiramente, para cada caracter irredutível χ_i de G sobre $\overline{K}$ coloquemos

$$e_i = \frac{\chi_i(1)}{|G|}\sum_{g\in G} Tr_{K(\chi_i)/K}(\chi_i(g^{-1}))g.$$

Então, pela Proposição 4.4 segue que $A_i = K[G]e_i$ é uma componente simples de $K[G]$ e, pelo Lema 4.1, existe $(i_1, \ldots, i_{t_i}) \in I$ tal que $e_i = \sum_{j=1}^{t_i} e_{\chi_{i_j}}$. Disso, obtemos

$$e_i = \sum_{g\in G} \left(\frac{\chi_i(1)}{|G|} Tr_{K(\chi_i)/K}(\chi_i(g^{-1})) \right) g = \sum_{g\in G} \left(\frac{1}{|G|} \sum_{j=1}^{t_i} \chi_{i_j}(1)\chi_{i_j}(g^{-1}) \right) g,$$

e portanto, $\chi_i(1)Tr_{K(\chi_i)/K}(\chi_i(g^{-1})) = \sum_{j=1}^{t_i} \chi_{i_j}(1)\chi_{i_j}(g^{-1})$, para todo $g \in G$.

Usando o Teorema 4.3, vem

$$\sum_{j=1}^{t_i} \chi_{i_j}(1)\chi_{i_j}(g) = \sum_{j=1}^{t_i} \chi_{i_j}(1)\chi_{i_j}(g^{-1}), \quad \text{para todo } g \in G.$$

Dessa forma, $\chi_i(1)Tr_{K(\chi_i)/K}(\chi_i(g)) = \chi_i(1)Tr_{K(\chi_i)/K}(\chi_i(g^{-1}))$, para todo $g \in G$, isto é, $Tr_{K(\chi_i)/K}(\chi_i(g) - \chi_i(g^{-1})) = 0$, para todo $g \in G$.

Agora assumindo (2) vamos provar (1). Se A_i é uma componente simples de $K[G]$, pela Proposição 4.4, existe algum caracter irredutível χ_i de G sobre $\overline{K}$ tal que $A_i = K[G]e_i$, onde $e_i = \frac{\chi_i(1)}{|G|} \sum_{g\in G} Tr_{K(\chi_i)/K}(\chi_i(g^{-1}))g$. Como

$$\sigma(e_i) = \frac{\chi_i(1)}{|G|} \sum_{g\in G} Tr_{K(\chi_i)/K}(\chi_i(g^{-1}))g^{-1} = \frac{\chi_i(1)}{|G|} \sum_{g\in G} Tr_{K(\chi_i)/K}(\chi_i(g))g$$

e por hipótese $Tr_{K(\chi_i)/K}(\chi_i(g)) = Tr_{K(\chi_i)/K}(\chi_i(g^{-1}))$, para todo $g \in G$, obtemos

$$\sigma(e_i) = \frac{\chi_i(1)}{|G|} \sum_{g\in G} Tr_{K(\chi_i)/K}(\chi_i(g^{-1}))g = e_i.$$

Logo, pela Proposição 3.22, concluímos que $\sigma(A_i) = A_i$. ■

O próximo resultado nos diz que, para um corpo ordenado K, a condição (1) da proposição anterior é sempre válida.

Proposição 4.6. *Se K é um corpo ordenado e G um grupo finito, então $\sigma(A_i) = A_i$ para toda componente simples A_i de $K[G]$.*

Demonstração: Pelo Teorema 3.26, basta mostrarmos que neste caso σ é anisotrópica. Para isso, seja $x = \sum_{g\in G} a_g g$ um elemento de $K[G]$, então

$$\sigma(x)x = \sum_{g\in G} a_g g^{-1} \sum_{h\in G} a_h h = \sum_{g\in G}\sum_{h\in G}(a_g a_h)(g^{-1}h),$$

fazendo $\mu = g^{-1}h$, obtemos

$$\sigma(x)x = \sum_{\mu\in G} b_\mu \mu,$$

com $b_\mu = \sum_{g^{-1}h=\mu} a_g a_h$. Logo, $\sigma(x)x = 0$ se, e somente se, $b_\mu = 0$ para cada $\mu \in G$. Em particular, tomando $\mu = 1$, segue que $0 = b_1 = \sum_{g=h} a_g a_h = \sum_{g\in G} a_g^2$. Como K é um corpo ordenado, pela Observação 1.25, devemos ter $a_g = 0$, para todo $g \in G$. Portanto, $x = 0$. ■

O próximo resultado estabelece mais condições para que a involução canônica de $K[G]$ seja de primeira espécie em cada uma de suas componentes simples, tais condições envolvem a estrutura de G e seus caracteres.

Definição 4.7. Seja G um grupo finito, dizemos que G é um *(c)-grupo* se para todo $g \in G$ temos $g \sim g^{-1}$, isto é, existe $\gamma \in G$ tal que $\gamma g \gamma^{-1} = g^{-1}$.

Teorema 4.8. *As seguintes condições são equivalentes:*

(1) *G é um (c)-grupo.*

(2) *A restrição de σ ao $Z(K[G])$ é a identidade.*

(3) *$\sigma_{|_{A_i}}$ é uma involução de primeira espécie, para todo $1 \leq i \leq G(K)$.*

(4) *Para cada caracter irredutível χ_i de G em $\overline{K}$, temos $\chi_i(g) = \chi_i(g^{-1})$, para todo $g \in G$.*

Demonstração: (1) $\Rightarrow$ (2) Claramente σ é K-linear, como $\{\gamma_{g_1}, \ldots, \gamma_{g_{s(G)}}\}$ é uma base para o K-espaço vetorial $Z(K[G])$, é suficiente mostrarmos que $\sigma(\gamma_{g_i}) = \gamma_{g_i}$, para todo $1 \leq i \leq s(G)$. De fato, temos por hipótese que G é um (c)-grupo, assim

$C_g = C_{g^{-1}}$, para todo $g \in G$. Logo,

$$\sigma(\gamma_{g_i}) = \sum_{h \in C_{g_i}} h^{-1} = \sum_{x \in C_{g_i^{-1}}} x = \sum_{x \in C_{g_i}} x = \gamma_{g_i}, \quad \text{para todo } 1 \leq i \leq s(G).$$

(2) $\Rightarrow$ (3) Suponhamos que $\sigma_{|_{Z(K[G])}}$ é a identidade. Uma vez que $e_i \in Z(K[G])$ obtemos $\sigma(e_i) = e_i$, para todo $1 \leq i \leq s(G)$. Aplicando a Proposição 3.22 decorre $\sigma(A_i) = A_i$, para todo $1 \leq i \leq s(G)$. Portanto, $\sigma_{|_{A_i}}$ é uma involução. Para provarmos que $\sigma_{|_{A_i}}$ é de primeira espécie, tomemos $x \in Z(A_i)$, o fato que $Z(A_i) = Z(K[G])e_i \subset Z(K[G])$ implica que $x \in Z(K[G])$. Por hipótese temos $\sigma(x) = x$, e portanto, $\sigma_{|_{A_i}}$ é uma involução de primeira espécie.

(3) $\Rightarrow$ (1) Assumimos que $\sigma_{|_{A_i}}$ é uma involução de primeira espécie, para todo $1 \leq i \leq s(G)$. Mostremos que $g \sim g^{-1}$, para todo $g \in G$. Com efeito, observemos que $\sum_{h \in C_g} he_i \in Z(K[G])e_i = Z(A_i)$, para todo $1 \leq i \leq s(G)$. Por hipótese temos $\sigma\left(\sum_{h \in C_g} he_i\right) = \sum_{h \in C_g} he_i$, ou seja, $\sum_{h \in C_g} h^{-1}e_i = \sum_{h \in C_g} he_i$, para todo $1 \leq i \leq s(G)$. Agora, usando o fato que $1 = \sum_{i=1}^{G(K)} e_i$ obtemos

$$\sum_{h \in C_g} h^{-1}.1 = \sum_{i=1}^{G(K)} \left(\sum_{h \in C_g} h^{-1}e_i\right) = \sum_{i=1}^{G(K)} \left(\sum_{h \in C_g} he_i\right) = \sum_{h \in C_g} h.1\,.$$

Como G é uma base de $K[G]$, estas somas tem as mesmas parcelas e obtemos que $C_g = C_{g^{-1}}$, para todo $g \in G$. Portanto, G é um (c)-grupo.

(1) $\Rightarrow$ (4) Suponhamos que G é um (c)-grupo, assim $C_g = C_{g^{-1}}$, para todo $g \in G$. Uma vez que o caracter é constante nas classes de conjugação, concluímos que $\chi_i(g) = \chi_i(g^{-1})$, para todo $g \in G$.

(4) $\Rightarrow$ (3) Vamos mostrar que σ é uma involução de primeira espécie em cada componente simples de $\overline{K}[G]$. Primeiramente, mostremos que $\sigma(A_i) = A_i$, para todo $1 \leq i \leq s(G)$. Para isso, observemos que as seqüências em I, nesse caso, tem comprimento um e $|I| = s(G)$. Então, seja $(j) \in I$ e $g \in G$, por hipótese, temos

$\chi_j(g)-\chi_j(g^{-1})=0$ e isso implica que $\chi_j(1)(\chi_j(g)-\chi_j(g^{-1}))=0$. Assim a condição (2) do Teorema 4.3 é satisfeita, e portanto, $\sigma(A_i)=A_i$, para toda componente simples A_i de $\overline{K}[G]$.

Resta-nos mostrar que σ fixa os elementos do $Z(A_i)$. De fato, relembremos que $A_i \simeq M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia isomorfa de $\overline{K}$ em seu centro. Como $\overline{K}$ é algebricamente fechado, devemos ter $D_i=\overline{K}$, assim $A_i \simeq M_{n_i}(\overline{K})$. Disso segue que $Z(A_i) \simeq Z(M_{n_i}(\overline{K})) \simeq \overline{K}$. Como a involução canônica fixa os elementos de $\overline{K}$, temos o resultado. ■

Vimos, na Proposição 3.27 do capítulo anterior, que a condição "σ anisotrópica" implica $\sigma(A_i)=A_i$, para todo $1 \leq i \leq G(K)$. Como aplicação do Teorema 4.8, segue um contra-exemplo mostrando que a recíproca não é verdadeira.

Contra-exemplo 4.9. Consideremos S_3 o grupo simétrico e $\mathbb{C}$ o corpo dos números complexos. Sabemos que $S_3=\{1,t,c,tc,tc^{-1},c,c^{-1}\}$, onde $t^2=(tc)^2=(tc^{-1})^2=c^3=1$ e $tct^{-1}=c^{-1}$. Mais ainda, S_3 possui 3 classes de conjugação: $C_1=\{1\}$, $C_2=\{t,tc,tc^{-1}\}$ e $C_3=\{c,c^{-1}\}$. Não é difícil verificarmos que S_3 é um (c)-grupo.

Vimos no Capítulo 2, que a tábua de caracteres de S_3 sobre $\mathbb{C}$ é a seguinte:

	1	t	c
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Portanto, $\mathbb{C}[S_3]=\bigoplus_{i=1}^{3} A_i$, com A_i gerado por $e_{\chi_i}=\dfrac{\chi_i(1)}{|S_3|}\sum_{g\in S_3}\chi_i(g^{-1})g$. Mais precisamente, $e_{\chi_1}=\dfrac{1}{6}(\gamma_1+\gamma_t+\gamma_c)$, $e_{\chi_2}=\dfrac{1}{6}(1-\gamma_t+\gamma_c)$ e $e_{\chi_3}=\dfrac{1}{3}(2-\gamma_c)$. Como S_3 é um (c)-grupo, o Teorema 4.8 nos dá $\sigma(A_i)=A_i$, para todo $1 \leq i \leq 3$. Porém, mostraremos que σ não é anisotrópica, ou seja, exibiremos um elemento $e \in \mathbb{C}[S_3]$ tal que $e \neq 0$ e satisfaz $\sigma(e)e=0$.

De fato, sabemos que $\sigma(A_i) = A_i$, para todo $1 \leq i \leq 3$, assim, pela Proposição 3.22, devemos ter $\sigma(e_{\chi_i}) = e_{\chi_i}$, para todo $1 \leq i \leq 3$. Agora substituindo $e_{\chi_3} = \frac{1}{3}(2 - \gamma_c)$ em $ce_{\chi_3} + c^{-1}e_{\chi_3}$ obtemos

$$ce_{\chi_3} + c^{-1}e_{\chi_3} = -e_{\chi_3}. \tag{4.1}$$

Então, se tomarmos $x = \frac{i}{\sqrt{3}}(1 + 2c)e_{\chi_3} \in A_3$ e usarmos (4.1), teremos $x^2 = e_{\chi_3}$ e $\sigma(x) = -x$. Com isso, podemos mostrar que $e = \frac{1}{2}(e_{\chi_3} + x) \neq 0$ é um idempotente de A_3 satisfazendo $\sigma(e) = e_{\chi_3} - e$. Logo, $\sigma(e)e = (e_{\chi_3} - e)e = e_{\chi_3}e - e^2 = e - e = 0$.

Finalizaremos essa seção mostrando que se G é um (c)-grupo finito e A_i é uma componente simples de $K[G]$, então toda involução de primeira espécie sobre A_i pode ser obtida a partir de σ.

Proposição 4.10. *Sejam G um (c)-grupo finito e τ uma involução sobre uma componente simples A_i de $K[G]$. Então as seguintes condições são equivalentes:*

(1) *τ é uma involução de primeira espécie sobre A_i.*

(2) *$\tau = int(a_i) \circ \sigma_{|_{A_i}}$, para algum $a_i \in A_i$ inversível tal que $\sigma(a_i) = \pm a_i$.*

Demonstração: Assumimos que τ é uma involução de primeira espécie sobre A_i, e mostremos a validade de (2). Para isso, consideremos $F_i = Z(A_i)$. Como $A_i \simeq M_{n_i}(D_i)$ com D_i um anel com divisão, temos que $F_i = Z(A_i) \simeq Z(M_{n_i}(D_i)) \simeq Z(D_i)$. É fácil verificarmos que $Z(D_i)$ é um corpo, e portanto, F_i também o é. Vamos mostrar que $\tau \circ \sigma_{|_{A_i}} : A_i \to A_i$ é um F_i-automorfismo. Com efeito, sendo G um (c)-grupo, a condição (1) do Teorema 4.8 é satisfeita, logo, $\sigma_{|_{A_i}}$ também é uma involução de primeira espécie. Dessa forma, temos $\tau \circ \sigma_{|_{A_i}}(\lambda a) = \tau(\lambda \sigma_{|_{A_i}}(a)) = \lambda\tau(\sigma_{|_{A_i}}(a)) = \lambda(\tau \circ \sigma_{|_{A_i}}(a))$, para todo $a \in A_i$ e $\lambda \in F_i$.

Agora, observemos que A_i é uma F_i-álgebra central simples, então, pelo Teorema de Skolen-Noether 3.9 e seu Corolário 3.10, existe $a_i \in A_i$, inversível, tal que $\tau \circ \sigma_{|_{A_i}} = int(a_i)$. Portanto, $\tau = int(a_i) \circ \sigma_{|_{A_i}}$. Mostremos que $\sigma(a_i) = \pm a_i$. De fato,

como $\tau \circ \tau(x) = x$, obtemos $x = \tau \circ \tau(x) = a_i\sigma(a_i\sigma(x)a_i^{-1})a_i^{-1} = a_i\sigma(a_i^{-1})x\sigma(a_i)a_i^{-1}$, ou ainda, $\sigma(a_i)a_i^{-1}x = x\sigma(a_i)a_i^{-1}$, para todo $x \in A_i$. Isto implica que $\sigma(a_i)a_i^{-1} \in F_i$, logo, existe $\lambda \in F_i$ tal que $\sigma(a_i)a_i^{-1} = \lambda$, ou seja, $\sigma(a_i) = \lambda a_i$. Resta nos mostrar que $\lambda = \pm 1$. Com efeito, $a_i = \sigma(\sigma(a_i)) = \sigma(\lambda a_i) = \lambda\sigma(a_i) = \lambda.\lambda a_i = \lambda^2 a_i$. Logo, $\lambda^2 = 1$ e, como F_i é corpo, devemos ter $\lambda = \pm 1$. Como queríamos provar.

Agora, suponhamos que (2) seja verdadeiro e mostremos (1). Por hipótese $\tau = int(a_i) \circ \sigma_{|_{A_i}}$, para algum $a_i \in A_i$, inversível, tal que $\sigma(a_i) = \pm a_i$. Primeiramente mostremos que τ é uma involução sobre A_i. Realmente, dados $x, y \in A_i$ temos que

$$\tau(x+y) = a_i\sigma(x+y)a_i^{-1} = a_i\sigma(x)a_i^{-1} + a_i\sigma(y)a_i^{-1} = \tau(x) + \tau(y),$$

$$\tau(xy) = a_i\sigma(xy)a_i^{-1} = a_i\sigma(y)\sigma(x)a_i^{-1} = a_i\sigma(y)a_i^{-1}a_i\sigma(x)a_i^{-1} = \tau(y)\tau(x) \text{ e}$$

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

Como $\sigma(a_i) = \pm a_i$, temos duas possibilidades: se $\sigma(a_i) = a_i$, então $\tau(\tau(x)) = a_ia_i^{-1}xa_ia_i^{-1} = x$; caso $\sigma(a_i) = -a_i$ vem $\tau(\tau(x)) = a_i(-a_i^{-1})x(-a_i)a_i^{-1} = -(-x) = x$. Em ambos os casos obtemos $\tau(\tau(x)) = x$. Portanto, τ é uma involução sobre A_i. Para verificarmos que é de primeira espécie, tomemos $\lambda \in Z(A_i)$. Logo, $\tau(\lambda) = a_i\sigma(\lambda)a_i^{-1} = a_i\lambda a_i^{-1} = \lambda a_ia_i^{-1} = \lambda$, ou seja, $\tau_{|_{Z(A_i)}}$ é a identidade. ■

4.2 Involução Canônica de $K[G]$ onde K é Real Fechado

Começaremos esta seção demonstrando o Teorema de Frobenius, o qual nos diz que existem poucas possibilidades para as álgebras com divisão sobre um corpo real fechado. Mas antes, enunciaremos um lema que nos será útil, porém, sua demonstração é um tanto técnica e será omitida.

Lema 4.11. *Sejam D uma álgebra com divisão sobre um corpo K com centro Z, e subcorpo maximal F contendo Z. 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: Ver [6], Teorema 6.6, pg 459. ■

Agora, podemos enunciar e demonstrar o Teorema de Frobenius.

Teorema 4.12. (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 $\mathbb{H}$, dos Hamiltonianos.*

Demonstração: Seja Z o centro de D e F um subcorpo maximal de D que contém Z. Assim temos $D \supset F \supset Z \supset K$, como $dim_K D < \infty$, devemos ter $dim_K F < \infty$, e portanto, F é uma extensão algébrica de K. Conseqüentemente, sendo K real fechado, pelo Corolário 1.31, temos $F = K$ ou $F \simeq K\sqrt{-1}$, logo $dim_K F \leq 2$. Como $dim_K F = dim_Z F \,.\, dim_K Z \leq 2$ vem

$$dim_Z F \leq dim_K F \leq 2, \tag{4.2}$$

donde temos que a $dim_Z F$ é finita. Então pelo lema anterior

$$dim_F D = dim_Z F \quad \text{e} \quad dim_Z D = (dim_Z F)^2. \tag{4.3}$$

Analisando (4.2) e (4.3), as únicas possibilidades para $dim_Z D$ são $dim_Z D = 1$ ou $dim_Z D = 4$. Se $dim_Z D = 1$, por (4.3) temos que $D = F$, e portanto, $D = K$ ou $D \simeq K\sqrt{-1}$.

Se $dim_Z D = 4$, por (4.3) temos $dim_Z F = 2 = dim_F D$. Mas, já vimos que $dim_K F = dim_Z F \,.\, dim_K Z \leq 2$, assim, devemos ter $dim_K Z = 1$ e $dim_K F = 2$. Disso, segue que $Z = K$ e $F \simeq K(\sqrt{-1})$. Além disso, D não é comutativo, caso contrário D seria um corpo, e portanto, extensão algébrica própria de $K(\sqrt{-1})$, contrariando o fato de $K(\sqrt{-1})$ ser algebricamente fechado pelo Teorema 1.30. Uma vez que F é isomorfo a $K(\sqrt{-1})$ podemos representar $F = K(i)$, para algum $i \in F$ tal que $i^2 = -1$. A aplicação $\varphi : F \to F$ 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 3.9, φ pode ser

estendido para um automorfismo interno β de D, dado por $\beta(x) = dxd^{-1}$ para $d \neq 0$, $d \in D$. Como $-i = \beta(i) = did^{-1}$, temos $-id = di$, e $\beta(\beta(i))$ nos dá $id^2 = d^2i$. 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 β são os elementos de K e $\beta(d^2) = dd^2d^{-1} = d^2$, 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 β 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 $k = ij$. Para mostrarmos que $\{1, i, j, k\}$ é uma base de D sobre K, basta considerarmos os conjuntos $D^+ = \{x \in D : xi = ix\}$ e $D^- = \{x \in D : xi = -ix\}$, assim devemos ter $D = D^+ \oplus D^-$, pois dado $x \in D$, podemos escrever $x = \frac{1}{2}(x - ixi) + \frac{1}{2}(x + ixi)$, com $(x - ixi) \in D^+$ e $(x + ixi) \in D^-$. Usando o fato que $\{1, i\}$ e $\{j, k\}$ são conjuntos linearmente independentes em D^+ e D^- respectivamente, sobre K, e $dim_K D^+ = dim_K D^- = 2$, segue que $\{1, i\}$ e $\{j, k\}$ são bases de D^+ e D^- respectivamente, sobre K. Portanto, $\{1, i, j, k\}$ é uma base de D sobre K. Também, não é difícil mostrar que existe um isomorfismo de K-álgebras $D \simeq \mathbb{H}$. ■

Para K real fechado e G um grupo finito, $K[G]$ é semisimples e, pelo Teorema de Frobenius, suas componentes simples são da forma $M_n(D)$ com $D = K$, $K(\sqrt{-1})$ ou $\mathbb{H}$. O teorema a seguir identifica a involução canônica sobre uma componente simples de $K[G]$ com a involução conjugada transposta sobre a álgebra de matrizes.

Teorema 4.13. (Scharlau, [12]) *Seja K um corpo real fechado e G um grupo finito. Então toda componente simples A_i, da álgebra de grupo $K[G]$ é invariante pela involução canônica. Se σ é a involução canônica em $K[G]$ temos que $(A_i, \sigma_{|_{A_i}}) \simeq (M_n(D), t \circ {}^-)$, onde $D = K$, $K(\sqrt{-1})$ ou $\mathbb{H}$ e ${}^-$ é a identidade em K, a conjugação complexa em $K(\sqrt{-1})$ e a involução canônica em $\mathbb{H}$.*

Demonstração: Da Proposição 4.6 segue $\sigma(A_i) = A_i$, visto que todo corpo real fechado é ordenado. Para o resto da demonstração, ver [12], Teorema 13.3. ■

Para o caso em que G é um (c)-grupo, esse teorema pode ser melhorado como segue.

Teorema 4.14. *Sejam K um corpo real fechado e G um grupo finito. Então as seguintes condições são equivalentes:*

(1) *G é um (c)-grupo.*

(2) *Para cada componente simples A_i de $K[G]$ temos*

$$(A_i, \sigma_{|_{A_i}}) \simeq (M_n(K), t) \quad ou \quad (A_i, \sigma_{|_{A_i}}) \simeq (M_n(\mathbb{H}), t \circ {}^-),$$

onde t é a involução transposição e $^-$ é a involução canônica de $\mathbb{H}$.

Demonstração: Suponhamos que G é um (c)-grupo. Pelo Teorema 4.8, segue que $\sigma_{|_{A_i}}$ é uma involução de primeira espécie, para toda componente simples A_i de $K[G]$. Então, usando o Teorema 4.13, devemos ter

$$(A_i, \sigma_{|_{A_i}}) \simeq (M_n(K), t) \quad \text{ou} \quad (A_i, \sigma_{|_{A_i}}) \simeq (M_n(\mathbb{H}), t \circ {}^-),$$

pois $(M_n(K(\sqrt{1})), t \circ {}^-)$ é uma involução de segunda espécie (veja o Exemplo 3.17). Reciprocamente, assumimos $(A_i, \sigma_{|_{A_i}}) \simeq (M_n(K), t)$ ou $(A_i, \sigma_{|_{A_i}}) \simeq (M_n(\mathbb{H}), t \circ {}^-)$ para cada componente simples A_i de $K[G]$. Logo, $\sigma_{|_{A_i}}$ é uma involução de primeira espécie, para toda componente simples A_i de $K[G]$. Aplicando o Teorema 4.8, segue que G é um (c)-grupo. ■

Observação 4.15. O Teorema 4.14 pode ser usado como uma ferramenta importante para determinarmos as componentes simples de $K[G]$, quando K é real fechado. Realmente, vimos que $A_i \simeq M_{n_i}(D_i)$, onde D_i é uma álgebra com divisão de dimensão finita sobre K. Assim, o Teorema 4.13 juntamente com o Teorema 4.14, implica que $M_n(K(\sqrt{-1}))$ participa na decomposição de $K[G]$ se, e somente se, G não é um (c)-grupo.

Na seqüência, veremos algumas condições para que o teorema acima ocorra.

Teorema 4.16. *Sejam G um grupo finito e K um corpo real fechado. Então as seguintes condições são equivalentes:*

(1) *$K(\chi_i) = K$, para todo caracter irredutível χ_i de G sobre $\overline{K}$.*

(2) *$G(K) = s(G)$*

(3) *$\{e_1, e_2, \ldots, e_{G(K)}\}$ é uma base para o K-espaço vetorial $Z(K[G])$.*

(4) *G é um (c)-grupo.*

(5) *$\sigma_{|_{A_i}}$ é uma involução de primeira espécie, para todo $1 \leq i \leq G(K)$.*

Demonstração: (1) $\Leftrightarrow$ (2) Suponhamos que $K(\chi_i) = K$, para todo caracter irredutível χ_i de G sobre $\overline{K}$, então para cada $1 \leq i \leq s(G)$, temos $\chi_i(g) \in K$, para todo $g \in G$. Logo, $e_{\chi_i} \in K[G]$, para todo $1 \leq i \leq s(G)$. Assim $\{e_{\chi_1}, e_{\chi_2}, \ldots, e_{\chi_{s(G)}}\}$ é uma família completa de idempotentes primitivos centrais de $K[G]$, e portanto, necessariamente $G(K) = s(G)$. Reciprocamente, se $G(K) = s(G)$, então, pelo Lema 4.1, $e_i = \sum_{j=1}^{t} e_{\chi_{i_j}}$. Agora, pela ortogonalidade dos e_i's e dos $e_{\chi_{i_j}}$'s, estas somas têm uma única parcela. Assim existe algum $1 \leq j_i \leq s(G)$ tal que $e_i = e_{\chi_{j_i}}$, para todo $1 \leq i \leq s(G)$. Portanto, $e_{\chi_i} \in K[G]$, para todo $1 \leq i \leq s(G)$. Disso vem $\chi_i(g) \in K$, para todo $g \in G$, donde concluímos que $K(\chi_i) = K$, para todo caracter irredutível χ_i de G sobre $\overline{K}$.

(2) $\Leftrightarrow$ (3) Já vimos que $Z(K[G])$ é um K-espaço vetorial de dimensão $s(G)$. Agora observemos que $e_1, e_2, \ldots, e_{G(K)}$ são linearmente independentes em $Z(K[G])$. De fato, suponhamos que $e_1, e_2, \ldots, e_{G(K)}$ são linearmente dependentes, assim existem $\lambda_i \in K$, $i = 1, \ldots, G(K)$, não todos nulos tais que $\lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_{G(K)} e_{G(K)} = 0$, digamos que $\lambda_{i_0} \neq 0$, para algum $i_0 \in \{1, \ldots, G(K)\}$. Logo, se multiplicarmos ambos os lados da última igualdade por $\lambda_{i_0}^{-1} e_{i_0}$ e usarmos o fato que $e_i e_j = 0$, se $i \neq j$, obtemos $e_{i_0} = 0$, o que não pode ocorrer. Isso implica que $e_1, e_2, \ldots, e_{G(K)}$ são linearmente independentes em $Z(K[G])$. Conseqüentemente, $G(K) = s(G)$ se, e somente se, $\{e_1, e_2, \ldots, e_{G(K)}\}$ é uma base do K-espaço vetorial $Z(K[G])$.

(1) $\Leftrightarrow$ (4) Como K é real fechado, então $K(\chi_i) = K$ se, e somente se, $\chi_i(g) = \chi_i(g^{-1})$, para todo $g \in G$. Então a equivalência segue do Teorema 4.8.

(4) $\Leftrightarrow$ (5) Conseqüência do Teorema 4.8. ■

Se as condições equivalentes do teorema acima são satisfeitas, então para cada $1 \leq i \leq s(G)$ temos $e_i = e_{\chi_i}$. Em outras palavras, $A_i = K[G]e_{\chi_i}$ onde $e_{\chi_i} = \frac{\chi_i(1)}{|G|}\sum_{g\in G}\chi_i(g^{-1})g$.

Agora, do Teorema 4.14, segue que se G é um (c)-grupo, então toda componente simples A_i de $K[G]$ é uma álgebra central simples sobre K. Podemos provar isto diretamente usando os caracteres de G.

Corolário 4.17. *Se G é um (c)-grupo finito e K é um corpo real fechado, então cada componente simples A_i de $K[G]$ é uma álgebra central simples sobre K.*

Demonstração: Para cada componente simples A_i de $K[G]$, existe uma caracter irredutível χ_i de G sobre $\overline{K} = K(\sqrt{-1})$ tal que $A_i = K[G]e_{\chi_i}$. Como G é um (c)-grupo, o Teorema 4.16 implica que $K(\chi_i) = K$. Agora, por [13], Proposição 1.4, pg. 7, o centro de A_i é $Z(A_i) = Ke_{\chi_i} \simeq K$. ■

4.3 (c)-grupo

Relembremos que um grupo finito é chamado (c)-grupo se $g \sim g^{-1}$, para todo elemento $g \in G$, em outras palavras, existe $\gamma \in G$ tal que $\gamma\, g\, \gamma^{-1} = g^{-1}$. Vimos, nas seções anteriores, a importância dos (c)-grupos para identificarmos cada componente simples da álgebra de grupo $K[G]$. Nosso objetivo nesta seção é mostrar que, em alguns casos especiais, podemos determinar quando um grupo finito é um (c)-grupo. Começamos com alguns exemplos de tais grupos.

Exemplo 4.18. O grupo simétrico S_n é um (c)-grupo. De fato, como todo caracter irredutível χ_i de S_n sobre $\mathbb{C}$ tem seus valores em $\mathbb{Z}$ (ver [9], pg. 87), segue que,

$\mathbb{R}(\chi_i) = \mathbb{R}$. Portanto, pelo Teorema 4.16, S_n é um (c)-grupo.

Exemplo 4.19. Se G é um (c)-grupo finito comutativo, então a condição $g \sim g^{-1}$, para todo $g \in G$, é equivalente a $g^2 = 1$, para todo $g \in G$. Conseqüentemente, $G \simeq (\mathbb{Z}/2\mathbb{Z})^r$, para algum $r \in \mathbb{N}$.

Exemplo 4.20. O grupo dos quatérnios Q de ordem 8 é um (c)-grupo. De fato, temos que $Q = \{1, y, y^2, y^{-1}, x, x^{-1}, yx, yx^{-1}\}$ com $x = yx^{-1}y^{-1}$, $y^2 = x^2$ e $x^4 = y^4 = 1$. Claramente $1 \sim 1$ e $x \sim x^{-1}$. Também não é difícil verificarmos que $y = (yx)y^{-1}(xy)^{-1}$, $y^2 = yy^2y^{-1}$ e $yx = (xy)yx^{-1}(xy)^{-1}$. Assim obtemos $y \sim y^{-1}$, $y^2 \sim (y^2)^{-1} = y^2$ e $yx \sim (yx)^{-1} = yx^{-1}$. Portanto, Q é um (c)-grupo.

Lema 4.21. *Se G é um (c)-grupo finito não trivial, então G tem ordem par.*

Demonstração: Suponhamos que a ordem de G é ímpar. Seja $g \in G$, como G é um (c)-grupo, existe $\gamma \in G$ tal que $g = \gamma\, g^{-1}\, \gamma^{-1}$. O fato que $|G|$ é ímpar e $|\gamma|$ divide $|G|$, implica que $|\gamma|$ também é ímpar. Assim, temos

$$g = \gamma(\gamma g \gamma^{-1})\gamma^{-1} = \gamma^2 g \gamma^{-2} = \gamma^3 g^{-1} \gamma^{-3} = \gamma^4 g \gamma^{-4} = \ldots = \gamma^{|\gamma|} g^{-1} \gamma^{-|\gamma|} = g^{-1},$$

isto é, $g^2 = 1$, uma vez que $|g|$ divide $|G|$ que é ímpar, devemos ter $|g| = 1$, e portanto, $G = \{1\}$, o que não pode ocorrer. Logo, a ordem de G é par. ■

Sejam H e K dois grupos e $\tau : K \to \mathrm{Aut(H)}$ um homomorfismo de grupos. Podemos definir em $H \times K$ uma estrutura de grupo através da multiplicação $(h, k).(h', k') = (h\tau(k)(h'), kk')$. Esse grupo é conhecido como *produto semi-direto* de H e K e denotaremos por $H \times_\tau K$. O elemento neutro de $H \times_\tau K$ é $(1, 1)$ e o inverso de (h, k) é $(\tau(k^{-1})(h^{-1}), k^{-1})$. Mais ainda, $H \times_\tau K$ é comutativo se, e somente se, H e K são ambos grupos comutativos e $\tau(k) = I_H$, para todo $k \in K$. Neste caso, $H \times_\tau K$ é o produto direto usual de $H \times K$.

Proposição 4.22. *Sejam $H = (\mathbb{Z}/2\mathbb{Z})^m$ e $K = (\mathbb{Z}/2\mathbb{Z})^n$, onde $m, n \in \mathbb{N}^*$. Então, para todo homomorfismo de grupos $\tau : K \to \mathrm{Aut}(H)$ temos que $H \times_\tau K$ é um (c)-grupo.*

Demonstração: Sejam $\tau : K \to \mathrm{Aut}(H)$ um homomorfismo de grupos e (h,k) um elemento de $H \times_\tau K$. Vamos mostrar que $(h,k) \sim (h,k)^{-1}$. Primeiramente, notemos que $(h,1)(h,1) = (h\tau(1)(h), 1.1) = (h^2, 1) = (1,1)$, isso implica que $(h,1) = (h,1)^{-1}$, para todo $h \in H$. Logo,

$$(h,1)(h,k)(h,1)^{-1} = (h\tau(1)(h), 1k)(h,1) = (h^2,k)(h,1) = (1,k)(h,1) = (\tau(k)(h),k).$$

Se mostrarmos que $(\tau(k)(h),k) = (h,k)^{-1}$ teremos $(h,k) \sim (h,k)^{-1}$, como desejamos. Com efeito,

$(h,k)\,(\tau(k)(h),k) = (h(\tau(k)\circ\tau(k))(h), k^2) = (h\tau(k^2)(h),1) = (h^2,1) = (1,1)$

$(\tau(k)(h),k)\,(h,k) = (\tau(k)(h)\tau(k)(h), k^2) = ((\tau(k)(h))^2, 1) = (1,1).$

Portanto, $(h,k)^{-1} = (\tau(k)(h),k)$, como queríamos. ■

Proposição 4.23. *Sejam H um grupo finito comutativo e $K = \langle\sigma\rangle$ um grupo de ordem 2. Então a aplicação $\tau_I : K \to \mathrm{Aut}(H)$ definida por $\tau_I(\sigma)(h) = h^{-1}$, para todo $h \in H$, é um homomorfismo de grupos que dota $H \times_{\tau_I} K$ com uma estrutura de (c)-grupo.*

Demonstração: Claramente, a aplicação τ_I é um homomorfismo de grupos, e portanto, já vimos que $H \times_{\tau_I} K$ tem estrutura de grupo. Resta-nos mostrar que $(h,k) \sim (h,k)^{-1}$, para todo $(h,k) \in H \times_{\tau_I} K$. Como $K = \{1,\sigma\}$, basta mostrarmos que $(h,1) \sim (h,1)^{-1}$ e $(h,\sigma) \sim (h,\sigma)^{-1}$, para todo $h \in H$. Com efeito, dado $h \in H$ temos $(h,\sigma)(h,\sigma) = (h\tau_I(\sigma)(h), \sigma^2) = (hh^{-1}, 1) = (1,1)$, isto implica que $(h,\sigma) = (h,\sigma)^{-1}$, e portanto, $(h,\sigma) \sim (h,\sigma)^{-1}$. Além disso, temos

$$(h,\sigma)(h,1)(h,\sigma)^{-1} = (hh^{-1},\sigma)(h,\sigma) = (1,\sigma)(h,\sigma) = (h^{-1},1),$$

ou seja, $(h,1) \sim (h^{-1},1) = (h,1)^{-1}$. ■

Proposição 4.24. *Sejam H um grupo finito comutativo de ordem ímpar e $K = \langle\sigma\rangle$ um grupo de ordem 2. Se $\tau : K \to \mathrm{Aut}(H)$ é um homomorfismo de grupos, então as seguintes condições são equivalentes:*

(1) $H \times_{\tau_I} K$ *é um (c)-grupo.*

(2) $\tau(\sigma)(h) = h^{-1}$, *para todo* $h \in H$, *isto é,* $\tau = \tau_I$.

Demonstração: (2) $\Rightarrow$ (1) Segue da Proposição 4.23.

(1) $\Rightarrow$ (2) Seja $h \in H$ tal que $h \neq 1$. Vamos mostrar que $\tau(\sigma)(h) = h^{-1}$. Por hipótese temos que $(h,k) \sim (h,k)^{-1}$, para todo $(h,k) \in H \times_{\tau_I} K$, em particular $(h,1) \sim (h,1)^{-1} = (h^{-1},1)$. Assim, existe $(x,y) \in H \times_{\tau_I} K$ tal que $(x,y)(h,1)(x,y)^{-1} = (h^{-1},1)$. Mas, $(x,y)(h,1)(x,y)^{-1} = (\tau(y)(h),1)$. Disso, segue que $(\tau(y)(h),1) = (h^{-1},1)$, e portanto, $\tau(y)(h) = h^{-1}$. Temos duas possibilidades para y, que são $y = 1$ ou $y = \sigma$. Se $y = 1$, então $\tau(1)(h) = h^{-1}$, ou seja, $h = h^{-1}$, e portanto $h^2 = 1$. Como $h \neq 1$, segue que $|h| = 2$, que não divide $|G|$. Logo, devemos ter $y = \sigma$ que prova $\tau(\sigma)(h) = h^{-1}$. ■

O exemplo que segue nos mostra que a condição " a ordem de H ser ímpar ", na proposição anterior, é necessária.

Exemplo 4.25. Sejam $H = \{1, a, b, ab\}$ o grupo de Klein e $\tau : K \to \mathrm{Aut}(H)$ o homomorfismo de grupos definido por:

$$\tau(\sigma)(a) = b,\ \tau(\sigma)(b) = a,\ \tau(\sigma)(ab) = ab.$$

Notemos que, dado $h \in H$ temos $(h,1)(h,1) = (h\tau(1)(h),1) = (h^2,1) = (1,1)$, isto é, $(h,1) = (h,1)^{-1}$, e portanto $(h,1) \sim (h,1)^{-1}$. Além disso, da igualdade $(h,\sigma)^{-1} = (\tau(\sigma)(h),\sigma)$, e usando o fato que

$$(1,\sigma)(h,\sigma)(1,\sigma)^{-1} = (\tau(\sigma)(h),1)(1,\sigma) = (\tau(\sigma)(h),\sigma)$$

obtemos $(h,\sigma) \sim (h,\sigma)^{-1}$. Isso mostra que $H \times_{\tau_I} K$ é um (c)-grupo, mas $\tau(\sigma)(a) \neq a^{-1}$.

Agora, vejamos que $H \times_{\tau_I} K$ é gerado pelos elementos (a,σ) e $(b,1)$ que satisfazem as seguintes condições: $|(a,\sigma)| = 4$, $|(b,1)| = 2$ e $(b,1)(a,\sigma)(b,1) = (a,\sigma)^{-1}$. Conseqüentemente, $H \times_{\tau_I} K \simeq D_4$.

Corolário 4.26. *O grupo diedral D_n é um (c)-grupo.*

Demonstração: Sejam $H = \langle a \rangle$ um grupo cíclico de ordem n e $K = \langle b \rangle$ um grupo de ordem 2. Consideremos o homomorfismo $\tau : K \to \mathrm{Aut}(H)$ definido por $\tau(b)(a) = a^{-1}$, para todo $a \in H$. Então, pela Proposição 4.23, segue que $G = H \times_\tau K$ é um (c)-grupo. Notemos que G é gerado pelos elementos $\alpha = (a, 1)$ e $\beta = (1, b)$, basta observarmos que $\alpha^i = (a^i, 1)$ e $\alpha^i\beta = (a^i, b)$, para todo $i = 1, \ldots, n-1$. Além disso, α e β satisfazem

$$\alpha^n = \beta^2 = (1, 1) \quad \text{e} \quad \beta\alpha\beta^{-1} = \alpha^{-1}.$$

Logo, $G = \langle\, \alpha, \beta \,:\, \alpha^n = \beta^2 = (1, 1) \;\text{ e }\; \beta\alpha\beta^{-1} = \alpha^{-1} \,\rangle$. Conseqüentemente, $G \simeq D_n$, provando que D_n é um (c)-grupo. ■

Teorema 4.27. *Se p é um primo, então todo grupo G de ordem $2p$ é cíclico ou é o diedral.*

Demonstração: Ver [11], Teorema 4.19, pg. 82. ■

Proposição 4.28. *Sejam p um número primo tal que $p > 2$ e G um grupo de ordem $2p$. Então, G é um (c)-grupo se, e somente se, $G \simeq D_p$.*

Demonstração: Assumimos que G é um (c)-grupo de ordem $2p$. Pelo Teorema 4.27, G é cíclico ou $G \simeq D_p$. Mostraremos que G não é comutativo, isso acarretará $G \simeq D_p$, visto que um grupo cíclico é comutativo. Com efeito, suponhamos por absurdo, que G é comutativo. Dado um elemento $g \in G$, existe $\gamma \in G$ tal que $g = \gamma g^{-1}\gamma^{-1}$, usando a comutatividade de G obtemos $g = g^{-1}$. Logo, $g^2 = 1$ para todo $g \in G$, o que é absurdo, pois G deve conter um elemento de ordem $p > 2$. Reciprocamente, se $G \simeq D_p$, o resultado segue do Corolário 4.26. ■

É interessante notarmos que se G é um (c)-grupo finito, então todo elemento $g \in G$ satisfazendo $|g| > 2$ tem uma classe de conjugação C_g de cardinalidade par.

De fato, suponhamos que a cardinalidade de C_g é ímpar. O fato que G é um (c)-grupo implica que $g^{-1} \in C_g$, para todo $g \in G$, assim, deve existir $h \in C_g$ tal que $h = h^{-1}$. Uma vez que $g \sim h$, devemos ter $|g| = |h|$ e, portanto, $|g| \leq 2$, o que não ocorre.

Para finalizarmos nosso trabalho, listamos abaixo os (c)-grupos finitos de ordem ≤ 30 obtidos nos exemplos e resultados desta seção.

n	(c)-grupos de ordem n
2	$\mathbb{Z}/2\mathbb{Z}$
4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
6	D_3
8	Q, D_4, $(\mathbb{Z}/2\mathbb{Z})^3$
10	D_5
12	D_6
14	D_7
16	$D_4 \times \mathbb{Z}/2\mathbb{Z}$, $Q \times \mathbb{Z}/2\mathbb{Z}$, D_8, $(\mathbb{Z}/2\mathbb{Z})^4$
18	D_9, $(\mathbb{Z}/3\mathbb{Z})^2 \times_{\tau_I} \mathbb{Z}/2\mathbb{Z}$
20	D_{10}
22	D_{11}
24	$D_6 \times \mathbb{Z}/2\mathbb{Z}$, D_{12}, S_4
26	D_{13}
28	D_{14}
30	D_{15}

Bibliografia

[1] ALBERT, A. A., *Structure of algebras*, AMS Colloquium Publications **24** (1939).

[2] BAYER-FLUCKIGER, E.; SHAPIRO, D. B. e TIGNOL, J. -P., *Hyperbolic Involutions*, Math. Z. **214**, n°3, 461-476, (1993).

[3] CURTIS, W. C. e REINER. I., *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.

[4] BOULAGOUAZ, M. e OUKHTITE, L., *Involutions of semisimple group algebras*, Arab. J. Sci. Eng, **25**, n°2, 133-149, (2000).

[5] GONÇALVES, A., *Tópicos em representação de grupos*, 9° Colóquio Brasileiro de Matemática, Brasília, 1973.

[6] HUNGERFORD, T. W., *Algebra*, Springer-Verlag, New York, 1974.

[7] LAM, T. Y., *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics **67**, American Mathematical Society, Providence, 2004.

[8] LANG, SERGE, *Algebra*, 3ªed., Addison-Wesley Publishing Company Inc., Reading, 1995.

[9] MALLIAVIN, M. P., *Les groupes finis et leurs représentations complexes*, Masson, Paris, 1995.

[10] MILIES, C. P. e SEHGAL. S. K., *An introduction to group rings*, Dordrecht: Kluwer Academic Publishers, 2002.

[11] ROTMAN, J. J., *An introduction to the theory of groups*, Springer-Verlag, 1995.

[12] SCHARLAU, W., *Quadratic and Hermitian Forms*, Springer-Verlag, Berlin-Heidekberg, 1985.

[13] TOSHIHIK, YAMADA., *The Schur subgroup of the Brauer group*, Springer-Verlag, Berlin, 1974.

Índice Remissivo