André Luís dos Santos Duarte da Silva

Componentes Simples de Álgebras de Grupo

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da Capes

Santo André, 2016

Universidade Federal do ABC

Centro de Matemática, Computação e Cognição

André Luís dos Santos Duarte da Silva

Componentes Simples de Álgebras de Grupo

Orientador: Prof. Dr. Francisco César Polcino Milies

Dissertação de mestrado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Mestre em Matemática

Este exemplar corresponde à versão final da dissertação defendida pelo aluno André Luís dos Santos Duarte da Silva, e orientada pelo Prof. Dr. Francisco César Polcino Milies.

Santo André, 2016

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Duarte da Silva, André Luís dos Santos
Componentes Simples de Álgebras de Grupo / André Luís dos Santos Duarte da Silva. — 2016.

72 fls.

Orientador: Francisco César Polcino Milies

Dissertação (Mestrado) — Universidade Federal do ABC, Programa de Pós-Graduação em Matemática, Santo André, 2016.

1. Álgebra. 2. Álgebras de Grupo. I. Polcino Milies, Francisco César. II. Programa de Pós-Graduação em Matemática, 2016. III. Título.

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.

Santo André, 06 **de** Maio **de 20**16**.**

Assinatura do autor: ______________________

Assinatura do orientador: ______________________

Programa de Pós-Graduação em Matemática
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017
ppg.matematica@ufabc.edu.br

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Andre Luis dos Santos Duarte da Silva, realizada em 4 de março de 2016:

Prof.(a) Dr.(a) **Francisco Cesar Polcino Milies** (UFABC) – Presidente

Prof.(a) Dr.(a) **Maria de Lourdes Merlini Giuliani** (UFABC) – Membro Titular

Prof.(a) Dr.(a) **Raul Antonio Ferraz** (USP) – Membro Titular

Prof.(a) Dr.(a) **Alegria Gladys Chalom** (USP) – Membro Suplente

Prof.(a) Dr.(a) **Renata Rodrigues Marcuz Silva** (USP) – Membro Suplente

RESUMO

Seja G um grupo finito, $\mathbb{F}$ um corpo. Berman ([Ber]) e Witt ([Witt]) calcularam, independentemente, o número de componentes simples da álgebra de grupo semisimples $\mathbb{F}G$. Nesse trabalho esboçamos uma prova do mesmo resultado devida à R. Ferraz que usa integralmente técnicas de álgebra de grupo. Além disso, calculamos o posto das unidades centrais de $\mathbb{Z}G$ e determinamos as componentes simples do centro de $\mathbb{F}G/J(\mathbb{F}G)$, quando $\mathbb{F}$ satisfaz uma condição teórica.

Palavras-chave: Álgebra, Álgebras de Grupo

ABSTRACT

Let G be a finite group, $\mathbb{F}$ a field. Berman ([Ber]) and Witt ([Witt]) evaluated independently the number of simple components of the semisimple group algebra $\mathbb{F}G$. In this paper we outline a proof of the same result, due to R. Ferraz entirely in terms group algebra techniques. Furhermore, we compute the rank of the central units of $\mathbb{Z}G$ and determine the simple central components of $\mathbb{F}G/J(\mathbb{F}G)$ provided that $\mathbb{F}$ satisfies a field theoretical condition.

Keywords:Algebra, Group Algebras

NOTAÇÃO

$\|G\|$	ordem do grupo G
$H < G$	H subgrupo de G
$A \times B$	produto direto dos grupos A e B
$\mathcal{Z}(X)$	centro de X, onde denota um anel ou um grupo
$Aut(X)$	o conjunto dos automorfismos de X, onde denota um anel ou um grupo
$GL(n, F)$	grupo linear geral de grau n sobre o corpo F
$tr(A)$	traço da matriz A
$car(F)$	característica do corpo F
RG	anel de grupo RG
$supp(\alpha)$	suporte do elemento $\alpha \in RG$
$\mathcal{U}(R)$	grupo das unidades do anel R
K/F	extensão K do corpo F
$mdc(a, b)$	máximo divisor comum entre a e b
$mmc(a, b)$	mìnimo múltiplo comum entre a e b
$J(R)$	radical de Jacobson do anel R
$Gal(E, F)$	grupo de Galois de E sobre F
$[E : F]$	grau da extensão E sobre F
$(G : H)$	índice do grupo G sobre H
$M_n(R)$	anel das matrizes com coeficientes no anel R
(a)	ideal gerado pelo elemento a
$< g >$	subgrupo gerado pelo elemento g
$\mathcal{O}_K$	anel dos inteiros algébricos de K
$dim_F(V)$	dimensão do espaço vetorial V sobre F
$C_F(g)$	classe F-conjugada de g
F_q	corpo finito com q elementos
Γ_g	classe de conjugação de g

CONTEÚDO

1 RESULTADOS PRELIMINARES 3
- 1.1 Grupo de Galois 4
- 1.2 Anéis Semisimples 5
- 1.3 Radical de Jacobson 6
- 1.4 Inteiros Algébricos 8
- 1.5 Produto Tensorial 9

2 ÁLGEBRA DE GRUPO SEMISIMPLES 15
- 2.1 Álgebras de Grupo Semisimples 16
- 2.2 Centro de uma Álgebra de Grupo 18
- 2.3 Álgebras de grupo sobre corpos 19

3 NÚMERO DE COMPONENTES SIMPLES 23
- 3.1 A ação do grupo de Galois 23
- 3.2 O Teorema de Berman-Witt 33

4 AS UNIDADES CENTRAIS DE ZG 37
- 4.1 Algumas propriedades do centro de QG 37
- 4.2 O posto das unidades centrais de ZG 40

5 AS COMPONENTES SIMPLES DO CENTRO DE FG/J(FG) 45
- 5.1 Componentes simples do centro de FG/J(FG) 45
- 5.2 As F-classes ciclotômicas como órbitas 48
- 5.3 A prova do Teorema Principal 49
- 5.4 Extensões ciclotômicas cíclicas 54
- 5.5 Um contra exemplo 55

Referência Bibliográfica 58

INTRODUÇÃO

O cálculo do número de componentes simples, de uma álgebra de grupo semisimples, é de fundamental importância na determinação da estrutura destas álgebras. Os matemáticos S. Berman e E. Witt, utilizaram a Teoria de Caracteres para determinar o número de componentes simples em uma álgebra de grupo semisimples ([Ber],[Witt]). No obstante, uma prova recente do mesmo resultado [RF1], devida à R. Ferraz, usa integralmente técnicas de álgebra de grupo. Neste presente trabalho, tivemos por objetivo, detalhar a demonstração de Ferraz, bem como apresentar aplicações do Teorema.

No capítulo 1 e 2, apresentamos alguns conceitos básicos que foram utilizados ao longo deste trabalho.

No capítulo 3, tratamos do método de R. Ferraz para calcular o número de componentes simples de uma álgebra de grupo semisimples e da demonstração do Teorema de Berman-Witt.

No capítulo 4, aplicamos a técnica de Ferraz para calcular o posto das unidades centrais em $\mathbb{Z}G$. A partir disto, apresentamos uma prova alternativa, utilizando os resultados apresentados, de um Teorema devido à Ritter e Sehgal.

No capítulo 5, ao supor uma restrição teórica sobre o corpo $\mathbb{F}$, caracterízamos as componentes simples do centro da álgebra $\mathbb{F}G/J(\mathbb{F}G)$. Além disso, expomos um contra-exemplo, quando a restrição teórica assumida não é satisfeita.

1 RESULTADOS PRELIMINARES

Neste capítulo apresentamos algumas definições e resultados bem conhecidos da Teoria de Anéis. Estes resultados se encontram em [NJ], [Fr], [PS].

Definição 1.1. *Seja* $\mathbb{F}$ *um corpo e* $f(x)$ *um polinômio mônico em* $\mathbb{F}[x]$. *Então, uma extensão* $\mathbb{E}$ *de* $\mathbb{F}$ *é chamada um* ***corpo de decomposição de*** $f(x)$ *sobre* $\mathbb{F}$ *se*

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$$

em $\mathbb{E}[x]$ *e*

$$\mathbb{E} = \mathbb{F}(r_1, \cdots, r_n),$$

ou seja, $\mathbb{E}$ *é gerado pelas raízes de* $f(x)$.

Definição 1.2. *Seja* $\mathbb{F}$ *um corpo. Um* ***polinômio irredutível*** $p(x) \in \mathbb{F}[x]$ *é dito* ***separável*** *se possui raízes distintas. Um* ***polinômio*** $f(x) \in \mathbb{F}[x]$ *é dito* ***separável*** *se seus fatores irredutíveis são separáveis.*

Definição 1.3. *Uma* ***extensão*** *algébrica* $\mathbb{E}$ *do corpo* $\mathbb{F}$ *é* ***separável*** *se o polinômio minimal de todo elemento de* $\mathbb{E}$ *é separável.*

Um Teorema relacionado com este conceito é o seguinte.

Teorema 1.4. *[Fr, Teorema 51.9] Se* $\mathbb{K}$ *é uma extensão finita de* $\mathbb{E}$ *e* $\mathbb{E}$ *é uma extensão finita de* $\mathbb{F}$, *isto é,* $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$, *então* $\mathbb{K}$ *é separável sobre* $\mathbb{F}$ *se e somente se* $\mathbb{K}$ *é sepáravel sobre* $\mathbb{E}$, *e* $\mathbb{E}$ *é separável sobre* $\mathbb{F}$.

Definição 1.5. *Um corpo* $\mathbb{F}$ *é* ***perfeito*** *se toda extensão finita* $\mathbb{K}$ *de* $\mathbb{F}$ *é uma extensão separável.*

A seguinte proposição é a junção dos Teoremas 51.13 e 51.14 de [Fr].

Proposição 1.6. *[Fr, pg. 440]*

1. *Todo corpo de característica zero é perfeito.*
2. *Todo corpo finito é perfeito.*

Um resultado clássico da Teoria dos Corpos, em que extrairemos um corolário útil, é o Teorema do Elemento Primitivo.

Teorema 1.7. *[Fr, Teorema 51.15] Seja $\mathbb{K}$ uma extensão finita e separável de um corpo $\mathbb{F}$. Então existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{F}(\alpha)$.*

Corolário 1.8. *Se $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, então existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$.*

Neste trabalho, faremos bastante uso de um tipo específico de extensão de corpos. A referida extensão é a seguinte.

Definição 1.9. *Seja n um número inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre um corpo $\mathbb{K}$ é chamado o n-ésimo **corpo ciclotômico** sobre $\mathbb{K}$, e denotado $\mathbb{K}_{(n)}$. As raízes de $x^n - 1$ são chamadas de **n-ésimas raízes da unidade** sobre $\mathbb{K}$, e o conjunto de todas essas raízes é denotado por $E_{(n)}$.*

A partir disto, temos o seguinte resultado.

Teorema 1.10. *[RH, Teorema 2.42] Seja n um número inteiro positivo e $\mathbb{K}$ um corpo de característica p. Seguem as seguintes afirmações:*

1. *Se p não divide n, então $E_{(n)}$ é um grupo cíclico de ordem n com respeito a multiplicação em $\mathbb{K}_{(n)}$.*
2. *Se p divide n, escreva $n = mp^s$, com inteiros positivos m e s, e m não divisível por p. Então $\mathbb{K}_{(n)} = \mathbb{K}_{(m)}$, e $\mathbb{E}_{(n)} = \mathbb{E}_{(m)}$, e as raízes de $x^n - 1$ em $\mathbb{K}_{(n)}$ são os m elementos de $\mathbb{E}_{(m)}$, cada qual com multiplicidade p^s.*

1.1 GRUPO DE GALOIS

Seja $\mathbb{E}$ uma extensão do corpo $\mathbb{F}$ e denote $Aut(\mathbb{E})$ o conjunto dos automorfismos de corpos de $\mathbb{E}$. O grupo

$$Gal(\mathbb{E}, \mathbb{F}) = \{\sigma \in Aut(\mathbb{E}) | \sigma(a) = a, \forall a \in \mathbb{F}\} \tag{1}$$

será chamado o **grupo de Galois** de $\mathbb{E}$ sobre $\mathbb{F}$.

Seja H um subgrupo de $Aut(\mathbb{E})$. O subcorpo

$$\mathbb{E}^H = \{a \in \mathbb{E} | \sigma(a) = a, \forall \sigma \in H\} \tag{2}$$

de $\mathbb{E}$ é chamado o **subcorpo de $\mathbb{E}$ fixado por H**.

Lema 1.11. *[NJ, Lema 1] Seja $\mathbb{E}/\mathbb{F}$ um corpo de decomposição de um polinômio separável em $\mathbb{F}[X]$. Então*

$$|Gal(\mathbb{E},\mathbb{F})| = [\mathbb{E}:\mathbb{F}].$$

Definição 1.12. *A extensão algébrica $\mathbb{E}$ do corpo $\mathbb{F}$ é dita **normal** se todo polinômio irredutível em $\mathbb{F}[X]$, que possui uma raíz em $\mathbb{E}$, é um produto de fatores lineares em $\mathbb{E}[X]$.*

Teorema 1.13. *[NJ, Teorema 4.7] Seja $\mathbb{E}$ uma extensão do corpo $\mathbb{F}$. Então as seguintes condições sobre $\mathbb{E}$ são equivalentes:*

1. *$\mathbb{E}$ é um corpo de decomposição sobre $\mathbb{F}$ de um polinômio separável $f(x)$.*
2. *$\mathbb{F} = \mathbb{E}^G$ para algum grupo finito G de automorfismos de $\mathbb{E}$.*
3. *$\mathbb{E}$ é normal, separável e de dimensão finita sobre $\mathbb{F}$.*

A seguir enunciamos o Teorema que tem um papel central na Teoria de Galois e que utilizaremos com frequência neste trabalho.

Teorema 1.14. *[NJ, pg. 239] Seja $\mathbb{E}$ uma extensão do corpo $\mathbb{F}$ satisfazendo alguma das condições equivalentes do Teorema anterior. Seja G o grupo de Galois de $\mathbb{E}$ sobre $\mathbb{F}$. Seja Γ o conjunto dos subgrupos de G, e Σ o conjunto dos corpos entre $\mathbb{E}$ e $\mathbb{F}$. As aplicações $H \mapsto \mathbb{E}^H$, $\mathbb{K} \mapsto Gal(\mathbb{E},\mathbb{K})$, $H \in \Gamma$, $\mathbb{K} \in \Sigma$, são inversas uma da outra. Além disso, valem as seguites propriedades:*

1. *$H_1 \supset H_2 \Leftrightarrow \mathbb{E}^{H_1} \subset \mathbb{E}^{H_2}$*
2. *$|H| = [\mathbb{E}:\mathbb{E}^H]$, $(G:H) = [\mathbb{E}^H,\mathbb{F}]$.*
3. *H é normal em $G \Leftrightarrow \mathbb{E}^H$ é normal sobre $\mathbb{F}$. Neste caso*

$$Gal(\mathbb{E}^H,\mathbb{F}) \simeq G/H.$$

1.2 ANÉIS SEMISIMPLES

Nesta seção, vamos abordar de modo sucinto, a propriedade de semisimplicidade de anéis. Este conceito é muito importante e permeia o trabalho.

Definição 1.15. *Seja R um anel e M um R-módulo.*

1. *O R-**módulo** M é chamado **semisimples** se todo submódulo de M é um somando direto.*

2. *O **anel** R é chamado **semisimples** se o módulo ${}_RR$ é semisimples.*

Existe uma relação entre um anel R semisimples e os R-módulos semisimples. A proposição seguinte nos fornecerá tal relação.

Proposição 1.16. *[PS, Teorema 2.5.7] 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.*

Um resultado central para o nosso trabalho é o Teorema de Wedderburn-Artin. Este Teorema foi originalmente provado em 1907, para álgebras de dimensão finita, pelo matemático escocês Joseph Wedderburn. Mais tarde, Emil Artin generalizou esse resultado.

Teorema 1.17. *[PS, Teorema 2.6.18] Um anel R é semisimples se e somente se é isomorfo a uma soma direta de álgebras de matrizes sobre anéis de divisão:*

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

1.3 RADICAL DE JACOBSON

O conceito de radical de Jacobson será utilizado para estudar, mais a frente, alguns anéis que não são semisimples.

Definição 1.18. *Seja R um anel. O **radical de Jacobson** de R, denotado por $J(R)$, é a interseção de todos os seus ideais maximais à esquerda.*

Dado um R-módulo M, o anulador de M é o conjunto

$$ann(M) = \{x \in R | xm = 0, \forall m \in M\}.$$

Definição 1.19. *Um módulo não-nulo M cujos únicos submódulos são (0) e o próprio M é chamado **simples**.*

Com estas definições podemos fazer a seguinte afirmação.

Teorema 1.20. *Seja R um anel. Então*

$$J(R) = \cap_{W\, simples} ann(W),$$

onde W é um R-módulo.

Demonstração: Suponha $x \in J(R)$ e W um R-módulo simples. Então para todo $w \in W$ não nulo, $Rw = W$ e $ann(W)$ é um ideal à esquerda maximal. Portanto $xw = 0$, para todo $w \in W$, e consequentemente $xW = 0$.

Reciprocamente, suponha $x \in \cap_{W\,\text{simples}}\, ann(W)$ e $\mathcal{M}$ um ideal à esquerda maximal. Então $R/\mathcal{M}$ é um R-módulo simples e $x(R/\mathcal{M}) = 0$. Logo, $x \in \mathcal{M}$. ∎

Note que o radical de Jacobson é um ideal bilateral, logo faz sentido tomar o quociente.

Lema 1.21. *[PS, Lema 2.7.5] Seja R um anel. Então $J(R/J(R)) = (0)$.*

Proposição 1.22. *[PS, Proposição 2.7.13] Seja R um anel. Se I é um ideal nil de R, então $I \subset J(R)$*

Proposição 1.23. *[PS, Teorema 2.7.14] Seja R um anel artiniano. Então $J(R)$ é um ideal nilpotente de R e todo ideal nil é nilpotente.*

Teorema 1.24. *[PS, Teorema 2.7.16] Seja R um anel semisimples. Então R é um anel artiniano e seguem as seguintes afirmações:*

1. *R não contém ideais nilpotentes bilaterais não nulos.*
2. *R não contém ideais nilpotentes à esquerda não nulos.*
3. *$J(R) = (0)$.*

Reciprocamente, se R é artiniano e qualquer uma das condições é satisfeita, então R é semisimples.

Apesar de não demonstrarmos esse Teorema, damos os seguintes corolários, que nos serão úteis no desenrolar de nosso trabalho.

Corolário 1.25. *Se R for um anel artiniano então $R/J(R)$ é semisimples.*

Demonstração: Sabemos pelo lema 1.21 que $J(R/J(R)) = (0)$. Uma vez que R é artiniano, e que o quociente de anel artiniano é também artiniano, concluímos que $R/J(R)$ é artiniano. Agora, pelo Teorema 1.24, segue que $R/J(R)$ é semisimples. ∎

Corolário 1.26. *Seja R um anel e I um ideal de R. Se $J(R/I) = 0$ então $J(R) \subset I$.*

Demonstração: Todo ideal maximal de R/I é da forma L/I onde L é um ideal maximal de R contendo I. Observe que $\cap(L/I) = \cap_{L\,\text{máximal}}(L+I)/I = (J(R)+I)/I$. Pela hipótese de $J(R/I) = 0$, assim, concluímos que $J(R) \subset I$. ∎

1.4 INTEIROS ALGÉBRICOS

Uma extensão finita $\mathbb{K}$ do corpo dos números racionais $\mathbb{Q}$ é chamado um **corpo de números algébricos**, ou simplesmente, um **corpo numérico**. Um elemento $\alpha \in \mathbb{K}$ é chamado um **inteiro algébrico** se satisfaz uma equação mônica

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0,$$

com $a_i \in \mathbb{Z}$. Os inteiros algébricos de $\mathbb{K}$ formam um anel, denotado usualmente por $\mathcal{O}_{\mathbb{K}}$.

Observação. *O anel dos inteiros algébricos do corpo dos números racionais $\mathbb{Q}$ é igual a $\mathbb{Z}$, o anel dos números inteiros.*

Lema 1.27. *[PS, Lema 2.8.1] O anel $\mathcal{O}_{\mathbb{K}}$ é finitamente gerado e $\mathbb{K} = \mathbb{Q}\mathcal{O}_{\mathbb{K}}$.*

Definição 1.28. *Seja R um anel comutativo, com unidade, sem divisores de zero. As **unidades** $u_1, \cdots, u_k$ de R são ditas **independentes**, sempre que a relação*

$$u_1^{m_1} \cdots u_k^{m_k} = 1$$

com $m_i \in \mathbb{Z}$, implica que $m_1 = \cdots = m_k = 0$.

Observe que, cada u que pertence a um conjunto independente de unidades não pode ser uma raíz da unidade.

Visto que, um corpo númerico $\mathbb{K}$ esta contido em $\mathbb{C}$, o corpo dos números complexos, os homomorfismos de $\mathbb{K}$ são todos complexos.

Definição 1.29. *Seja $\mathbb{K}$ um corpo numérico de grau n sobre $\mathbb{Q}$. A **assinatura** de um corpo numérico é o par $[r, c]$, onde r é o número de homomorfismos de $\mathbb{K}$ cuja imagem esta contida em $\mathbb{R}$, $2c$ é o número de homomorfismos complexos não-reais e $n = r + 2c$.*

Seja $p(x)$ um polinômio irredutível que define o corpo numérico $\mathbb{K}$ por uma de suas raízes. A assinatura de $\mathbb{K}$ também será chamada a assinatura de $p(x)$. Neste caso, r será o número de raízes reais de $p(x)$ e $2c$ será o número de raízes complexas não-reais de $p(x)$.

Agora vamos enunciar um resultado fundamental, conhecido como o Teorema das Unidades de Dirichlet.

Teorema 1.30. *[PS, Teorema 2.8.2] Seja $\mathbb{K} \supset \mathbb{Q}$ uma extensão finita de grau $n = r + 2c$, onde r e $2c$ são os números de homomorfismos reais e complexos de $\mathbb{K}$, respectivamente. Seja $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$ e $\mathcal{U} = \mathcal{U}(\mathcal{O}_{\mathbb{K}})$ seu grupo das unidades. Então $\mathcal{U}$ é um grupo abeliano finitamente gerado. Além disso, $\mathcal{U} = C \times F$ onde C é um grupo cíclico finito, e F é livre de torção de posto $\rho = r + c - 1$.*

Este Teorema primeiro nos diz que faz sentido considerar o posto livre de $\mathcal{U}(\mathcal{O}_{\mathbb{K}})$ e depois nos fornece seu valor.

1.5 PRODUTO TENSORIAL

Outro conceito que utilizaremos com frequência é o de produto tensorial de R-módulos.

Definição 1.31. *Seja R um anel, M um R-módulo à direita e N um R-módulo à esquerda. Seja A grupo abeliano, escrito aditivamente. Uma **função balanceada** f do produto cartesiano $M \times N$ em A é uma função satisfazendo:*

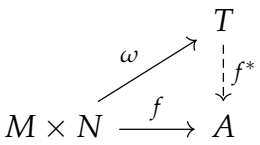
1. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$.
2. $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$.
3. $f(m, rn) = f(mr, n)$.

para todo $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $r \in R$.

Definição 1.32. *Sejam M um R-módulo à direita e N um R-módulo à esquerda. Um grupo abeliano T, junto com uma função balanceada $\omega : M \times N \to T$ é chamado um **produto tensorial** de M e N se as seguintes propriedades valem:*

1. *Os elementos da forma $\omega(m,n)$, $m \in M$, $n \in N$ geram T (como grupo aditivo).*

2. *Para qualquer grupo aditivo A e qualquer função balanceada $f : M \times N \to A$, existe um homomorfismo de grupos $f^* : T \to A$ tal que $f = f^* \circ \omega$; ou seja, tal que o seguinte diagrama seja comutativo:*



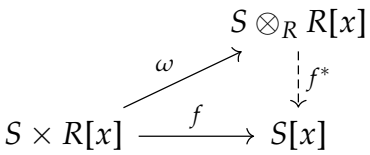
O produto tensorial de M e N será denotado por $M \otimes_R N$.

Observe que, se M é um R-módulo à direita e N um S-módulo à esquerda, então o produto tensorial $M \otimes_R N$ sempre existe [PS, Teorema 2.8.2].

Proposição 1.33. *Sejam $R \subset S$ anéis. Então*

$$S \otimes_R R[x] \simeq S[x].$$

Demonstração: Inicialmente definimos $f : S \times R[x] \to S[x]$ por $f(s, p(x)) = sp(x)$. Esta função f é balanceada e, com isso, temos o seguinte diagrama



onde $f = f^* \circ \omega$. Agora defina $g : S[x] \to S \otimes_R R[x]$ como

$$g\Big(\sum_i s_i x^i\Big) = \sum_i s_i \otimes x^i.$$

Note que, se $ax^i = bx^i$, $a, b \in \mathbb{S}$, então $a = b$ e $a \otimes \overline{x^i} = b \otimes \overline{x^i}$. Assim, g está bem definida. Além disso, a função g é um homomorfismo de R-módulos.

Agora, precisamos apenas calcular $f^* \circ g$ bem como $g \circ f^*$.

$$\begin{aligned} f^* \circ g\Big(\sum_i s_i x^i\Big) &= f^*\Big(\sum_i s_i \otimes x^i\Big) \\ &= \sum_i f^* \circ \omega(s_i, x^i) \\ &= \sum_i f(s_i, x^i) \\ &= \sum_i s_i x^i. \end{aligned}$$

Com isso, $f^* \circ g = 1$. Por outro lado,

$$\begin{aligned} g \circ f^*\left(s \otimes \sum_i r_i x^i\right) &= g \circ f\left(s, \sum_i r_i x^i\right) \\ &= \sum_i g(\sum_i (sr_i)x^i) \\ &= \sum_i (sr_i) \otimes x^i. \\ &= s \otimes \left(\sum_i r_i x^i\right). \end{aligned}$$

Ou seja, $g \circ f^* = 1$. Desta forma, f^* é um isomorfismo de R-módulos.

■

Proposição 1.34. *Seja* $\mathbb{K}$ *uma extensão do corpo* $\mathbb{F}$ *e* $p(x)$ *um polinômio em* $\mathbb{F}[x]$. *Então*

$$\frac{\mathbb{F}[x]}{(p(x))} \otimes_{\mathbb{F}} \mathbb{K} \simeq \frac{\mathbb{K}[x]}{(p(x))}.$$

Demonstração: Denote o elemento $q(x) + (p(x))$ de $\mathbb{F}[x]/(p(x))$ por $\overline{q(x)}$. Defina a função

$$f : \frac{\mathbb{F}[x]}{(p(x))} \times \mathbb{K} \to \frac{\mathbb{K}[x]}{(p(x))}$$

como $f(\overline{q(x)}, \alpha) = \overline{\alpha q(x)}$. Pela definição de produto tensorial sabemos que existe

$$f^* : \frac{\mathbb{F}[x]}{(p(x))} \otimes_{\mathbb{F}} \mathbb{K} \to \frac{\mathbb{K}[x]}{(p(x))}$$

tal que o diagrama abaixo seja comutativo:

$$\begin{array}{ccc} & & \frac{\mathbb{F}[x]}{(p(x))} \otimes_{\mathbb{F}} \mathbb{K} \\ & \overset{\omega}{\nearrow} & \Big\downarrow {\scriptstyle f^*} \\ \frac{\mathbb{F}[x]}{(p(x))} \times \mathbb{K} & \xrightarrow{\quad f \quad} & \frac{\mathbb{K}[x]}{(p(x))} \end{array}$$

Para mostrar o que queremos, basta que f^* seja um isomorfismo. Por isso, definimos

$$g : \frac{\mathbb{K}[x]}{(p(x))} \to \frac{\mathbb{F}[x]}{(p(x))} \otimes_{\mathbb{F}} \mathbb{K}$$

como

$$g\left(\overline{\sum_i a_i x^i}\right) = \sum_i \overline{x^i} \otimes a_i.$$

Note que, se $\overline{ax^i} = \overline{bx^i}$, $a, b \in \mathbb{K}$, então $\overline{ax^i - bx^i} = \overline{0} = \overline{\sum_i 0x^i}$. Assim, $0 = g(\overline{0}) = g(\overline{(a-b)x^i}) = \overline{x^i} \otimes (a-b)$. Logo, $\overline{x^i} \otimes a = \overline{x^i} \otimes b$. A mesma construção vale para quaisquer outros elementos, de sorte que, g está bem definida. Além disso, a função g é um homomorfismo de $\mathbb{F}$-álgebras.

Nesta altura, somente nos resta calcular as composições $g \circ f^*$ e $f^* \circ g$.

$$\begin{aligned} g \circ f^* \left(\overline{\sum_i a_i x^i} \otimes \alpha \right) &= g \circ f \left(\overline{\sum_i a_i x^i}, \alpha \right) \\ &= g \left(\overline{\sum_i \alpha a_i x^i} \right) \\ &= \sum_i \overline{x^i} \otimes (\alpha a_i) \\ &= \overline{\sum_i a_i x^i} \otimes \alpha. \end{aligned}$$

Logo, $g \circ f^* = 1$. Por outro lado,

$$\begin{aligned} f^* \circ g \left(\overline{\sum_i a_i x^i} \right) &= f^* \left(\sum_i \overline{x^i} \otimes (\alpha a_i) \right) \\ &= \sum_i f^* \circ \omega(\overline{x^i}, a_i) \\ &= \sum_i f(\overline{x^i}, a_i) \\ &= \overline{\sum_i a_i x^i}. \end{aligned}$$

Deste modo, $f^* \circ g = 1$. Portanto, f^* é um isomorfismo de $\mathbb{F}$-álgebras.

■

Proposição 1.35. *Seja $\mathbb{K}$ uma extensão finita do corpo $\mathbb{F}$ e $\mathcal{A}$ uma álgebra sobre $\mathbb{F}$ de dimensão finita. Então são verdadeiras as seguintes afirmações.*

1. *Se $\mathcal{I}$ é um ideal de $\mathcal{A}$, então*

$$\mathbb{K} \otimes_{\mathbb{F}} \frac{\mathcal{A}}{\mathcal{I}} \simeq \frac{\mathbb{K} \otimes_{\mathbb{F}} \mathcal{A}}{\mathbb{K} \otimes_{\mathbb{F}} \mathcal{I}}, \tag{3}$$

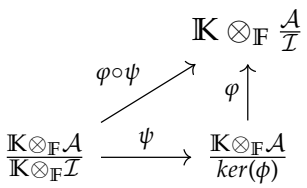
   como $\mathbb{K}$-álgebras.

2. $\mathbb{K} \oplus_{\mathbb{F}} J(\mathcal{A}) \subset J(\mathbb{K} \oplus_{\mathbb{F}} \mathcal{A})$.

Demonstração: A função $\phi : \lambda \otimes a \mapsto \lambda \otimes (a + \mathcal{I})$ é um epimomorfismo de $\mathbb{K}$-álgebras de $\mathbb{K} \otimes_{\mathbb{F}} \mathcal{A}$ em $\mathbb{K} \otimes_{\mathbb{F}} (\mathcal{A}/\mathcal{I})$. O ideal $\mathbb{K} \otimes_{\mathbb{F}} \mathcal{I}$ esta contido no kernel de ϕ. Logo, a função

$$\psi : \frac{\mathbb{K} \otimes_{\mathbb{F}} \mathcal{A}}{\mathbb{K} \otimes_{\mathbb{F}} \mathcal{I}} \to \frac{\mathbb{K} \otimes_{\mathbb{F}} \mathcal{A}}{ker(\phi)} \tag{4}$$

definida por $\psi(\alpha + \mathbb{K} \otimes_{\mathbb{F}} \mathcal{I}) = \alpha + ker(\phi)$, é um epimorfismo de $\mathbb{K}$-álgebras. Pelo Teorema do homomorfismo para álgebras, existe um isomorfismo $\varphi : (\mathbb{K} \otimes_{\mathbb{F}} \mathcal{A})/ker(\phi) \to \mathbb{K} \otimes_{\mathbb{F}} (\mathcal{A}/\mathcal{I})$ de $\mathbb{K}$-álgebras. Assim temos o seguinte diagrama.



Já que $\varphi \circ \psi$ é um epimorfismo de $\mathbb{K}$-álgebras e

$$\begin{aligned} dim_{\mathbb{K}}\left(\frac{\mathbb{K} \otimes_{\mathbb{F}} \mathcal{A}}{\mathbb{K} \otimes_{\mathbb{F}} \mathcal{I}}\right) &= dim_{\mathbb{K}}(\mathbb{K} \otimes_{\mathbb{F}} \mathcal{A}) - dim_{\mathbb{K}}(\mathbb{K} \otimes_{\mathbb{F}} \mathcal{I}) \\ &= dim_{\mathbb{K}}\left(\mathbb{K} \otimes_{\mathbb{F}} \frac{\mathcal{A}}{\mathcal{I}}\right), \end{aligned}$$

segue a válidade da primeira afirmação.

Pela proposição 1.23, o ideal $J(\mathcal{A})$ é nil, logo, $\mathbb{K} \oplus_{\mathbb{F}} J(\mathcal{A})$ é nil. Pela proposição 1.22 segue que $\mathbb{K} \oplus_{\mathbb{F}} J(\mathcal{A}) \subset J(\mathbb{K} \oplus_{\mathbb{F}} \mathcal{A})$. ■

2 ÁLGEBRA DE GRUPO SEMISIMPLES

O conceito de Álgebra de Grupo apareceu discretamente em um artigo de 1854 intitulado "On the Theory of Groups as Depending on the Symbolic Equation $\theta^n = 1$", de Arthur Cayley. Contudo, apenas cerca de 40 anos depois este conceito apareceu explicitamente no trabalho de Theodor Molien. Somente a partir da segunda metade da década de 1920, a noção de Álgebra de Grupo mostrou-se relevante; principalmente, pelo fato de alguns trabalhos pioneiros traçarem uma forte ligação entre a Teoria de Álgebras de Grupo e a Teoria de Representações de Grupo [PS, pg.127-128]. Desde então a Teoria de Álgebras de Grupo tem exercido papel central em diversas areas de pesquisa como Álgebra Homológica, Topologia Algébrica, K-Teoria Algébrica e a Teoria de Códigos Corretores de Erros.

No entanto, o que é uma Álgebra de Grupo? Para responder tal pergunta precisamos de um grupo multiplicativo G e um anel R com unidade. Com eles definimos a **álgebra de grupo** RG como sendo a R-álgebra associativa livre com base G, e com a multiplicação definida distributivamente usando a operação do grupo. De modo geral, podemos considerar os elementos de RG como somas formais do tipo

$$\sum_{g \in G} a_g g,$$

onde $a_g \in R$. Esta soma formal é apenas uma maneira de escrever a função de G em R, que toma valores a_g no elemento g do grupo. Disto segue que, $\sum_{g \in G} a_g g = \sum_{g \in G} b_g g$ se e somente se $a_g = b_g$ para todo $g \in G$.

Dado um elemento $\alpha = \sum_{g \in G} a_g g$, definimos o suporte de α como seguinte subconjunto de G,

$$supp(\alpha) = \{g \in G | a_g \neq 0\}.$$

Define-se também a soma e o produto como

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

e

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

onde $c_\gamma = \sum_{gh=\gamma} a_g b_h$. Ao definir os elementos como somas formais, junto com as operações acima, temos que RG é um anel, o **anel de grupo** de G sobre R.

Se para cada $r \in R$ e $\alpha = \sum_{g\in G} a_g g \in RG$ definirmos

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

teremos que RG também tem estrutura de R-módulo.

No caso em que R é comutativo, para todo $\alpha \in R$ e $x, y \in RG$, vale também a igualdade

$$\alpha(x.y) = (\alpha x).y = x.(\alpha y).$$

Desta maneira, RG é uma R-álgebra. Se fizermos a identificação

$$g \mapsto \sum_{g\in G} a_g g,$$

onde $a_g = 1$ e $a_h = 0$ se $h \neq g$, teremos G uma base do anel de grupo RG.

Como exemplo, suponha $G =< g >$ um grupo cíclico infinito. Então os elementos de RG são unicamente escritos como somas finitas da forma

$$\sum_{-\infty}^{\infty} a_i g^i$$

onde os coeficientes a_i são zero a menos de um numero finito deles. O homomorfismo natural $R[X] \to RG$ definido por $X \mapsto g$ é uma função injetora. Então segue que RG esta contido isomorficamente entre o anel de polinômios $R[X]$ e o corpo das funções racionais $R(X)$.

2.1 ÁLGEBRAS DE GRUPO SEMISIMPLES

As álgebras semisimples de dimensão finita podem se decompor em objetos atômicos, que se comportam melhor em diversos casos. Nesta seção iremos apresentar um critério para que uma álgebra de grupo seja semisimples e, consequentemente, possua uma

decomposição em álgebras simples. Este resultado é conhecido como o Teorema de Maschke (Veja [PS, Teorema 3.4.7]). Além disso, veremos como decompor uma tal álgebra e como são seus constituintes simples.

Teorema 2.1. *[PS, Teorema 3.4.7] Seja G um grupo. Então, o anel de grupo RG é semisimples se e somente se as seguintes condições valem:*

1. *R é um anel semisimples;*
2. *G é finito;*
3. *$|G|$ é invertível em R.*

Corolário 2.2. *Seja G um grupo finito e $\mathbb{K}$ um corpo. Então, $\mathbb{K}G$ é semisimples se e somente se $car(\mathbb{K}) \nmid |G|$.*

O Teorema de Wedderburn-Artin 1.17, nos permite decompor um anel semisimples como soma de álgebras de matrizes. No entanto, desejamos reescreve-lo à luz do conceito de álgebras de grupo.

Teorema 2.3. *[PS, Teorema 3.4.9] Seja G um grupo finito e $\mathbb{K}$ um corpo tal que $char(\mathbb{K}) \nmid |G|$. Então*

1. *$\mathbb{K}G$ é uma soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$, as componentes simples de $\mathbb{K}G$. Cada B_i é um anel simples.*
2. *Cada ideal bilateral de $\mathbb{K}G$ é uma soma direta de alguns membros da família $\{B_i\}_{1\leq i\leq r}$.*
3. *Cada componente simples B_i é isomorfa a um anel de matrizes da forma $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia isomorfa de $\mathbb{K}$ no seu centro, e o isomorfismo*

$$\mathbb{K}G \overset{\phi}{\simeq} \oplus_{i=1}^{r} M_{n_i}(D_i) \tag{5}$$

   é um isomorfismo de $\mathbb{K}$-álgebras.

4. *Em cada anel de matrizes $M_{n_i}(D_i)$, o conjunto*

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ & & \cdots & \\ x_{n_i} & 0 & \cdots & 0 \end{bmatrix} : x_1, x_2, \cdots, x_{n_i} \in D_i \right\} \simeq {D_i}^{n_i} \tag{6}$$

é um ideal minimal à esquerda.
Dado $x \in \mathbb{K}G$, considere $\phi(x) = (\alpha_1, \cdots, \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ e defina o produto de x por um elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. Com essa definição, I_i se torna um $\mathbb{K}G$-módulo simples.

5. *$I_i \ncong I_j$ se $i \neq j$.*

6. *Qualquer $\mathbb{K}G$-módulo simples é isomorfo a algum I_i, $1 \leq i \leq r$.*

Desde que, todo ideal de uma álgebra semisimples é gerada por um idempotente, ou seja, um elemento e satisfazendo $e^2 = e$, e os ideais são bilaterais se e somente se o idempotente é central, o Teorema acima pode ser traduzido pelo seguinte (Veja [PS, Teorema 2.5.11]).

Teorema 2.4. *Seja $\mathbb{K}G = \oplus_{i=1}^{r} B_i$ a decomposição do anel semisimples $\mathbb{K}G$ como uma soma direta de ideais bilaterais minimais. Então existe uma família $\{e_1, e_2, \cdots, e_r\}$ de elementos não nulos de $\mathbb{K}G$ tal que:*

1. *Para cada i, $1 \leq i \leq r$, e_i é um idempotente central.*

2. *$e_i e_j = 0$, se $i \neq j$.*

3. *$e_1 + e_2 + \cdots + e_r = 1$.*

4. *Para cada i, $1 \leq i \leq r$, e_i não pode ser escrito como uma soma $e_i = {e'}_i + {e''}_i$ de idempotentes centrais não nulos com ${e'}_i {e''}_i = 0$.*

Os idempotentes nesse Teorema são conhecidos como os **idempotentes centrais primitivos** de $\mathbb{K}G$.

2.2 CENTRO DE UMA ÁLGEBRA DE GRUPO

O centro de um anel R é o conjunto dos elementos de R que comutam com todos os outros. A seguir, iremos descrever o centro de uma álgebra de grupo.

Definição 2.5. *Seja G um grupo, R um anel comutativo e seja $\{\Gamma_i\}_{i \in I}$ o conjunto das classes de conjugação de G que contém apenas um número finito de elementos. Para cada índice $i \in I$ ponha $\gamma_i = \widehat{\Gamma_i} = \sum_{x \in \Gamma_i} x$. Esses elementos são chamados as **somas de classe** de G sobre R.*

Teorema 2.6. *[PS, Teorema 3.6.2] Seja G um grupo e seja R um anel comutativo. Então, o conjunto $\{\gamma_i\}_{i\in I}$ de todas as somas de classes formam uma base de $\mathcal{Z}(RG)$, o centro de RG sobre R.*

Proposição 2.7. *[PS, Proposição 3.6.3] Seja G um grupo finito e seja $\mathbb{K}$ um corpo algebricamente fechado tal que $char(\mathbb{K}) \nmid |G|$. Então, o número de componentes simples de $\mathbb{K}G$ é igual ao número de classes de conjugação de G.*

Definição 2.8. *Um corpo $\mathbb{K}$ é chamado um **corpo de decomposição para um grupo finito** G se a álgebra de grupo $\mathbb{K}G$ é isomorfa a uma soma direta de anéis de matrizes sobre $\mathbb{K}$.*

Com essa definição temos o seguinte.

Proposição 2.9. *Seja G um grupo finito, e seja $\mathbb{K}$ um corpo de decomposição para G tal que $char(\mathbb{K}) \nmid |G|$. Então, o número de componentes simples de $\mathbb{K}G$ é igual ao número de classes de conjugação de G.*

Demonstração: A demonstração é exatamente a mesma de [PS, Proposição 3.6.3]. ∎

2.3 ÁLGEBRAS DE GRUPO SOBRE CORPOS

No último capítulo precisaremos de dois resultados técnicos em uma de nossas demonstrações. Entretanto, já iremos fornecer a prova.

Teorema 2.10. *Seja $\mathbb{K}$ um extensão finita do corpo $\mathbb{F}$ e G um grupo finito. Então*

$$J(\mathbb{K}G) = \mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G).$$

Além disso, temos que

$$\frac{\mathbb{K}G}{J(\mathbb{K}G)} \simeq \mathbb{K} \otimes_{\mathbb{F}} \frac{\mathbb{F}G}{J(\mathbb{F}G)}, \tag{7}$$

como $\mathbb{K}$-álgebras.

Demonstração: Da proposição 1.35 temos que $\mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G) \subset J(\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G)$ bem como $\mathbb{K} \otimes_{\mathbb{F}} (\mathbb{F}G/J(\mathbb{F}G)) \overset{\phi}{\simeq} (\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G)/(\mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G))$. A $\mathbb{K}$-álgebra $\mathbb{K} \otimes_{\mathbb{F}} (\mathbb{F}G/J(\mathbb{F}G))$ é semisimples e, assim, $(\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G)/(\mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G))$ é também semisimples. Pelo Teorema

1.24 e do Corolário1.26 segue que $J(\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G) \subset \mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G)$. Logo temos a primeira afirmação.

Considere a função

$$\psi : \frac{\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G}{\mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G)} \to \frac{\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G}{J(\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G)}$$

definida por $\psi(\alpha + \mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G)) = \alpha + J(\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G)$. Esta função é um epimorfismo de $\mathbb{K}$-álgebras. Assim temos o seguinte diagrama.

$$\begin{array}{ccc} & & \frac{\mathbb{K}\otimes_{\mathbb{F}}\mathbb{F}G}{J(\mathbb{K}\otimes_{\mathbb{F}}\mathbb{F}G)} \\ & \overset{\psi\circ\phi}{\nearrow} & \uparrow \psi \\ \mathbb{K}\otimes_{\mathbb{F}} \frac{\mathbb{F}G}{J(\mathbb{F}G))} & \xrightarrow{\phi} & \frac{\mathbb{K}\otimes_{\mathbb{F}}\mathbb{F}G}{\mathbb{K}\otimes_{\mathbb{F}}J(\mathbb{F}G)} \end{array}$$

A função $\psi \circ \phi$ é um epimorfismo de $\mathbb{K}$-álgebras de dimensão finita e

$$dim_{\mathbb{K}} \left(\mathbb{K} \otimes_{\mathbb{F}} \frac{\mathbb{F}G}{J(\mathbb{F}G)} \right) = dim_{\mathbb{K}} \left(\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G \right) - dim_{\mathbb{K}} \left(\mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G) \right)$$

Por outro lado,

$$dim_{\mathbb{K}} \left(\frac{\mathbb{K}G}{J(\mathbb{K}G)} \right) = dim_{\mathbb{K}}(\mathbb{K}G) - dim_{\mathbb{K}}(J(\mathbb{K}G)))$$
$$dim_{\mathbb{F}}(\mathbb{K}) dim_{\mathbb{F}}(\mathbb{F}G) - dim_{\mathbb{F}}(J(\mathbb{K}G)).$$

Uma vez que $dim_{\mathbb{K}}(J(\mathbb{K}G)) = dim_{\mathbb{K}} \left(\mathbb{K} \otimes_{\mathbb{F}} J(\mathbb{F}G) \right)$, temos que $\mathbb{K}G/J(\mathbb{K}G)$ e $\mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}G/J(\mathbb{F}G)$ possuem a mesma dimensão sobre $\mathbb{K}$, e consequentemente, são isomorfos. ∎

Lema 2.11. *Seja $\mathbb{K}$ uma extensão finita do corpo $\mathbb{F}$. Seja D um anel de divisão que contém $\mathbb{F}$ no seu centro, e cuja dimensão sobre $\mathbb{F}$ seja finita. Então*

$$\mathcal{Z}(\mathbb{K} \otimes_{\mathbb{F}} D) = \mathbb{K} \otimes_{\mathbb{F}} \mathcal{Z}(D).$$

Demonstração: Se $\alpha \otimes \beta \in \mathbb{K} \otimes_{\mathbb{F}} \mathcal{Z}(D)$ então $(\alpha \otimes \beta).(\gamma \otimes \pi) = (\gamma \otimes \pi)(\alpha \otimes \beta)$, para todo $\gamma \otimes \pi \in \mathbb{K} \otimes_{\mathbb{F}} D$. Logo, $\mathbb{K} \otimes_{\mathbb{F}} \mathcal{Z}(D) \subset \mathcal{Z}(\mathbb{K} \otimes_{\mathbb{F}} D)$.

Reciprocamente, seja $\{\alpha_1, \cdots, \alpha_n\} \subset \mathbb{K}$ uma $\mathbb{F}$-base. Então todo elemento de $\mathbb{K} \otimes_{\mathbb{F}} D$ se escreve como $\sum_i \alpha_i \otimes d_i$, $d_i \in D$.

Note que, se $\sum_i \alpha_i \otimes d_i = 0$ e $d_i = \sum_j a_j v_j$, onde $\{v_j\}$ é uma $\mathbb{F}$-base de D e $a_j \in \mathbb{F}$, então

$$0 = \sum_{i=1}^{n} \alpha_i \otimes d_i = \sum_{i,j} a_j(\alpha_i \otimes v_i).$$

Como $\{\alpha_i \otimes v_j\}$ é uma $\mathbb{F}$-base de $\mathbb{K} \otimes_{\mathbb{F}} D$, segue que $a_j = 0$, para todo j. Logo, $d_i = 0$, para todo i.

Agora, seja $\alpha \in \mathcal{Z}(\mathbb{K} \otimes_{\mathbb{F}} D)$ com $\alpha = \sum_{i=1}^{n} \alpha_i \otimes d_i$. Para cada $d \in D$,

$$0 = \alpha.(1 \otimes d) - (1 \otimes d).\alpha = \sum_{i=1}^{n} \alpha_i \otimes (d_i d - d d_i).$$

Pelo que observamos, $d_i d = d d_i$, para todo $i = 1, \cdots, n$. Portanto, $\mathcal{Z}(\mathbb{K} \otimes_{\mathbb{F}} D) \subset \mathbb{K} \otimes_{\mathbb{F}} \mathcal{Z}(D)$, e segue o resultado. ∎

Proposição 2.12. *Seja $\mathbb{K}$ uma extensão de $\mathbb{F}$ finita e G um grupo finito. Então*

$$\mathcal{Z}\left(\mathbb{K} \otimes_{\mathbb{F}} \frac{\mathbb{F}G}{J(\mathbb{F}G)}\right) \simeq \mathbb{K} \otimes_{\mathbb{F}} \mathcal{Z}\left(\frac{\mathbb{F}G}{J(\mathbb{F}G)}\right).$$

Demonstração: A álgebra $\mathbb{F}G/J(\mathbb{F}G)$ é semisimples, logo,

$$\frac{\mathbb{F}G}{J(\mathbb{F}G)} \simeq \oplus_{i=1}^{r} M_{n_i}(D_i). \tag{8}$$

Por um lado, se aplicarmos o produto tensorial temos

$$\mathbb{K} \otimes_{\mathbb{F}} \left(\frac{\mathbb{F}G}{J(\mathbb{F}G)}\right) \simeq \oplus_{i=1}^{r} M_{n_i}(\mathbb{K} \otimes_{\mathbb{F}} D_i).$$

Se tomarmos o centro

$$\mathcal{Z}\left(\mathbb{K} \otimes_{\mathbb{F}} \left(\frac{\mathbb{F}G}{J(\mathbb{F}G)}\right)\right) \simeq \oplus_{i=1}^{r} \mathcal{Z}(\mathbb{K} \otimes_{\mathbb{F}} D_i).$$

Por outro lado, da equação 8,

$$\mathcal{Z}\left(\frac{\mathbb{F}G}{J(\mathbb{F}G)}\right) \simeq \oplus_{i=1}^{r} \mathcal{Z}(D_i),$$

e tomando o produto tensorial,

$$\mathbb{K} \otimes_{\mathbb{F}} \mathcal{Z}\left(\frac{\mathbb{F}G}{J(\mathbb{F}G)}\right) \simeq \oplus_{i=1}^{r} \mathbb{K} \otimes_{\mathbb{F}} \mathcal{Z}(D_i).$$

Pelo Lema 2.11 sabemos que $\mathcal{Z}(\mathbb{K} \otimes_{\mathbb{F}} D_i) = \mathbb{K} \otimes_{\mathbb{F}} \mathcal{Z}(D_i)$, para todo $1 \leq i \leq r$. Logo, segue o resultado.

∎

3 NÚMERO DE COMPONENTES SIMPLES

No capítulo anterior notamos que, quando $\mathbb{K}$ é um corpo de decomposição para G, o número de componentes simples de $\mathbb{K}G$ é igual à dimensão de $\mathcal{Z}(\mathbb{K}G)$ sobre $\mathbb{K}$. Neste caso, o número de classes de conjugação de G é igual à $dim_{\mathbb{K}}(\mathcal{Z}(\mathbb{K}G))$ e, portanto, igual ao número de componentes simples de $\mathbb{K}G$. Se $\mathbb{K}$ não é um corpo de decomposição para G, a resposta não é obtida com tanta facilidade. Na década de 1950, Samuil Berman e Ernst Witt foram, no entanto, capazes de calcular esse número no caso geral usando a Teoria de Caracteres. Nesta seção, forneceremos uma prova desse resultado devida à Raul Ferraz, que é desenvolvida inteiramente em termos da estrutura da álgebra de grupo.

Seja $\mathbb{K}G$ uma álgebra de grupo de um grupo finito G sobre um corpo $\mathbb{K}$. Ao longo desta seção, sempre assumiremos a hipótese de que a característica do corpo $\mathbb{K}$, não divide a ordem de G. Desta maneira, pelo Teorema de Maschke, a álgebra de grupo $\mathbb{K}G$ será sempre semisimples.

Antes de começarmos a descrever a técnica para calcular o número de componentes simples de uma álgebra de grupo semisimples, enunciemos o seguinte resultado, devido à Richard Brauer.

Teorema 3.1. *[Do, Teorema 17.2],[Do, Corolário 24.11] Seja G um grupo finito de expoente m e seja θ um raíz primitiva da unidade de ordem m. Se $\mathbb{K}$ é um corpo tal que car$(\mathbb{K}) \nmid |G|$ então $\mathbb{K}(\theta)$ é um corpo de decomposição para G.*

3.1 A AÇÃO DO GRUPO DE GALOIS

Seja $\mathbb{K}$ um corpo de característica p, G um grupo finito de expoente m contendo s diferentes classes de conjugação. Seja θ uma raíz primitiva da unidade de ordem m. Então, existe um isomorfismo $\phi : \mathbb{K}(\theta)G \to \oplus_{i=1}^{s} M_{n_i}(\mathbb{K}(\theta))$ de $\mathbb{K}(\theta)$-álgebras.

Para cada $1 \leq i \leq s$, tome $\pi_i : \oplus_{j=1}^{s} M_{n_j}(\mathbb{K}(\theta)) \to M_{n_i}(\mathbb{K}(\theta))$ a projeção natural definida por

$$(A_1, \cdots, A_s) \in \oplus_{j=1}^{s} M_{n_j}(\mathbb{K}(\theta)) \overset{\pi_i}{\mapsto} A_i.$$

Com isso, para cada índice i, considere a função

$$T_i : \mathbb{K}(\theta)G \to M_{n_i}(\mathbb{K}(\theta)),$$

onde $T_i = \pi_i \circ \phi$, a composição de ϕ com a projeção natural π_i. Note que T_i é um homomorfismo de $\mathbb{K}(\theta)$-álgebras, e se I_{n_i} é a matriz identidade de $M_{n_i}(\mathbb{K}(\theta))$, então $I_{n_i} = T_i(1) = T_i(g.g^{-1}) = T_i(g).T_i(g^{-1})$, ou seja, para cada $g \in G$, $T_i(g) \in GL(n_i, \mathbb{K}(\theta))$.

Ainda convém lembrar que $M_{n_i}(\mathbb{K}(\theta)) \simeq End(n_i\mathbb{K}(\theta))$, como $\mathbb{K}(\theta)$-álgebras. Desta maneira, podemos conceber $T_i : \mathbb{K}(\theta)G \to End(n_i\mathbb{K}(\theta))$, que são representações da álgebra $\mathbb{K}(\theta)G$.

O espaço $n_i\mathbb{K}(\theta)$ é também um $\mathbb{K}(\theta)G$-módulo simples, pelo Teorema 2.3, e para cada $g \in G$, $T_i(g) \in GL(n_i\mathbb{K}(\theta))$. Logo, ao restringirmos T_i aos elementos de G temos que

$$T_i : G \to GL(n_i\mathbb{K}(\theta)),$$

são representações irredutíveis do grupo G sobre $\mathbb{K}(\theta)$. Essas representações T_i, $1 \leq i \leq s$, são irredutíveis pelo fato de, para cada índice i, $n_i\mathbb{K}(\theta)$ ser um $\mathbb{K}(\theta)G$-módulo simples (Veja [PS, prop 4.2.2]). Pelo Teorema 2.3, temos também que $n_i\mathbb{K}(\theta) \ncong n_j\mathbb{K}(\theta)$ se $i \neq j$. Portanto, T_i e T_j não são equivalentes se $i \neq j$. Além disso, $\phi = T_1 \oplus T_2 \oplus \cdots \oplus T_s$ e as representações T_i, de G sobre $\mathbb{K}(\theta)$, são de grau $n_i = dim_{\mathbb{K}(\theta)}(n_i\mathbb{K}(\theta))$. A cada representação T_i, $1 \leq i \leq s$, seja χ_i o caracter provido pela respectiva representação T_i.

Se restringirmos ϕ ao centro de $\mathbb{K}(\theta)G$, e identificarmos as matrizes diagonais, cujas entradas diagonais são iguais, com os elementos de $\mathbb{K}(\theta)$, temos que

$$\phi(\mathcal{Z}(\mathbb{K}(\theta)G)) = \underbrace{\mathbb{K}(\theta) \oplus \cdots \oplus \mathbb{K}(\theta)}_{s}. \tag{9}$$

A soma de classe $\gamma_g \in \mathcal{Z}(\mathbb{K}(\theta)G)$, portanto, $\phi(\gamma_g) \in s\mathbb{K}(\theta)$. Desde que $\phi = (T_1 \oplus \cdots \oplus T_s)$ obtemos que

$$T_i(\gamma_g) = \begin{bmatrix} \alpha & & \\ & \ddots & \\ & & \alpha \end{bmatrix} \in \mathbb{K}(\theta)I_{n_i}. \tag{10}$$

O elemento γ_g é igual à $\sum_{h\in\Gamma_g} h$, e cada elemento $h \in \Gamma_g$ é da forma $x^{-1}gx$, onde $x \in G$. Deste modo, $T_i(h) = T_i(x^{-1}gx) = T_i(x^{-1})T_i(g)T_i(x) = T_i(g)$. Disto segue que,

$$\begin{aligned} T_i(\gamma_g) &= T_i\Big(\sum_{h\in\Gamma_g} h\Big) \\ &= \sum_{h\in\Gamma_g} T_i(g) \\ &= |\Gamma_g| T_i(g). \end{aligned}$$

Em consequência disto, o traço $tr(T_i(\gamma_g)) = |\Gamma_g| tr(T_i(g))$. Como $\chi_i(g) = tr(T_i(g))$ e o traço de $T_i(\gamma_g)$ também é igual a $n_i\alpha$, temos que $n_i\alpha = |\Gamma_g|\chi_i(g)$. Portanto,

$$T_i(\gamma_g) = \frac{|\Gamma_g|\chi_i(g)}{n_i} I_{n_i}. \tag{11}$$

Outra consequência da equação 9 é que todo automorfismo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$ pode ser estendido a $\phi(\mathcal{Z}(\mathbb{K}(\theta)G))$. Isto é feito, definindo $\sigma(k_1, \cdots, k_s) = (\sigma(k_1), \cdots, \sigma(k_s))$ para todo $(k_1, \cdots, k_s) \in \phi(\mathcal{Z}(\mathbb{K}(\theta)G))$.

Para cada automorfismo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$ denotaremos por σ^ϕ o automorfismo de $\mathcal{Z}(\mathbb{K}(\theta)G)$ definido por $\sigma^\phi = \phi^{-1} \circ \sigma \circ \phi$. Com isso, o grupo de Galois $Gal(\mathbb{K}(\theta), \mathbb{K})$ age em $\mathcal{Z}(\mathbb{K}(\theta)G)$. Porém, antes de verificarmos como σ^ϕ age no conjunto $\mathcal{B} = \{\gamma_g : g \in G\}$ das somas de classe, que sabemos ser uma $\mathbb{K}$-base de $\mathcal{Z}(\mathbb{K}(\theta)G)$, enunciemos um resultado bastante conhecido de Álgebra de Linear que nos será útil.

Lema 3.2. *[HK, Teorema 6, pg. 204] Seja V um espaço vetorial de dimensão finita sobre o corpo $\mathbb{K}$ e seja T um operador linear em V. Então T é diagonalizável se e somente se o polinômio minimal para T tem a forma*

$$p(X) = (X - c_1) \cdots (X - c_k)$$

onde $c_1, \cdots c_k$ são elementos distintos em $\mathbb{K}$.

Se $T^m = I$, então o polinômio minimal de T sobre $\mathbb{K}(\theta)$ divide $p(X) = X^m - 1$. Como $car(\mathbb{K}) \nmid |G|$, o polinômio $p(X)$ possui m raízes distintas em $\mathbb{K}(\theta)$. Assim o polinômio minimal de T sobre $\mathbb{K}(\theta)$ fatora-se em polinômios lineares distintos. Pelo lema acima, T é diagonalizável. Além disso, note que, se λ for um autovalor de T, então existe um autovetor não nulo $v \in V$ de λ tal que $v = T^m(v) = \lambda^m v$. Assim, λ é um raiz da unidade de ordem m.

Os automorfismos $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$ mandam raízes primitivas da unidade em raízes primitivas da unidade, de modo que, cada σ manda θ em θ^i para algum i. Verifiquemos que tal inteiro i é relativamente primo com m.

Lema 3.3. *Se o automorfismo $\sigma(\theta) = \theta^i$ esta em $Gal(\mathbb{K}(\theta), \mathbb{K})$ então $mdc(i, m) = 1$.*

Demonstração: Suponha $\sigma(\theta) = \theta^i$. Como σ é sobrejetora, existe um inteiro r, $1 \leq r \leq m-1$, tal que $\sigma(\theta^r) = \theta$. No entanto, $\theta = \sigma(\theta^r) = (\sigma(\theta))^r = \theta^{ir}$, de modo que, $\theta^{1-ir} = 1$. Com isso, $1 - ir \equiv 0(mod\ o(\theta))$, onde $o(\theta)$ é a ordem de θ. Como $o(\theta) = m$, temos que $1 = ir + ms$, para algum inteiro s, significando $mdc(i, m) = 1$. ∎

Teorema 3.4. *Se $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$, com $\sigma(\theta) = \theta^i$, então $\sigma^{\phi}(\gamma_g) = \gamma_{g^i}$.*

Demonstração: Para mostrar que $\sigma^{\phi}(\gamma_g) = \gamma_{g^i}$ é suficiente mostrar que $\sigma(\phi(\gamma_g)) = \phi(\gamma_{g^i})$.

Sabemos que $\phi = T_1 \oplus \cdots \oplus T_s$ e $T_j(\gamma_g) = (|\Gamma_g|\chi_j(g))/n_j$. Logo

$$\phi(\gamma_g) = \left(\frac{|\Gamma_g|\chi_1(g)}{n_1}, \cdots, \frac{|\Gamma_g|\chi_s(g)}{n_s} \right).$$

Aplicando σ a equação acima, temos

$$\sigma(\phi(\gamma_g)) = \left(\frac{|\Gamma_g|\sigma(\chi_1(g))}{n_1}, \cdots, \frac{|\Gamma_g|\sigma(\chi_s(g))}{n_s} \right). \tag{12}$$

O lema 3.3 nos permite afirmar que $mdc(i, m) = 1$. Assim, temos uma bijeção $h \mapsto h^i$ de Γ_g em Γ_{g^i}, cuja inversa é dada por $k \mapsto k^{\lambda}$, onde λ é o inteiro tal que $i\lambda \equiv 1(mod\ m)$.

Como

$$\phi(\gamma_{g^i}) = \left(\frac{|\Gamma_{g^i}|\chi_1(g^i)}{n_1}, \cdots, \frac{|\Gamma_{g^i}|\chi_s(g^i)}{n_s} \right)$$

e $|\Gamma_g| = |\Gamma_{g^i}|$, nos resta apenas mostrar que $\sigma(\chi_j(g)) = \chi_j(g^i)$.

Observe que, sendo T_j um homomorfismo, $(T_j(g))^m = T_j(g^m) = T_j(1) = I_{n_j}$, para todo $g \in G$, onde $I_{n_j} \in M_{n_i}(\mathbb{K}(\theta))$ é a matriz identidade.

Como vimos acima, $T_j(g)$ é diagonalizável com autovalores da forma $\theta^{t_1}, \cdots, \theta^{t_s}$, onde t_k são números inteiros, $1 \leq k \leq s$. Desta forma, existe $L_j \in GL(n_j, \mathbb{K}(\theta))$ tal que

$$T_j(g) = L_j \begin{bmatrix} \theta^{t_1} & & \\ & \ddots & \\ & & \theta^{t_s} \end{bmatrix} {L_j}^{-1}.$$

Por definição, $\chi_j(g) = tr(T_j(g)) = \theta^{t_1} + \cdots + \theta^{t_s}$, e assim, $\sigma(\chi_j(g)) = \sum_{k=1}^{s} \theta^{it_k}$. Por outro lado,

$$T_j(g^i) = L_j \begin{bmatrix} \theta^{it_1} & & \\ & \ddots & \\ & & \theta^{it_s} \end{bmatrix} {L_j}^{-1}.$$

Portanto, $\chi_j(g^i) = \sum_{k=1}^{s} \theta^{it_k}$ é igual à $\sigma(\chi_j(g))$. ∎

Agora, sabendo que $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$ se $\sigma(\theta) = \theta^i$, com i relativamente primo com m, e tendo em vista o Teorema acima, concluímos que os elementos de $Gal(\mathbb{K}(\theta), \mathbb{K})$ agem no conjunto $\mathcal{B} = \{\gamma_g : g \in G\}$ das somas de classe como permutações. Seja S_g a órbita γ_g pela ação de $Gal(\mathbb{K}(\theta), \mathbb{K})$, isto é,

$$S_g = \{\sigma^\phi(\gamma_g) : \sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})\} = \{\gamma_{g^i} : \exists \sigma \in Gal(\mathbb{K}(\theta), \mathbb{K}) \quad \text{com} \quad \sigma(\theta) = \theta^i\}.$$

A cada órbita S_g podemos associar o elemento $\eta_g = \sum_{\gamma \in S_g} \gamma$. Por definir S_g e η_g desta maneira, segue diretamente que $\sigma^\phi(S_g) = S_g$ e $\sigma^\phi(\eta_g) = \eta_g$ para todo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$.

Seja V_g o $\mathbb{K}$-subespaço vetorial de $\mathbb{K}G$ gerado pelos elementos em S_g. Já que cada elemento γ_g é central, fica claro que $V_g \subset \mathcal{Z}(\mathbb{K}G)$.

Proposição 3.5. *Seja $\alpha \in V_g$ e suponha que $\sigma^\phi(\alpha) = \alpha$ para todo σ em $Gal(\mathbb{K}(\theta), \mathbb{K})$. Então $\alpha = k\eta_g$ para algum $k \in \mathbb{K}$.*

Demonstração: Suponha $S_g = \{\gamma_1, \gamma_2, \cdots, \gamma_\mu\}$. Para γ_j e cada $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$, temos que $\sigma^\phi(\gamma_j) = \gamma_{j'}$ para algum j', $1 \leq j' \leq \mu$.

Escreva $\alpha = \sum_{j=1}^{\mu} k_j \gamma_j$ com $k_j \in \mathbb{K}$, $1 \leq k \leq \mu$. Segue da definição de S_g que, para cada índice $1 \leq i \leq \mu$, existe um automorfismo $\sigma_i \in Gal(\mathbb{K}(\theta), \mathbb{K})$ tal que $\sigma_i^\phi(\gamma_1) = \gamma_i$. Sendo $\sigma_i^\phi(\alpha) = \alpha$, temos

$$\sum_{j=1}^{\mu} k_j \gamma_j = \alpha = \sigma_i^\phi\Big(\sum_{j=1}^{\mu} k_j \gamma_j\Big) = \sum_{j=1}^{\mu} k_j \sigma_i^\phi(\gamma_j).$$

Agora, o coeficiente de γ_i no lado direita da equação é k_1, enquanto no lado esquerdo é k_i, onde $k_i = k_1$. Como isso vale para todo índice i, $1 \leq i \leq \mu$, temos que $\alpha = k_1\eta_g$, como afirmado. ∎

Seja ν o número de S_g órbitas diferentes. Seja $\tau = \{g_1, \cdots, g_\nu\}$ um conjunto de elementos em G tal que $\{\gamma_{g_1}, \cdots, \gamma_{g_\nu}\}$ é um conjunto de representantes dessas órbitas. Desta forma, $\mathcal{B} = \bigcup_{g \in \tau} S_g$ e, já que isso é uma base de $\mathcal{Z}(\mathbb{K}G)$ sobre $\mathbb{K}$, temos que $\mathcal{Z}(\mathbb{K}G) = \bigoplus_{g \in \tau} V_g$. Além disso, porquanto $\sigma^\phi(S_g) = S_g$, temos que $\sigma^\phi(V_g) = V_g$ para todo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$ e todo $g \in G$.

Corolário 3.6. *Seja α um elemento de $\mathcal{Z}(\mathbb{K}G)$. Então $\sigma^\phi(\alpha) = \alpha$ para todo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$ se e somente se α é uma combinação linear dos elementos do conjunto $\{\eta_g | g \in \tau\}$.*

Demonstração: Considere $\alpha \in \mathcal{Z}(\mathbb{K}G)$. Então $\alpha = \sum_{g\in\tau} v_g$ com $v_g \in V_g$. Como observado acima, $\sigma^\phi(v_g) \in V_g$ para todo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$ e todo $g \in \tau$. Se $\sigma^\phi(\alpha) = \alpha$, segue que $\sigma^\phi(v_g) = v_g$. Pela proposição anterior, isso implica $v_g = k_g\eta_g$ para algum $k_g \in \mathbb{K}$. Logo, $\alpha = \sum_{g\in\tau} k_g\eta_g$. A recíproca é trivial. ∎

Agora, seja $\mathcal{A}$ o $\mathbb{K}$-subespaço vetorial de $\mathbb{K}G$ gerado pelos elementos do conjunto $\{\eta_g : g \in \tau\}$ que, em vista do corolário acima, é igual a

$$\mathcal{A} = \{\alpha \in \mathcal{Z}(\mathbb{K}G) : \sigma^\phi(\alpha) = \alpha, \forall\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})\}.$$

Proposição 3.7. *Seja α um elemento de $\mathbb{K}G$. Então $\alpha \in \mathcal{A}$ se e somente se $\phi(\alpha) \in \underbrace{\mathbb{K} \oplus \cdots \oplus \mathbb{K}}_{s} \subset \underbrace{\mathbb{K}(\theta) \oplus \cdots \oplus \mathbb{K}(\theta)}_{s} = \phi(\mathcal{Z}(\mathbb{K}(\theta)G))$.*

Demonstração: Seja α um elemento de $\mathbb{K}G$. Então

$$\alpha \in \mathcal{A} \text{ se e somente se } \sigma^\phi(\alpha) = \alpha \text{ para todo } \sigma \in Gal(\mathbb{K}(\theta), \mathbb{K}),$$

e isso ocorre se e somente se $\sigma(\phi(\alpha)) = \phi(\alpha)$ para todo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$. Já havíamos mencionado que identificaríamos as matrizes diagonais, cujas entradas diagonais são iguais, com os elementos de $\mathbb{K}(\theta)$. Com isso, $\phi(\alpha) = (a_1, \cdots, a_s), a_i \in \mathbb{K}(\theta)$, $1 \leq i \leq s$, e $\sigma(a_1, \cdots, a_s) = (\sigma(a_1), \cdots, \sigma(a_s))$ para todo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$. Assim, segue que $\sigma(\phi(\alpha)) = \phi(\alpha)$ se e somente se $\sigma(a_i) = a_i$ para todo $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$, e isso acontece se e somente se $a_i \in \mathbb{K}$, $1 \leq i \leq s$. ∎

A seguir demonstraremos dois lemas. O primeiro é quase imediato, mas será utilizado no segundo lema e no Teorema chave desta seção.

Lema 3.8. *Seja $\mathbb{K}$ um corpo e $\psi : A \to B$ um isomorfismo de $\mathbb{K}$-álgebras. O elemento $\alpha \in A$ é algébrico sobre $\mathbb{K}$ se e somente se $\psi(\alpha)$ é algébrico sobre $\mathbb{K}$. Além disso, os elementos α e $\psi(\alpha)$ possuem o mesmo polinômio minimal sobre $\mathbb{K}$.*

Demonstração: Se α é algébrico sobre $\mathbb{K}$ então existe um polinômio $f(X)$ em $\mathbb{K}[X]$ tal que $f(\alpha) = 0$. Se $f(X) = \sum_{i=1}^n c_i X^i$ então $0 = f(\alpha) = \sum_{i=1}^n c_i\alpha^i$. Logo, $0 = \psi(\sum_{i=1}^n c_i\alpha^i) = \sum_{i=1}^n c_i\psi(\alpha)^i$. Por conseguinte, $\psi(\alpha)$ é algébrico sobre $\mathbb{K}$. A recíproca se obtém por proceder de maneira análoga, apenas considerando ψ^{-1} em vez de ψ.

Agora, seja $p_\alpha(X) \in \mathbb{K}[X]$ o polinômio minimal de α. Então, $p_\alpha(\psi(\alpha)) = 0$, de modo que o polinômio minimal de $\psi(\alpha)$ divide $p_\alpha(X)$. Analogamente, α é raíz do polinômio minimal de $\psi(\alpha)$. Visto que ambos os polinômios minimais de α e $\psi(\alpha)$ são mônicos, concluímos que são os dois iguais a $p_\alpha(X)$. ∎

Lema 3.9. *Seja $p_\alpha(X) \in \mathbb{K}[X]$ o polinômio minimal de um elemento $\alpha \in \mathcal{Z}(\mathbb{K}G)$. Então $\alpha \in \mathcal{A}$ se e somente se $p_\alpha(X) = (X - k_1)\cdots(X - k_t)$, $k_i \in \mathbb{K}$, $1 \leq i \leq t$, é o produto de fatores lineares distintos.*

Demonstração: Como ϕ é um isomorfismo, segue que α e $\phi(\alpha)$ possuem o mesmo polinômio minimal. Suponhamos primeiro que $\alpha \in \mathcal{A}$. Pela proposição 3.7 temos que $\phi(\alpha) = (a_1, \cdots, a_s)$, com $a_i \in \mathbb{K}$, $1 \leq i \leq s$. Note que, se um polinômio $f(X)$ possui α como raíz então os a_i são raízes de $f(X) \in \mathbb{K}$, $1 \leq i \leq s$. Agora, se tomarmos $\{k_1, \cdots, k_t\}$ o conjunto formado pelos elementos $a_1, \cdots, a_s$ de $\mathbb{K}$, então $g(X) = (X - k_1)\cdots(X - k_t) \in \mathbb{K}[X]$ satisfaz $g(\alpha) = 0$, de modo que, o polinômio minimal $p_\alpha(X)$ divide $g(X)$. Entretanto, $p_\alpha(X)$ possui α como raíz, e pelo que observamos acima, $p_\alpha(a_i) = 0$, $1 \leq i \leq s$. Em consequência disto, toda raíz de $g(X)$ é também uma raíz de $p_\alpha(X)$, e como as raízes de $g(X)$ são todas distintas, temos que $g(X)$ divide $p_\alpha(X)$. Ambos os polinômios $g(X)$ e $p_\alpha(X)$ são mônicos e, portanto, devem ser iguais.

Reciprocamente, suponhamos que $p_\alpha = (X - k_1)\cdots(X - k_t)$, $k_i \in \mathbb{K}$, $1 \leq i \leq t$. Escrevamos outra vez $\phi(\alpha) = (a_1, \cdots, a_s)$, mas agora com $a_i \in \mathbb{K}(\theta)$, $1 \leq i \leq s$. Visto que $p_\alpha(X)$ é o polinômio minimal de α, segue que $p_\alpha(\alpha) = 0$. Isto implica em $p_\alpha(a_i) = 0$, $1 \leq i \leq s$. Logo, cada a_i, $1 \leq i \leq s$, é um elemento de $\{k_1, \cdots, k_t\} \subset \mathbb{K}$ e, assim, α pertence a $\mathcal{A}$. ∎

A esta altura, estamos quase prontos para demonstrar o Teorema principal desta seção. Antes, utilizemos o Teorema de Wedderburn para escrever

$$\mathbb{K}G \overset{\varphi}{\simeq} \oplus_{i=1}^{r} M_{n_i}(D_i), \tag{13}$$

onde D_i é um anel de divisão, com $\mathbb{K} \subset \mathcal{Z}(D_i) = \mathbb{K}_i$, $1 \leq i \leq r$. Então $\varphi(\mathcal{Z}(\mathbb{K}G)) = \oplus_{i=1}^{r} \mathbb{K}_i$, com r é o número de componentes simples de $\mathcal{Z}(\mathbb{K}G)$.

Por fim, podemos enunciar e demonstrar o Teorema que nos permitirá obter o número de componentes simples de uma álgebra de grupo semisimples.

Teorema 3.10. *Com a notação acima,* $\varphi(\mathcal{A}) = \bigoplus_{i=1}^{r} \mathbb{K} \subset \bigoplus_{i=1}^{r} \mathbb{K}_i$. *O conjunto* $\{\varphi(\eta_g)| \quad g \in \tau\}$ *é uma base de* $\bigoplus_{i=1}^{r} \mathbb{K}$. *Assim, o número de componentes simples de* $\mathbb{K}G$ *é o número de diferentes órbitas de somas de classes* γ_g *pela ação de* $Gal(\mathbb{K}(\theta), \mathbb{K})$.

Demonstração: Já sabemos que qualquer elemento $\beta \in \varphi(\mathcal{A})$, da forma $\beta = \varphi(\alpha)$ com $\alpha \in \mathcal{A} \subset \mathcal{Z}(\mathbb{K}G)$, possui o mesmo polinômio minimal de α. Pelo Lema 3.9, o polinômio minimal de α é o produto de fatores lineares distintos em $\mathbb{K}[X]$. Assim, o conjunto $\varphi(\mathcal{A})$ é composto pelos elementos $\beta \in \varphi(\mathcal{Z}(\mathbb{K}G)) = \bigoplus_{i=1}^{r} \mathbb{K}_i$ tal que o polinômio minimal de β é o produto de fatores lineares em distintos $\mathbb{K}[X]$. No entanto, a última condição ocorre se e somente se $\beta \in \bigoplus_{i=1}^{r} \mathbb{K}$. Portanto, $\varphi(\mathcal{A}) = \bigoplus_{i=1}^{r} \mathbb{K}$ como afirmamos.

Além disso, pelo fato de que $\{\eta_g | g \in \tau\}$ é uma base para $\mathcal{A}$ sobre $\mathbb{K}$, decorre que $\{\varphi(\eta_g) | g \in \tau\}$ é uma base para $\bigoplus_{i=1}^{r} \mathbb{K}$ sobre $\mathbb{K}$. Logo, o número de órbitas é $\nu = |\{\eta_g | g \in \tau\}| = dim_{\mathbb{K}} \bigoplus_{i=1}^{r} \mathbb{K} = r$.

■

Exemplo. *Seja* $A_4 \subset S_4$ *o grupo alternado de ordem 12. Considere a seguinte apresentação para* A_4,

$$A_4 = < a, b, c | a^2 = b^3 = c^3 = abc = 1 > .$$

Qualquer elemento de A_4 *pode ser escrito da forma* $a^i b^j c^k$, *onde* $0 \leq j, k \leq 2$ *e* $i = 0, 1$. *No entanto, existem elementos cuja apresentação não é única. Alguns desses casos são os seguintes*

$$\begin{array}{ll} abc = 1 & bc = a \\ ab = c^2 & b = ac^2 \\ abc^2 = c & ac = bc^2. \end{array}$$

Assim, podemos explicitar A_4 *do seguinte modo.*

$$A_4 = \{1, a, b, b^2, c, c^2, ab^2, ac, b^2c, b^2c^2, ab^2c, ab^2c^2\}.$$

Além disso, podemos deduzir as seguintes relações úteis.

$$\begin{aligned} ba &= b^2c; \\ ca &= b^2; \\ cb &= b^2c^2. \end{aligned}$$

A fim de ilustrar o cálculo das classes de conjugação de A_4, vamos calcular a classe de conjugação de $a \in A_4$. Para tanto, a seguir, calculamos os conjugados de a em A_4.

$$1a1 = a;$$

$$aaa = a;$$

$$\begin{aligned} b^2ab &= b(ba)b \\ &= b(b^2c)b \\ &= cb; \end{aligned}$$

$$\begin{aligned} bab^2 &= b(ab)b \\ &= bc^2b \\ &= (bc^2)b \\ &= acb; \end{aligned}$$

$$\begin{aligned} c^2ac &= (ab)ac \\ &= a(ba)c \\ &= a(b^2c)c \\ &= ab^2c^2 \\ &= acb; \end{aligned}$$

$$\begin{aligned} cac^2 &= c(ac^2) \\ &= cb; \end{aligned}$$

$$\begin{aligned} (ba)a(ab^2) &= bab^2 \\ &= acb; \end{aligned}$$

$$\begin{aligned} (c^2a)a(ac) &= c^2ac \\ &= acb; \end{aligned}$$

$$\begin{aligned}(c^2b)a(b^2c) &= c^2a(cb)c\\ &= c^2a(b^2c^2)c\\ &= c^2ab^2\\ &= c(ca)b^2\\ &= cb;\end{aligned}$$

$$\begin{aligned}(cb)a(b^2c^2) &= c(acb)c^2\\ &= (ca)(cb)c^2\\ &= b^2b^2c^2c^2\\ &= bc\\ &= a;\end{aligned}$$

$$\begin{aligned}(c^2ba)a(ab^2c) &= c^2bab^2c\\ &= cb;\end{aligned}$$

$$\begin{aligned}(cba)a(ab^2c^2) &= cbab^2c^2\\ &= a.\end{aligned}$$

As classes de conjugação de A_4 são

$$\begin{aligned}&\{1\};\\ &\{a, cb, acb\};\\ &\{b, cb^2, b^2c, c^2\};\\ &\{c, ac, b^2, c^2b\}.\end{aligned}$$

Com isso, temos as somas de classes

$$\begin{aligned}\gamma_1 &= 1;\\ \gamma_2 &= a + cb + acb;\\ \gamma_3 &= b + cb^2 + b^2c + c^2;\\ \gamma_4 &= c + ac + b^2 + c^2b.\end{aligned}$$

Observe que o exponte de A_4 é igual a 6. Considere θ uma raíz primitiva da unidade de ordem 6. Neste caso, temos que $Gal(\mathbb{Q}(\theta), \mathbb{Q}) = \{I, \sigma\}$, onde I é a identidade e $\sigma(\theta) = \theta^5$. Nosso próximo passo é calcular as órbitas da ação do grupo de Galois em $\{\gamma_i\}$.

Sem nenhum esforço, temos que $S_1 = \{1\}$ *é uma órbita. Para calcular uma outra classe, note que* $(cb)^2 = 1$*, e assim,* $(cb)^5 = cb$*. Do mesmo modo,* $(acb)^2 = 1$*, resultando em* $(acb)^5 = acb$*. Com isso,*

$$\begin{aligned}\sigma(\gamma_2) &= a^5 + (cb)^5 + (acb)^5 \\ &= a + cb + acb \\ &= \gamma_2.\end{aligned}$$

Se fizermos cálculos parecidos com os que já esboçamos, teremos que $(cb^2)^5 = ac$ *e* $(b^2c)^5 = c^2b$*. Assim,*

$$\begin{aligned}\sigma(\gamma_3) &= b^5 + (cb^2)^5 + (b^2c)^5 + (c^2)^5 \\ &= b^2 + ac + c^2b + c \\ &= \gamma_4.\end{aligned}$$

Como $(ac)^5 = cb^2$ *e* $(c^2b)^5 = b^2c$*, segue que*

$$\begin{aligned}\sigma(\gamma_4) &= c^5 + (ac)^5 + (c^2b)^5 + (b^2)^5 \\ &= c^2 + cb^2 + b^2c + b \\ &= \gamma_3.\end{aligned}$$

Portanto, as órbitas da ação de $Gal(\mathbb{Q}(\theta), \mathbb{Q})$ *em* $\{\gamma_i | i = 1, 2, 3, 4\}$ *são*

$$\begin{aligned}S_1 &= \{1\}, \\ S_2 &= \{\gamma_2\}, \\ S_3 &= \{\gamma_3, \gamma_4\}.\end{aligned}$$

Pelo Teorema acima, $\mathbb{Q}A_4$ *possui 3 componentes simples.*

3.2 O TEOREMA DE BERMAN-WITT

Sejam G um grupo finito, m o expoente de G e θ uma m-ésima raíz da unidade sobre um corpo $\mathbb{K}$, tal que $car(\mathbb{K}) \nmid |G|$. Para cada $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$, escrevemos $\sigma(\theta) = \theta^i$, com i um inteiro positivo, e temos uma ação do grupo de Galois em G, dada por $g^\sigma \mapsto g^i$.

Denotamos $\Psi_\sigma : G \to G$ a função que manda $g \in G$ em g^σ. Dizemos que dois elementos a, b em G são $\mathbb{K}$-conjugados se

$$x^{-1}bx = a^i,$$

para algum $x \in G$ e algum $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$, com $\sigma(\theta) = \theta^i$. A $\mathbb{K}$-conjugação é uma relação de equivalência, de modo que G pode ser particionado em classes de equivalência. Essas classes de equivalência são chamadas classes $\mathbb{K}$-conjugadas do grupo G. Observe também que elementos na mesma classe $\mathbb{K}$-conjugada tem a mesma ordem.

Se x é um elemento de Γ_g então $x = h^{-1}gh$, para algum $h \in G$. Ao notar que $\Psi_\sigma(x) = x^i = h^{-1}g^ih \in \Gamma_{g^i}$, afirmamos que a $\mathbb{K}$-conjugação leva classe de conjugação em classe de conjugação. Neste caso, dizemos que as classes de conjugação de G, Γ_g e Γ_{g^i}, são $\mathbb{K}$-conjugadas

Lema 3.11. *Seja $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$, com $\sigma(\theta) = \theta^i$, e Γ_g, $\Gamma_{g'}$ as classes de conjugação de g, g', respectivamente. Então $\Psi_\sigma(\Gamma_g) = \Gamma_{g'}$ se e somente se existe $h \in G$ tal que $g' = h^{-1}g^ih$.*

Demonstração: Suponhamos que $\Psi_\sigma(\Gamma_g) = \Gamma_{g'}$. Já que $g' \in \Gamma_{g'}$, para algum $h \in G$, temos $g' = \Psi_\sigma(h^{-1}gh) = h^{-1}g^ih$. Reciprocamente, se $x \in \Gamma_{g'}$ então $x = k^{-1}g'k$, para algum $k \in G$. Como agora estamos supondo que $g' = h^{-1}g^ih$, temos $x = (hk)^{-1}g^i(hk) = \Psi_\sigma((hk)^{-1}g(hk))$, quer dizer, $\Gamma_{g'} \subset \Psi_\sigma(\Gamma_g)$. Se $y = \Psi_\sigma(k^{-1}gk)$ então $y = k^{-1}g^ik = (h^{-1}k)^{-1}g(h^{-1}k) \in \Gamma_{g'}$. Assim provamos a outra inclusão, de jeito que $\Psi_\sigma(\Gamma_g) = \Gamma_{g'}$, como queríamos mostrar. ∎

Em vista deste Lema, dizemos que duas classes de conjugação de G, Γ_g e $\Gamma_{g'}$, são $\mathbb{K}$-conjugadas, se existe $\sigma \in Gal(\mathbb{K}(\theta), \mathbb{K})$, tal que $\Psi_\sigma(\Gamma_g) = \Gamma_{g'}$.

Para cada $x \in G$, usamos a notação $C_{\mathbb{K}}(x)$, para a classe $\mathbb{K}$-conjugada do elemento x. Afim de relacionar esses dois conceitos de conjugação, considere

$$I_{\mathbb{K}} = \{k | \exists \sigma \in Gal(\mathbb{K}(\theta), \mathbb{K}) \text{ com } \sigma(\theta) = \theta^k\}.$$

Então, podemos escrever a classe $\mathbb{K}$-conjugada de um elemento g em G como

$$C_{\mathbb{K}}(g) = \{h^{-1}g^ih | h \in G \text{ e } i \in I_{\mathbb{K}}\}.$$

Da mesma maneira, podemos escrever a classe $\mathbb{K}$-conjugada de Γ_g como

$$\{\Gamma_{g^i} | i \in I_{\mathbb{K}}\}.$$

A partir disto, temos que

$$C_{\mathbb{K}}(g) = \bigcup_{i \in I_{\mathbb{K}}} \Gamma_{g^i}. \tag{14}$$

Em vista disso, concluímos que o número de classes $\mathbb{K}$-conjugadas distintas de elementos $g \in G$ é igual ao número de classes $\mathbb{K}$-conjugadas distintas de classes Γ_g.

Exemplo. *Para cada $\sigma \in Gal(\mathbb{Q}(\theta), \mathbb{Q})$ existe um inteiro i tal que $\sigma(\theta) = \theta^i$, com $mdc(i, m) = 1$. Por outro lado, para cada inteiro positivo j, tal que $mdc(j, m) = 1$ temos que σ_j definido por $\sigma_j(\theta) = \theta^j$ é um elemento de $Aut(\mathbb{Q}) = Gal(\mathbb{Q}(\theta), \mathbb{Q})$. Portanto, as órbitas S_g dos elementos γ_g em $\mathcal{B} = \{\gamma_g : g \in G\}$ pela ação de $Gal(\mathbb{Q}(\theta), \mathbb{Q})$ são os conjuntos*

$$S_g = \{\gamma_{g^i} : mdc(j, m) = 1\}. \tag{15}$$

Segue que

$$C_{\mathbb{Q}}(g) = \bigcup_{mdc(j,m)=1} \Gamma_{g^j}. \tag{16}$$

Agora, afirmamos que

$$C_{\mathbb{R}}(g) = \Gamma_g \cup \Gamma_{g^{-1}}. \tag{17}$$

De fato, o anel $\mathbb{R}(\theta)$ é ou igual a $\mathbb{R}$ ou igual a $\mathbb{C}$. Se $\mathbb{R}(\theta) = \mathbb{R}$ então $Gal(\mathbb{Q}, \mathbb{Q}) = \{1\}$. Claramente $S_g = \{\gamma_g\}$ e $C_{\mathbb{R}}(g) = \Gamma_g$. Em adição, se isso ocorre temos que $\theta = \pm 1$. Por conseguinte, o exponte do grupo G é igual à 2, e $g = g^{-1}$ para todo $g \in G$. Então $\Gamma_g = \Gamma_{g^{-1}}$ e $C_{\mathbb{R}}(g) = \Gamma_g \cup \Gamma_{g^{-1}}$.

Por outro lado $\mathbb{R}(\theta) = \mathbb{C}$ e existe um único elemento não trivial σ_0 em $Gal(\mathbb{C}, \mathbb{Q})$, ou seja, a conjugação complexa. Se θ é uma raíz da unidade temos que $\sigma_0(\theta) = \theta^{-1}$. Assim $C_{\mathbb{R}}(g) = \bigcup_{\sigma \in \{-1,1\}} \Gamma_{g^\sigma} = \Gamma_g \cup \Gamma_{g^{-1}}$, como havíamos afirmado.

Essas classes são importantes, já que, o número de componentes simples de uma álgebra de grupo semisimples $\mathbb{K}G$ é igual ao número de classes $\mathbb{K}$-conjugadas de G.

Teorema 3.12 (Berman [Ber], Witt, [Witt]). *Seja $\mathbb{K}G$ uma álgebra de grupo semisimples. O número de componentes simples de $\mathbb{K}G$ é igual ao número de classes $\mathbb{K}$-conjugadas de G.*

Demonstração: Denotamos por S_g a órbita de γ_g pela ação do grupo de Galois $Gal(\mathbb{K}(\theta), \mathbb{K})$, onde γ_g é uma soma de classe, e por η_g a soma de todos os elementos de S_g. Seja ν o número de órbitas distintas S_g, e seja τ o conjunto formado por elementos $g_1, \cdots, g_\nu$ de G, tal que $S_{g_1}, \cdots, S_{g_\nu}$ são as órbitas distintas da ação de

$Gal(\mathbb{K}(\theta), \mathbb{K})$. Sendo assim, para cada η_g, e consequentemente para cada S_g, temos que $C_{\mathbb{K}}(g) = supp(\eta_g)$. Então, podemos escrever

$$\eta_g = \sum_{h \in C_{\mathbb{K}}(g)} h.$$

Como cada $h \in G$ esta no suporte de apenas um η_g, temos que $G = \dot{\bigcup}_{g \in \tau} C_{\mathbb{K}}(g)$. Disto segue que, o número de classes $\mathbb{K}$-conjugadas distintas $C_{\mathbb{K}}(g)$ é ν. Uma vez que ν também é igual ao número de componentes simples de $\mathbb{K}G$, pelo Teorema 3.10, concluímos que o número de $\mathbb{K}$-classes conjugadas de G é igual ao número de componentes simples de $\mathbb{K}G$. ∎

Exemplo. *Seja Q_8 o grupo dos Quatérnios. Considere a seguinte apresentação*

$$Q_8 = < i, j | \quad i^4 = 1, i^2 = j^2, i^j = i^{-1} > .$$

As classes de conjugação de Q_8 são

$$\{1\}$$
$$\{-1\}$$
$$\{i, -i\}$$
$$\{j, -j\}$$
$$\{ij, -ij\}.$$

Como o expoente deste grupo é igual a 4, seja θ uma raíz primitiva da unidade de ordem 4. Considere $\mathbb{Q}$ o conjunto dos números racionais e $\mathbb{F}_3$ o corpo de Galois com 3 elementos. Então o grupo de Galois $Gal(\mathbb{Q}(\theta) : \mathbb{Q})$ é isomorfo ao grupo cíclico C_2 de ordem 2. Uma vez que as $\mathbb{Q}$-classes de Q_8 são iguais as classes de conjugação, temos que $\mathbb{Q}Q_8$ possui 5 componentes simples. Além disso, o corpo $\mathbb{F}_3$ é um corpo de decomposição para Q_8. Logo,

$$\mathbb{F}_3 Q_8 \simeq \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus M_2(\mathbb{F}_3).$$

4 AS UNIDADES CENTRAIS DE ZG

Em seu notável artigo "The Units of group rings"[Hi], Graham Higman mostrou que, se G for um grupo finito, o grupo das unidades centrais de $\mathbb{Z}G$, denotado por $\mathcal{Z}(U(\mathbb{Z}G))$, é igual à $\{-1,1\} \times \mathcal{Z}(G) \times A_G$, onde A_G é um subgrupo abeliano livre de posto finito. Neste capítulo objetivamos calcular o posto do grupo das unidades centrais de $\mathbb{Z}G$ quando G é um grupo finito, não necessariamente abeliano. Além disso, vamos determinar qual a condição sobre o grupo G para que as unidades centrais de $\mathbb{Z}G$ sejam triviais.

4.1 ALGUMAS PROPRIEDADES DO CENTRO DE QG

Seja G um grupo finito de ordem n, com t classes de conjugação $\Gamma_1, \cdots, \Gamma_t$. Sejam $g_1, \cdots g_t$ os representantes destas classes e $\gamma_1 \cdots, \gamma_t$ as somas de classes, respectivamente.

Do corolário 2.2, no capítulo 2, sabemos que a álgebra de grupo $\mathbb{Q}G$ é semisimples, de sorte que, pelo Teorema 2.3, é isomorfa a uma soma direta de álgebras de matrizes, ou seja,

$$\mathbb{Q}G \simeq \oplus_{i=1}^{m} M_{n_i}(D_i).$$

Se considerarmos o centro de $\mathbb{Q}G$, denotado por $\mathcal{Z}(\mathbb{Q}G)$, então

$$\mathcal{Z}(\mathbb{Q}G) \simeq \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_m,$$

onde os corpos $\mathbb{K}_i$, $1 \leq i \leq m$, são extensões finitas de $\mathbb{Q}$. Pelo Teorema de Berman-Witt, visto no capítulo anterior, o inteiro m é o número de $\mathbb{Q}$-classes de G, denotado por $n_{\mathbb{Q}}(G)$. A fim de simplificar a notação, ponha $A = \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_m$. Além disso, sempre que for apropriado, iremos supor $A = \mathcal{Z}(\mathbb{Q}G)$. Seja $\mathcal{O}_j$ o anel dos inteiros algébricos de $\mathbb{K}_j$, $1 \leq j \leq m$.

Teorema 4.1. *O grupo das unidades do anel dos inteiros de A, denotado $\mathcal{O}_A$, é isomorfo ao produto direto $\mathcal{U}(\mathcal{O}_1) \times \cdots \times \mathcal{U}(\mathcal{O}_m)$.*

Demonstração: Se $\alpha \in \mathcal{O}_A$, então existe um polinômio $f(x) \in \mathbb{Z}[x]$ tal que $f(\alpha) = 0$. Já que $\mathcal{O}_A$ é um subconjunto de A, podemos escrever $\alpha = (\alpha_1, \cdots, \alpha_m)$. Note também que, $0 = f(\alpha) = (f(\alpha_1), \cdots, f(\alpha_m))$, ou seja, $f(\alpha_j) = 0$ para todo $1 \leq j \leq m$. Portanto, cada $\alpha_j \in \mathcal{O}_j$, $1 \leq j \leq m$.

Reciprocamente, se $\beta = (\beta_1, \cdots, \beta_m) \in \mathcal{U}(\mathcal{O}_1) \times \cdots \times \mathcal{U}(\mathcal{O}_m)$ então existe $f_i(x) \in \mathbb{Z}[x]$, $1 \leq i \leq m$, tal que $f_i(\beta_i) = 0$. Desta forma, defina $f(x) = f_1(x) \cdots f_m(x)$. Com isso,

$$\begin{aligned} f(\beta) &= (f(\beta_1), \cdots, f(\beta_m)) \\ &= \left(\prod_j f_j(\beta_1), \cdots, \prod_j f_j(\beta_m) \right) = \mathbf{0}, \end{aligned}$$

onde $\mathbf{0} = (0, \cdots, 0) \in A$. Sendo assim, concluímos que $\mathcal{O}_A = \mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_m$.

Agora falta apenas estudar as unidades. Todavia, é fácil ver que, o grupo das unidades de uma soma direta de anéis R_i é igual ao produto direto das unidades destes anéis R_i. Portanto, temos que $\mathcal{U}(\mathcal{O}_A) = \mathcal{U}(\mathcal{O}_1) \times \cdots \times \mathcal{U}(\mathcal{O}_m)$.

■

No capítulo 1, vimos que os grupos $\mathcal{U}(\mathcal{O}_i)$, $1 \leq i \leq m$, são grupos abelianos finitamente gerados. Desde que $\mathcal{U}(\mathcal{O}_A) = \mathcal{U}(\mathcal{O}_1) \times \cdots \times \mathcal{U}(\mathcal{O}_m)$, temos que $\mathcal{U}(\mathcal{O}_A)$ é também um grupo abeliano finitamente gerado. Nosso objetivo será enunciar um Teorema cujo conteúdo nos permitirá calcular o posto livre de $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ em termos do posto de $\mathcal{U}(\mathcal{O}_A)$. Antes, porém, precisamos de alguns resultados.

Seja 1_G o caracter principal de G e $\chi_1 = 1_G, \chi_2, \cdots, \chi_r$ um conjunto completo de caracteres complexos irredutíveis do grupo G de graus $n_1, n_2, \cdots, n_t$, respectivamente. Considere também $e_1, e_2, \cdots, e_t$ um sistema completo de idempotentes ortogonais minimais, onde e_i corresponde caracter χ_i, $1 \leq i \leq r$.

No capítulo 2 vimos que o conjunto $\{\gamma_1, \cdots, \gamma_t\}$ é um base do centro de $\mathbb{Q}G$ sobre os racionais. Desde que $\{e_1, e_2, \cdots, e_t\}$ também seja uma base para o mesmo espaço, deve haver uma matriz mudança de base como relação a estas bases. Segundo [CR1, Teorema 33.8], podemos escrever

$$e_i = \frac{n_i}{n} \sum_{j=0}^{t} \overline{\chi_i(g_j)} \gamma_j. \tag{18}$$

Com isso, podemos demonstrar o seguinte resultado.

Teorema 4.2. *Existe um inteiro k tal que a k-ésima potência de qualquer unidade no anel dos inteiros de $\mathcal{Z}(\mathbb{Q}G)$ esta em $\mathcal{Z}(\mathbb{Z}G)$.*

Demonstração: Seja h o expoente do grupo G. Do capítulo anterior sabemos que $\mathbb{Q}(\theta)$, onde $\theta = \sqrt[h]{1}$, é um corpo de decomposição para G.

Agora, tomemos k como o número de classes de resíduos módulo $n = |G|$ em $\mathbb{Q}(\theta)$ que são primos com n. Seja α uma unidade do anel dos inteiros de $\mathcal{Z}(\mathbb{Q}G)$. Então, podemos escrever

$$\alpha = \sum_{i=1}^{m} b_i e_i$$

onde os e_i são os idempotentes descritos acima e $b_i \in \mathbb{Q}(\theta)$, $1 \leq i \leq m$, Além disso, como α é inversível, devemos ter $b_i \neq 0$. Isto porque existe β tal que $\alpha\beta = 1$; se $\beta = \sum_{i=1}^{m} d_i e_i$, então $\alpha\beta = \sum_{i=1}^{m} b_i d_i e_i = 1$. Como $1 = \sum_{i=1}^{m} e_i$, e os e_i são linearmente independentes, segue que $b_i d_i = 1$, para todo i. O inverso de α é igual a $\sum_{b_i \neq 0}^{m} b_i^{-1} e_i$ em $\mathbb{Q}(\theta)G$. Como $e_i^2 = e_i$, $e_i e_j = 0$ se $i \neq j$, e $\sum_i e_i = 1$ segue que os b_i, $1 \leq i \leq m$, são unidades em $\mathbb{Q}(\theta)$ e assim, primos com n. Pelo Teorema de Fermat para ideais

$$b_i^k \equiv 1 (mod\ n).$$

Ou seja, existem c_i inteiros em $\mathbb{Q}(\theta)$ tais que $b_i^k - 1 = nc_i$, $1 \leq i \leq m$. Como $1 = \sum_{i=1}^{m} e_i$, segue que

$$\begin{aligned} \alpha^k &= \sum_{i=1}^{m} b_i^k e_i \\ &= 1 + \sum_{i=1}^{m} (b_i^k - 1) e_i \\ &= 1 + \sum_{i=1}^{m} n c_i e_i. \end{aligned}$$

Pela equação 18 temos que ne_i são inteiros algébricos. Como o anel dos inteiros algébricos de $\mathbb{Q}$ é igual aos inteiros $\mathbb{Z}$ segue que α^k pertence a $\mathcal{Z}(\mathbb{Z}G)$.

■

Neste instante, podemos demonstrar o Teorema que havíamos mencionado no início.

Teorema 4.3. *Seja $\rho(\mathcal{U}(\mathcal{O}_A))$ o posto livre de $\mathcal{U}(\mathcal{O}_A)$ e ρ_G o posto livre de $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. Então $\rho_G = \rho(\mathcal{U}(\mathcal{O}_A))$.*

Demonstração: Seja α um elemento de $\mathcal{U}(\mathcal{O}_A)$. Já que $\mathcal{U}(\mathcal{O}_A)$ esta contido em A, e estamos supondo $A = \mathcal{Z}(\mathbb{Q}G)$, temos pelo Teorema 4.2 que, existe um inteiro k tal que β^k esta em $\mathcal{Z}(\mathbb{Z}G)$, para todo $\beta \in \mathcal{U}(\mathcal{O}_A)$. Logo, $\alpha^k \in \mathcal{Z}(\mathbb{Z}G)$ e se α^{-1} é o inverso de $\alpha \in \mathcal{U}(\mathcal{O}_A)$, então $(\alpha^k)^{-1} = \alpha^{-k} = (\alpha^{-1})^k$ também pertence a $\mathcal{Z}(\mathbb{Z}G)$. Portanto, para todo $\alpha \in \mathcal{U}(\mathcal{O}_A)$ vale que $\alpha^k \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$.

Por simplicidade, ponha $\rho(\mathcal{U}(\mathcal{O}_A)) = \ell$. Da Teoria dos Números Algébricos sabemos que existe um conjunto independente de unidades $\{u_1, \cdots, u_\ell\}$ de $\mathcal{U}(\mathcal{O}_A)$. Pelo que discutimos acima, $\{u_1^k, \cdots, u_\ell^k\}$ esta contido em $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. Além disso, uma vez que o conjunto $\{u_1, \cdots, u_\ell\}$ é independente, se $(u_1^k)^{m_1} \cdots (u_\ell^k)^{m_\ell} = 1$ então $m_i = 0$ para todo $1 \leq i \leq \ell$. Assim, o conjunto $\{u_1^k, \cdots, u_l^k\}$ é independente em $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. Como a cardinalidade de qualquer conjunto independente em $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ é menor do que o posto ρ_G, temos que $\rho(\mathcal{U}(\mathcal{O}_A)) = \ell \leq \rho_G$.

Por outro lado, $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ é um subgrupo de $\mathcal{U}(\mathcal{O}_A)$. Com isso, $\rho(\mathcal{U}(\mathcal{O}_A)) \geq \rho_G$, e pelo visto acima, concluímos que $\rho(\mathcal{U}(\mathcal{O}_A)) = \rho_G$. ∎

4.2 O POSTO DAS UNIDADES CENTRAIS DE ZG

Com o Teorema 4.3 em mente, vamos calcular o posto livre $\rho(\mathcal{U}(\mathcal{O}_A))$. Seja $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$ de grau n. Neste caso, $\mathbb{K}$ é um corpo numérico, e seu grau deve satisfaz $n = r + 2c$, onde r denota o número de homomorfismos reais de $\mathbb{K}$ e c o número de pares de homomorfismos complexos de $\mathbb{K}$ (Veja definição 1.29). Seja o par $[r, c]$ a assinatura de $\mathbb{K}$.

Teorema 4.4. *Seja $[r_i, c_i]$ a assinatura de $\mathbb{K}_i$, $1 \leq i \leq m$. Fixe $r_0 = \sum_{i=1}^m r_i$, $c_0 = \sum_{i=1}^m c_i$, e denote $\rho(\mathcal{U}(\mathcal{O}_A))$ o posto livre de $\mathcal{U}(\mathcal{O}_A)$. Então $\rho(\mathcal{U}(\mathcal{O}_A)) = r_0 + c_0 - m$.*

Demonstração: Sendo $\mathcal{O}_A = \mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_m$, onde $\mathcal{O}_i$ é o anel dos inteiros algébricos de $\mathbb{K}_i$, $1 \leq i \leq m$, temos que

$$\mathcal{U}(\mathcal{O}_A) = \mathcal{U}(\mathcal{O}_1) \times \cdots \times \mathcal{U}(\mathcal{O}_m).$$

Pelo Teorema das Unidades de Dirichlet, temos que cada $\mathcal{U}(\mathcal{O}_i)$ é um grupo abeliano finitamente gerado, cujo posto de livre é igual a $r_i + c_i - 1$. O Teorema também nos

permite escrever $\mathcal{U}(\mathcal{O}_i) \simeq C_i \times L_i$, onde C_i é um grupo cíclico finito e L_i é um grupo livre de torção de posto $r_i + c_i - 1$. Assim

$$\begin{aligned} U(\mathcal{O}_A) &\simeq C_1 \times L_1 \times \cdots \times C_m \times L_m \\ &\simeq (C_1 \times \cdots \times C_m) \times (L_1 \times \cdots \times L_m) \\ &\simeq T \times L. \end{aligned}$$

onde $T = C_1 \times \cdots \times C_m$ é um grupo de torção e $L = L_1 \times \cdots \times L_m$ é livre de torção. Assim, o posto livre de $U(\mathcal{O}_A)$ é igual a soma do posto dos L_i. Ou seja, $\rho(\mathcal{U}(\mathcal{O}_A)) = \sum_{i=1}^{m}(r_i + c_i - 1) = r_0 + c_0 - m$.

■

Já temos algo em mãos, mas podemos fazer melhor, ou seja, podemos expressar o posto de $\mathcal{U}(\mathcal{O}_A)$ em termos de números que já sabemos calcular. Nesta direção, começamos pelo seguinte.

Teorema 4.5. *Seja $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$ e seja $[r, c]$ sua assinatura. Então*

$$\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \underbrace{\mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{r} \oplus \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{c}.$$

Em particular, se $n_s(\mathbb{K}, \mathbb{R})$ denota o número de componentes simples de $\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$, então $n_s(\mathbb{K}, \mathbb{R}) = r + c$.

Demonstração: Uma vez que $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, sabemos que é uma extensão algébrica. Assim, todo elemento de $\mathbb{K}$ possui polinômio minimal sobre $\mathbb{Q}$. Note também que, pelo corolário 1.8, existe um $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$. Seja $p_\alpha(x)$ o polinômio minimal de α sobre $\mathbb{Q}$. Sendo $[r, c]$ a assinatura de $\mathbb{K}$, o polinômio $p_\alpha(x)$ possui r raízes reais e $2c$ raízes complexas. Sejam $\alpha_1, \cdots, \alpha_r$, as raízes reais e $\beta_1, \bar{\beta}_1, \cdots, \beta_c, \bar{\beta}_c$ as raízes complexas de $p_\alpha(x)$. Assim, $p_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_r) q_1(x) \cdots q_c(x)$, onde $q_i(x) = (x - \beta_i)(x - \bar{\beta}_i)$. Dito tudo isto, temos que

$$\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R} \simeq \frac{\mathbb{Q}[x]}{(p_\alpha)} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \frac{\mathbb{R}[x]}{(p_\alpha)}.$$

Pelo Teorema Chinês dos Restos para anéis temos que

$$\frac{\mathbb{R}[x]}{(p_\alpha)} \simeq \frac{\mathbb{R}[x]}{(x - \alpha_1)} \oplus \cdots \oplus \frac{\mathbb{R}[x]}{(x - \alpha_r)} \oplus \frac{\mathbb{R}[x]}{(q_1)} \oplus \cdots \oplus \frac{\mathbb{R}[x]}{(q_t)}.$$

A função $f(x) \in \mathbb{R}[x] \mapsto f(a_i)$ é um epimorfismo de anéis, cujo kernel é igual ao ideal $(x - a_i)$, $1 \leq i \leq r$. Assim sendo, $\mathbb{R}[x]/(x - \alpha_i) \simeq \mathbb{R}$, $1 \leq i \leq r$. Ainda convém ressaltar que $q_j(x) \in \mathbb{R}[x]$, $1 \leq j \leq c$, é um polinômio mônico, irredutível e de grau 2. Assim, $\mathbb{R}[x]/(q_j) \simeq \mathbb{C}$, $1 \leq j \leq c$. Com isso, chegamos que

$$\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \underbrace{\mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{r} \oplus \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{c}.$$

E claramente $n_s(\mathbb{K}, \mathbb{R}) = r + c$. ∎

Uma consequência é a sequinte afirmação.

Corolário 4.6. *Seja $A = \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_m$ uma soma direta de extensões finitas de $\mathbb{Q}$ e seja $[r_i, c_i]$ a assinatura de K_i, $1 \leq i \leq m$. Fixe $r_0 = \sum_{i=1}^{m} r_i$, $c_0 = \sum_{i=1}^{m} c_i$. Então*

$$A \otimes_{\mathbb{Q}} \mathbb{R} \simeq \underbrace{\mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{r_0} \oplus \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{c_0}. \tag{19}$$

Em particular, se $n_s(A, \mathbb{R})$ denota o número de componentes simples de $A \otimes_{\mathbb{Q}} \mathbb{R}$, então $n_s(\mathbb{K}, \mathbb{R}) = r_0 + c_0$.

Demonstração: Do Teorema anterior temos que

$$\begin{aligned} A \otimes_{\mathbb{Q}} \mathbb{R} &= (\mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_m) \otimes_{\mathbb{Q}} \mathbb{R} \\ &\simeq (\mathbb{K}_1 \otimes_{\mathbb{Q}} \mathbb{R}) \oplus \cdots \oplus (\mathbb{K}_m \otimes_{\mathbb{Q}} \mathbb{R}) \\ &\simeq (r_1\mathbb{R} \oplus c_1\mathbb{C}) \oplus \cdots \oplus (r_m\mathbb{R} \oplus c_m\mathbb{C}) \\ &\simeq r_0\mathbb{R} \oplus c_0\mathbb{C}. \end{aligned}$$

∎

Por saber que o número de componentes simples de $A \otimes_{\mathbb{Q}} \mathbb{R}$ é $n_s(A, \mathbb{R}) = r_0 + c_0$, e que o posto livre de $\mathcal{U}(\mathcal{O}_A)$ é $\rho(\mathcal{U}(\mathcal{O}_A)) = r_0 + c_0 - m$, pelo teorema 4.4, obtemos imediatamente o seguinte Teorema.

Teorema 4.7. *Seja $A = \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_m$ uma soma direta de extensões finitas de $\mathbb{Q}$ tal que $A \simeq \mathcal{Z}(\mathbb{Q}G)$. Então $\rho(\mathcal{U}(\mathcal{O}_A)) = n_s(A, \mathbb{R}) - m$.*

Agora estamos prontos para provar o Teorema principal deste capítulo.

Teorema 4.8. *Sejam G um grupo finito, $n_{\mathbb{R}}(G)$ o número de $\mathbb{R}$-classes de G, $n_{\mathbb{Q}}(G)$ o número de $\mathbb{Q}$-classes de G e ρ_G o posto livre de $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. Então $\rho_G = n_{\mathbb{R}}(G) - n_{\mathbb{Q}}(G)$.*

Demonstração: Pelo que provamos até agora, temos que $\rho_G = \rho(\mathcal{U}(\mathcal{O}_A))$ e $\rho(\mathcal{U}(\mathcal{O}_A)) = n_s(A, \mathbb{R}) - m$. Por ser m o número de componentes simples de $\mathcal{Z}(\mathbb{Q}G)$, deve ser obrigatóriamante igual $n_{\mathbb{Q}}(G)$, o número de $\mathbb{Q}$-classes de G. Desta maneira, basta mostrar que $n_{\mathbb{R}}(G)$ é igual a $n_s(A, \mathbb{R})$. Para tanto, note que $n_{\mathbb{R}}(G)$ é igual ao número de componentes simples de $\mathcal{Z}(\mathbb{R}G)$ e, pelo Lema 2.11,

$$\mathcal{Z}(\mathbb{Q}G) \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathcal{Z}(\mathbb{Q}G \otimes_{\mathbb{Q}} \mathbb{R}) \simeq \mathcal{Z}(\mathbb{R}G). \tag{20}$$

Já que $\mathcal{Z}(\mathbb{Q}G) \simeq \mathbb{K}_1 \oplus \cdots \oplus \mathbb{K}_m$, segue que o número de componentes simples de $\mathcal{Z}(\mathbb{Q}G) \otimes_{\mathbb{Q}} \mathbb{R}$ é igual a $n_s(A, \mathbb{R})$.

■

Se o grupo das unidades centrais de $\mathbb{Z}G$ é composto de elementos da forma $\pm g$, onde $g \in \mathcal{Z}(G)$, ou seja, se $\mathcal{Z}(U(\mathbb{Z}G)) = \{-1, 1\} \times \mathcal{Z}(G)$, então o posto livre deste grupo é igual a zero. A recíproca também vale, isto é, se o posto livre do grupo das unidades centrais de $\mathbb{Z}G$ é zero, então $\mathbb{Z}G$ possui apenas unidades centrais triviais. Desta maneira, podemos estudar os grupos G tais que $\mathbb{Z}G$ possui apenas unidades centrais triviais por calcular o posto livre ρ_G de $\mathcal{Z}(U(\mathbb{Z}G))$.

Outro modo de caracterizar o grupo $\mathcal{Z}(U(\mathbb{Z}G))$ se estabelece através do seguinte Teorema, devido a Ritter e Sehgal (Veja [RS]).

Teorema 4.9. *Seja G um grupo finito. Todas as unidades centrais de $\mathbb{Z}G$ são triviais se e somente se para todo $g \in G$ e todo número natural j, $mdc(j, |G|) = 1$, temos que g^j é conjugado a g ou g^{-1}.*

Demonstração: Já vimos acima que todas as unidades centrais de $\mathbb{Z}G$ são triviais se e somente se o posto livre ρ_G das unidades centrais de $\mathbb{Z}G$ é zero.

Para cada $g \in G$, denote $C_{\mathbb{Q}}(g)$ a $\mathbb{Q}$-classe de g e $C_{\mathbb{R}}(g)$ a $\mathbb{R}$-classe de g. Pelo que já vimos no capítulo 3, na equação 17, $C_{\mathbb{R}}(g) = \Gamma_g \cup \Gamma_{g^{-1}}$. Desta forma, para cada $g \in G$, e para cada número natural j com $mdc(j, |G|) = 1$, a afirmação

$$\text{"}O \text{ elemento } g^j \text{ é conjugado a } g \text{ ou } g^{-1}\text{"}$$

é equivalente a

$$"O \text{ elemento } g^j \in C_{\mathbb{R}}(g)."$$

Além disso, para cada número natural j, vale que o $mdc(j, |G|) = 1$ se e somente se $mdc(j, m) = 1$, pois $|G|$ e o expoente m de G possuem os mesmos divisores primos.

Por tudo isso, basta mostrar que, o posto livre ρ_G é zero se e somente se $g^j \in C_{\mathbb{R}}(g)$, para todo número natural j, tal que $mdc(j, m) = 1$.

Na equação 16 do capítulo anterior, escrevemos que

$$C_{\mathbb{Q}}(g) = \bigcup_{mdc(j,m)=1} \Gamma_{g^j}.$$

Como $g^j \in C_{\mathbb{R}}(g)$ implica $\Gamma_{g^i} \subset C_{\mathbb{R}}(g)$, temos que $g^j \in C_{\mathbb{R}}(g)$, para todo j com $mdc(j, m) = 1$, se e somente se $\cup_{mdc(j,m)=1}\Gamma_{g^j} \subset C_{\mathbb{R}}(g)$, ou seja, se e somente se $C_{\mathbb{Q}}(g) \subset C_{\mathbb{R}}(g)$. Ainda vimos que $C_{\mathbb{R}}(g) \subset C_{\mathbb{Q}}(g)$, para todo $g \in G$.

Em suma, podemos escrever que

$$"O \text{ elemento } g^j \text{ está em } C_{\mathbb{R}}(g), \text{ para todo } j \text{ com } mdc(j, m) = 1$$
$$\text{se e somente se } C_{\mathbb{Q}}(g) = C_{\mathbb{R}}(g)."$$

No Teorema 4.8, calculamos o posto livre das unidades centrais de $\mathbb{Z}G$ como $\rho_G = n_{\mathbb{R}}(G) - n_{\mathbb{Q}}(G)$. Portanto,

$$"\rho_G = 0 \text{ se e somente } n_{\mathbb{R}}(G) = n_{\mathbb{Q}}(G)."$$

Uma vez que

$$"n_{\mathbb{R}}(G) = n_{\mathbb{Q}}(G) \text{ se e somente se } C_{\mathbb{Q}}(g) = C_{\mathbb{R}}(g),"$$

segue o resultado pretendido.

■

5 AS COMPONENTES SIMPLES DO CENTRO DE FG/J(FG)

O matemático Burkhard Külshammer determinou a estrutura do centro da álgebra $A/J(A)$, onde A é uma álgebra finita sobre um corpo finito ([KH, Korollar E]). Nesta seção vamos tratar de um Teorema devido a Raul Ferraz, que estende o resultado de Külshammer para algumas álgebras de grupo infinitas.

Seja $\mathbb{F}$ um corpo de característica $p \geq 0$, e G um grupo finito com expoente e. Se $p > 0$ podemos escrever e como

$$e = mp^s,$$

onde $mdc(m, p) = 1$. Se $p = 0$, considere $m = e$. Seja θ um raíz primitiva da unidade de ordem m. Do capítulo 1 sabemos que $\mathbb{F}(\theta)$ é um corpo de decomposição para o polinômio separável $f(x) = x^m - 1$.

Daqui em diante, denotaremos

$$I_{\mathbb{F}} = \{k | \exists \sigma \in Gal(\mathbb{F}(\theta), \mathbb{F}) \text{ com } \sigma(\theta) = \theta^k\}.$$

Um elemento g de G é chamado um p'-elemento se a ordem de g não é divisível por p. Se g é um p'-elemento de G definimos a $\mathbb{F}$-classe de g como o conjunto

$$\mathcal{C}(g) = \{hg^k h^{-1} | h \in G, k \in I_{\mathbb{F}}\}. \tag{21}$$

Como os expoentes k são invertíveis módulo m e a ordem dos p'-elemento divide m, as $\mathbb{F}$-classes de G formam uma partição do subconjunto de todos os p'-elementos de G. Estas classes foram utilizadas em outro Teorema devido à Berman e Witt.

Teorema 5.1. *[Ber], [Witt], [CR2, Teorema 21.5] Seja $\mathbb{F}$ um corpo e G um grupo finito. O número de $\mathbb{F}G$-módulos irredutíveis não isomorfos é igual ao número de $\mathbb{F}$-classes de G.*

5.1 COMPONENTES SIMPLES DO CENTRO DE FG/J(FG)

Pelo critério de Maschke, sabemos que nem sempre $\mathbb{F}G$ é uma álgebra de grupo semisimples. Este é o caso se $car(\mathbb{F})$ divide a ordem de G, onde G é um grupo finito. No

entanto, podemos tomar o quociente de $\mathbb{F}G$ pelo radical de Jacobson $J(\mathbb{F}G)$, de forma que, $J(\mathbb{F}G/J(\mathbb{F}G)) = 0$. Neste caso, sendo G um grupo finito, a álgebra de grupo $\mathbb{F}G$ é um anel artiniano. Logo temos o seguinte.

Teorema 5.2. *A álgebra $\mathbb{F}G/J(\mathbb{F}G)$ é semisimples.*

Pelo Teorema 1.17, a álgebra $\mathbb{F}G/J(\mathbb{F}G)$ é isomorfa a uma soma direta de álgebras de matrizes sobre anéis de divisão. Ou seja

$$\frac{\mathbb{F}G}{J(\mathbb{F}G)} \simeq \bigoplus_{i=1}^{t} M_{n_i}(D_i),$$

onde D_i são anéis de divisão. Neste caso, t é o número de componentes simples de $\mathbb{F}G/J(\mathbb{F}G)$.

Lema 5.3. *O número de componentes simples de $\mathbb{F}G/J(\mathbb{F}G)$ é igual ao número de $\mathbb{F}G$-módulos simples não isomorfos.*

Demonstração: Sejam $M_1, \cdots, M_k$ todos os $\mathbb{F}G$-módulos simples não isomorfos, isto é, qualquer $\mathbb{F}G$-módulo simples é isomorfo a algum destes e os módulos M_i são dois a dois não isomorfos. Conforme vimos no capítulo 2, o Teorema 2.3 nos permite tomar ideais à esquerda minimais $I_i \subset M_{n_i}(D_i)$, da forma

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ & & \cdots & \\ x_{n_i} & 0 & \cdots & 0 \end{bmatrix} : x_1, x_2, \cdots, x_{n_i} \in D_i \right\} \simeq {D_i}^{n_i}.$$

onde $1 \leq i \leq t$. Basicamente, usando a mesma construção do Teorema 2.3, temos que os ideais I_i, $1 \leq i \leq t$, são $(\mathbb{F}G/J(\mathbb{F}G))$-módulos simples. Se para cada $x \in \mathbb{F}G$ considerarmos o elemento $x + J(\mathbb{F}G) \in \mathbb{F}G/J(\mathbb{F}G)$ então poderemos perfeitamente considerar os ideais I_i como $\mathbb{F}G$-módulos simples, definindo $x.y = \bar{x}.y$, para todo $y \in I_i$. Além disso, $I_i \ncong I_j$ se $i \neq j$. Desta maneira, cada $\mathbb{F}G$-módulo I_i deve ser isomorfo a M_j, $1 \leq i \leq k$. Portanto $t \leq k$.

Por outro lado, pelo Teorema 1.20, no capítulo 1, para cada $1 \leq i \leq k$, vale que

$$J(\mathbb{F}G)M_i = (0). \tag{22}$$

Isto significa que $J(\mathbb{F}G) \subset Ann(M_i)$ e, portanto, M_i é um $(\mathbb{F}G/J(\mathbb{F}G))$-módulo. Já que cada M_j é simples e qualquer $\mathbb{F}G/J(\mathbb{F}G)$-módulo simples é isomorfo a algum I_i, $1 \leq i \leq t$, obtemos que $k \leq t$. Logo $t = k$.

■

Este Lema nos permite reescrever o Teorema de Berman-Witt que enunciamos acima.

Teorema 5.4. *O número de componentes simples de $\mathbb{F}G/J(\mathbb{F}G)$ é igual ao número de $\mathbb{F}$-classes de G.*

A fim de descrever a técnica que iremos expor adiante é importante usarmos uma pequena variação da definição de $\mathbb{F}$-classes. Denotemos $\gamma_g \in \mathbb{F}G$ a soma de classe de g, ou seja, a soma de todos os conjugados de g.

Definição 5.5. *Seja g um p'-elemento. O conjunto*

$$S(\gamma_g) = \{\gamma_{g^k} | k \in I_{\mathbb{F}}\}. \tag{23}$$

*diz-se a $\mathbb{F}$-**classe ciclôtomica** de γ_g.*

Quando $\mathbb{F}G$ é semisimples, usamos no capitulo 3 esse conceito para provar o Teorema 5.4 e providenciar uma base da álgebra $\oplus_{i=1}^{r}\mathbb{F}e_i$, onde $\{e_1, \cdots, e_r\}$ é um conjunto de idempotentes primitivos centrais de $\mathbb{F}G$.

Conforme vimos também no capítulo 3, o número de $\mathbb{F}$-classes ciclôtomicas de G, que no caso eram as órbitas da ação do grupo de Galois em $\{\gamma_g | g \in G\}$, é igual ao número de $\mathbb{F}$-classes de G. Entretanto, o número de elementos nas correspondentes classes são diferentes. Pelo fato descrito acima, podemos afirmar o seguinte.

Teorema 5.6. *O número de componentes simples de $\mathbb{F}G/J(\mathbb{F}G)$ é igual ao número de $\mathbb{F}$- classes ciclotômicas em G.*

Visto que $\mathbb{F}(\theta)$ é um corpo de decomposição para $\mathbb{F}G$, podemos descrever o centro de $\mathbb{F}G/J(\mathbb{F}G)$ como

$$\mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G)) \simeq \bigoplus_{i=1}^{t} \mathbb{K}_i,$$

onde t é igual ao número de componentes simples de $\mathbb{F}G/J(\mathbb{F}G)$ e os corpos $\mathbb{K}_i$, $1 \leq i \leq t$ são tais que $\mathbb{F} \subset \mathbb{K}_i \subset \mathbb{F}(\theta)$.

Já temos um método para determinar t, ou seja, sabemos calcular o número de componentes simples pelo Teorema 5.4. Agora, nos falta determinar os corpos $\mathbb{K}_i$, $1 \leq i \leq t$. Se $Gal(\mathbb{F}(\theta), \mathbb{F})$ é cíclico de ordem n, podemos determinar as componentes simples de $\mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G))$, ou seja, os corpos $\mathbb{K}_i$, $1 \leq i \leq t$. Esta afirmação vale pelo fato

de, em um grupo cíclico, todos os subgrupos serem unicamente determinados pela sua ordem, a saber, um divisor de n. Pela Teoria de Galois sabemos que cada subgrupo de $Gal(\mathbb{F}(\theta), \mathbb{F})$ corresponde a um corpo $\mathbb{F}_i$ satisfazendo $\mathbb{F} \subset \mathbb{F}_i \subset \mathbb{F}(\theta)$ e cujo grau da extensão é justamente o ordem do subgrupo correspondente. Uma vez que o subgrupo é unicamente determinado pela sua ordem, a extensão $\mathbb{F}_i$ é unicamente determinada pelo grau $[\mathbb{F}_i : \mathbb{F}]$. Assim, para caracterizar o centro de $\mathbb{F}G/J(\mathbb{F}G)$, precisamos neste momento, apenas de uma maneira de calcular o grau das extensões $\mathbb{K}_i$, $1 \leq i \leq t$. Isto nos é fornecido pelo próximo resultado, que apontamos que o principal Teorema deste capítulo.

Teorema 5.7 (Principal)**.** *Seja $\mathbb{F}$, G e θ como acima e suponha que $Gal(\mathbb{F}(\theta), \mathbb{F})$ é cíclico. Seja t o número de $\mathbb{F}$-classes ciclotômicas em G. Se $\mathbb{K}_1, \cdots, \mathbb{K}_t$ são as componentes simples de $\mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G)))$ e $S_1, \cdots, S_t$ são as $\mathbb{F}$-classes ciclotômicas de G, então com uma apropriada reordenação dos índices, temos $|S_i| = [\mathbb{K}_i, \mathbb{F}]$.*

Ainda não estamos prontos para demonstrar esse Teorema. No entanto, enunciemos o seguinte corolário.

Corolário 5.8. *Sejam $\mathbb{F}$, G e θ como acima e suponha que o grupo $Gal(\mathbb{F}(\theta), \mathbb{F})$ é cíclico. Seja t o número de componentes simples de $\mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G)))$, $S_1, \cdots, S_t$ as $\mathbb{F}$-classes ciclotômicas de G e n_i a cardinalidade de S_i, $1 \leq i \leq t$. Então*

$$\mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G))) \simeq \bigoplus_{i=1}^{t} \mathbb{F}_{n_i}$$

onde $\mathbb{F}_{n_i}$ denota o único corpo entre $\mathbb{F}(\theta)$ e $\mathbb{F}$ e $\mathbb{F}$ é tal que $[\mathbb{F}_{n_i} : \mathbb{F}] = n_i$.

5.2 AS F-CLASSES CICLOTÔMICAS COMO ÓRBITAS

Seja $\bar{j}$ a classe de um inteiro j módulo m. Para qualquer p'-elemento g de G, defina $g^{\bar{j}} = g^j$. Existe um único homomorfismo injetivo $\iota : Gal(\mathbb{F}(\theta), \mathbb{F}) \to \mathcal{U}(\mathbb{Z}_m)$, tal que $\sigma(\theta) = \theta^{\iota(\sigma)}$, para todo $\sigma \in Gal(\mathbb{F}(\theta), \mathbb{F})$. Observe que, como $\mathcal{U}(\mathbb{Z}_m)$ é um grupo abeliano, segue que $Gal(\mathbb{F}(\theta), \mathbb{F})$ é também um grupo abeliano.

Seja $\mathcal{B}$ o seguinte conjunto

$$\mathcal{B} = \{\gamma_g | g \text{ é um } p'\text{-elemento de } G\}.$$

Para cada γ_g em $\mathcal{B}$ e todo $\sigma \in Gal(\mathbb{F}(\theta), \mathbb{F})$, definimos

$$\sigma(\gamma_g) = \gamma_{g^{\iota(\sigma)}}.$$

Uma $\mathbb{F}$-classe ciclotômica pode ser escrita como

$$S(\gamma_g) = \{\sigma(\gamma_g) | \sigma \in Gal(\mathbb{F}(\theta), \mathbb{F})\}.$$

Isso significa que as $\mathbb{F}$-classes ciclotômicas são precisamente as órbitas da ação de $Gal(\mathbb{F}(\theta), \mathbb{F})$ em $\mathcal{B}$. Quando $Gal(\mathbb{F}(\theta), \mathbb{F})$ é cíclico de ordem n, gerado por σ, as $\mathbb{F}-$ classes ciclotômicas de uma soma de classe $\gamma \in \mathcal{B}$ podem ser escritas como

$$S(\gamma) = \{\gamma, \sigma(\gamma), \cdots, \sigma^{i-1}(\gamma)\},$$

onde i é o menor inteiro positivo tal que σ^i gera o estabilizador de γ. Consequentemente, i divide n e $\sigma^k(\gamma) = \gamma$ se e somente se i divide k.

5.3 A PROVA DO TEOREMA PRINCIPAL

Nesta seção assumiremos que o grupo $Gal(\mathbb{F}(\theta), \mathbb{F})$ é cíclico de ordem n, gerado por σ, ou seja,

$$Gal(\mathbb{F}(\theta), \mathbb{F}) = \{I, \sigma, \sigma^2, \cdots \sigma^{n-1}\}.$$

Denotaremos por $\mathbb{F}_d$ o único corpo entre $\mathbb{F}(\theta)$ e $\mathbb{F}$ tal que $[\mathbb{F}_d : \mathbb{F}] = d$.

Antes de provar o Teorema 5.7, tentemos traçar uma linha de raciocínio. Nosso primeiro passo é relembrar que as $\mathbb{F}$-classes ciclotômicas em G podem ser vistas como órbitas de uma ação de grupo. Logo, a cardinalidade das $\mathbb{F}$-classes ciclotômicas dividem n, a ordem do grupo $Gal(\mathbb{F}(\theta), \mathbb{F})$.

Observe também que, sendo $\mathbb{F}(\theta)/\mathbb{F}$ uma extensão de Galois de grau n, para todo corpo intermediário $\mathbb{F} \subset \mathbb{K} \subset \mathbb{F}(\theta)$ temos que $[\mathbb{K} : \mathbb{F}]$ também é um divisor de n. Em vista disso, para cada divisor i de n, vamos contar quantas $\mathbb{F}$-classes ciclotômicas existem de cardinalidade i e quantos componentes simples de $\mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G))$ existem de grau i sobre $\mathbb{F}$. O Teorema acima seguirá se ambos os números forem os mesmos. Por isso, vamos nos preocupar em mostrar que tais números são de fato iguais.

Seja i um divisor de n. Denote por a_i o número de $\mathbb{F}$-classes ciclôtomicas de cardinalidade i e por b_i o número de componentes simples de $\mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G))$ de grau i sobre $\mathbb{F}$.

Esses números são tais que $\sum_{i|n} a_i$ e $\sum_{i|n} b_i$ são iguais ao número de componentes simples de $\mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G))$. Para mostrar que $a_i = b_i$, para todo i divisor de n, precisamos de mais informações. Por esse motivo, vamos calcular o número de componentes simples das álgebras $\mathbb{F}_dG/J(\mathbb{F}_dG))$, para cada divisor d de n, sabendo que tal número é igual ao número de $\mathbb{F}_d$-classes ciclotômicas. Este cálculo será realizado de duas maneiras diferentes. A primeira é a seguinte.

Proposição 5.9. *Sejam d e i divisores de n e sejam $\mathbb{F}_d$ e a_i como acima. Então, o número de componentes simples de $\mathbb{F}_dG/J(\mathbb{F}_dG)$ é igual à $\sum_{i|n} mdc(i,d)a_i$.*

Demonstração: Observe que $Gal(\mathbb{F}_d(\theta), \mathbb{F}_d) \subset Gal(\mathbb{F}(\theta), \mathbb{F}) =< \sigma >$, e sendo $Gal(\mathbb{F}_d(\theta), \mathbb{F}_d)$ um subgrupo de ordem n/d, tem-se que este é gerado por $< \sigma^d >$. Com isso, toda $\mathbb{F}_d$-classe ciclotômica de γ esta contida na $\mathbb{F}$-classe ciclotômica de γ. Uma vez que tanto as $\mathbb{F}_d$-classes ciclotômicas quanto as $\mathbb{F}$-classes ciclotômicas formam uma partição de $\{g \in G | g \text{ é } p' - \text{elemento}\}$ temos que, toda $\mathbb{F}$-classe ciclotômica é uma união disjunta de $\mathbb{F}_d$-classes ciclotômicas. Assim, precisamos apenas mostrar que cada $\mathbb{F}$-classe ciclotômica de cardinalidade i é a união de exatamente ℓ $\mathbb{F}_d$-classes ciclotômicas, onde $\ell = mdc(i,d)$.

Seja então S uma $\mathbb{F}$-classe ciclotômica de cardinalidade i e $\gamma \in S$. Então a $\mathbb{F}_d$-classe ciclotômica de γ é

$$S_d = \{\gamma, \sigma^d(\gamma), \cdots, \sigma^{d(\ell-1)}(\gamma)\} \tag{24}$$

onde ℓ é o menor inteiro positivo tal que $\sigma^{d\ell}(\gamma) = \gamma$. Como $\sigma^i(\gamma) = \gamma$, e é o menor inteiro tal que isso ocorre, temos que i divide $d\ell$, ou seja, $dl = mmc(i,d)$. Com isso, concluímos que qualquer $\mathbb{F}_d$-classe ciclotômica contida em S possui $\ell = mmc(i,d)/d$ elementos. Portanto, S possui $i/\ell = i/(mmc(i,d)/d) = mdc(i,d)$ $\mathbb{F}_d$-classes ciclotômicas. ■

A segunda maneira envolverá cálculos com produtos tensoriais. Por isso, precisamos do seguinte lema.

Lema 5.10. *Seja $\mathbb{F}$ um corpo tal que $Gal(\mathbb{F}(\theta), \mathbb{F})$ é cíclico. Para dois divisores i e j de n, sejam $\mathbb{F}_i$ e $\mathbb{F}_j$ corpos tais que $\mathbb{F} \subset \mathbb{F}_i, \mathbb{F}_j \subset \mathbb{F}(\theta)$ e $[\mathbb{F}_i, \mathbb{F}] = i$, $[\mathbb{F}_j, \mathbb{F}] = j$. Então*

$$\mathbb{F}_i \otimes_{\mathbb{F}} \mathbb{F}_j \simeq mdc(i,j)\mathbb{F}_\ell \tag{25}$$

onde ℓ denota o $mmc(i,j)$.

Demonstração: Sabemos que $\mathbb{F}_i$ é separável e de dimensão finita sobre $\mathbb{F}$. Então existe um $\alpha \in \mathbb{F}_i$ tal que $\mathbb{F}_i = \mathbb{F}(\alpha)$. Seja $p(x)$ o polinômio minimal de α sobre $\mathbb{F}$. então $\mathbb{F}_i \simeq \mathbb{F}[x]/(p(x))$. Assim

$$\mathbb{F}_i \otimes_{\mathbb{F}} \mathbb{F}_j \simeq \mathbb{F}[x]/(p(x)) \otimes_{\mathbb{F}} \mathbb{F}_j \simeq \mathbb{F}_j[x]/(p(x)) \tag{26}$$

Seja $p(x) = p_1(x) \cdots p_s(x)$, onde $p_i(x)$ são polinômios irredutíveis em $\mathbb{F}_j[X]$ e α_i é raíz de $p_i(x)$, $1 \leq i \leq s$. Então, pelo Teorema Chinês dos Restos, $\mathbb{F}_j[X]/(p(X)) \simeq \oplus_{k=1}^{s} \mathbb{F}_j[X]/(p_k(X))$, e assim

$$\mathbb{F}_i \otimes_{\mathbb{F}} \mathbb{F}_j \simeq \oplus_{k=1}^{s} \frac{\mathbb{F}_j[x]}{(p_k(x))} \simeq \oplus_{k=1}^{s} \mathbb{F}_j(\alpha_k). \tag{27}$$

Visto que a extensão $\mathbb{F}(\theta)/\mathbb{F}$ é cíclica e $\mathbb{F} \subset \mathbb{F}_i \subset \mathbb{F}(\theta)$, segue que $Gal(\mathbb{F}_i, \mathbb{F})$ é um subgrupo normal de $Gal(\mathbb{F}(\theta), \mathbb{F})$. Pelo Teorema Fundamental da Teoria de Galois, $\mathbb{F}_i/\mathbb{F}$ é uma extensão normal.

Ao ser $p(x)$ irredutível e separável em $\mathbb{F}[x]$, segue que este se decompõem em fatores lineares em $\mathbb{F}_i[X]$. Como $\alpha_1, \cdots, \alpha_s$ são raízes distintas de $p(x)$, temos que todas estas raízes pertencem a $\mathbb{F}_i$. Logo, $\mathbb{F}_i = \mathbb{F}(\alpha_k)$, $1 \leq k \leq s$.

Notamos que neste caso, $\mathbb{F}_j(\alpha_k) = \mathbb{F}_i\mathbb{F}_j$. Afirmamos que $\mathbb{F}_i\mathbb{F}_j = \mathbb{F}_\ell$, onde $\ell = mmc(i, j)$. De fato, pela Teoria de Galois temos que

$$Gal(\mathbb{F}(\theta), \mathbb{F}_i\mathbb{F}_j) = Gal(\mathbb{F}(\theta), \mathbb{F}_i) \cap Gal(\mathbb{F}(\theta), \mathbb{F}_j) =< \sigma^i > \cap < \sigma^j >=< \sigma^\ell > .$$

onde $\ell = mmc(i, j)$.

Mais uma vez, usando a Teoria de Galois, temos que $< \sigma^l >$ corresponde a um único corpo $\mathbb{F} \subset \mathbb{F}_l \subset \mathbb{F}(\theta)$ tal que $[\mathbb{F}_l : \mathbb{F}] = l$. Portanto, pela unicidade destes corpos intermediários, temos que $\mathbb{F}_i\mathbb{F}_j = \mathbb{F}_l$ e assim $\mathbb{F}_i \otimes_{\mathbb{F}} \mathbb{F}_j \simeq s\mathbb{F}_l$. Se contarmos as dimensões chegamos que $ij = sl$, ou seja, $s = ij/mmc(i, j) = mdc(i, j)$.

■

Já estamos prontos para cálcular o número de componentes simples de $\mathbb{F}_dG/J(\mathbb{F}_dG)$ usando o produto tensorial.

Proposição 5.11. *Com a notação acima, o número de componentes simples de* $\mathbb{F}_dG/J(\mathbb{F}_dG)$ *é* $\sum_{i|n} mdc(i, d)b_i$.

Demonstração: Pela proposição 2.10,

$$\mathcal{Z}\left(\frac{\mathbb{F}_d G}{J(\mathbb{F}_d G)}\right) \simeq \mathcal{Z}\left(\mathbb{F}_d \otimes_{\mathbb{F}} \frac{\mathbb{F}G}{J(\mathbb{F}G)}\right).$$

Pela proposição 2.12,

$$\mathcal{Z}\left(\mathbb{F}_d \otimes_{\mathbb{F}} \frac{\mathbb{F}G}{J(\mathbb{F}G)}\right) \simeq \mathbb{F}_d \otimes_{\mathbb{F}} \mathcal{Z}\left(\frac{\mathbb{F}G}{J(\mathbb{F}G)}\right)$$

Desde que $\mathbb{F}_d \otimes_{\mathbb{F}} \mathcal{Z}(\mathbb{F}G/J(\mathbb{F}G)) \simeq \oplus_{i|n} b_i \mathbb{F}_i$, obtemos o seguinte

$$\begin{aligned}\mathcal{Z}\left(\frac{\mathbb{F}_d G}{J(\mathbb{F}_d G)}\right) &\simeq \mathbb{F}_d \otimes_{\mathbb{F}} \left(\oplus_{i|n} b_i \mathbb{F}_i\right) \\ &\simeq \oplus_{i|n} b_i (\mathbb{F}_i \otimes_{\mathbb{F}} \mathbb{F}_d) \\ &\simeq \oplus_{i|n} b_i mdc(i,d) \mathbb{F}_{mmc(i,d)}\end{aligned}$$

onde usamos o lema 5.10 no último isomorfismo. Portanto, o número de componentes simples de $\mathcal{Z}(\mathbb{F}_d/J(\mathbb{F}_d G))$ é igual à $\sum_{i|n} mdc(i,d) b_i$.

■

A esta altura já podemos retornar ao nosso problema inicial, a saber, demonstrar o Teorema 5.7.

Na demonstração utilizaremos o seguinte.

Definição 5.12. *A função $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ definida por*

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n \text{ não é livre de quadrados} \\ (-1)^r & \text{se } \quad n = p_1 p_2 \cdots p_r \text{ é a fatoração em primos de } n \end{cases}$$

chama-se a ***função de Moebius****.*

Prova do Teorema 5.7 Para demonstrar o teorema basta mostrar que $a_i = b_i$, para todo i divisor de n.

Sabemos pelas proposições acima que $\sum_{i|n} mdc(i,d) a_i = \sum_{i|n} mdc(i,d) b_i$, para todo d divisor de n. Suponha $1 = d_1 < d_2 < \cdots < d_s = n$ os divisores de n. Assim, temos que

$$\begin{bmatrix} mdc(d_1,d_1) & mdc(d_2,d_1) & \cdots & mdc(d_s,d_1) \\ mdc(d_1,d_2) & mdc(d_2,d_2) & \cdots & mdc(d_s,d_2) \\ \vdots & \vdots & & \vdots \\ mdc(d_1,d_s) & mdc(d_2,d_s) & \cdots & mdc(d_s,d_s) \end{bmatrix} \begin{bmatrix} a_{d_1} - b_{d_1} \\ a_{d_2} - b_{d_2} \\ \vdots \\ a_{d_s} - b_{d_s} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Denotemos M a matriz acima, cujo coeficientes são os máximos divisores comuns dos divisores de n.

Se mostrarmos que M é invertível teremos mostrado o que queríamos. Para tanto, fixado um divisor j de n, considere a seguinte função aritmética

$$f_j(i) = \begin{cases} \varphi(i) & \text{se i divide j,} \\ 0 & \text{caso contrário.} \end{cases}$$

onde φ é a função de Euler. Pela definição de f_j, segue que

$$mdc(i,j) = \sum_{d|mdc(i,j)} \varphi(d) = \sum_{d|i} f_j(d).$$

Seja μ a função de Moebius. Se utilizarmos a fórmula de inversão de Moebius (Veja [NZM, Teorema 4.8]), chegamos que

$$f_j(i) = \sum_{d|i} \mu\left(\frac{i}{d}\right) mdc(d,j).$$

Podemos estender μ para os números racionais fazendo $\mu(q) = 0$ se $q \notin \mathbb{Z}$. Considere a seguinte matriz

$$\widetilde{M} = \begin{bmatrix} \mu(d_1/d_1) & \mu(d_1/d_2) & \cdots & \mu(d_1/d_s) \\ \mu(d_2/d_1) & \mu(d_2/d_2) & \cdots & \mu(d_2/d_s) \\ \vdots & \vdots & & \vdots \\ \mu(d_s/d_1) & \mu(d_s/d_2) & \cdots & \mu(d_s/d_s) \end{bmatrix}.$$

Nosso último passo é mostrar que $\widetilde{M}$ e $\widetilde{M}M$ são matrizes inversíveis, logo, M é também inversível.

Ao considerar $1 = d_1 < d_2 < \cdots < d_s = n$, temos que $\mu(d_j/d_k) = 0$ se $j < k$, ou seja, $\widetilde{M}$ é uma matriz triangular inferior. Todas as entradas da diagonal de $\widetilde{M}$ são iguais a 1, de modo que $\widetilde{M}$ é invertível. Agora, seja $\widetilde{M}M = [e_{jk}]$, onde $e_{jk} = \sum_{l=1}^{s} \mu(d_j/d_l) mdc(d_k, d_l)$. Dado que, todo d_l, $1 \leq l \leq s$, é divisor de n e $\mu(d_j/d_l) = 0$, se d_l não divide d_j, adquirimos a seguinte igualdade

$$e_{jk} = \sum_{d|n} \mu(d_j/d) mdc(d, d_k) = f_{d_k}(d_j). \tag{28}$$

Se $j > k$ então $d_j > d_k$. Desse modo, $f_{d_k}(d_j) = 0$, e pela igualdade acima, $e_{jk} = 0$ se $j > k$. Se $j = k$ então $e_{jk} = \varphi(d_j) \neq 0$. Assim sendo, a matriz $\widetilde{M}M$ é invertível, posto que é diagonal superior e a diagonal é constituida de entradas não nulas.

■

Nosso primeiro exemplo é no caso semisimples.

Exemplo. *No capítulo 3 consideramos um exemplo de como calcular o número de componentes de* $\mathbb{Q}A_4$*, onde* A_4 *é o grupo alternado de ordem* 12*. Ao considerar a apresentação*

$$A_4 =< a, b, c | a^2 = b^3 = c^3 = abc = 1 >,$$

vimos que as $\mathbb{Q}$*-classes ciclotômicas de* A_4 *são*

$$\begin{aligned} S_1 &= \{1\}, \\ S_2 &= \{\gamma_2\}, \\ S_3 &= \{\gamma_3, \gamma_4\}. \end{aligned}$$

onde $\gamma_1 = 1$*,* $\gamma_2 = a + cb + acb$*,* $\gamma_3 = b + cb^2 + ab + c^2$*,* $\gamma_4 = c + ac + b^2 + c^2b$*. Neste caso, temos duas* $\mathbb{Q}$*-classes ciclotômicas de cardinalidade* 1 *e outra de cardinalidade* 2*. Assim,*

$$\mathcal{Z}(\mathbb{Q}A_4) \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}\left(\frac{1 + i\sqrt{3}}{2}\right)$$

onde $\theta = (1 + i\sqrt{3})/2$ *é a raíz primitiva da unidade de ordem 6.*

Exemplo. *Seja* $\mathbb{F}_2$ *um corpo com dois elementos, e* $G = C_2 = \{1, x\}$ *um grupo com dois elementos. Apenas o elemento neutro de G possui ordem não divisível por* $2 = car(\mathbb{F}_2)$*. Logo, possui apenas uma* $\mathbb{F}$*-classe ciclotômica com apenas o elemento 1. Pelo que mostramos*

$$\mathcal{Z}\left(\frac{\mathbb{F}_2C_2}{J(\mathbb{F}_2C_2)}\right) \simeq \mathbb{F}_2.$$

5.4 EXTENSÕES CICLOTÔMICAS CÍCLICAS

Nesta seções vamos tratar das condições para que o grupo $Gal(\mathbb{F}(\theta) : \mathbb{F})$ seja cíclico. De início começamos com os corpos de característica positiva.

Proposição 5.13. *Se um corpo* $\mathbb{F}$ *possui característica* $p > 0$*, m é um número positivo tal que p não divide m e* θ *é uma raíz primitiva da unidade de ordem m. Então* $\mathbb{F}(\theta)$ *é uma extensão gailosiana de* $\mathbb{F}$ *e o grupo* $Gal(\mathbb{F}(\theta) : \mathbb{F})$ *é cíclico.*

Demonstração: Se $\mathbb{F}$ é um corpo finito então todas extensões finitas $\mathbb{K}$ são extensões de galoisianas de $\mathbb{F}$ e $Gal(\mathbb{F}(\theta) : \mathbb{F})$ é cíclico.

Se $\mathbb{F}$ é um corpo infinito de característica p então $\mathbb{F}_p$ é um subcorpo de $\mathbb{F}$ e $\mathbb{F}(\theta)$ é a composição de $\mathbb{F}$ e $\mathbb{F}_p(\theta)$. Portanto podemos concluir que $\mathbb{F}(\theta)$ é uma extensão finita gailosiana de $\mathbb{F}$ e que

$$Gal(\mathbb{F}(\theta) : \mathbb{F}) \simeq Gal(\mathbb{F}_p(\theta) : \mathbb{F} \cap \mathbb{F}_p(\theta))$$

por restrições.

Como $\mathbb{F} \cap \mathbb{F}_p(\theta)$ é um corpo finito, segue que $Gal(\mathbb{F}(\theta) : \mathbb{F})$ é cíclico. ∎

Em vista dessa proposição e do corolário 5.8, podemos determinar a estrutura do centro de $\mathbb{F}G$ sempre que $\mathbb{F}$ é um corpo de característica positiva e $\mathbb{F}G$ é semisimples, contanto que conheçamos as classes conjugadas de G.

No caso particular em que o corpo $\mathbb{F}$ é finito podemos reescrever o corolário 5.8.

Teorema 5.14. *Seja q uma potência de um número primo e G um grupo finito, com $mdc(q, |G|) = 1$. Se t é o número de componentes de $\mathbb{F}_qG$ e n_i é a cardinalidade de S_i, onde S_i, $1 \leq i \leq t$, são as $\mathbb{F}_q$-classes ciclotômicas. Então*

$$\mathcal{Z}(\mathbb{F}_qG) \simeq \oplus_{i=1}^{t} \mathbb{F}_{q^{n_i}}. \tag{29}$$

Em particular, se G é um grupo abeliano então

$$\mathbb{F}_qG \simeq \oplus_{i=1}^{t} \mathbb{F}_{q^{n_i}}. \tag{30}$$

O outro caso que vamos considerar é $\mathbb{F} = \mathbb{Q}$.

Neste caso, sabemos que $Gal(\mathbb{Q}(\theta) : \mathbb{Q})$ é isomorfo a $\mathcal{U}(\mathbb{Z}_m)$. Além disso, sabemos que $\mathcal{U}(\mathbb{Z}_m)$ é cíclico se e somente se $m = 1, 2, 4, p^n$ ou $2p^n$, onde p é um primo ímpar (Veja [JJ, Teorema 6.11]).

Assim, quando o expoente de G é igual a alguns destes números, podemos utilizar o método descrito para determinar a estrutura de $\mathcal{Z}(\mathbb{Q}G)$.

5.5 UM CONTRA EXEMPLO

Nesta seção mostraremos que o Teorema 5.7 não precisa valer se a hipótese de $Gal(\mathbb{F}(\theta) : \mathbb{F})$ ser cíclico não está verificada.

Seja G um grupo dado pela apresentação

$$< a, b, c | a^2 = b^8 = c^2 = 1, ab = ba, ac = ca, bc = acb^7 > .$$

Primeiro, note que

$$(ab^j)^8 = a^8(b^j)^8 = 1.$$

Como

$$b^j c = a^j c b^{7j},$$

e consequentemente,

$$\begin{aligned}(b^j c)^2 &= a^j c b^{7j} b^j c \\ &= a^j,\end{aligned}$$

temos que $(b^j c)^4 = 1$. Além disso,

$$(ab^j c)^4 = a^{4(1+j)}(b^j c)^4 = 1.$$

Assim, concluímos que todo elemento $g \in G$ satisfaz $g^8 = 1$. Como $b \in G$ tem ordem 8, segue que o expoente de G é igual à 8.

Seja θ uma raíz primitiva da unidade de ordem 8. O $Gal(\mathbb{Q}(\theta) : \mathbb{Q})$ é isomorfo à $\mathcal{U}(\mathbb{Z}_8)$, que por sua vez é isomorfo ao grupo de Klein de ordem 4, pois tem ordem 4 e todos os seus elementos possuem ordem 2.

Existem exatamente 14 classes de conjugação em G.

$$\begin{aligned}&\{1\}, \{a\}, \{b^4\}, \{ab^4\}, \{b, ab^7\}, \{b^2, b^6\}, \\ &\{b^3, ab^5\}, \{b^5, ab^3\}, \{b^7, ab\}, \{ab^2, ab^6\}, \\ &\{c, acb^6, cb^4, acb^2\}, \{ac, cb^6, acb^4, cb^2\}, \\ &\{cb, acb^7, cb^5, acb^3\}, \{acb, cb^7, acb^5, cb^3\}.\end{aligned}$$

As somas de classes são os seguintes elementos.

$$\begin{aligned}
&\gamma_1 = 1, \gamma_2 = a,\\
&\gamma_3 = b^4, \gamma_4 = ab^4,\\
&\gamma_5 = b + ab^7, \gamma_6 = b^2 + b^6,\\
&\gamma_7 = b^3 + ab^5, \gamma_8 = b^5 + ab^3,\\
&\gamma_9 = b^7 + ab, \gamma_{10} = ab^2, ab^6,\\
&\gamma_{11} = c + acb^6 + cb^4 + acb^2,\\
&\gamma_{12} = ac + cb^6 + acb^4 + cb^2,\\
&\gamma_{13} = cb + acb^7 + cb^5 + acb^3,\\
&\gamma_{14} = acb + cb^7, acb^5 + cb^3.
\end{aligned}$$

Então, se calcularmos as $\mathbb{Q}$-classes ciclotômicas de G obteremos:

- $\mathbb{Q}$-classes ciclotômicas de cardinalidade 1:

$$\begin{aligned}
S_1 = \{\gamma_1\}, S_2 = \{\gamma_2\},\\
S_3 = \{\gamma_3\}, S_4 = \{\gamma_4\},\\
S_5 = \{\gamma_6\}, S_6 = \{\gamma_{10}\},\\
S_7 = \{\gamma_{11}\}, S_8 = \{\gamma_{12}\}.
\end{aligned}$$

- $\mathbb{Q}$-classes ciclotômicas de cardinalidade 2:

$$S_9 = \{\gamma_{13}, \gamma_{14}\}.$$

- $\mathbb{Q}$-classes ciclotômicas de cardinalidade 4:

$$S_{10} = \{\gamma_5, \gamma_7, \gamma_8, \gamma_9\}.$$

Já que existem 10 $\mathbb{Q}$-classes ciclotômicas em G, a decomposição de Weddderburn de $\mathcal{Z}(\mathbb{Q}G)$ deve ter 10 componentes simples. Se o Teorema 5.7 fosse válido neste caso, teríamos 8 componentes simples de grau 1 sobre $\mathbb{Q}$, uma componente simples de grau 2 e uma componente simples de grau 4 sobre $\mathbb{Q}$. No entanto, $\mathbb{Q}G$ possui a seguinte decomposição de Wedderburn (Veja [Ver, pg. 195, Group Type 32/27]):

$$\mathbb{Q}G \simeq 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus 2M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\sqrt{2})) \oplus M_2(\mathbb{Q}(\sqrt{2}i))$$

e o centro de $\mathbb{Q}G$ é o seguinte

$$\mathcal{Z}(\mathbb{Q}G) \simeq 6\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{2}i),$$

ou seja, o centro de $\mathbb{Q}G$ possui 6 componentes simples de grau 1 e 4 componentes simples de grau 2 sobre $\mathbb{Q}$. Isto mostra que a hipótese de $Gal(\mathbb{K}(\theta) : \mathbb{K})$ ser cíclico, no Teorema 5.7, é imprescindível.

BIBLIOGRAFIA

[Ber] S. D. Berman; *The number of irreducible representations of a finite group over an arbitrary field,* Dokl. Akad. Nauk. 106 (1956),767-169 (em Russo).

[CR1] C. W. Curtis, I. Reiner ; *Representation Theory of Finite Groups and Associative Algebras,* Wiley classics, John Wiley and Sons, New York, 1988.

[CR2] C. W. Curtis, I. Reiner ; *Methods of Representation Theory of Finite Groups and Associative Algebras,,* Wiley classics, John Wiley and Sons, New York, 1988.

[Do] L. Dornhoff; *Group Representation Theory,* Parte A, Dekker, New York, 1971.

[RF1] R. A. Ferraz; *Simple components and central units in group algebras,* Journal of Algebra, 279 (2004), 191-203.

[RF2] R. A. Ferraz; *Simple components of the center of FG/J(FG),* Comm. Algebra, 36,9 (2008), 3191-3199.

[RF1] R. A. Ferraz; *Simple components and central units in group algebras,* Journal of Algebra, 279 (2004), 191-203.

[Fr] J. B. Frailegh; *A First Course in Abstract Algebra,* Addison Wesley, 7° edição, New York, 1985.

[Hi] G. Higman; *The Units of group rings,* Proc. London Math. Soc. 2,(46)(1940) 231-248.

[HK] K. Hoffman, R. Kunze; *Linear Algebra,*Prentice-Hall, 2 edição, 1971.

[NJ] N. Jacobson; *Basic Algebra I,* Dover , 2° edição, New York, 1985.

[JJ] G. A. Jones, J. M. Jones; *Elementary Number Theory,* Springer Undergraduate Mathematics Series, Springer-Verlag, London, 1998.

[KH] B. Külshammer; *Bemerkungen über die Gruppenalgebra als Symmetrische Algebra III,* (em Alemão) J. of Algebra, 88, (1984), 279-291.

[RH] R. Lidl, Harald Niederreiter; *Finite Fields,* Cambridge University Press, 2° edição, New York, 1997.

[NZM] I. Niven, Herbert S. Zuckerman, Hugh L. Montgomery; *An Introduction to the Theory of Numbers,* John Wiley and Sons, 5° edição, 1991.

[PS] C. Polcino Milies, S. K. Sehgal; *An introduction to group rings,* Algebras and Applications, Kluwer Academic Publishers, Dortrecht (2002).

[RS] J. Ritter, Sudarshan K Sehgal; *Integral Group Rings with Trivial Central Units,* Proc. Amer. Math. soc. 108 (2)(1990) 327-329.

[Ver] C.R.G. Vergara; *Wedderburn decomposition of small rational group algebras, in Group, rings and group rings: Lecture Notes in Pure and Applied Mathematics,* ed. A. Giambruno, C. Polcino Milies e S.K. Sehgal, Chapman and Hall C.R.Q., New York, **vol.248**, 2006, pg. 191-200.

[Witt] E. Witt; *Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlenkörper,* J. Reine Angew. Math 190 (1952),231-245.