# CARACTERIZAÇÃO DE GRUPOS FINITOS QUE POSSUEM UMA ÚNICA REPRESENTAÇÃO IRREDUTÍVEL DE GRAU MAIOR QUE 1

por

JOSIANE COSTA SILVA

IM-UFRJ

2006

# Caracterização de grupos finitos que possuem uma única representação irredutível de grau maior que 1

por

**Josiane Costa Silva**

Dissertação submetida ao Corpo Docente do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para a obtenção do grau de Mestre em Matemática.

Área de concentração : Álgebra

À Deus e à minha família.

# Agradecimentos


- Ao soberano Deus, por renovar-me a fé nele e a quem devo tudo o que tenho e sou;
- Aos que oraram e continuam orando por mim;
- Ao meu orientador, prof. Dr. Guilherme Augusto de La Rocque Leal, pela paciência e dedicação durante todo o tempo de desenvolvimento e execução deste trabalho;
- Aos colegas André Luiz e Roberto Ferraz, pela ajuda e contribuições ;
- A todos que em algum momento e de alguma forma me ajudaram.

# Resumo

Nesta dissertação temos por objetivo determinar todos os grupos finitos $G$ que possuem uma única $K$-representação irredutível de grau maior que 1, onde $K$ é um corpo algebricamente fechado de característica zero. Esse problema será tratado via os anéis de grupos $KG$, o que é possível dada bijeção existente entre $KG$-módulos livres de dimensão finita sobre $K$ e representações de $G$ sobre $K$.

# Abstract

In this thesis, we aim to determine all finite groups having only one $K$-representation of degree greater than one, where $K$ is an algebraically closed field of characteristic zero. This problem will be treated via the group ring $KG$, which is possible since there exists a bijection between free $KG$-modules of finite rank over $K$ and representations of $G$ over $K$.

# Sumário

# Introdução

Nesta dissertação , classificamos todos os grupos finitos que possuem exatamente uma $K$-representação irredutível de grau maior que um, onde $K$ é um corpo algebricamente fechado de característica zero. Com essa finalidade, Gary Seitz (ver [7]) provou o seguinte teorema, que constitui o principal resultado deste trabalho:

"Um grupo finito $G$ possui exatamente uma $K$-representação irredutível de grau maior que um se e somente se:

- $|G| = 2^k$, $k$ é ímpar, $Z(G) = G'$ e $|G'| = 2$;

ou

- $G$ é isomorfo ao grupo de todas as transformações $x \to ax + b$, $a \neq 0$, sobre um corpo de ordem $p^n \neq 2$."

Como exemplos desses grupos aparecem o grupo dihedral de ordem oito e o grupo dos quatérnios de ordem oito, sobre o corpo $C$ dos complexos.

Este trabalho está dividido em três capítulos. No capítulo 1 destacamos alguns conceitos da Teoria de grupos, importantes para o estudo dos capítulos posteriores, a saber: *sistema Sylow de grupo*, *normalizador de sistema de grupo*, entre outros.

No capítulo 2 encontramos resultados básicos da teoria de anéis de grupos. Nesse momento vemos como são obtidas as decomposições em soma direta das álgebras de grupos abelianos. Ainda no capítulo 2 encontramos o conceito de representações de grupos e alguns exemplos concretos. A importância desse conceito para esse trabalho reside na relação existente entre representações e módulos feita via anel de grupo, conforme visto na seção 2.6. Com isso, podemos entender o problema da irredutibilidade de uma representação analisando o seu módulo correspondente.

Por fim, no capítulo 3, estudamos dois lemas necessários para a verificação do teorema de Gary Seitz, cuja demonstração é o principal resultado deste trabalho e que consta nesse capítulo.

# Capítulo 1

# Preliminares

Abaixo descreveremos as propriedades de uma classe de subgrupos de grupos solúveis finitos, chamada *normalizadores de sistema*. Observe antes que grupos solúveis de ordem finita podem ser caracterizados como grupos cujos subgrupos de Sylow possuem complementos. Ver [2].

Portanto, se $G$ é um grupo solúvel finito de ordem $|G| = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, onde $p_i$ é primo e $n_i$ é inteiro positivo, $1 \leq i \leq r$; então, todo $p_i$-Sylow $S_{p_i}$ de $G$ admite um subgrupo complementar $S'_{p_i}$, denominado *$p_i$-complemento de Sylow* de $G$, isto é, $S'_{p_i} \cap S_{p_i} = \{1\}$ e $S'_{p_i} S_{p_i} = G$, $1 \leq i \leq r$. Consequentemente,

$$|S'_{p_i}| = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} \cdot p_{i+1}^{n_{i+1}} \cdots p_r^{n_r} \text{ e } [G : S'_{p_i}] = p_i^{n_i}.$$

Se

$$S'_{p_1}, S'_{p_2}, \cdots, S'_{p_r}$$

é um conjunto completo qualquer de complementos de Sylow de $G$ para cada um dos $r$ primos $p_i$, então, as $2^r$ interseções distintas que podem ser formadas entre os $S'_{p_i}$, $1 \leq i \leq r$, é chamada de um *sistema de Sylow* de $G$.

**Definição 1.1** *Um subgrupo $H$ de um grupo $G$ é dito um $S$-subgrupo de $G$ se e somente se $mdc(|H|, [G : H]) = 1$.*

Em particular, os membros de um sistema de Sylow de $G$ são todos $S$-subgrupos.

Além disso, um sistema de Sylow de $G$ contém um conjunto completo de subgrupos de Sylow

$$S_{p_1}, S_{p_2}, \cdots, S_{p_r},$$

onde $S_{p_i} = \cap_{j \neq i}\{S'_{p_j}\}$, $1 \leq i \leq r$.

**Definição 1.2** *Se $\wp$ é um sistema de Sylow de $G$ qualquer, então, o subgrupo de $G$*

$$N(\wp) = N = \{g \in G; g^{-1}Kg = K, \forall K \in \wp\}$$

*é dito um* normalizador de sistema *de $G$. Isto é, $N$ é a interseção dos normalizadores de elementos de $\wp$.*

Seja $G$ um grupo solúvel finito e seja

$$G = L_0 \geq L_1 \geq \cdots \geq L_i \geq L_{i+1} \geq \cdots \geq L_{n-1} \geq L_n = 1$$

a série nilpotente inferior de $G$, ou seja, $L_{i+1}$ é o menor subgrupo normal de $L_i$ com quociente $L_i/L_{i+1}$ nilpotente. O comprimento $n$ dessa série é chamado *comprimento nilpotente* de $G$.

**Teorema 1.1** *Seja $G$ um grupo solúvel de comprimento nilpotente 2 no qual $L_1$ é abeliano. Então os normalizadores de sistema de $G$ são complementares a $L_1$ e todo complemento de $L_1$ é um normalizador de sistema.*

Ao leitor interessado na demonstração desse teorema recomendamos [1], pág. 91

Nas definições e resultado que seguem, usaremos as seguintes notações :

- $\Omega$, conjunto finito de $n$ elementos arbitrários
- $\Delta$, subconjunto de $\Omega$
- $S^{\Omega}$, conjunto de todas as permutações de elementos de $\Omega$
- Se $G \subset S^{\Omega}$, $G$ será chamado de *grupo de permutações sobre* $\Omega$

- $\Delta^G = \{\delta^g; \delta \in \Delta, g \in G\}$, onde $\delta^g$ denota a imagem de $\delta \in \Delta$ pela permutação $g \in G$.

**Definição 1.3** *Seja $G$ um grupo de permutações de $\Omega$. Dizemos que $\Delta \subseteq \Omega$ é um* bloco fixo *de $G$ ou que é invariante por $G$, se $\Delta = \Delta^G$.*

Denotaremos por $G_\Delta$ o subgrupo de $G$ cujos elementos fixam $\Delta$. Se $\Delta$ consiste de um único ponto $\alpha$, escrevemos $G_\Delta = G_\alpha$. Note que todo grupo de permutação sobre $\Omega$ possui os blocos fixos triviais $\phi$ e $\Omega$. Com isso temos a seguinte

**Definição 1.4** *Se um grupo de permutações $G$ sobre $\Omega$ não possui blocos fixos não-triviais, então $G$ é chamado* transitivo. *Caso contrário, é dito* intransitivo.

**Definição 1.5** *Dizemos que um grupo permutação $G$ sobre $\Omega$ é* semiregular *se, para cada $\alpha \in \Omega$, $G_\alpha = 1$.*

**Definição 1.6** *Um grupo permutação $G$ sobre $\Omega$ é dito* regular *se é ao mesmo tempo semiregular e transitivo.*

**Proposição 1.1** *Todo grupo abeliano $G$ transitivo sobre $\Omega$ é regular e $G$ é seu próprio centralizador em $S^\Omega$.*

A demonstração dessa proposição pode ser encontrada em [7], pág. 9.

**Proposição 1.2** *Todas as órbitas de um grupo semiregular $G$ têm o mesmo comprimento $|G|$.*

Seja $G$ um grupo, não necessariamente finito e seja $H$ um subgrupo de $G$ de índice finito. Seja $\tau = \{t_1 = 1, t_2, \cdots, t_k\}$ um transversal de $H$ em $G$, isto é, $\tau$ é um conjunto completo de representantes das classes laterais à direita de $H$ em $G$. O grupo $G$ age sobre as classes laterais à direita de $H$ em $G$ da seguinte forma:

$$\pi : g \rightarrow \begin{pmatrix} Ht_1 & Ht_2 & \cdots & Ht_k \\ (Ht_1)g & (Ht_2)g & \cdots & (Ht_k)g \end{pmatrix},$$

para cada $g \in G$.

**Teorema 1.2** *A função $\pi : g \mapsto \pi_g$ definida acima, é um homomorfismo de $G$ em $S(G/H)$, o grupo das permutações de elementos de $G/H$. O kernel é o maior subgrupo normal de $G$ contido em $H$.*

**Demonstração** É de verificação imediata que $\pi$ é um homomorfismo. Seja $K = ker\pi$ e seja $N$ o maior subgrupo normal de $G$ contido em $H$. Primeiramente vejamos que $K \subseteq N$. Seja $g \in K$, isto é, $g \in G$ tal que $\pi_g = 1$. Então, $Hxg = Hx$, $\forall x \in G$. Equivalentemente, $x^{-1}Hxg = x^{-1}Hx$, ou ainda, $H^x g = H^x$, tal que $g \in \bigcap_{x\in G} H^x$.

Fixado $x \in G$, arbitrário, temos que $\forall y \in G$, $y^{-1}H^x y = H^{xy} \subset \bigcap_{x\in G} H^x$, ou seja, $\bigcap_{x\in G} H^x$ é subgrupo normal de $G$. Se $y \in \bigcap_{x\in G} H^x$, então $y \in H^x$, $\forall x \in G$. Em particular, $y \in H$. Segue-se daí que $\bigcap_{x\in G} H^x$ é um subgrupo normal de $G$ contido em $H$.

Agora, se $L$ é um subgrupo normal de $G$, arbitrário, tal que $L \subset H$, então $\forall y \in G$, $y^{-1}Ly \subset L \subset H \subset \bigcap_{x\in G} H^x$. Em particular, $L \subset \bigcap_{x\in G} H^x$. Portanto, $N = \bigcap_{x\in G} H^x$. Assim, se $g \in K$, temos que $g \in \bigcap_{x\in G} H^x = N$ e, portanto, $K \subseteq N$.

Para a inclusão inversa, tome $g \in N$. Então, $Hxg = H(xgx^{-1})x = Hx$, pois $xgx^{-1} \in N$, tal que $\pi_g = 1$ e $N \subseteq K$, o que completa a prova. □

**Definição 1.7** *Um subgrupo $Z^*$ de um grupo $G$ é dito o* hipercentro *de $G$ se $Z^*$ é o limite da série central superior de $G$:*

$$1 = Z_0 < Z_1 < \cdots,$$

*onde $Z_i$ é o único subgrupo de $G$ tal que $Z_i/Z_{i-1} = Z(G/Z_{i-1})$.*

Note que se $G$ é nilpotente, então o hipercentro de $G$ é o próprio $G$ e se $Z(G) = \{1\}$, então a série central superior de $G$ se reduz à série trivial $\{1\}$, cujo hipercentro é também trivial.

# Capítulo 2

# Anéis de Grupos

## 2.1 Resultados Básicos

Seja $G$ um grupo (não necessariamente finito) e $R$ um anel comutativo com unidade 1. Denotemos por $RG$ o conjunto de todas as combinações lineares formais da forma

$$\alpha = \sum_{g \in G} a_g g$$

onde $a_g \in R$ e $a_g = 0$ para quase todo $g$, isto é, apenas um número finito de coeficientes são diferentes de 0 em cada uma dessas somas.

Dado um elemento $\alpha = \sum_{g \in G} a_g g$, definimos o *suporte* de $\alpha$ como sendo o subconjunto de elementos de $G$ que aparecem, de fato, na expressão de $\alpha$ e denotamos por $sup(\alpha)$; isto é,

$$sup(\alpha) = \{g \in G : a_g \neq 0\}.$$

Dados dois elementos $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g \in RG$, temos que $\alpha = \beta$ se e somente se $a_g = b_g$, $\forall g \in G$.

Definimos a *soma* de dois elementos em $RG$ por:

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

e o *produto* por:

$$\alpha\beta = \sum_{g,h \in G} a_g b_h gh.$$

Podemos definir ainda um produto de elementos em $RG$ por elementos $\lambda \in R$ como:

$$\lambda\alpha = \lambda(\sum_{g\in G} a_g g) = \sum_{g\in G} (\lambda a_g)g.$$

É fácil verificar que $RG$, com esta última operação e a operação soma, torna-se um $R$-módulo.

**Definição 2.1** *O conjunto $RG$, com as operações soma e produto definidas acima, é chamado* **anel de grupo de $G$ sobre $R$.**

O grupo G pode ser identificado como um subconjunto de $RG$ através da função $i$: $G \to RG$ que atribui a cada elemento $x \in G$ o elemento $i(x) = \sum_{g\in G} a_g g$, onde $a_x = 1$ e $a_g = 0$ se $g \neq x$. Com essa identificação $G$ é uma base de $RG$ sobre $R$.

Definimos ainda a função $j : R \to RG$ dada por: $j(y) = \sum_{g\in G} a_g g$, onde $a_{1_G} = y$ e $a_g = 0$, se $g \neq 1_G$. É de verificação imediata que $j$ é um homomorfismo de anéis e, com isso, $R$ pode ser identificado como um subanel de $RG$.

Com as identificações acima, segue imediatamente que: $\forall r \in R$ e $\forall g \in G$, $rg = gr$ em $RG$. Se $R$ é comutativo, então $r\alpha = r(\sum_{g\in G} a_g g) = \sum_{g\in G} (ra_g)g = \sum_{g\in G} (a_g r)g = (\sum_{g\in G} a_g g)r = \alpha r$, de onde temos $R \subset Z(RG)$, o *centro* de $RG$.

**Definição 2.2** *O homomorfismo de anéis $\varepsilon : RG \to R$ dado por:*

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

*é chamado* **função de aumento** *de $RG$ e seu kernel, denotado por $\Delta(G)$, é chamado* **ideal de aumento** *de $RG$.*

**Proposição 2.1** *O conjunto $\{g - 1 : g \in G, g \neq 1\}$ é uma base de $\Delta(G)$ sobre $R$.*

**Demonstração** Seja $\alpha \in RG$ tal que $\alpha \in \Delta(G)$. Segue que $\varepsilon(\alpha) = \varepsilon(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g = 0$. Podemos escrever então $\alpha = \sum_{g\in G} a_g g - 0 = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g - 1)$, $\forall a_g \in R$ e $\forall g \in G$, o que mostra que $\{g - 1 : g \in G, g \neq 1\}$ é um conjunto gerador de $\Delta(G)$ sobre $R$.

Esse conjunto é também linearmente independente. Basta ver que, dada combinação linear nula $\sum_{g\in G}\lambda_g(g-1)=\sum_{g\neq 1}\lambda_g g-\sum_{g\in G}\lambda_g=0$, $\lambda_g\in R$, decorre do fato de $g$ pertencer a $G$ e $G$ ser uma base para $RG$ , que $\lambda_g=0$, $\forall g\in G$. □

Portanto, podemos escrever

$$\Delta(G)=\{\sum_{g\in G}a_g(g-1):g\in G, g\neq 1, a_g\in R\}$$

onde apenas um número finito de coeficientes $a_g$ são diferentes de 0.

Dado um grupo $G$ e um anel $R$, denotemos por $S(G)$ o *conjunto de todos os subgrupos de* $G$ e por $I(RG)$ o *conjunto de todos os ideais à esquerda de* $RG$.

**Definição 2.3** *Seja $H\in S(G)$. Denotemos por $\Delta_R(G,H)$ o ideal à esquerda de $RG$ gerado pelo conjunto $\{h-1:h\in H\}$; isto é,*

$$\Delta_R(G,H)=\{\sum_{h\in H}a_h(h-1):a_h\in RG\}.$$

A menos que se mencione o contrário o anel $R$ é fixo, o que nos permitirá usar a notação mais simples $\Delta(G,H)$ no lugar de $\Delta_R(G,H)$. Note que o ideal $\Delta(G,G)$ é o ideal $\Delta(G)$, *kernel* da função de aumento.

**Lema 2.1** *Seja $H\in S(G)$ e seja $S$ um conjunto de geradores de $H$. Então, o conjunto $\{s-1:s\in S\}$ é um conjunto de geradores de $\Delta(G,H)$ como um ideal à esquerda de $RG$.*

**Demonstração** Para todo $h\in H$, temos que $h=s_1s_2\cdots s_r$, onde $s_i\in S$, $1\leq i\leq r$. Definemos *comprimento de $h\in H$* como sendo o menor $t$ tal que $h$ é produto de $t$ elementos de $S$. Provaremos por indução sobre o comprimento de $h$, que $h-1$ pertence ao ideal de $RG$ gerado por $\{s-1:s\in S\}$ e mostramos assim o lema, visto que $\{h-1:h\in H\}$ é um gerador de $\Delta(G,H)$. De fato, para $t=1$, $h=s_1\Longleftrightarrow h-1=s_1-1$, tal que $s_1\in S$. Suponha que o resultado se verifique para $t=n$. Fazendo $t=n+1$, podemos escrever $h-1=s_1s_2\cdots s_{n+1}-1-s_1+s_1=s_1(s_2\cdots s_{n+1}-1)+s_1-1$. Da hipótese de indução temos que $s_2\cdots s_{n+1}-1$ está no ideal de $RG$ gerado por $\{s-1:s\in S\}$. Logo, $h-1$

também está. Portanto, para todo comprimento $t$ de $h \in H$, $h-1$ está no ideal gerado por $\{s-1 : s \in S\}$, de onde o resultado segue. □

Seja $\tau = \{q_i\}_{i\in I}$ um *transversal* de $H$ em $G$. Assuma em $\tau$ o elemento identidade de $G$ como representante da classe $H$. Temos que $\forall g \in G$, $g = q_i h_i$, onde $q_i \in \tau$ e $h_i \in H$. Enunciamos, com isso, a seguinte

**Proposição 2.2** *O conjunto* $B_H = \{q(h-1) : q \in \tau, h \in H, h \neq 1\}$ *é uma base de* $\Delta_R(G,H)$ *sobre* $R$.

**Demonstração** Mostraremos inicialmente que $B_H$ é linearmente independente. De fato, para uma combinação linear nula $\sum_{i,j} \lambda_{ij} q_i(h_j - 1) = 0$, $\lambda_{ij} \in R$, temos que: $\sum_{i,j} \lambda_{ij} q_i(h_j-1) = \sum_{i,j} \lambda_{ij} q_i h_j - \sum_{i,j} \lambda_{ij} q_i = 0$. Os elementos de $G$ que figuram nesta última equação são distintos. Com efeito, fixando-se $q_i$ e fazendo $h_j$ percorrer $H$, temos, por definição de $q_i$, que os elementos $q_i h_j$ pertencem a classes laterais distintas, e, portanto, são distintos. Como elementos de $G$ são l.i. sobre $R$, temos $\lambda_{ij} = 0$, $\forall i, j$.

$B_H$ é também gerador de $\Delta_R(G,H)$ sobre $R$. De fato, se $x \in \Delta_R(G,H)$, então $x$ se escreve como: $x = \sum_{h\in H} RG(h-1) = \sum_{h\in H} (\sum_{g\in G} a_g g)(h-1) = \sum_{h\in H} (\sum_{g\in G} a_g (g(h-1)))$. Assim, basta mostrar que $g(h-1)$ pode ser escrito como combinação linear dos elementos de $B_H$, $\forall g \in G$, $\forall h \in H$.

Se $g \in G$ então $g = q_i h_i$, $q_i \in \tau$, $h_i \in H$. Logo,

$$g(h-1) = q_i h_i (h-1) = q_i h_i h - q_i h_i - q_i + q_i = q_i(h_i h - 1) - q_i(h_i - 1),$$

de onde segue o resultado. □

Note que:

$$\begin{aligned} \Delta(G,G) &= < q(g-1); q \in \tau, g \in G, g \neq 1 > \\ &= < 1_G(g-1) = g-1; g \in G, g \neq 1 > \\ &= \Delta(G), \end{aligned}$$

como $R$-módulos e, portanto, fazendo $H = G$, a proposição 2.2 nos dá a proposição 2.1.

Daremos agora uma interpretação para $\Delta(G,H)$ quando $H$ é subgrupo normal de $G$. De fato, se $H \triangleleft G$, então o homomorfismo canônico $\omega : G \to G/H$ pode ser estendido a um epimorfismo $\omega^* : RG \to R(G/H)$ tal que:

$$\omega^*(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \omega(g)$$

**Proposição 2.3** *Com as notações acima, $ker(\omega^*) = \Delta(G,H)$.*

**Demonstração** Se $\alpha \in RG$, então $\alpha = \sum_{g\in G} a_g g = \sum_{i,j} a_{ij} q_i h_j$, $q_i \in \tau$, $h_j \in H$. Seja $\bar{q_i}$ a classe de $q_i$ em $G/H$. Então:

$$\omega^*(\alpha) = \omega^*(\sum_{i,j} a_{ij} q_i h_j) = \sum_{i,j} a_{ij}\overline{q_i h_j} = \sum_{i,j} a_{ij}\bar{q}_i.$$

Logo, $\alpha \in ker(\omega^*) \iff \sum_{i,j} a_{ij}\bar{q}_i = \sum_i (\sum_j a_{ij})\bar{q}_i = 0 \implies \sum_j a_{ij} = 0$, $\forall i$, pois $G/H$ é base de $R(G/H)$ sobre $R$, em particular, é l.i. sobre $R$. Portanto,

$$\alpha \in ker(\omega^*) \implies \alpha = \alpha - 0 = \sum_{i,j} a_{ij} q_i h_j - \sum_i (\sum_j a_{ij}) q_i = \sum_{i,j} a_{ij} q_i (h_j - 1) \in \Delta(G,H).$$

Temos assim $ker(\omega^*) \subset \Delta(G,H)$.

Agora, se $\alpha \in \Delta(G,H)$, então $\alpha = \sum_{i,j} \lambda_{ij} q_i (h_j - 1)$, $\lambda_{ij} \in R$, $q_i \in \tau$, $h_j \in H$. Logo,

$$\omega^*(\alpha) = \sum_{i,j} \lambda_{ij}\bar{q}_i\overline{(h_j - 1)} = \sum_{i,j} \lambda_{ij}\bar{q}_i(\bar{h_j} - \bar{1}) = \sum_{i,j} \lambda_{ij}\bar{q}_i 0 = 0,$$

o que implica $\alpha \in ker(\omega^*)$. Portanto, $\Delta(G,H) \subset ker(\omega^*)$. □

**Corolário 2.1** *Seja $H$ um subgrupo normal de um grupo $G$. Então, $\Delta(G,H)$ é um ideal bilateral de $RG$ e*

$$\frac{RG}{\Delta(G,H)} \simeq R(G/H).$$

**Demonstração** Como $\omega^*$ é um homomorfismo de anéis, segue diretamente da proposição 2.3 que, se $H \triangleleft G$, então $\Delta(G,H) = ker(\omega^*)$, que é um ideal bilateral de RG.

Agora, sendo $\omega^* : RG \to R(G/H)$ por definição um epimorfismo, o resultado desejado segue do teorema de homomorfismo de anéis . □

Como um caso particular, vemos que $\Delta(G)$ é o *kernel* do epimorfismo $\varepsilon$ induzido pela função trivial $G \to G/G = \{1\}$.

Temos construído até aqui função $\Delta : S(G) \to I(RG)$ que faz corresponder a subgrupos normais $H$ de $G$, ideais bilaterais $\Delta(G, H)$ de $RG$. Definiremos agora uma função $\nabla : I(RG) \to S(G)$ por:

$$\nabla(I) = \{g \in G : g - 1 \in I\}$$

para todo ideal $I \in I(RG)$.

$\nabla(I)$, assim definido, é subgrupo de $G$. Com efeito,

- $\forall g, h \in \nabla(I)$, $gh - 1 = gh - g + g - 1 = g(h-1) + g - 1 \in I$
- $\forall g \in \nabla(I)$, $g^{-1} - 1 = -1 + g^{-1} = -g^{-1}g + g^{-1} = -g^{-1}(g-1) \in I$.

Se $I$ é ideal bilateral de $RG$, então, $\forall x \in G$, $\forall g \in \nabla(I)$,

$$x^{-1}gx - 1 = x^{-1}gx - g + g - 1 = g(x^{-1}x - 1) + g - 1 = g - 1 \in I;$$

ou seja, $x^{-1}gx \in \nabla(I)$, $\forall x \in G, \forall g \in \nabla(I)$, e portanto, $\nabla(I)$ é subgrupo normal de $G$.

A relação entre as funções $\Delta$ e $\nabla$ é dada pela seguinte

**Proposição 2.4** *Se $H \in S(G)$, então $\nabla(\Delta(G, H)) = H$.*

**Demonstração** Seja $x \in \nabla(\Delta(G, H))$ e suponha que $x \notin H$. Temos então $x = qh$, onde $h \in H$, $q \in \tau$ e $q \neq 1$. Podemos assim escrever: $x - 1 = qh - 1 = qh - q + q - 1 = q(h-1) + q - 1 \iff q - 1 = (x-1) - q(h-1)$. Como $q(h-1) \in \Delta(G, H)$ e da hipótese sobre $x$, temos $x - 1 \in \Delta(G, H)$, ocorre que $q - 1$ dado na última equação pertence a $\Delta(G, H)$. Portanto, $q - 1 = \sum_{i,j} \lambda_{ij} q_i (h_j - 1) = \sum_{i,j} \lambda_{ij} q_i h_j - \sum_i (\sum_j \lambda_{ij}) q_i$, com $\lambda_{ij} \in R$. Segue dessa última igualdade que:

$$\sum_{i,j} \lambda_{ij} q_i h_j = 0 \quad e \quad \sum_i (\sum_j \lambda_{ij}) q_i = q - 1. \tag{2.1}$$

Da equação à esquerda em (2.1) e do fato de $G$ ser l.i. sobre $R$, temos que $\lambda_{ij} = 0$, $\forall i, j$, o que gera uma contradição pela equação em (2.1) à direita. Logo, $x \in H$ e, portanto, $\nabla(\Delta(G, H)) \subset H$.

A inclusão oposta segue trivialmente do fato de $h-1$ pertencer a $\Delta(G,H)$ e, portanto, a igualdade se verifica. □

Temos, contudo que $\Delta \circ \nabla \neq Id(RG)$, a função identidade em $RG$. Tome, por exemplo, $I = RG$. Ocorre que $\nabla(I) = \nabla(RG) = \{g \in G : g-1 \in RG\} = G$, para o qual temos $\Delta(\nabla(RG)) = \Delta(G, \nabla(RG)) = \Delta(G,G) = \Delta(G)$, que afirmamos ser diferente de $RG$. De fato, $1_G \in RG$ com a expressão $1_G = \sum_{g\in G} a_g g$, onde $a_{1_G} = 1$ e $a_g = 0$, $\forall g \neq 1_G$. Mas, $\varepsilon(1_G) = \varepsilon(\sum_{g\in G} a_g g) = \sum_{g\in G} g = a_{1_G} \neq 0$. Logo, $1_G \in RG$ é tal que $1_G \notin ker\varepsilon = \Delta(G)$, o que nos dá $\Delta(\nabla(RG)) \neq RG$.

## 2.2 Semisimplicidade

Determinaremos nesta seção condições necessárias e suficientes sobre $R$ e $G$ para que o anel de grupo $RG$ seja semisimples artiniano. Para esse fim, enunciaremos alguns conceitos e resultados relacionados a *anuladores*.

**Definição 2.4** *Seja $X$ um subconjunto de um anel de grupo $RG$. O* **anulador à esquerda** *de $X$ é o conjunto:*

$$Ann_e(X) = \{\alpha \in RG : \alpha x = 0, \forall x \in X\}.$$

*De maneira análoga, definimos o* anulador à direita *de $X$ por:*

$$Ann_d(X) = \{\alpha \in RG : x\alpha = 0, \forall x \in X\}.$$

**Definição 2.5** *Dado um anel de grupo $RG$ e um subconjunto finito $Y$ do grupo $G$, denotemos por $\hat{Y}$ o seguinte elemento de $RG$:*

$$\hat{Y} = \sum_{y\in Y} y$$

**Lema 2.2** *Seja $H$ um subgrupo de um grupo $G$ e seja $R$ um anel. Então:*

- *$Ann_d(\Delta(G,H)) \neq 0 \iff H$ é finito. Neste caso, temos: $Ann_d(\Delta(G,H)) = \hat{H} \cdot RG$.*

- *Se $H \triangleleft G$, então o elemento $\hat{H}$ é central em $RG$. Temos, neste caso: $Ann_d(\Delta(G,H)) = Ann_e(\Delta(G,H)) = RG \cdot \hat{H}$.*

**Demonstração** Suponha que $Ann_d(\Delta(G,H)) \neq 0$ e seja $\alpha = \sum_{g\in G} a_g g \neq 0$ um elemento em $Ann_d(\Delta(G,H))$. Então, $\forall h \in H$,

$$(h-1)\alpha = 0 \Longleftrightarrow \alpha = h\alpha \Longleftrightarrow \alpha = \sum_{g\in G} a_g g = \sum_{g\in G} a_g hg.$$

Se $g_0 \in sup(\alpha)$, então, a igualdade acima mostra que $hg_0 \in sup(\alpha)$, $\forall h \in H$; ou ainda, $Hg_0 \subset sup(\alpha)$. Visto que $sup(\alpha)$ é um conjunto finito e $|Hg_0| = |H|$ concluímos que $H$ deve ser finito.

Se $H$ é finito, digamos $H = \{h_1, h_2, ..., h_n\}$, então, $\forall h \in H$,

$$(h-1)(\sum_{i=1}^{n} h_i) = \sum_{i=1}^{n} hh_i - \sum_{i=1}^{n} h_i = \sum_{i=1}^{n} h_i - \sum_{i=1}^{n} h_i = 0.$$

Portanto, existe $\alpha \in RG$ não-nulo, por exemplo $\alpha = \sum_{i=1}^{n} h_i$, tal que $x\alpha = 0$, $\forall x \in \Delta(G,H)$, de onde segue que $Ann_d(\Delta(G,H)) \neq 0$.

Verifiquemos agora a igualdade $Ann_d(\Delta(G,H)) = \hat{H} \cdot RG$, supondo $H$ finito.

Se $\alpha = \sum_{g\in G} a_g g \in Ann_d(\Delta(G,H))$, então, de argumento anterior, temos $\alpha = \sum_{g\in G} a_g hg$, $\forall h \in H$. Logo, usando as notações acima, podemos escrever: $\alpha = \sum_{g\in G} a_g h_1 g$, $\alpha = \sum_{g\in G} a_g h_2 g$, $\cdots$, $\alpha = \sum_{g\in G} a_g h_n g$. Somando essas $n$ expressões de $\alpha$, obtemos:

$$n\alpha = \sum_{g\in G} a_g \hat{H} g = \hat{H}(\sum_{g\in G} a_g g) \Longleftrightarrow \alpha = [\hat{H}(\sum_{g\in G} a_g g)]/n = \hat{H}\beta,$$

onde $\beta = \alpha/n \in RG$. Temos assim uma inclusão.

Agora, $\forall \alpha \in RG$, $(h-1)\hat{H}\alpha = h\hat{H}\alpha - \hat{H}\alpha = \hat{H}\alpha - \hat{H}\alpha = 0$, o que implica que $\hat{H}\alpha \in Ann_d(\Delta(G,H))$, de onde segue a inclusão oposta.

Passemos ao item seguinte: Se $H \triangleleft G$, então, $\forall g \in G$, temos $g^{-1}Hg = H$. Logo, $g^{-1}\hat{H}g = \sum_{x\in H} g^{-1}xg = \sum_{y\in H} y = \hat{H}$ o que nos dá $\hat{H}g = g\hat{H}$, $\forall g \in G$; isto é, $\hat{H}$ central em $G$ e, portanto, $\hat{H} \cdot RG = RG \cdot \hat{H}$; ou seja, $\hat{H}$ central em $RG$.

Consequentemente temos $0 = (h-1)\hat{H}\alpha = (h-1)\beta\hat{H} = \hat{H}(h-1)\beta = \hat{H}\beta(h-1)$, de onde segue que $\hat{H}\alpha \in Ann_d(\Delta(G,H)) \Longleftrightarrow \hat{H}\beta \in Ann_e(\Delta(G,H))$, $\forall \alpha, \beta \in RG$ tal que $\hat{H}\alpha = \beta\hat{H}$. Portanto, $Ann_e(\Delta(G,H)) = Ann_d(\Delta(G,H)) = \hat{H} \cdot RG = RG \cdot \hat{H}$. □

**Corolário 2.2** *Seja $G$ um grupo finito. Então:*

- $Ann_e(\Delta(G)) = Ann_d(\Delta(G)) = R \cdot \hat{G}$
- $Ann_d(\Delta(G)) \bigcap \Delta(G) = \{a\hat{G}; a \in R, a|G| = 0\}$.

**Demonstração** Fazendo $H = G$ no lema anterior, obtemos $Ann_e(\Delta(G)) = Ann_d(\Delta(G)) = RG \cdot \hat{G} = R \cdot \hat{G}$. Verifiquemos essa última igualdade: $\forall\ \alpha = \sum_{g \in G} a_g g$ em $RG$,

$$\alpha \cdot \hat{G} = (\sum_{g \in G} a_g g) \cdot \hat{G} = \sum_{g \in G} a_g (g\hat{G}) = \sum_{g \in G} a_g \hat{G} = (\sum_{g \in G} a_g) \cdot \hat{G} = r \cdot \hat{G},$$

tal que $r = \sum_{g \in G} a_g \in R$.

Agora, tomando $\alpha$ em $Ann_d(\Delta(G)) = R \cdot \hat{G}$ e sabendo que $\Delta(G) = Ker(\varepsilon)$, escrevemos $\alpha = a \cdot \hat{G} \in \Delta(G) \iff 0 = \varepsilon(\alpha) = a \cdot \varepsilon(\hat{G}) = a|G|$, $a \in R$. □

Os resultados seguintes serão úteis na demonstração do próximo teorema.

**Lema 2.3** *Seja $I$ um ideal bilateral de um anel $R$. Suponha que exista um ideal à esquerda $J$ tal que $R = I \oplus J$ (como $R$-módulos). Então, $J \subset Ann_d(I)$.*

**Demonstração** Sejam $x \in J$ e $y \in I$. Como $J$ é ideal à esquerda e $I$ é ideal bilateral de R, temos que: $yx \in I \cap J = \{0\} \Longrightarrow yx = 0 \Longrightarrow x \in Ann_d(I)$ e, portanto, $J \subset Ann_d(I)$. □

**Lema 2.4** *Se o ideal de aumento $\Delta(G)$ é um somando direto de $RG$ como um $RG-$módulo, então $G$ é finito e $|G|$ é inversível em $R$.*

**Demonstração** Se $\Delta(G)$ é somando direto de $RG$, então, do lema acima, temos $Ann_d(\Delta(G)) \neq 0$. Do lema 2.2, segue que $G$ é finito e $Ann_d(\Delta(G)) = \hat{G} \cdot RG = \hat{G} \cdot R$.

Escreva $RG = \Delta(G) \oplus J$ e $1 = e_1 + e_2$, onde $e_1 \in \Delta(G)$ e $e_2 \in J$. Segue que $1 = \varepsilon(1) = \varepsilon(e_1) + \varepsilon(e_2)$. Como $e_1 \in \Delta(G) = ker(\varepsilon)$, a equação acima se reduz a $1 = \varepsilon(e_2)$, tal que $e_2 \in J$ e $J \subset Ann_d(\Delta(G))$, pelo lema 2.3. Logo, $e_2 = a \cdot \hat{G}$, para algum $a \in R$. Portanto, $1 = \varepsilon(e_2) = a\varepsilon(\hat{G}) = a|G|$, o que nos mostra que $|G|$ é inversível em $R$ e $|G|^{-1} = a$. □

Estamos agora prontos para enunciarmos o

**Teorema 2.1** *(de Maschke) Seja G um grupo. Então, o anel de grupo RG é semisimples artiniano se e somente se as seguintes condições são satisfeitas:*

- *R é um anel semisimples*
- *G é finito*
- $|G|$ *é inversível em R.*

**Demonstração** Suponha que $RG$ é semisimples. Então, o ideal $\Delta(G)$ e, consequentemente, o quociente $\frac{RG}{\Delta(G)}$ são semisimples, como $RG$-módulos. Do corolário 2.1 temos a expressão $\frac{RG}{\Delta(G)} \simeq R$, tomando $H = G$. Portanto, $R$ é semisimples. Além disso, como $RG$ é semisimples e artiniano, temos que $\Delta(G)$ é um somando direto de $RG$ como um $RG$-módulo. Segue então do lema 2.4, que $G$ é finito e $|G|$ é inversível em $R$.

Assuma agora que são verdadeiros os itens listados. Seja $M$ um $RG$-submódulo de $RG$. Se $R$ é semisimples, então $RG$ é semisimples como $R$-módulo. Logo, o conjunto constituído de todos os submódulos de $RG$ é um reticulado de complementares; isto é, para um dado submódulo $M$ existe um $R$-submódulo $N$ de $RG$ tal que $RG = M \oplus N$.

Seja $\pi : RG \to M$ a projeção canônica associada à soma direta acima. Para todo $x \in RG$, definamos a função

$$\pi^* : RG \to M$$

$$x \mapsto \frac{1}{|G|} \cdot \sum_{g \in G} g^{-1}\pi(gx).$$

Se provarmos que:

1. $\pi^*$ é $RG$-homomorfismo
2. $(\pi^*)^2 = \pi^*$
3. $Im(\pi^*) = M$

então, $ker(\pi^*)$ será um $RG$-submódulo tal que $RG = M \oplus ker(\pi^*)$ e o teorema estará provado.

1. Mostremos, inicialmente, que $\pi^*$ é um $R$-homomorfismo. De fato, $\forall r \in R, \forall x \in RG$

$$\begin{aligned} \pi^*(rx) &= \frac{1}{|G|} \cdot \sum_{g \in G} g^{-1}\pi(grx) = r(\frac{1}{|G|} \cdot \sum_{g \in G} g^{-1}\pi(gx)) \\ &= r\pi^*(x) \end{aligned}$$

e

$$\pi^*(x+y) = \pi^*(x) + \pi^*(y), \forall x, y \in RG,$$

que segue diretamente do fato: $\pi(m+n) = \pi(m) + \pi(n), \forall m \in M, \forall n \in N$.

Para provar que $\pi^*$ é um $RG$-homomorfismo, basta agora mostrar que $\pi^*(ax) = a\pi^*(x)$, $\forall x \in RG$ e $\forall a \in G$. Com efeito, $\forall \alpha = \sum_{g \in G} a_g g \in RG$,

$$\begin{aligned} \pi^*(\alpha x) &= \pi^*((\sum_{g \in G} a_g g)x) = \sum_{g \in G} a_g \pi^*(gx) \\ &= \sum_{g \in G} a_g g\pi^*(x) = (\sum_{g \in G} a_g g)\pi^*(x) \\ &= \alpha\pi^*(x). \end{aligned}$$

Assim, $\forall x \in RG$, $\forall a \in G$, temos:

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

Tomando $t = ga$ nessa última expressão e fazendo $g$ percorrer todos os elementos de $G$, temos que $t$ também varia sobre todos os elementos de $G$. Portanto,

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

2. Para todo $x \in RG$, $\pi^*(x) \in M$. Logo, $(\pi^*)^2(x) = \pi^*(\pi^*(x)) = \pi^*(x)$, $\forall x \in RG$ e, portanto, $\pi^*$ *é* uma projeção.

3. Dado $x \in RG$, temos que $\pi(gx) \in M$, $\forall g \in G$, pois $Im(\pi) = M$. Como $M$ é um $RG$-submódulo, ocorre que $g^{-1}\pi(gx) \in M$, $\forall g \in G$. Logo, $\forall x \in RG$, $\pi^*(x) = \frac{1}{|G|} \cdot \sum_{g \in G} g^{-1}\pi(gx) \in M$. Portanto, $Im\pi^* \subseteq M$.

Agora, se $m \in M$, então $\pi(m) = m$. Como $M$ é um $RG$-submódulo, temos que $gm \in M$, $\forall g \in G$, o que implica $\pi(gm) = gm$. Assim,

$$\begin{aligned} \pi^*(m) &= \frac{1}{|G|} \cdot \sum_{g \in G} g^{-1}\pi(gm) = \frac{1}{|G|} \cdot \sum_{g \in G} g^{-1}gm \\ &= \frac{1}{|G|} \cdot \sum_{g \in G} m = \frac{1}{|G|} \cdot |G| \cdot m \\ &= m. \end{aligned}$$

A igualdade acima mostra que $M \subseteq Im(\pi^*)$, o que verifica o teorema. □

O caso em que $R = K$ é um corpo é de particular importância, por exemplo, por sua implicação na teoria de representação de grupos. Como consequência do teorema acima temos o seguinte

**Corolário 2.3** *Seja $G$ um grupo finito e seja $K$ um corpo. Então, $KG$ é semisimples se e somente se $car(K)$ não divide $|G|$.*

**Demonstração** Segue diretamente da seguinte equivalência: $car(K)$ não divide $|G|$ se e somente se $|G|$ é inversível em $K$. De fato, se $KG$ é semisimples e de dimensão finita, então, do teorema de Maschke segue que $|G|$ é inversível em $K$ e, da equivalência acima, que $car(K)$ não divide $|G|$.

A recíproca é verificada diretamente do referido teorema, observando-se a equivalência acima, o fato de $G$ ser um grupo finito e $K$ um corpo, o que implica trivialmente a semisimplicidade de $K$, como $K$-módulo. □

O teorema seguinte nada mais é do que o teorema de Wedderburn-Artin aplicado a álgebras de grupos.

**Teorema 2.2** *Seja $G$ um grupo finito e seja $K$ um corpo tal que $car(K)$ não divide $|G|$. Então:*

- *$KG$ é uma soma direta de um número finito de ideais bilaterais $\{B_i\}_{1 \leq i \leq r}$, as componentes simples de $KG$. Cada $B_i$ é um anel simples.*

- *Qualquer ideal bilateral de KG é uma soma direta de alguns dos membros da família* $\{B_i\}_{1\leq i\leq r}$.

- *Cada componente simples* $B_i$ *é isomorfa a um anel de matrizes quadradas da forma* $M_{n_i}(D_i)$*, onde* $D_i$ *é um anel de divisão contendo uma cópia isomorfa de K no seu centro, e o isomorfismo*

$$KG \overset{\phi}{\simeq} \oplus_{i=1}^{r} M_{n_i}(D_i)$$

  *é um isomorfismo de K-álgebras.*

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

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

  *é um ideal minimal à esquerda.*

  *Dado* $x \in KG$*, consideremos* $\phi(x) = (\alpha_1, \alpha_2, \cdots, \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ *e defina o produto de x por um elemento* $m_i \in I_i$ *por* $xm_i = \alpha_i m_i$*. Com esta definição* $I_i$ *se torna um KG-módulo simples.*

- $I_i \not\simeq I_j$*, se* $i \neq j$.

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

Na seção seguinte, mostraremos as conexões entre o teorema de Wedderburn-Artin e a teoria de representação de grupos.

**Corolário 2.4** *Seja G um grupo finito e seja K um corpo algebricamente fechado tal que car(K) não divide* $|G|$*. Então:*

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(K)$$

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

**Demonstração** Como $car(K)$ não divide $|G|$, temos, do teorema de Wedderburn-Artin que:

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i),$$

onde $D_i$ é um anel de divisão contendo uma cópia de $K$ no seu centro.

Se calcularmos dimensões sobre $K$ em ambos os lados da equação acima, teremos

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

de onde segue que cada anel de divisão é de dimensão finita sobre $K$. Como $K$ é algebricamente fechado, temos que $D_i = K$, $1 \leq i \leq r$, de onde segue o resultado. □

## 2.3 Álgebras de grupos abelianos

Nesta seção daremos uma descrição completa do anel de grupo de um grupo abeliano finito $G$ sobre um corpo $K$ tal que $car(K)$ não divide $|G|$.

Iniciaremos com o caso onde $G$ é cíclico. Então, seja $G =< a : a^n = 1 >$; isto é, $G$ é cíclico finito de ordem $n$ e seja $K$ um corpo tal que $car(K)$ não divide $|G|$. Considere a função

$$\phi : K[X] \to KG$$

$$f(x) \mapsto f(a).$$

É de verificação imediata que $\phi$ é um homomorfismo de anéis. Agora, $\forall \alpha \in KG$; $\alpha = \sum_{a_i \in G} \alpha_{a^i} a^i$, tal que $\alpha_{a^i} \in K$, o que implica $\alpha = \sum_{a_i \in G} \alpha_{a^i} a^i = f(a)$, para algum polinômio $f(x) \in K[X]$. Logo, $\phi$ é um epimomorfismo. Temos assim $\dfrac{K[X]}{ker(\phi)} \simeq KG$.

Visto que $K[X]$ é um domínio de ideais principais, temos que $ker(\phi) =< f_0 >$; i.e., $ker(\phi)$ é o ideal gerado pelo polinômio $f_0$, tal que $f_0$ é o mônico, irredutível em $K[X]$, de menor grau não-nulo tal que $f_0(a) = 0$. Como $x^n - 1 \in ker(\phi)$, temos que $x^n - 1$ é

divisível por $f_0$, o que implica que $grau f_0 \leq n$. Suponha que $grau f_0 = r < n$. Então: $f_0(a) = c_0 + c_1 a + \cdots + c_r a^r = 0 \Rightarrow c_i = 0, \forall i \in \{0, \cdots, r\}$, pois $G$ é linearmente independente sobre $K$. Segue que $f_0 \equiv 0$ e, portanto, uma contradição .

Assim, temos que $f_0$ divide $x^n - 1$ e $grau f_0 = n$. Logo $f_0 = x^n - 1$. Portanto, $KG \simeq \dfrac{K[X]}{ker(\phi)} = \dfrac{K[X]}{< x^n - 1 >}$ .

Seja $x^n - 1 = f_1 f_2 \cdots f_t$ a decomposição de $x^n - 1$ como um produto de polinômios irredutíveis em $K[X]$. Visto que $car(K)$ não divide $|G| = n$, temos que $f_i \neq f_j$, se $i \neq j$. Do Teorema do Resto Chinês, obtemos:

$$\frac{K[X]}{< x^n - 1 >} \simeq \frac{K[X]}{< f_1 >} \oplus \frac{K[X]}{< f_2 >} \oplus \cdots \oplus \frac{K[X]}{< f_t >} \simeq KG.$$

Seja $\xi_i$ uma raiz de $f_i$, $1 \leq i \leq t$. Então, temos que $\dfrac{K[X]}{< f_i >} \simeq K(\xi_i)$. Consequentemente,

$$KG \simeq K(\xi_1) \oplus K(\xi_2) \oplus \cdots \oplus K(\xi_t),$$

onde $K(\xi_i)$ é uma *extensão ciclotômica* de $K$.

Mostramos, assim, que *$KG$ é isomorfo a uma soma direta de extensões ciclotômicas de $K$.*

Note que: o elemento $a$ corresponde à classe $X + < f_0 >$, sob o isomorfismo $KG \simeq \dfrac{K[X]}{ker(\phi)} = \dfrac{K[X]}{< f_0 >}$. Sob o isomorfismo $KG \simeq \dfrac{K[X]}{< f_1 >} \oplus \cdots \oplus \dfrac{K[X]}{< f_t >}$, $a$ corresponde ao elemento $(X + < f_1 >, \cdots, X + < f_t >)$ e, finalmente, $a$ é levado em $(\xi_1, \cdots, \xi_t)$ no último isomorfismo acima.

Vejamos alguns exemplos.

**Exemplo 2.1** Sejam $G =< a : a^7 = 1 >$ e $K = Q$, o corpo dos números racionais. A decomposição de $X^7 - 1$ em $Q[X]$ é

$$X^7 - 1 = (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1).$$

Se $\xi$ é uma raiz primitiva da unidade de ordem 7, então

$$QG \simeq Q \oplus Q(\xi).$$

□

**Exemplo 2.2** Sejam $G =< a : a^6 = 1 >$ e $K = Q$. A decomposição de $X^6 - 1$ como produto de polinômios irredutíveis em $Q[X]$ é

$$X^6 - 1 = (X - 1)(X + 1)(X^2 + X + 1)(X^2 - X + 1).$$

Temos que $\frac{-1+\sqrt{3}i}{2}$ é uma raiz de $X^2 + X + 1$ e $\frac{1+\sqrt{3}i}{2}$ uma raiz de $X^2 - X + 1$. Portanto,

$$QG \simeq Q \oplus Q \oplus Q(\tfrac{-1+\sqrt{3}i}{2}) \oplus Q(\tfrac{1+\sqrt{3}i}{2})$$

Notemos que os dois últimos somandos são, na verdade, iguais. □

Seja $G$ ainda um grupo cíclico de ordem $n$. Desejamos dar uma descrição mais precisa de $KG$, onde $K$ é um corpo tal que $car(K)$ não divide $|G|$. Relembremos, para isso, alguns conceitos importantes.

Para um inteiro positivo $d$, o *polinômio ciclotômico* de ordem $d$, denotado por $\Phi_d$, é o polinômio dado por $\Phi_d = \Pi_j(X - \xi_j)$, onde $\xi_j$ percorre todas as $d$-ésimas raízes primitivas da unidade. Além disso, temos que $X^n - 1 = \Pi_{d|n}\Phi_d$; isto é, $X^n - 1$ é o produto de todos os polinômios ciclotômicos $\Phi_d$ em $K[X]$, onde $d$ é um divisor de $n$. Para cada $d$, seja $\Phi_d = \Pi_{i=1}^{a_d} f_{d_i}$, a decomposição de $\Phi_d$ como um produto de polinômios irredutíveis em $K[X]$. Então, a decomposição de $KG$ pode ser escrita na forma:

$$KG \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} \frac{K[X]}{< f_{d_i} >} \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} K(\xi_{d_i}),$$

onde $\xi_{d_i}$ denota uma raiz de $f_{d_i}$, $1 \leq i \leq a_d$. Segue diretamente de comentário anterior.

Para um $d$ fixo, todos os elementos $\xi_{d_i}$ são raízes primitivas da unidade de ordem $d$, visto que uma raiz de $f_{d_i}$ é uma raiz de $\Phi_d(X)$, o $d$-ésimo ciclotômico sobre $K$. Portanto, $K(\xi_{d_i}) = K(\xi_{d_j}) = K(\xi_d)$, $\forall 1 \leq i, j \leq a_d$. Podemos assim reescrever o isomorfismo acima como

$$KG \simeq \oplus_{d|n} a_d K(\xi_d)$$

onde $\xi_d$ é uma raiz primitiva da unidade de ordem $d$ e $a_d K(\xi_d)$ é uma notação para o somatório $K(\xi_d) \oplus \cdots \oplus K(\xi_d)$, com $a_d$ termos $K(\xi_d)$.

Além disso, temos que $grau(f_{d_i}) = [K(\xi_d) : K]$, para todo polinômio $f_{d_i}$, $1 \leq i \leq a_d$; isto é, os polinômios $f_{d_i}$ possuem o mesmo grau, $1 \leq i \leq a_d$. Segue, portanto, da decomposição de $\Phi_d(X)$ que

$$grau\Phi_d(X) = \phi(d) = \sum_{i=1}^{a_d} grau(f_{d_i}) = \sum_{i=1}^{a_d} [K(\xi_d) : K] = a_d[K(\xi_d) : K],$$

onde $\phi(d)$ é a função de Euler dada por:

$$\phi(d) = \#\{n \in Z : 1 \leq n < d \ , \ mdc(n, d) = 1\}.$$

Como $G$ é um grupo cíclico de ordem $n$, para cada divisor $d$ de $n$, o número de elementos de ordem $d$ em $G$ é $n_d = \phi(d)$. Equivalentemente, se $H$ é um grupo cíclico de ordem $d$ em $G$, então $H$ tem $\phi(d)$ geradores. Com efeito, basta verificarmos os itens 1 e 2 que seguem abaixo.

1. Se $s < d$ e $mdc(s, d) = 1$, então, $h^s$ é um gerador de $H$, para um gerador $h$ de $H$.

   De fato, se $\tilde{H} =< h^s >$ e $|\tilde{H}| = p$, então $p$ divide $d = |H|$. Por outro lado, $(h^s)^p = h^{sp} = 1$ e como $| < h > | = |H| = d$, temos que $d|sp$. Mas $mdc(s, d) = 1$. Logo, $d$ divide $p$. Portanto, $d = p$, de onde concluímos que $H = \tilde{H}$ e que $h^s$ também é um gerador de $H$, para todo inteiro $s$ tal que $mdc(s, d) = 1$.

2. Se $h^s$, $s < d$, é um gerador de $H$, então $mdc(s, d) = 1$.

   Suponhamos que $mdc(s, d) \neq 1$. Então, existe $p > 1$ tal que $s = pq_1$ e $d = pq_2$, onde $q_1$, $q_2$ são inteiros diferentes de 1. Segue que, $(h^s)^{q_2} = h^{pq_1q_2} = h^{(pq_2)q_1} = (h^d)^{q_1} = 1 \iff (h^s)^{q_2} = 1$, o que é uma contradição , visto que $| < h^s > | = d > q_2 > 0$. Portanto, $mdc(s, d) = 1$ sempre que $h^s$, $s < d$, for um gerador de $H$.

Posto isto, podemos escrever: $\phi(d) = n_d = a_d[K(\xi_d) : K]$ se e somente se

$$a_d = \frac{n_d}{[K(\xi_d) : K]}.$$

**Exemplo 2.3** Seja $G =< a : a^n = 1 >$ um grupo cíclico de ordem $n$ e seja $K = Q$, o corpo dos números racionais. Visto que $X^n - 1 = \prod_{d|n} \Phi_d(x)$, onde $\Phi_d(x)$ é irredutível sobre $Q$, para cada $d$ que divide $n$, podemos escrever

$$Q < a > \simeq \oplus_{d|n} Q(\xi_d),$$

onde $\xi_d$ é uma raiz de $\Phi_d(x)$. □

A descrição obtida acima pode ser estendida a anéis de grupos abelianos finitos arbitrários, como nos mostra o seguinte

**Teorema 2.3** *(Perlis-Walker) Seja $G$ um grupo abeliano finito, de ordem $n$, e seja $K$ um corpo tal que car(K) não divide n. Então:*

$$KG \simeq \oplus_{d|n} a_d K(\xi_d)$$

*onde $\xi_d$ denota uma d-ésima raiz primitiva da unidade e $a_d = \frac{n_d}{[K(\xi_d : K)]}$. Nesta fórmula, $n_d$ denota o número de elementos de ordem d em G.*

A demonstração desse teorema pode ser encontrada em [5], pág. 147.

## 2.4 Algumas subálgebras comutativas

Trataremos nesta seção de alguns resultados e conceitos importantes na determinação da estrutura de uma álgebra de grupo que é semisimples.

**Definição 2.6** *Seja $G$ um grupo e $R$ um anel comutativo e seja $\{C_i\}_{i\in I}$, o conjunto das classes de conjugação de $G$ que contém apenas um número finito de elementos. Definamos em $RG$, $\forall i \in I$,*

$$\gamma_i = \hat{C}_i = \sum_{x\in C_i} x.$$

*Estes elementos são chamados* somas de classe *de $G$ sobre $R$.*

**Teorema 2.4** *Seja $G$ um grupo e $R$ um anel comutativo. Então $\{\gamma_i\}_{i\in I}$, o conjunto de todas as somas de classe, forma uma $R$-base de $Z(RG)$, o centro de $RG$.*

**Demonstração** Vejamos inicialmente que $\forall i \in I$, $\gamma_i \in Z(RG)$; isto é, $\gamma_i g = g\gamma_i$, $\forall g \in I$. De fato, $\forall g \in G$, temos que: $g^{-1}\gamma_i g = g^{-1}(\sum_{x\in C_i} x)g = \sum_{x\in C_i} g^{-1}xg = \sum_{y\in C_i} y = \gamma_i$.

O conjunto $\{\gamma_i\}_{i\in I}$ é um gerador de $Z(RG)$ como $RG$-módulo. Com efeito, tome $\alpha = \sum_{g\in G} \alpha_g g \in Z(RG)$. Sejam $a, b \in G$, tais que $a$ e $b$ pertencem a mesma classe de conjugação , isto é, $b = x^{-1}ax$, para algum $x \in G$. Então

$$\alpha = x^{-1}\alpha x \iff \alpha_a a + \sum_{g\neq a} \alpha_g g = \alpha_a(x^{-1}ax) + \sum_{g\neq a} \alpha_g(x^{-1}gx) = \alpha_a b + \sum_{g\neq a} \alpha_g(x^{-1}gx).$$

Da igualdade acima, temos que $\alpha_a = \alpha_b$. Denotando esses coeficientes comuns por $a_i$, podemos escrever

$$\sum_{i\in I} a_i \bar{g}_i = \sum_{i\in I} a_i(g_i + x^{-1}g_i x + \cdots) = \sum_{i\in I} a_i \gamma_i,$$

tal que $\gamma_i = \sum_{h\in C_i} h$ e $C_i = \bar{g}_i$, $\forall g_i \in G$. Logo, $\{\gamma_i\}_{i\in I}$ gera $Z(RG)$, como $R$-módulo.

Além disso, $\{\gamma_i\}_{i\in I}$ é linearmente independente. Basta ver que, dada combinação linear nula $\sum_i \lambda_i\gamma_i = 0$, $\lambda_i \in R$,

$$0 = \sum_i \lambda_i\gamma_i = \sum_i \lambda_i(\sum_{x\in C_i} x) = \sum_i \sum_{x\in C_i} \lambda_i x \Longrightarrow \lambda_i = 0, \forall i \in I,$$

pois as classes $C_i$ são disjuntas e elementos de $G$ são l.i. sobre $R$. Portanto, $\{\gamma_i\}_{i\in I}$ é uma $R$-base de $Z(RG)$. □

**Proposição 2.5** *Seja $G$ um grupo finito e $K$ um corpo algebricamente fechado tal que $car(K)$ não divide $|G|$. Então, o número de componentes simples de $KG$ é igual ao número de classes de conjugação de $G$.*

**Demonstração** Pelo teorema 2.3, é suficiente mostrar que o número de componentes simples de $KG$ é igual a $dim_K Z(KG)$. Segue do teorema 2.2 que

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(K)$$

de onde obtemos $Z(KG) \simeq \oplus_{i=1}^{r} Z(M_{n_i}(K))$. Para um anel de matrizes $M_n(K)$, temos que

$$Z(M_n(K)) = \{\alpha I; \alpha \in K\} \simeq K,$$

onde $I$ é a matriz identidade de ordem $n$. De fato, a igualdade pode ser verificada tomando-se $A \in Z(M_n(K))$ e fazendo-se o produto $A\varepsilon_{ij}$, $i = j$, onde $\varepsilon_{ij}$ é a matriz de ordem $n$ que tem 1 na posição $ij$ e 0 nas demais.

Portanto, $Z(KG) \simeq \oplus_{i=1}^{r} Z(M_{n_i}(K)) \simeq K \oplus \cdots \oplus K$, onde $K$ aparece $r$ vezes nesse somatório. Segue daí que $dim_K Z(KG) = r$, que é o número de componentes simples de $KG$. □

**Definição 2.7** *Chamamos um corpo $K$ de* corpo de decomposição *para um grupo finito $G$ se a álgebra de grupo $KG$ é isomorfa a uma soma direta de anéis de matrizes sobre $K$.*

Note que corpos algebricamente fechados são corpos de decomposição para qualquer grupo finito $G$.

Notemos que, se $e$ é um idempotente central em um anel $R$, então ele induz uma decomposição de $R$ como uma soma direta: $R = Re \oplus R(1-e)$. De fato, $\forall r \in R$, $r = re + r(1-e)$ e se $x \in Re \cap R(1-e)$, então $x = re = r'(1-e)$, tal que $r, r' \in R$; de onde temos $x = re = re^2 = r'(1-e)e = r'e - r'e^2 = 0$.

**Lema 2.5** *Seja $R$ um anel com unidade e seja $H$ um subgrupo de um grupo $G$. Se $|H|$ é inversível em $R$, então $e_H = \frac{1}{|H|}\ \hat{H}$ é um idempotente de $RG$. Além disso, se $H \triangleleft G$, então $e_H$ é central em $RG$.*

**Demonstração** Se $|H|$ é inversível, então podemos definir $e_H = \frac{1}{|H|}\hat{H}$. Vejamos que $e_H$ é idempotente:

$$\begin{aligned} e_H^2 &= e_H e_H = \frac{1}{|H|^2}\hat{H}\hat{H} = \frac{1}{|H|^2}(\sum_{h\in H} h)\hat{H} \\ &= \frac{1}{|H|^2}\sum_{h\in H} h\hat{H} = \frac{1}{|H|^2}\sum_{h\in H}\hat{H} \\ &= \frac{1}{|H|^2}|H|\hat{H} = \frac{1}{|H|}\hat{H} \\ &= e_H. \end{aligned}$$

Do lema 2.2, temos que se $H \triangleleft G$, então $RG\hat{H} = \hat{H}RG$. Logo, $e_H$ é central em $RG$. □

O próximo resultado nos mostra como é a decomposição obtida com esses idempotentes.

**Proposição 2.6** *Seja $R$ um anel e seja $H$ um subgrupo normal de um grupo $G$. Se $|H|$ é inversível em $R$, então $e_H = \frac{1}{|H|}\hat{H}$ induz em $RG$ a decomposição*

$$RG = RGe_H \oplus RG(1-e_H),$$

*onde* $RGe_H \simeq R(G/H)$ *e* $RG(1-e_H) = \Delta(G,H)$.

**Demonstração** Do lema 2.5 segue que $e_H$ é central em $RG$. Logo,

$$RG = RGe_H \oplus RG(1-e_H).$$

Seja $\phi : G \to Ge_H$ a função definida por $\phi(g) = ge_H$, $\forall g \in G$.

$\vdash$: $\phi$ é isomorfismo de grupos. Com efeito, $\phi(gg') = (gg')e_H = (gg')e_H^2 = (ge_H)(g'e_H) = \phi(g)\phi(g')$. Logo, $\phi$ é homomorfismo. Agora, $\phi$ é injetivo, pois $\phi(g) = e_H \iff ge_H = g\frac{1}{|H|}\hat{H} = \frac{1}{|H|}\hat{H} \iff g\hat{H} = \hat{H} \iff g \in H$, tal que $e_H$ é a identidade de $Ge_H$; e é de verificação imediata que $\phi$ é sobrejetivo.

Do teorema de homomorfismo de grupos, obtemos $G/H \simeq Ge_H$. Como $Ge_H$ é base de $RGe_H$ sobre $R$, temos que $RGe_H \simeq R(G/H)$.

$\vdash$: $RGe_H$ é um ideal bilateral de $RG$. De fato,

- $\forall a_1, a_2 \in RG$, $a_1e_H + a_2e_H = (a_1+a_2)e_H \in RGe_H$;
- $\forall a, a_1 \in RG$, $a(a_1e_H) = (aa_1)e_H \in RGe_H$ e $(a_1e_H)a = (e_Ha_1)a = e_H(a_1a) = (a_1a)e_H \in RGe_H$.

$\vdash$: $RG(1-e_H)$ é um ideal à esquerda de $RG$. De fato,

- $\forall a_1, a_2 \in RG$, $a_1(1-e_H) + a_2(1-e_H) = (a_1+a_2)(1-e_H) \in RGe_H$;
- $\forall a, a_1 \in RG$, $a(a_1(1-e_H)) = (aa_1)(1-e_H) \in RG(1-e_H)$

Segue dessas afirmações e do lema 2.3 que $RG(1-e_H) = Ann(RGe_H)$, e por argumento análogo ao do lema 2.2, mostramos facilmente que $Ann(RGe_H) = \Delta(G,H)$. □

**Definição 2.8** *Seja $R$ um anel e $G$ um grupo finito tal que $|G|$ é inversível em $R$. O idempotente $e_G = \frac{1}{|G|}\hat{G}$ é chamado* idempotente principal *de $RG$.*

**Corolário 2.5** *Seja $R$ um anel e seja $G$ um grupo finito tal que $|G|$ é inversível em $R$. Então podemos escrever $RG$ como:*

$$RG \simeq R \oplus \Delta(G).$$

**Demonstração** Da proposição 2.6, temos que $RG \simeq RGe_G \oplus RG(1 - e_G)$, tal que $e_G = \frac{1}{|G|}\hat{G}$, $RGe_G \simeq R(G/G) = R$ e $RG(1 - e_G) = \Delta(G, G) = \Delta(G)$. Portanto, $RG \simeq R \oplus \Delta(G)$. □

**Lema 2.6** *Seja $R$ um anel comutativo e seja $I$ um ideal de uma álgebra de grupo $RG$. Então: $RG/I$ é comutativo se e somente se $\Delta(G, G') \subset I$, onde $G'$ é o subgrupo comutador de $G$.*

**Demonstração** Tome $G' =< [g, h]; g, h \in G >$, o subgrupo comutador de $G$. Desejamos mostrar que $\forall g, h \in G$, $g^{-1}h^{-1}gh - 1 \in I$ e, com isso, mostrar que $\Delta(G, G') \subset I$, como ideal de $RG$. De fato, $\forall g, h \in G$, $gh - hg \in I$. Logo,

$$gh - hg = (hg)(hg)^{-1}gh - hg = hg(g^{-1}h^{-1})gh - hg = hg(g^{-1}h^{-1}gh - 1) \in I.$$

Como $I$ é ideal de $RG$, temos que $(hg)^{-1}(gh - hg) = g^{-1}h^{-1}gh - 1 \in I$.

Agora, $gh - hg = hg(g^{-1}h^{-1}gh - 1) \in \Delta(G, G')$. Se $\Delta(G, G') \subset I$, então:

$$\forall g, h \in G,\ gh - hg = i,\ i \in I \iff gh \equiv hg(mod I)$$

e, portanto, $RG/I$ é comutativo. □

**Proposição 2.7** *Seja $RG$ uma álgebra de grupo semisimples. Se $G'$ denota o subgrupo comutador de $G$, então podemos escrever:*

$$RG = RGe_{G'} \oplus \Delta(G, G'),$$

*onde $RGe_{G'} \simeq R(G/G')$ é a soma de todas as componentes simples comutativas de $RG$ e $\Delta(G, G')$ é a soma das demais.*

**Demonstração** Da proposição 2.6 segue a soma direta desejada. Basta observar que $G' \triangleleft G$ e que as hipóteses $G$ finito e $|G|$ inversível em $R$ (RG é semisimples) implicam $G'$ finito e $|G'|$ inversível em $R$, pois $|G| = k|G'|, k \in R \iff 1 = (|G|^{-1}k)|G'|$.

Note que $RGe_{G'} \simeq R(G/G')$ é semisimples, pois $R$ é semisimples, $G/G'$ é um grupo finito e $|G/G'|$ é inversível em $R$. Além disso, $R(G/G')$ é comutativo, pois $G/G'$ é

abeliano. Logo, $RGe_{G'} \simeq R(G/G')$ é soma direta de componentes simples comutativas de $RG$.

Agora, suponha que $\Delta(G, G') = A \oplus B$, onde $A$ é componente simples comutativa e $B$ seu complemento. Então, o quociente $RG/B \simeq RGe_{G'} \oplus A$ é comutativo. Logo, pelo lema anterior $\Delta(G, G') \subset B$, o que implica em $A = \{0\}$. Portanto, $\Delta(G, G')$ é a soma das componentes simples não-comutativas de $RG$. □

## 2.5 Representação de grupos

**Definição 2.9** *Seja $G$ um grupo, $R$ um anel comutativo e $V$ um $R$-módulo de dimensão finita. Uma* **representação de $G$ sobre $R$,** *com espaço de representação $V$ é um homomorfismo de grupos $T : G \to GL(V)$, onde $GL(V)$ é o grupo de $R$-automorfismos de $V$. A dimensão de $V$ é chamada grau da representação $T$ e será denotada por $gr(T)$.*

Fixada uma base de $V$ sobre $R$, podemos definir um isomorfismo $\phi$ de $GL(V)$ sobre o grupo $GL(n, R)$ de matrizes $n \times n$ inversíveis com coeficientes em $R$, associando a cada $T \in GL(V)$ sua matriz com respeito à base escolhida.

**Definição 2.10** *Seja $G$ um grupo e $R$ um anel comutativo. Uma* **representação matricial de grau n** *de $G$ sobre $R$ é um homomorfismo de grupos $T : G \to GL(n, R)$.*

**Exemplo 2.4** Seja $G$ um grupo e $R$ um anel comutativo. A aplicação $T : G \to GL(n, R)$ dada por $T(g) = I_n$, $\forall g$, onde $I_n$ é a matriz identidade de $GL(n, R)$, é chamada *representação trivial* de $G$ sobre $R$ de grau $n$. □

**Exemplo 2.5 A representação regular**

Seja $G$ um grupo finito de ordem $n$ e seja $R$ um anel comutativo. Definiremos uma representação de $G$ sobre $R$. Tomaremos como um espaço de representação $RG$, o anel de grupo de $G$ sobre $R$.

Definamos uma aplicação $T : G \to GL(RG)$ como segue: a cada elemento $g \in G$, associamos a função linear $T_g$ que age na base $G$ por multiplicação à esquerda; isto é, $T_g(g_i) = gg_i$. De fato, esta é uma representação de $G$, pois

$$T_{gh}(y) = (gh)y = g(hy) = T_g(T_h(y)) = (T_g \circ T_h)(y).$$

Enumeremos os elementos de $G$ em uma ordem $G = \{g_1 = 1, \cdots, g_n\}$. Logo, na representação matricial correspondente, com respeito a base $G$ de $RG$, a imagem de cada elemento $g \in G$ é uma matriz de permutação pois, $\forall g \in G$, $T_g$ age na base $G$ permutando os seus elementos. Em particular, para $g \neq 1$, $gg_i \neq g_i \iff T_g(g_i) \neq g_i$. Então, todos os elementos na diagonal de $T_g$ são iguais a zero, o que nos dá *traço* $T_g$ =0 se $g \neq 1$ e *traço* $T_1 = n = |G|$.

A representação assim definida é chamada *a representação regular de G sobre R.*

Como ilustração verificaremos esta representação para o grupo de Klein, isto é, o grupo $G = \{1, a, b, ab\}$, com três elementos de ordem 2, que enumeramos como $g_1 = 1$, $g_2 = a$, $g_3 = b$, $g_4 = ab$. Temos então: $T_a(g_1) = g_2$, $T_a(g_2) = g_1$, $T_a(g_3) = g_4$, $T_a(g_4) = g_3$, cuja matriz associada é:

$$\rho_a = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

De maneira análoga, obtemos :

$$\rho_b = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\rho_{ab} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\rho_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

que são as matrizes associadas a $T_b$, $T_{ab}$ e $T_1$, respectivamente. □

**Exemplo 2.6 Algumas representações de grupos cíclicos**

Seja $G = \{1, a, a^2, \cdots, a^{m-1}\}$ grupo cíclico de ordem $m$ e seja $K$ um corpo. Se $G =< a >$, então uma representação matricial $A : G \to GL(n, K)$ está completamente determinada pela matriz $A(a)$, pois $A(a^r) = A(a)^r$. Para verificar que $A$ é na verdade um homomorfismo de grupos e então uma representação , é suficiente que $A(a)^m = I$, a matriz identidade de ordem $n$.

Suponha que $car(K)$ não divide $|G| = m$ e que $K$ contém uma $m$-ésima raiz primitiva da unidade $\xi$. Então, a função $A : G \to GL(1, K)$ dada por $A(a) = \xi$ é uma representação unidimensional de $G$ sobre $K$. Além disso, se $\{\xi_1, \cdots, \xi_m\}$ é o conjunto de todas as $m$-ésimas raízes distintas da unidade, então a função $B : G \to GL(m, K)$ dada por

$$B(a) = \begin{bmatrix} \xi_1 & 0 & \cdots & 0 \\ 0 & \xi_2 & \cdots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \cdots & \xi_m \end{bmatrix}$$

é uma representação de $G$ sobre $K$, de grau $m$. De fato, $B(a)^m = I$.

A representação regular de $G$ é dada por:

$$\Gamma(a) = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ . & . & & . & . \\ . & . & & . & . \\ . & . & & . & . \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

□

**Definição 2.11** *Duas representações $T : G \mapsto GL(V)$ e $\bar{T} : G \mapsto GL(W)$ de um grupo $G$ sobre o mesmo corpo $K$ são ditas* equivalentes *se existe um isomorfismo $\phi : V \to W$ tal que:*

$$\bar{T}_g = \phi \circ T_g \circ \phi^{-1}, \forall g \in G.$$

**Definição 2.12** *Duas representações matriciais $A : G \to GL(n, K)$ e $B : G \to GL(n, K)$ de um grupo $G$ sobre o mesmo corpo $K$ são ditas* equivalentes *se existe uma matriz inversível $U \in GL(n, K)$ tal que:*

$$A(g) = UB(g)U^{-1}, \forall g \in G.$$

**Exemplo 2.7 Representações de $D_4$**

Consideremos o grupo de todas as simetrias de um quadrado. Sejam $a$ a rotação anti-horária através de um ângulo $\frac{\pi}{2}$ e $b$ a reflexão através de um eixo que contém uma das diagonais desse quadrado. Esse grupo, denotado por $D_4$, é chamado *o grupo dihedral de ordem 8* e dado por:

$$D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

onde $a^4 = 1$, $b^2 = 1$, $baba = 1$.

Para dar uma representação $A : D_4 \to GL(n, K)$ sobre um corpo $K$, é suficiente determinar matrizes $A(a)$ e $A(b)$ tais que $A(a)^4 = I$, $A(b)^2 = I$ e $A(b)A(a)A(b)A(a) = I$.

É fácil determinar quatro representações diferentes de $D_4$ de grau 1, sobre qualquer corpo $K$ de característica diferente de 2, digamos,

$$A(a) = 1 \text{ e } A(b) = 1$$
$$B(a) = 1 \text{ e } B(b) = -1$$
$$C(a) = -1 \text{ e } C(b) = 1$$
$$D(a) = -1 \text{ e } D(b) = -1$$

Pensando no significado geométrico de $a$ e $b$, podemos obter ainda uma outra representação $W$ de $D_4$, de grau 2, dada por:

$$W(a) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

e

$$W(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

□

Note que, a menos de equivalência, o grupo $D_4$ possui uma única representação de grau maior que um e é, portanto, um exemplo da classe de grupos que pretendemos classificar.

**Exemplo 2.8 Soma direta de representações**

Sejam $T : G \to GL(V)$ e $S : G \to GL(W)$ duas representações de um grupo $G$ sobre um anel comutativo $R$. Definamos uma representação de $G$ sobre $R$ com espaço de representação $V \oplus W$, chamado *soma direta das representações dadas*, denotado por $T \oplus S$, onde:

$$(T \oplus S)_g = T_g \oplus S_g, \, \forall g \in G.$$

Se escolhermos bases $\{v_1, \cdots, v_n\}$ e $\{w_1, \cdots, w_m\}$ de $V$ e $W$, respectivamente, e denotarmos por $g \mapsto A(g)$ e $g \mapsto B(g)$ as representações matriciais correspondentes nessas bases, então $T \oplus S$ com respeito à base $\{(v_1, 0), \cdots, (v_n, 0), (0, w_1), \cdots, (0, w_m)\}$ de $V \oplus W$, é dada por:

$$g \mapsto \begin{bmatrix} A(g) & 0 \\ 0 & B(g) \end{bmatrix}$$

□

**Exemplo 2.9** Seja $G$ um grupo cíclico de ordem $m$ e seja $K$ um corpo que contém $\{\xi_1, \cdots, \xi_m\}$ o conjunto de todas as raízes da unidade de ordem $m$. Consideremos as representações $B$ e $\Gamma$ do exemplo 2.6 e seja

$$U = \begin{bmatrix} \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\ \xi_2 & \xi_2^2 & \cdots & \xi_2^m \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \xi_m & \xi_m^2 & \cdots & \xi_m^m \end{bmatrix}$$

Como $U$ é uma matriz de Vandermonde com $det(U) = \prod_{1 \leq i \leq j \leq m}(\xi_i - \xi_j) \neq 0$, então $U \in GL(m, K)$ *e* $B(a)U = U\Gamma(a)$. Decorre daí que $B(g) = U\Gamma(g)U^{-1}$, $\forall g \in G$, o que mostra que essas representações são equivalentes. □

**Definição 2.13** *Uma representação $T : G \to GL(V)$ de um grupo $G$ sobre um corpo $K$ é chamada* irredutível *se $V$ é um espaço não-nulo cujos subespaços invariantes sob $T$ são apenas os subespaços triviais $\{0\}$ e $V$.*

## 2.6 Representações e módulos

Nosso objetivo nesta seção é mostrar a relação existente entre representações e módulos via o conceito de anel de grupo.

**Proposição 2.8** *Seja $G$ um grupo e $R$ um anel comutativo com unidade. Então, existe uma bijeção entre representações de $G$ sobre $R$ e $RG$-módulos livres de dimensão finita sobre $R$.*

**Demonstração** Seja $T : G \to GL(V)$ uma representação de $G$ sobre um anel comutativo com unidade $R$, onde $V$ é um $R$-módulo de dimensão finita. A essa representação associamos o espaço $V$, que se torna um $RG$-módulo com a operação por escalar $\alpha$, dada por:

$$\alpha v = (\sum_{g\in G} a_g g)v = \sum_{g\in G} a_g(gv) = \sum_{g\in G} T_g(v),\ \alpha \in RG,\ \forall v \in V.$$

De fato, essa operação satisfaz as propriedades:

1. $\alpha(v_1+v_2) = (\sum_{g\in G} a_g g)(v_1+v_2) = \sum_{g\in G} a_g T_g(v_1+v_2) = \sum_{g\in]G} a_g T_g(v_1) + \sum_{g\in G} a_g T_g(v_2) = \alpha v_1 + \alpha v_2$;

2. $(\alpha+\alpha_1)v = (\sum_{g\in G} (a_g + a_{1_g})g)v = \sum_{g\in G} (a_g + a_{1_g})T_g(v) = \sum_{g\in G} a_g T_g(v) + \sum_{g\in G} a_g T_g(v) = \alpha v + \alpha_1 v$;

3. $(\alpha\alpha_1)v = (\sum_{g,h\in G} \alpha_g \alpha_{1_h} gh)v = \sum_{g,h\in G} (\alpha_g \alpha_{1_h})T_{gh}(v) = \sum_{g,h\in G} (\alpha_g \alpha_{1_h})T_g(T_h(v)) = \alpha(\alpha_1 v)$.

Reciprocamente, se $M$ é um $RG$-módulo de dimensão finita sobre $R$, definimos uma representação de $G$ sobre $R$ atribuindo a cada elemento $g \in G$ o $R$-automorfismo $T_g : M \to M$ dado por: $T_g(m) = gm$, $\forall m \in M$. De fato, $T_g$ assim definida age em uma base de $M$ por multiplicação à esquerda. Do exemplo 2.5 segue que $T_g$ é isomorfismo de $V$. Logo a aplicação $T : G \to GL(M)$ definido por $T(g) = T_g$, é tal que $T_{gh}(m) = (gh)m = g(hm) = T_g(T_h(m)) = (T_g \circ T_h)(m)$.

É de verificação imediata que essas funções são inversas uma da outra. □

**Exemplo 2.10** Seja $G$ um grupo finito e considere $RG$ como um $RG$-módulo sobre ele mesmo. Sabemos que $RG$ possui dimensão finita $|G|$ sobre $R$. Logo, $\forall x \in G$, a representação $T_x : RG \to RG$ é dada por:

$$T_x(\sum_{g\in G} \alpha(g)g) = x(\sum_{g\in G} \alpha(g)g) = \sum_{g\in G} \alpha(g)xg$$

Isso significa que $x \in G$ age na base $G = \{g_1, \cdots, g_n\}$ por multiplicação à esquerda. Logo, a representação associada ao $RG$-módulo $RG$ é precisamente a *representação regular* de $G$. □

**Lema 2.7** *Seja $G$ um grupo e $R$ um anel. Seja $T : G \to GL(V)$ uma representação de $G$ sobre $R$, com espaço de representação $V$. Então, um subespaço $W \subset V$ é invariante sob $T$ se e somente se $W$ é um $RG$-submódulo de $V$.*

**Demonstração** Seja $W$ um $R$-subespaço de $V$, invariante sob $T$; isto é, $\forall g \in G$, $T_g(W) \subset W$.

Então,

1. $\forall w_1, w_2 \in W$, $w_1 - w_2 \in W$;
2. $\forall w \in W$, $\forall \alpha \in RG$, $\alpha w = (\sum_{g \in G} a_g g)w = \sum_{g \in G} a_g(gw) = \sum_{g \in G} a_g T_g(w) \in W$.

Portanto, $W$ é um $RG$-submódulo de $V$.

Seja $T$ a representação de $G$ sobre $R$ correspondente ao espaço $V$, como $RG$-módulo, e $W \subset V$ um $RG$-submódulo de $V$. Então, $T_g(w) = gw \in W$, $\forall g \in G$, $\forall w \in W$; isto é, $W$ é subespaço $T$-invariante. □

**Proposição 2.9** *Seja $G$ um grupo e seja $R$ um anel comutativo. Então:*

1. *Duas representações $T$ e $T'$ de $G$ sobre $R$ são equivalentes se e somente se os $RG$-módulos correspondentes são isomorfos;*

2. *Uma representação é irredutível se e somente se o $RG$-módulo correspondente é irredutível.*

**Demonstração**

1. Sejam $T : G \to GL(V)$ e $T' : G \to GL(W)$ representações equivalentes de $G$ sobre $R$. Então, existe isomorfismo $\phi : V \to W$ tal que $\forall g \in G$, $T'_g = \phi \circ T_g \circ \phi^{-1}$. Como $V$ e $W$ são os $RG$-módulos de dimensão finita sobre $R$ correspondentes a $T$ e $T'$, respectivamente, então segue o resultado.

   Por outro lado, se $V$ e $W$ são $RG$-módulos isomorfos, de dimensão finita sobre $R$, via isomorfismo $\phi$ e $T : G \to GL(V)$ e $S : G \to GL(W)$ são as representações correspondentes a $V$ e $W$, então:

$$\begin{aligned}(\phi \circ T_g \circ \phi^{-1})(w) &= (\phi \circ T_g)(\phi^{-1}(w)) = \phi(T_g(\phi^{-1}(w))) \\ &= \phi(g\phi^{-1}(w)) = g\phi(\phi^{-1}(w)) \\ &= gw = S_g(w).\end{aligned}$$

   Logo, $S_g = \phi \circ T_g \circ \phi^{-1}$, $\forall g \in G$, e portanto, $S$ e $T$ são equivalentes.

2. Seja $T : G \to GL(V)$ uma representação irredutível. Se o $RG$-módulo correspondente $V$ é redutível; isto é, $V = A \oplus B$, onde $A$ e $B$ são $RG$-submódulos de $V$, então, pelo lema 2.7, $A$ e $B$ são invariantes sob T, o que é uma contradição .

   Suponha agora que $V$ é irredutível. Suponha ainda que a representação correspondente $T : G \to GL(V)$ é redutível e seja $W \subset V$ o subespaço $T$-invariante. Como $W$ é não-vazio, podemos escrever $V = W \oplus (V \setminus W)$. Contradição . □

Observemos que se um $RG$-módulo $M$ admite uma decomposição como uma soma direta de submódulos $M = \oplus_{i=1}^{t} M_i$ e se $T$ e $T_i$ denotam as representações correspondentes a $M$ e $M_i$, $1 \leq i \leq t$, então: $T = \oplus_{i=1}^{t} T_i$. De fato, se $m = (m_1, m_2, \cdots, m_t) \in M$ e $T : G \to GL(M)$ é a representação correspondente ao $RG$-módulo $M$, então, $\forall g \in G$,

$$\begin{aligned} T_g(m) = gm &= (gm_1, gm_2, \cdots, gm_t) \\ &= (T_{1_g}(m_1), T_{2_g}(m_2), \cdots, T_{t_g}(m_t)), \end{aligned}$$

onde $T_{i_g}$, $1 \leq i \leq t$, é a imagem de $g$ pela representação irredutível $T_i : G \to GL(M_i)$, que está associada ao $RG$-módulo irredutível $M_i$. Portanto, $\forall g \in G$, $T_g = \oplus_{i=1}^{t} T_{i_g}$, o que implica $T = \oplus_{i=1}^{t} T_i$.

Mostraremos agora como as informações que temos sobre anéis de grupo nos ajudam a obter informações sobre representações de grupo.

Se $G$ é um grupo finito e $K$ é um corpo tal que $car(K)$ não divide $|G|$, então, $KG$ é semisimples. Nesse caso, todos os $KG$-módulos são semisimples.

Seja $KG$ um anel semisimples e $KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$, onde $D_i$, $1 \leq i \leq r$, são anéis de divisão contendo $K$ em seu centro. Então, calculando dimensões sobre $K$ em ambos os lados desta expressão, obtemos:

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

Como o módulo $I_i$ de $M_{n_i}(D_i)$ é isomorfo a $D_i^{n_i}$, o grau da representação correspondente $T_i$ é dado por: $grau(T_i) = [I_i : K] = [D_i^{n_i} : K] = n_i[D_i : K]$. Portanto, $|G| = \sum_{i=1}^{r} n_i grau(T_i)$.

Esse resultado e a proposição 2.5 nos dão o seguinte teorema:

**Teorema 2.5** *Seja $G$ um grupo finito e seja $K$ um corpo de decomposição para $G$. Então:*

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(K),$$

*onde $r$ é o número de classes de conjugação de $G$. Consequentemente, o número de representações irredutíveis, não-equivalentes de $G$ sobre $K$ é também $r$. Além disso,*

$$|G| = \sum_{i=1}^{r} n_i^2$$

**Exemplo 2.11 Representações do grupo dihedral de ordem 8**

Vimos no exemplo 2.7 que o grupo $D_4$ possui quatro representações diferentes de grau 1 e uma representação $W$ de grau 2 sobre $Q$, o corpo dos racionais. Então, na decomposição de $QD_4$ aparecem quatro componentes simples isomorfas a Q e essas são todas as suas componentes comutativas, pois $QD_4$ não é comutativo.

Seja $M_n(D)$ a componente simples correspondente à representação de grau 2. Como $2 = grau(W) = n[D : Q]$, então $n = 1$ e $[D : Q] = 2$ ou $n = 2$ e $[D : Q] = 1$. No primeiro caso, $QD_4$ é da forma:

$$QD_4 \simeq Q \oplus Q \oplus Q \oplus Q \oplus D \oplus D'$$

onde $D'$ deve ser também um anel de divisão, tal que $[D' : Q] = 2$. Como um anel de divisão de dimensão 2 sobre um corpo deve ser comutativo, então teríamos que $QD_4$ é comutativo, o que é uma contradição , pois $D_4$ é não-abeliano.

Consequentemente, devemos ter $n = 2$ e $D = Q$. Portanto,

$$QD_4 \simeq Q \oplus Q \oplus Q \oplus Q \oplus M_2(Q).$$

Como as representações dadas são também representações irredutíveis de $D_4$ sobre $C$, o corpo dos complexos, temos que:

$$CD_4 \simeq C \oplus C \oplus C \oplus C \oplus M_2(C).$$

□

Observe que dadas todas as representações irredutíveis, a menos de equivalência, de um grupo finito $G$ sobre corpo $K$, fica determinada a decomposição do anel de grupo $KG$ em soma direta de anéis mais simples, como no exemplo 2.11. Da mesma forma, dada decomposição em soma direta de $KG$, ficam determinadas as representações irredutíveis de $G$. Temos assim uma maneira de estudar as representações irredutíveis de $G$ sobre $K$, a saber: via decomposição do anel de grupo $KG$ em anéis mais simples.

# Capítulo 3

# Caracterização de grupos finitos que possuem uma única K-representação irredutível de grau maior que 1

Apresentamos neste capítulo o principal resultado deste trabalho. Veremos antes alguns lemas, onde usaremos as notações : $G$ para grupo finito, $G^{'}$ para grupo derivado de $G$ e $Z(G)$ para centro de $G$.

**Lema 3.1** *Um grupo finito $G$ possui uma única $K$-representação irredutível de grau maior que 1 se e somente se $G$ possui $[G : G^{'}] + 1$ classes de conjugação , onde $K$ é um corpo algebricamente fechado.*

**Demonstração** Seja

$$KG = KGe_{G'} \oplus KG(1 - e_{G'}),$$

tal que $KGe_{G'} \simeq K(G/G^{'})$ é a soma das componentes comutativas de $KG$ e $KG(1 - e_{G'}) = \Delta(G, G^{'})$ é a soma das demais componentes. Como $K$ é algebricamente fechado, as componentes comutativas de $KG$ são cópias de $K$ e o número de classes de conjugação de $G$ é o número de componentes simples de $KG$. O número de componentes simples comutativas de $KG$ é dado por:

$$dim_K K(G/G^{'}) = |G|/|G^{'}| = [G : G^{'}].$$

Se $G$ possui uma única $K$-representação irredutível de grau maior que 1, então a ela está associada a componente simples $\Delta(G, G^{'})$. Portanto, $KG$ possui $[G : G^{'}] + 1$ classes de conjugação .

Suponha agora que $G$ possui $[G : G^{'}] + 1$ classes de conjugação e escreva

$$KG = KGe_{G^{'}} \oplus \Delta(G, G^{'}) \simeq \oplus_{i=1}^{r} M_{n_i}(K),$$

onde $r$ é o número de componentes simples de $KG$. Segue-se então do fato de $K$ ser algebricamente fechado que $r = [G : G^{'}] + 1 \Longleftrightarrow r - 1 = [G : G^{'}] = dim_K K(G/G^{'})$, tal que $K(G/G^{'})$ é, a menos de isomorfismo, a soma das componentes comutativas de $KG$. Em termos matriciais,

$$KG \simeq K \oplus \cdots \oplus K \oplus M_{n_i}(K),$$

onde $K$ aparece $[G : G^{'}]$ vezes nesse somatório.

A componente simples $M_{n_i}(K)$ é tal que $n_i > 1$, de onde segue o resultado. □

Seja $\tau = \{g_0 = 1, g_1, g_2, \cdots, g_r\}$ um transversal de $G^{'}$ em $G$.

**Lema 3.2** *Um grupo finito $G$ possui $[G : G^{'}] + 1$ classes de conjugação se e somente se cada $g_i G^{'}$ é uma única classe de conjugação e $G^{'}$ é a união de duas classes de conjugação $\{1\}$ e $G^{'} - \{1\}$.*

**Demonstração** Para verificar que cada classe $g_i G^{'}$ é uma união de classes de conjugação , basta mostrar que $\forall x \in g_i G^{'}$, o conjugado de $x$ ainda está em $g_i G^{'}$. De fato, $\forall x \in g_i G^{'}$, $x = g_i g^{'}$, para algum $g^{'} \in G^{'}$. Logo, $\forall g \in G$, $g^{-1} x g = g^{-1} g_i g^{'} g = (g^{-1} g_i g)(g^{-1} g^{'} g) \in g_i G^{'}$, pois $g^{-1} g_i g \in g_i G^{'}$ e $g^{-1} g^{'} g \in g^{'} G^{'} = G^{'}$.

Concluímos que $G$ possui, pelo menos, $r+1$ classes de conjugação , a saber, o número de classes laterais de $G^{'}$ em $G$. Note que $G^{'} = (G^{'} - \{1\}) \bigcup \{1\}$ e, por hipótese, $G$ possui exatamente $[G : G^{'}] + 1 = r + 2$ classes de conjugação . Então, cada classe lateral $g_i G^{'}$ é uma única classe de conjugação e $G^{'}$ é a união das classes $G^{'} - \{1\}$ e $\{1\}$.

Suponha agora que cada $g_i G^{'}$ é uma única classe de conjugação , $i \geq 1$, e $G^{'}$ é a união das classes $G^{'} - \{1\}$ e $\{1\}$. Então $G$ possui $[G : G^{'}] + 1 = r + 2$ classes de conjugação e essas são as únicas classes de $G$. De fato, seja $x$ o representante de qualquer outra classe

de conjugação . Temos que $x = g_i g^{'}$, para algum $g_i \in \tau$, $g^{'} \in G^{'}$; isto é, $x \in \bar{g}_i = g_i G^{'}$ e, portanto, $\bar{x} = \bar{g}_i$. □

**Teorema 3.1** *Um grupo $G$ possui exatamente uma única $K$-representação irredutível de grau maior que 1 se e somente se:*

- $|G| = 2^k$, *$k$ é ímpar,* $Z(G) = G^{'}$ *e* $|G^{'}| = 2$;

*ou*

- *$G$ é isomorfo ao grupo de todas as transformações $x \to ax + b$, $a \neq 0$, sobre um corpo de ordem $p^n \neq 2$.*

**Demonstração** Suponha que $G$ possui uma única $K$-representação irredutível de grau maior que 1. Segue dos lemas 3.1 e 3.2 que $G$ age transitivamente por conjugação sobre $G^{'} - \{1\}$.

Como consequência temos que $G^{'}$ é abeliano, $G^{'}$ é abeliano elementar e $G^{'}$ é normal minimal em $G$. Com efeito, tome $x \in G^{'}$, $x \neq 1$, arbitrário. Para todo $y \in G^{'}$, $y \neq 1$, existe $g \in G$ tal que $y = g^{-1}xg$. Nesse caso, $y^2 = (g^{-1}xg)^2 = g^{-1}x^2g$, $\cdots$, $y^{\circ(x)} = (g^{-1}xg)^{\circ(x)} = g^{-1}x^{\circ(x)}g = 1$, $\forall y \in G^{'} - \{1\}$. Portanto, $\forall y \in G^{'} - \{1\}$, existe inteiro $k$ tal que $y^k = 1$ e o menor inteiro $k$ com essa propriedade, é primo. Caso contrário, $k = mn$ e $\forall g^{'} \in G^{'} - \{1\}, (g^{'})^m \neq 1$, pois $\circ(g^{'}) = k$ e $m < k$. Logo, $(g^{'})^m$ elemento de $G^{'}$ é tal que $(g^{'^m})^n = 1$, com $n < k$. Contradição . Portanto, $k$ é primo.

Mostremos que $G^{'}$ é abeliano. De fato, visto que $x \in G^{'} \Longrightarrow \circ(x) = k$, $k$ primo, temos que todos os elementos de $G^{'} - \{1\}$ possuem a mesma ordem (prima) e, portanto, $G^{'}$ é um $p$-grupo. Logo, $Z(G^{'})$ é não-trivial. Considere agora a aplicação $f_g : G^{'} \to G^{'}$ definida por $f_g(x) = g^{-1}xg$, $\forall g \in G$, $x \in G^{'}$. É de verificação imediata que $f_g$ é um automorfismo sobre $G^{'}$. Então, $f_g$ leva $Z(G^{'})$ em $Z(G^{'})$, o centro de $G^{'}$. Agora, $\forall x \in G^{'} - \{1\}$, $\{f_g(x); \forall g \in G\} = G^{'} - \{1\}$, pois $G^{'} - \{1\}$ é uma única classe de conjugação . Em particular, se $x \in Z(G^{'})$, $x \neq 1$, então $G^{'} - \{1\} = \{f_g(x); \forall g \in G\} \subseteq Z(G^{'})$, de onde segue que $G^{'}$ é abeliano.

Portanto, $G^{'}$ é $k$-abeliano elementar, onde $k$ é um número primo.

Mostremos agora que $G^{'}$ é normal minimal em $G$. Seja $H$ subgrupo de $G$ tal que $\{1\} \neq H < G^{'}$, $H \neq G^{'}$ e $H \triangleleft G$. Então, $\forall g \in G$, $g^{-1}Hg \subset H$. Tome $y \in G^{'} - H$, $y \neq 1$ e $x \in H$. Por hipótese, $G^{'} - \{1\}$ é uma única classe de conjugação . Logo, existe $g \in G$ tal que $x = g^{-1}yg$. Mas $x = g^{-1}yg \iff y = gxg^{-1} \in H$. Contradição . Portanto, não existe subgrupo próprio de $G^{'}$ normal em $G$, isto é, $G^{'}$ é normal minimal de $G$.

Sendo $G^{'}$ abeliano, podemos escrever $\{1\} \subset G^{'} \subset G$, tal que $\{1\} \triangleleft G^{'}$, $G^{'} \triangleleft G$ e $G^{'}/\{1\} = G^{'}$, $G/G^{'}$ são abelianos, isto é, $G$ admite uma série subnormal abeliana e, portanto, é solúvel.

Suponha que $|G^{'}| = 2$. Então, $G^{'} = Z(G)$. De fato, seja $G^{'} = \{1, g^{'}\}$. Como $G^{'}$ é uma única classe de conjugação e elementos conjugados têm mesma ordem, temos que $\forall x \in G$, $x^{-1}g^{'}x = g^{'} \iff g^{'}x = xg^{'}$, de onde segue que $G^{'} \subset Z(G)$. Tome agora $h \in G$, tal que $h$ não pertence a $G^{'}$. Como $\bar{h} = hG^{'} = \{h, hg^{'}\}$ é uma única classe de conjugação (lema 3.2), escrevemos $x^{-1}hx = hg^{'}$, para algum $x \in G$, o que implica que $h$ não pertence a $Z(G)$. Equivalentemente, temos que $h \in Z(G) \Longrightarrow h \in G^{'}$. Portanto, $Z(G) \subset G^{'}$.

Sendo $G^{'}$ central em $G$, podemos escrever $\{1\} \subset G^{'} \subset G$, tal que $\{1\}$ e $G^{'}$ são normais em $G$ e $G^{'} \subset Z(G)$, isto é, $G$ admite uma série central e, portanto, é nilpotente.

Nessas condições temos que $G$ é um 2-grupo. De fato, $G$ é nilpotente se e somente se $G$ é um produto direto de p-grupos. Digamos que $G = G_2 \times G_3 \times G_5 \times \cdots \times G_i \times \cdots$, onde $\{G_i\}_{i \in I}$ é um conjunto finito e cada $G_i$ é um i-grupo. Como $|G^{'}| = 2$, temos que $G^{'} \subset G_2$ e $\forall a, b \in G_i$, $i \geq 3$, $[a, b] = a^{-1}b^{-1}ab \in G_i \cap G^{'}$. Logo, $|[a, b]|$ divide $|G_i|$ e divide $|G^{'}| = 2$, o que nos dá $|[a, b]| = 1$, $\forall a, b \in G_i$, ou seja, $G_i$ é abeliano, $\forall i \geq 3$. Note que o elemento $h = (1, h_3, h_5, \cdots)$ está em $Z(G) = G^{'}$. Então, $h = (x, 1, 1, \cdots, 1)$, para $x \in G_2$. Portanto, $G = G_2$, ou seja, $G$ é um 2-grupo.

Seja $n > 1$ o grau de uma representação irredutível de $G$ sobre $K$, onde $K$ é um corpo algebricamente fechado de característica zero. Então, do lema 3.1,

$$KG \simeq K \oplus K \oplus \cdots \oplus K \oplus M_n(K),$$

onde aparecem $[G : G^{'}]$ cópias de $K$. Se $|G| = 2^m$, então

$$|G| = [G : G^{'}] + n^2 \iff 2^m = 2^{m-1} + n^2 \iff n^2 = 2^m - 2^{m-1} = 2^{m-1} \iff n = \sqrt{2^{m-1}}.$$

Como $n$ é inteiro, $m-1$ é par e, portanto, $m$ é ímpar. Temos assim verificado uma implicação .

Passemos ao segundo item. Suponha agora que $|G^{'}| = p^{j} > 2$. Neste caso, $Z(G) = 1$. De fato, digamos que $|G^{'}| = 3$ e $G^{'} = \{1, a, b\}$. Como $G$ age por conjugação sobre $G^{'} - \{1\} = \{a, b\}$ e $g_iG^{'} = \{g_i, g_ia, g_ib\}$, $g_i \in \tau$, é uma única classe de conjugação de $G$, então a única classe com um único elemento é $\{1\}$. Logo, $Z(G) = 1$, pois, $\forall a \in G$,

$$C_a = \{a\} \Longleftrightarrow g^{-1}ag = a, \forall g \in G \Longleftrightarrow ag = ga, \forall g \in G \Longleftrightarrow a \in Z(G).$$

Fica claro, desse modo, que $Z(G) = 1$ para qualquer ordem maior de $G^{'}$.

Observe que os grupos $G/G^{'}$ e $G^{'}$ são nilpotentes, pois $G/G^{'}$ e $G^{'}$ são abelianos. Logo, a série $G \geq G^{'} \geq 1$ é nilpotente de comprimento 2 e esse é também o comprimento nilpotente de $G$. De fato, basta ver que $G^{'}$ é normal minimal em $G$ e, portanto, a série $G \geq G^{'} \geq 1$ é a série nilpotente inferior de $G$.

Seja $\eta$ um normalizador de sistema de $G$. Então, do teorema 1.1, segue que $G{=}\eta\ G^{'}$ e $\eta \bigcap G^{'} = 1$.

Segue do teorema de isomorfismo para grupos que $\eta \simeq G/G^{'}$ que é, portanto, abeliano.

A ação de $\eta$ sobre $G^{'}$, por conjugação , é fiel. De fato, seja

$$\begin{array}{rcl} \phi \ : \ \eta & \longrightarrow & Aut(G^{'}) \\ n & \longmapsto & \phi_n : G^{'} \longrightarrow G^{'} \\ & & g^{'} \mapsto n^{-1}g^{'}n \end{array}$$

essa ação . É suficiente mostrar que $ker(\phi) = 1_G$. Para isso, tome $n \in ker(\phi)$, isto é, $n$ tal que $n^{-1}g^{'}n = g^{'}$, $\forall g^{'} \in G^{'}$. Agora, $\forall x \in G$, $x = eg^{'}$, com $e \in \eta$ , $g^{'} \in G^{'}$. Então, $\forall x \in G$,

$$n^{-1}xn = n^{-1}eg^{'}n = (n^{-1}en)(n^{-1}g^{'}n) = eg^{'} = x,$$

tal que $n^{-1}en = e$, pois $\eta$ é abeliano. Portanto, $n \in ker(\phi) \Longleftrightarrow n \in Z(G) = \{1_G\} \Longleftrightarrow n = 1_G$, onde a recíproca segue trivialmente. Daí concluímos que $\eta$ possui uma cópia em $Aut(G^{'})$.

Visto que $G^{'}$ é abeliano elementar e $|G^{'}| = p^j$, podemos escrever $G^{'} \simeq Z_p \times \cdots \times Z_p$, onde $Z_p$ aparece $j$ vezes. Nesse caso, $G^{'}$ é um $Z_p$-espaço vetorial.

Na representação $\phi$, $G^{'} \simeq {Z_p}^j$ não possui $Z_p$-subespaço invariante não-trivial, isto é, a ação de $\eta$ sobre $G^{'}$ é irredutível. De fato, vimos que a ação de $G$ sobre $G^{'} - \{1\}$, por conjugação , é transitiva; ou seja, $\forall x, y \in G^{'} - \{1\}$, existe $g \in G$ tal que $g^{-1}xg = y$. Podemos escrever $g = ng^{'}$, onde $n \in \eta$, $g^{'} \in G^{'}$. Então,

$$g^{-1}xg = y \Longleftrightarrow y = {g^{'}}^{-1}(n^{-1}xn)g^{'} = {g^{'}}^{-1}g^{'}(n^{-1}xn) = n^{-1}xn,$$

pois $n^{-1}xn \in G^{'}$ e $G^{'}$ é abeliano. Portanto, a ação transitiva de $G$ sobre $G^{'}$ se reduz à ação transitiva de $\eta$ sobre $G^{'}$, de onde concluímos a afirmação feita.

Na ação $\phi$ observe que $\forall n \in \eta$, $\phi_n : G^{'} \to G^{'}$ é uma transformação linear sobre $Z_p$ inversível, com ${\phi_n}^{-1} : x \mapsto nxn^{-1}$, $\forall x \in G^{'}$, onde $G^{'} \simeq {Z_p}^j$. Como a essas transformações estão associadas matrizes em $M_j(Z_p)$, o anel de matrizes de ordem $j$ com coeficientes em $Z_p$, e $M_j(Z_p)$ são todas as transformações lineares sobre ${Z_p}^j \simeq G^{'}$, podemos pensar em $\eta$ contido em $M_j(Z_p)$ via aplicação

$$\begin{array}{rccl} \varphi & : & \eta & \longrightarrow & M_j(Z_p) = \{matrizes\ j \times j\ com\ coeficientes\ em\ Z_p\} \\ & & n & \longmapsto & \varphi_n \end{array}$$

onde $\varphi_n$ é a representação matricial de $\phi_n$ em relação a uma base fixada, cujo kernel é $ker\varphi = \{1_G\}$.

Verifiquemos agora que o centralizador $C(\eta)$ de $\eta$ em $M_j(Z_p)$ é um anel de divisão. Basta mostrar que existe $L^{-1}$ em $C(\eta)$, $\forall L \in C(\eta)$, $L \neq 0$. Ou ainda, que $L$ é $1-1$ e sobrejetiva, $\forall L \neq 0$. Do teorema do núcleo e imagem, isso se reduz a mostrar que $L$ é sobrejetiva; isto é, que $L({Z_p}^j) = {Z_p}^j$. Verifiquemos então essa igualdade. Para todo $n \in \eta$, $n \neq 0$, $n$ é inversível; em particular, é sobrejetiva. Logo, $\forall L \in C(\eta)$, $L \neq 0$, $nL({Z_p}^j) = Ln({Z_p}^j) = L({Z_p}^j)$. Portanto, $L({Z_p}^j) \subseteq {Z_p}^j$ é $\eta$-invariante. Como $\eta$ age de modo irredutível sobre ${Z_p}^j$ e $L \neq 0$, temos que $L({Z_p}^j) = {Z_p}^j$.

Como $C(\eta)$ é um anel de divisão finito e, portanto, um corpo finito, temos que $C\ (\eta)^*$ é cíclico. Logo, $\eta$ também é cíclico, pois $\eta$ é abeliano o que implica que $\eta$ está contido em $C(\eta)^*$.

A ação de $\eta$ como um grupo de permutações sobre $G^{'} - \{1\}$ é transitiva; ou seja, $G^{'} - \{1\}$ é uma única órbita de $\eta$. Visto que $\eta$ é abeliano, essa ação é também regular, pela proposição 1.1. Em particular, $\eta$ é semiregular (definição 1.6). Então, pela proposição 1.2, temos que $|\eta| = |G^{'} - \{1\}| = p^j - 1$.

$\vdash$: $\eta$ é um subgrupo maximal em $G$. De fato, seja $L$ subgrupo de $G$ tal que $\eta < \mathrm{L} < \mathrm{G}$ e $\eta \neq \mathrm{L}$. Então, existe $l \in L$, $l = ng^{'}$, tal que $n \in \eta$, $g^{'} \in G^{'}$ e $g^{'} \neq 1$. É claro que $n^{-1} \in L$, pois $\eta < L$. Logo, $n^{-1}l = n^{-1}ng^{'} = g^{'} \in L$ e consequentemente $g^{'^{\eta}}$, a classe de $g^{'}$ na ação de $\eta$, por conjugação , sobre $G^{'}$, pertence a $L$. Mas essa ação é transitiva. Então, $g^{'^{\eta}} = G^{'} \subset L$. Como $L \supset G^{'}$ e $L \supset \eta$, temos que $L \supset G = \eta G^{'}$; ou seja, $L = G$ e, portanto, $\eta$ é maximal em $G$.

$\vdash$: A representação de $G$ sobre as classes de $\eta$ é primitiva. Com efeito, seja $\tau = \{t_1 = 1, t_2, \cdots, t_k\}$ um transversal de $\eta$ em $G$ e suponha que $\eta t_1 = \eta, \eta t_2, \cdots, \eta t_s$; com $s < k$, é um bloco não-trivial fixado pela ação de $G$ sobre $G/\eta$. Então, $\eta t_1 = \eta \cup \eta t_2 \cup \cdots \cup \eta t_s = M$ é um subgrupo de $G$. De fato, quaisquer que sejam $nt_i, n^{'}t_j \in M$, temos que $nt_i n^{'}t_j \in (\eta t_i)n^{'}t_j \subset \cup_{i=1}^{s} \eta t_i = M$. Ou seja, $M$ é fechado para a operação de $G$. Note ainda que $(nt_i)(t_i^{-1}n^{-1}t_i) = t_i \in M$ e, com isso, $t_i {t_i}^{-2} = t_i^{-1} \in M$. Assim, $\forall nt_i \in M$, ${t_i}^{-1}n^{-1} = (nt_i)^{-1} \in M$. Portanto, $M$ é um grupo tal que $\eta < M < G$ e $\eta \neq M \neq G$, o que contradiz a maximalidade de $\eta$ em $G$. Então, não existem blocos não-triviais fixados pela ação de $G$ sobre as classes de $\eta$, o que verifica a afirmação inicial.

Além disso, essa é uma representação fiel. De fato, se $\pi : G \to S(G/\eta)$ é essa representação , então basta mostrar que $ker\pi = \{1\}$. Para isso, observe que $ker\pi \subseteq \bigcap_{x \in G} \eta^x$ e que o grupo $\bigcap_{x \in G} \eta^x$ está contido no hipercentro de $G$ (ver [2]). Visto que o hipercentro de $G$ é $\{1\}$, pois $Z(G) = \{1\}$, então $ker\pi = \{1\}$.

Agora, usando o fato que $|\eta| = p^j - 1$ e aplicando resultado encontrado em [3], temos que $G$ é isomorfo ao grupo de todas as transformações $x \to ax + b$, $a \neq 0$, sobre um corpo de ordem $p^j$.

Para a recíproca, suponha primeiramente que $|G| = 2^k$, $G^{'} = Z(G)$ e $|G^{'}| = 2$. Digamos que $G^{'} = \{1, a\}$ e $\tau = \{g_o = 1, g_1, \cdots, g_r\}$ é um transversal de $G^{'}$ em $G$.

$\vdash$: $g_i G^{'} = \{g_i, g_i a\}$ é uma união de classes de conjugação . De fato, $x \in g_i G^{'} \Longrightarrow x = g_i g^{'}$, $g^{'} \in G^{'}$. Portanto, $\forall g \in G$, $g^{-1}xg = g^{-1}g_i g^{'}g = (g^{-1}g_i g)(g^{-1}g^{'}g) \in g_i G^{'}$.

Logo, $G$ possui, pelo menos, $r = [G : G^{'}] - 1$ classes de conjugação .

Suponha que $g_iG^{'}$ é união de classes de conjugação distintas, a saber, $g_iG^{'} = C_{g_i} \cup^{\cdot} C_{g_ia}$. Nesse caso, $\forall g \in G$, $g^{-1}g_ig = g_i \iff g_ig = gg_i$ e $g^{-1}(g_ia)g = (g_ia) \iff (g_ia)g = g(g_ia)$, de onde concluímos que $g_i$ e $g_ia$ pertencem a $Z(G) = G^{'}$. Então, $C_{g_i} = C_{g_ia} = G^{'}$. Contradição . Logo, $g_iG^{'}$ é uma única classe de conjugação , para $i \geq 1$.

Podemos escrever $G^{'} = (G^{'} - \{1\}) \cup \{1\}$, onde $G^{'} - \{1\} = \{a\}$ e $\{1\}$ são, cada uma, uma única classe de conjugação . Então, $G$ possui, pelo menos, $r + 2 = [G : G^{'}] + 1$ classes de conjugação , que afirmamos serem as únicas classes de $G$. De fato, se $x$ é representante de qualquer outra classe de conjugação , então $x = g_ig^{'}$, com $g_i \in \tau$, $g^{'} \in G^{'}$; isto é, $x \in \bar{g_i} = g_iG^{'}$, de onde temos $\bar{x} = \bar{g_i}$.

Portanto, do lema 3.1 segue que $G$ possui uma única $K$-representação irredutível de grau maior que 1.

Agora, suponha que $G$ é isomorfo ao grupo de todas as transformações $x \mapsto ax + b$, $a \neq 0$, sobre um corpo de ordem $p^n \neq 2$. Então, o grupo $G^{'}$ de $G$ corresponde ao grupo de todas as translações . De fato, sejam $f : x \mapsto ax+b$ e $g : x \mapsto cx+d$ transformações dadas como na hipótese. Então, estão definidas inversas $f^{-1} : x \mapsto \dfrac{1}{a}x - \dfrac{b}{a}$ e $g^{-1} : x \mapsto \dfrac{1}{c}x - \dfrac{d}{c}$. Por um cálculo direto, verificamos que o comutador $[f, g]$ de $f$ e $g$ é dado por

$$[f, g] = x + \frac{d(a-1) + b(1-c)}{ac},$$

que é uma translação . Agora, se $x \mapsto x + q$ é uma translação arbitrária, então $x \mapsto x + q \in G^{'}$. De fato, basta tomar, por exemplo, $a = b = d = 1$ e $c = \dfrac{1}{1+q}$ na expressão $\dfrac{d(a-1) + b(1-c)}{ac}$. Daí concluímos que $|G^{'}| = p^n$.

$\vdash$: Existem precisamente duas classes de conjugação em $G^{'}$. De fato, a translação trivial $x \mapsto x$ é uma classe de conjugação de $G^{'}$. Se $x \mapsto x + q$ é uma translação não-trivial, então, para toda transformação $x \mapsto ax + b \in G$, $a \neq 0$, temos que

$$\begin{aligned}(\frac{1}{a}x - \frac{b}{a}) \circ (x + q) \circ (ax + b) &= (\frac{1}{a}x - \frac{b}{a}) \circ (ax + (b + q)) = (\frac{1}{a}(ax + (b + q)) - \frac{b}{a}) \\ &= x + \frac{q}{a} = x + qa^{-1},\end{aligned}$$

tal que $a \in Q$ e $Q$ é um corpo de ordem $p^n$. Então, fazendo $a$ percorrer todos os elementos de $Q$, temos que $qa^{-1}$ percorre todos os elementos de $Q$ e, com isso, $x \mapsto x + qa^{-1}$

percorre todas as translações não triviais de $G$. Como $Q$ é finito, a classe de conjugação de $x \mapsto x + q$ é, portanto, $G^{'} - \{x \mapsto x\}$, o que verifica a afirmação feita.

Seja agora $x \mapsto rx + s$ uma transformação tal que $0 \neq r \neq 1$, isto é, $x \mapsto rx + s \in G - G^{'}$. Então, $\forall\ x \mapsto ax + b \in G$, $a \neq 0$, temos que:

$$\begin{aligned}(\frac{1}{a}x - \frac{b}{a}) \circ (rx + s) \circ (ax + b) &= (\frac{1}{a}x - \frac{b}{a}) \circ (r(ax + b) + s)) \\ &= \frac{1}{a}(arx + rb + s) - \frac{b}{a} \\ &= rx + \frac{rb + s - b}{a}.\end{aligned}$$

Novamente $\dfrac{rb + s - b}{a}$ percorre todos os elementos de $Q$, $\forall\ a, b \in Q$ e, portanto, a classe de conjugação de $x \mapsto rx + s$ corresponde a todas as transformações $x \mapsto rx + s$, $s \in Q$, $0 \neq r \neq 1$ fixo. Logo, existem $p^n - 2$ classes de conjugação em $G - G^{'}$. Como para cada $0 \neq r \neq 1$ fixado, existem $p^n$ transformações associadas, temos que $|G - G^{'}| = p^n(p^n - 2)$. Portanto, $|G| = |G - G^{'}| + |G^{'}| = p^n p^n - 2p^n + p^n = p^n(p^n - 1)$. Assim, $[G : G^{'}] = \dfrac{|G|}{|G^{'}|} = p^n - 1 \iff [G : G^{'}] + 1 = p^n$.

Ao todo, então, existem $2 + (p^n - 2) = p^n = [G : G^{'}] + 1$ classes de conjugação em $G$, o que completa a prova do teorema. $\square$

# Bibliografia


[1] R. W. Carter, *Splitting properties of soluble groups*, Journal London Math. Soc. 36 (1961), 89-94.

[2] P. Hall *On the system normalizers of a soluble group*, Proc. London Math. Soc. (2) 43 (1937), 507-528.

[3] B. Huppert, *Zweifach transitive, auflösbare Permutationsgruppen*, Math Z. 68 (1957), 126-150.

[4] M. I. Kargapolov e Ju. I. Merzljakov *Fundamentals of the Theory of Groups*, Translation of Osnovy teorii grupp, Springer-Verlag New York, Heidelberg, Berlin, 1979.

[5] C. P. Milies e S. K. Sehgal *An introduction to group rings*, Kluwer Academic Publishers, 2002.

[6] R. S. Pierce *Associative Algebras* Springer-Verlag New York, Heidelberg, Berlin, 1982.

[7] G. Seitz *Finite groups having only one irreducible representation of degree greater than one*, University of Oregon.

[8] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.