Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Grupos solúveis com finitas órbitas por automorfismos

Julia Mitsuno Kato Aiza Alvarez

Brasília

2022

Julia Mitsuno Kato Aiza Alvarez

Grupos solúveis com finitas órbitas por automorfismos

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasíia, como parte dos requisitos para obtenção do grau de MESTRE em Matemática.

Orientador:
Prof. Dr. Emerson Ferreira de Melo

Brasília

2022

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Grupos solúveis com finitas órbitas por automorfismos

por

Julia Mitsuno Kato Aiza Alvarez

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasíliacomo parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 19 de janeiro de 2022.

Comissão Examinadora:

Emerson Ferreira de Melo.

Prof. Dr. Emerson Ferreira de Melo- MAT/UnB (Orientador)

Prof. Dr. Alex Carrazedo Dantas – MAT/UnB (Membro)

Prof. Dr. Jhone Caldeira Silva– UFG (Membro)

Agradecimentos

Agradeço primeiramente a Deus, por nunca largar minha mão nos momentos que mais precisei.

A minha família pelo apoio e suporte, Tomoko, Hatsue, Kumiko e em especial a Mitsuno Ueno por me dar todo o tempo do mundo para estudar. Ao Rafael, por sempre acreditar em mim.

Aos professores do Departamento de Matemática da UnB pelos ensinamentos. Em especial ao meu orientador Emerson Ferreira de Melo, por toda a paciência, dedicação e compromisso durante a graduação e o mestrado. E aos professores participantes da banca Jhone Caldeira Silva, Alex Carrazedo Dantas e Raimundo de Araújo Bastos Júnior pelas correções e sugestões.

Aos meus colegas de curso e amigos pessoais, Francisca, André, Felipe, Eliezer, Fabi. E a todos que me ajudaram durante o trajeto.

Ao CNPq pelo apoio financeiro.

Resumo

Esta dissertação apresenta um estudo sobre grupos com finitas órbitas por automorfismos. O foco principal será classificar grupos com um determinado número de órbitas. Baseado nos artigos *"Soluble groups with few orbits under automorphisms"* e *"Automorphism Orbits of Finite Group"* classificamos os grupos finitos com 3 órbitas, os grupos de posto finito e ordem mista também com 3 órbitas e os grupos solúveis finitos com 4 órbitas.

Palavras-Chaves: Automorfismos, Grupos Solúveis, Órbitas por Automorfismos.

Abstract

This dissertation presents a study of groups with finite orbits by automorphisms. The main focus will be to classify groups given a number of orbits. Based on the articles *"Soluble groups with few orbits under automorphisms"* and *"Automorphism Orbits of Finite Group"* we classify finite groups with 3 orbits, finite rank mixed order groups also with 3 orbits, and finite soluble groups with 4 orbits.

Key-Words: Automorphisms, Soluble Groups, Automorphism Orbits.

Notações

Conjuntos

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$	conjunto dos inteiros, racionais e números reais
X, Y	conjuntos
$Sym(X)$	grupo das bijeções de X em X
$Sym(k)$	grupo das bijeções de um conjunto com k elementos
$x, y, ...$	elementos de um conjunto
$x^{\phi}, (x)\phi$	aplicar a função ϕ em x
$\mathfrak{R}, \mathfrak{P}$	conjunto de propriedades

Grupos

G, H	grupos, subgrupos
$g, h, ...$	elementos de um grupo
$g^h = h^{-1}gh$	g conjugado por h
$[g, h] = g^{-1}h^{-1}gh$	comutador de g e h
G^*	$G \setminus \{1\}$
$H^g = g^{-1}Hg$	H conjugado por g
$[H, G]$	comutador de subgrupos
$H \trianglelefteq G$, $H \triangleleft G$	H é normal em G, H é normal (próprio) em G
$\langle X_\lambda \vert \lambda \in \Lambda \rangle$	subgrupo gerado pelos subconjuntos X_λ
$\langle X \vert \mathfrak{R} \rangle$	apresentação do grupo com geradores X e relações $\mathfrak{R}$
$G^n = \langle g^n \vert g \in G \rangle$	subgrupo das n-ésimas potências de G
$H \rtimes K$	produto semidireto de H com K
$Stab_G(\alpha)$	estabilizador de α em G
$Orb_G(\alpha)$	órbita de α em G
$C_G(x)$, $C_G(H)$, $C_G(\phi)$	centralizador
$N_G(H)$	normalizador
$Aut(G)$	grupo dos automorfismos
$(G : H)$	conjunto das classes laterais
$\vert G : H \vert$	índice de H em G
$Cor_G(H)$	cerne normal
$\gamma_i(G)$	termos da séries central inferior

G'	subgrupo derivado
$G_{ab} = G/G'$	grupo abelianizado
$G^{(n)}$	termos da série derivada
$Z(G)$	centro do grupo
$p, q, ...$	números primos
$\pi(G)$	conjunto de todos os primos que dividem a ordem de G
$\pi \subseteq \pi(G)$	conjunto de primos que dividem a ordem de G
π'	$\pi(G) \setminus \pi$
$\Phi(G)$	subgrupo de Frattini
$O_\pi(G)$	maior π-subgrupo normal
$\Omega_i(P) = \langle\{x \in P \mid x^{p^i}\}\rangle$	
$\mho_i(P) = \langle\{x^{p^i \mid x \in P}\}\rangle$	
D_{2n}	grupo diedral de ordem $2n$
$Hom(G, H)$	grupo dos homomorfismo de G para H
$Tor(G)$	conjunto dos elementos de torção em G
$Syl_p(G)$	conjunto dos p-subgrupos de Sylow de G

Anéis e Módulos

$R, S, ...$	anéis
$U(R)$	unidades de R
$M, N, ...$	R-módulos
F	corpo
$F[X]$	anel de polinômios com coeficientes em F
$T_n(R)$	grupo das matrizes $n \times n$ triangulares sobre R
$UT(n, R)$	grupo das matrizes $n \times n$ unitriangulares sobre R

Álgebra Linear

V	espaço vetorial sobre o corpo F
α, β	vetores
T	transformação linear
$Z(\alpha; T)$	subespaço T-cíclico
$\mathcal{B} = \{\alpha_1, ..., \alpha_k\}$	base de um espaço vetorial
$dim_F(V)$	dimensão do espaço vetorial
$GL(n, F)$	grupo das matrizes não-singulares $n \times n$ em F
$GL(V, F)$	grupo das transformações lineares não-singulares de V em F

Sumário

Introdução

Sejam G um grupo e $Aut(G)$ seu grupo de automorfismos. O grupo dos automorfismos $Aut(G)$ age sobre G de maneira natural. As órbitas dessa ação são chamadas de *órbitas por automorfismos* de G e o número de órbitas é denotado por $\omega(G)$. Estamos interessados em classificar grupos baseados apenas no número de órbitas por automorfismos.

A classificação de grupos finitos com uma ou duas órbitas por automorfismos é bem conhecida, a saber, o grupo trivial e os p-grupos abelianos elementares. Apresentaremos essa classificação no Capítulo 3. No entanto, para um número maior de órbitas por automorfismos, a classificação dos grupos finitos não é tão simples. Dizemos que um grupo finito não trivial G tem ordem mista se G não é um p-grupo. No caso em que G tem ordem infinita, dizemos que G tem ordem mista se G possui elementos de ordem finita e infinita. Em 1986, Laffey e MacHale apresentaram a classificação de grupos finitos de ordem mista com três órbitas por automorfismos [12].

Teorema A [Laffey & MacHale (1986)]**.** *Seja G um grupo finito de ordem mista. As seguintes afirmações são equivalentes,*

1. $\omega(G) = 3$*;*
2. $|G| = p^n q$*, para primos p, q e para um inteiro $n \geq 1$, e G tem um p-subgrupo de Sylow P normal abeliano elementar. Além disso, p é uma raiz primitiva mod q (i.e. $q-1$ é o menor natural tal que $p^{q-1} \equiv 1$ mod q). Seja Q um q-subgrupo de Sylow de G. Então P, visto como $GF(p)Q$-módulo é a soma direta de $t \geq 1$ cópias do único $GF(p)Q$-módulo irredutível de dimensão $q-1$. Em particular, $|P| = p^{t(q-1)}$.*

No mesmo artigo, os autores caracterizaram também os grupos finitos solúveis de ordem mista com quatro órbitas por automorfismos.

Teorema B [Laffey & MacHale (1986)]**.** *Seja G um grupo finito solúvel de ordem mista*

tal que $\omega(G) = 4$. *Então* $|G| = p^a q^b$, *para* p, q *primos distintos. E o grupo* G *tem um* p*-subgrupo de Sylow normal* $P \in Syl_p(G)$. *Seja* $Q \in Syl_q(G)$. *Então um dos itens vale,*

1. Q *age livre-de-pontos-fixos em* P, $|Q| = q$ *e* $\omega(P) = 2$ *ou* $\omega(P) = 3$*;*
2. P *é abeliano elementar e* Q *é cíclico de ordem 4 ou o quatérnio de ordem 8;*
3. $G = P \times Q$, *onde* P *e* Q *são abelianos elementares.*

Os resultados acima valem quando o grupo é finito. No entanto, quando o grupo tem ordem infinita, ainda não se sabe muito sobre a classificação de grupos com poucas órbitas por automorfismos. Um resultado mais recente [1], por Bastos, Dantas e de Melo, apresenta uma caracterização de uma classe restrita de grupos infinitos com poucas órbitas por automorfismos.

Dizemos que um grupo G tem *posto* n se n é o menor inteiro positivo tal que todo grupo finitamente gerado é gerado por no máximo n elementos. Além disso, um grupo G é dito *radicável* se para todo inteiro positivo n e todo $g \in G$, existe $y \in G$ tal que $y^n = g$.

Em 2020, Bastos, Dantas e de Melo provaram em [1] uma decomposição dos grupos solúveis de posto finito com uma quantidade finita de órbitas por automorfismos.

Teorema C. *Seja* G *um grupo solúvel de posto finito. Se* $\omega(G) < \infty$, *então* G *possui um subgrupo* K *livre de torção, radicável, nilpotente e característico tal que*

$$G = K \rtimes H,$$

onde H *é um subgrupo finito de* G.

Também em [1], temos a classificação dos grupos solúveis infinitos de ordem mista e de posto finito com $\omega(G) = 3$.

Teorema D. *Seja* G *um grupo solúvel de ordem mista e de posto finito.* $\omega(G) = 3$ *se, e somente se,* $G = A \rtimes H$ *onde* $|H| = p$ *para algum primo* p, H *age livre de pontos fixos em* A *e* $A = \mathbb{Q}^n$ *para algum inteiro positivo* n.

Neste trabalho, temos como objetivo principal a demonstração dos Teoremas A, B, C e D. Para isso, no primeiro capítulo apresentamos resultados clássicos e bem conhecidos de Teoria de Grupos, Anéis e Módulos e Álgebra Linear. Apresentamos também um breve estudo sobre Representações de Grupos, Grupos Lineares e Automorfismos Livres de Pontos Fixos. Esses resultados serão usados nas demonstrações do teoremas principais.

O segundo capítulo tem dois objetivos. Apresentar propriedades básicas de órbitas por automorfismos e demonstrar o Teorema A.

O terceiro capítulo destina-se ao estudo de grupos infinitos de posto finito e com uma quantidade finita de órbitas por automorfismos. Apresentamos resultados trazidos em [1], incluindo as demonstrações dos Teoremas C e D.

Por fim, no quarto capítulo estudamos os grupos finitos de ordem mista e possuem quatros órbitas por automorfismos e provamos o Teorema B.

Capítulo

1

Preliminares

1.1 Definições e Resultados Básicos

1.1.1 Teoria de Grupos

Este capítulo tem como objetivo estabelecer definições e teoremas elementares que serão usados posteriormente nos resultados principais. Muitos resultados serão apresentados sem demonstração, para mais detalhes confira o capítulo 2 de [6].

Definição 1.1.1. *Sejam G um grupo e X um conjunto não vazio. Se existe uma regra que determina um novo elemento de X, denotado por $\alpha \cdot g$, para $\alpha \in X$ e $g \in G$. Dizemos que essa regra define uma ação de G em X se as seguintes condições valem,*

1. *$\alpha \cdot 1 = \alpha$ para todo $\alpha \in X$;*

2. *$(\alpha \cdot g) \cdot h = \alpha \cdot (gh)$ para todo $\alpha \in X$ e todo elemento $g, h \in G$.*

Suponha que G aja em X. Podemos notar que se $g \in G$ é arbitrário, então a função $\sigma_g : X \to X$ definida por $\alpha^{\sigma_g} = \alpha \cdot g$ possui um inverso: a função $\sigma_{g^{-1}}$. Então, σ_g é uma permutação do conjunto X, ou seja, σ_g pertence ao grupo simétrico $\mathrm{Sym}(X)$ que consiste de todas as permutações de X. Com efeito, o mapeamento $g \mapsto \sigma_g$ é um homomorfismo de G em $\mathrm{Sym}(X)$. Os homomorfismos que surgem de ações de grupos em conjuntos são ditos *representações permutacionais* de G.

Dado $\alpha \in X$ denotamos por $Stab_G(\alpha)$ o estabilizador de α, isto é, o conjunto

$$Stab_G(\alpha) = \{g \in G \mid \alpha^{\sigma_g} = \alpha\}.$$

Tal conjunto é um subgrupo de G. E denotamos por $Orb_G(\alpha)$ a G-órbita de α, isto é o conjunto

$$Orb_G(\alpha) = \{\alpha^{\sigma_g} \mid g \in G\}.$$

No contexto de ações de grupos, existem ações específicas que definem subgrupos importantes. A seguir veremos algumas delas.

Definição 1.1.2. *Dado $x \in G$ e considerando a ação por conjugação de G em G, chamamos de centralizador $C_G(x)$ de x em G, o estabilizador de x. Isto é,*

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

De maneira semelhante, definimos o centralizador de um subgrupo H em G, como sendo $C_G(H) = \{x \in G \mid hx = xh, \forall h \in H\}$. Ademais, considerando um automorfismo $\phi \in$Aut(G), definimos o centralizador de ϕ como $C_G(\phi) = \{x \in G \mid x^\phi = x\}$.

Definição 1.1.3. *Seja $H \leq G$, considerando a ação de conjugação de G nas classes laterais de H, chamamos de normalizador $N_G(H)$ o estabilizador de $H \in G$. Isto é,*

$$N_G(H) = \{g \in G \mid gH = Hg\}$$

Com isso, podemos enunciar um lema bem conhecido que envolve os subgrupos definidos acima.

Lema 1.1.4. *Seja $H \leq G$. Então o grupo quociente $N_G(H)/C_G(H)$ é isomorfo a um subgrupo de $Aut(H)$.*

Seja H um subgrupo de G, e suponha que G aja por multiplicação a esquerda sobre o conjunto $X := (G : H)$ das classes laterais esquerdas de H em G. Chamamos o núcleo dessa ação de cerne normal e denotamos por $Cor_G(H)$.

Grupos Nilpotentes e Grupos Solúveis

Agora vamos estudar brevemente grupos nilpotentes e grupos solúveis. Tais grupos surgem da generalização da propriedade comutativa, de forma que todo grupo abeliano é nilpotente e solúvel, mas existem grupos nilpotentes e solúveis que não são abelianos.

Primeiramente, vamos aos grupos nilpotentes. Eles formam uma classe mais restrita comparada aos grupos solúveis que serão apresentados a seguir, isto é, todo grupo nilpotente é solúvel. Mas nem todo grupo solúvel é nilpotente. Comecemos com a definição de série central.

Definição 1.1.5. *Uma série de um grupo G,*

$$1 = G_0 \trianglelefteq ... \trianglelefteq G_k = G$$

é chamada de série central se $G_i \trianglelefteq G$ e cada quociente G_{i+1}/G_i está contido no centro de G/G_i, com $0 \leq i < k$.

Definição 1.1.6. *Dizemos que G é nilpotente se admite uma série central.*

Exemplificaremos o conceito de grupo nilpotente. Um subgrupo M de um grupo G é dito maximal se não existe subgrupo próprio de G que contém M.

Definição 1.1.7. *O subgrupo de Frattini $\Phi(G)$ de um grupo G é a interseção de todos os subgrupos maximais de G. Caso G não possua subgrupos maximais $\Phi(G) = G$.*

O subgrupo de Frattini de um grupo finito é um exemplo de grupo nilpotente. Dados um grupo G e p um primo que divide $|G|$, denotaremos por $O_p(G)$ o subgrupo $\bigcap_{P \in Syl_p(G)} P$, que é um subgrupo maximal dentre os p-subgrupos normais.

Definição 1.1.8. *Os termos da série central inferior são definidos indutivamente da seguinte forma,*

$$\begin{aligned}
\gamma_1(G) &= G \\
\gamma_2(G) &= [\gamma_1(G), G] \\
\gamma_3(G) &= [\gamma_2(G), G] \\
&... \\
\gamma_i(G) &= [\gamma_{i-1}(G), G]
\end{aligned}$$

onde i é um inteiro positivo.

Os grupos nilpotentes finitos apresentam uma estrutura interessante, pois todo grupo nilpotente finito pode ser escrito como produto direto de seus Sylows. Assim como essa propriedade, existem muitas outras bem conhecidas que caracterizam grupos nilpotentes finitos. A seguir enunciamos algumas delas, para conferir as demonstrações veja o Capítulo 5.2 de [15]

Lema 1.1.9. *Se G é um p-grupo, então G é nilpotente.*

Lema 1.1.10. *Seja G um grupo finito, são equivalentes,*

1. *G é nilpotente;*

2. *Todo subgrupo maximal de G é normal e existe $p \in \pi(G)$ tal que $|G : M| = p$;*

3. *$G' \leq \Phi(G)$;*

4. *Todo p-subgrupo de Sylow de G é normal;*

5. *O grupo G é o produto direto dos seus p-subgrupos de Sylow.*

O lema seguinte foi apresentado como um exercício no Capítulo 10 de [7].

Lema 1.1.11. *Sejam a e b elementos de um grupo nilpotente G, onde $a^m = b^n = 1$ e $(m, n) = 1$. Então $[a, b] = 1$.*

Demonstração. Denote $w = [a, b]$ e suponha que $w \in \gamma_i(G)$, para algum i inteiro não negativo. Note que

$$\frac{\gamma_i(G)}{\gamma_{i+1}(G)} \leq Z\left(\frac{G}{\gamma_{i+1}(G)}\right),$$

então $w\gamma_{i+1}(G)$ é central em $\frac{G}{\gamma_{i+1}(G)}$. Pela identidade de comutadores $[ac, b] = [a, b]^c[c, b]$, com $c \in G$, temos que $w^n \in \gamma_{i+1}(G)$. E da mesma forma, $w^m \in \gamma_{i+1}(G)$, com isso $w \in \gamma_{i+1}(G)$. Pela arbitrariedade de i e como o grupo é nilpotente, concluímos que $w = 1$, e o lema está provado. □

Agora, vamos aos grupos solúveis. Tais grupos podem ser construídos como extensões finitas de grupos abelianos. E serão definidos a seguir.

Definição 1.1.12. *Consideremos a seguinte série:*

$$\begin{aligned} G^{(0)} &= G \\ G^{(1)} &= [G, G] \\ G^{(2)} &= [G^{(1)}, G^{(1)}] \\ &\cdots \\ G^{(n)} &= [G^{(n-1)}, G^{(n-1)}] \end{aligned}$$

para cada $n \geq 2$. Chamaremos essa série de série derivada do grupo G.

Definição 1.1.13. *Um grupo G é solúvel se existe um número natural n tal que $G^{(n)} = 1$.*

Em se tratando de grupos solúveis, o resultado abaixo é bem conhecido.

Lema 1.1.14. *Se G é um grupo solúvel, e N é um subgrupo normal minimal de G então N é abeliano elementar.*

O próximo resultado é o famoso critério de solubilidade de Burnside. Uma demonstração pode ser encontrada em 8.5.3 de [15].

Teorema 1.1.15 (Burnside)**.** *Se G é um grupo finito de ordem $p^a q^b$, onde p e q são primos distintos e a e b são inteiros positivos, então G é solúvel.*

1.1.2 Anéis e Módulos

O estudo de anéis e módulos nos levam ao estudo do produto tensorial que é uma ferramenta muito importante para a próxima seção. Os resultados desta seção baseiam-se principalmente no Capítulo 1.2 de [13], no Capítulo 1.2 de [11] e no Capítulo 1.2 de [10].

Definição 1.1.16 (R-módulo)**.** *Seja R um anel com unidade 1. Um grupo (aditivo) M com a operação $m \to mr \in M$ com $m \in M$ e $r \in R$ é R-módulo se para $m_1, m_2 \in M$ e $r_1, r_2 \in R$ valem*

1. $m_1 1 = m_1$;
2. $(m_1 \pm m_2)r_1 = m_1 r_1 \pm m_2$;
3. $m_1(r_1 \pm r_2) = m_1 r_1 \pm m_1 r_2$;
4. $(m_1 r_1)r_2 = m_1(r_1 r_2)$.

Todo grupo abeliano pode ser visto como um $\mathbb{Z}$-módulo de forma natural. De fato, para $r < 0$, temos que,

1. $ar = \underbrace{a + a + ... + a}_{\text{r}}$;
2. $a(-r) = (-a)r$;
3. $a0 = 0$.

Exemplo 1.1.1. *$\mathbb{Q}$ é um grupo abeliano com a soma, então $\mathbb{Q}$ pode ser visto como um $\mathbb{Z}$-módulo de forma natural, para $k > 0$ e $a \in \mathbb{Q}$,*

1. $ar = \underbrace{a + a + ... + a}_{r}$;
2. $a(-r) = (-a)r$;
3. $a0 = 0$.

Exemplo 1.1.2. *Se F é um corpo, então um F-módulo é um espaço vetorial sobre F.*

Um *submódulo* N de um R-módulo M é um subconjunto de M que é um módulo com as operações de adição e multiplicação induzidas. Se F é um corpo, então um F-submódulo é um subespaço vetorial de M sobre F.

Sejam M um R-módulo e N um R-submódulo de M. O grupo quociente $M/N = \{mN \mid m \in M\}$ pode ser visto como um *módulo quociente* sobre R,

1. $1m_1N = m_1N$;
2. $(r_1 + r_2)m_1N = r_1m_1N + r_2m_1N$;
3. $r_1(m_1N + m_2N) = r_1m_1N + r_1m_2N$;
4. $(r_1r_2)m_1N = r_1(r_2m_1N)$.

para $m_1, m_2 \in M$ e $r_1, r_2 \in R$.

O R-submódulo *gerado* por um conjunto X, denotado por $\langle X \rangle$, é igual ao menor submódulo que contém X. Dizemos que o conjunto X gera M se o submódulo gerado por X é o módulo M.

Seja R um anel com unidade 1. Um *R-módulo livre* F com geradores livres $\{x_i \mid i \in I\}$ é a soma direta de cópias isomorfas $x_iR = \{x_ir \mid r \in R\}$ do grupo aditivo de R com $(\sum_i x_ir_i)r = \sum_i x_i(r_ir)$.

Definição 1.1.17. *Sejam A e B K-módulos, onde K é um anel comutativo com unidade. O produto tensorial $A \otimes_K B$ é definido como sendo o módulo quociente do módulo livre $A \times B$ com geradores livres $a \otimes b$, $a \in A$, $b \in B$, pelo submódulo gerado por todos os elementos da forma*

1. $k(a \otimes b) - ka \otimes b$;
2. $ka \otimes b - a \otimes kb$;
3. $a \otimes (b_1 + b_2) - (a \otimes b_1 + a \otimes b_2)$;
4. $(a_1 + a_2) \otimes b - (a_1 \otimes b + a_2 \otimes b)$.

Onde $k \in K$; $a, a_1, a_2 \in A$; $b, b_1, b_2 \in B$.

Isso é equivalente a tomar o conjunto de somas,

$$\left\{ \sum k_{a,b} a \otimes b \mid a \in A, b \in B \right\}$$

e identificar os elementos,

1. $k(a \otimes b) = ka \otimes b = a \otimes kb$;
2. $a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$;
3. $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$.

Se os elementos $a_1, a_2, ..., a_s$ geram o R-módulo A e os elementos $b_1, b_2, ..., b_t$ geram o R-módulo B, então os st elementos $a_i \oplus b_j$ geram o R-módulo $A \oplus_R B$.

Produtos tensoriais são usados para estender o anel de escalares de um módulo. Seja A um R-módulo e suponha que R é um subanel de um anel L. Então L é também um R-módulo sobre a multiplicação por elementos de R e podemos formar um R-módulo $A \otimes_R L$. Para ilustrar a definição de produto tensorial, seguiremos com um exemplo.

Exemplo 1.1.3. *Considere o $\mathbb{Z}$-módulo $\mathbb{Z} \times \mathbb{Z}$ e veja que $\mathbb{Z}$ é um subanel de $\mathbb{C}$. Podemos formar o $\mathbb{Z}$-módulo $(\mathbb{Z} \times \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$, que pode ser visto como espaço vetorial sobre $\mathbb{C}$. A base de $\mathbb{Z} \times \mathbb{Z}$ é $\{(1,0),(0,1)\}$ e a base de $\mathbb{C}$ é $\{1\}$, então a base de $(\mathbb{Z} \times \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$ é $\{(1,0) \otimes 1, (0,1) \otimes 1\}$. Vamos estudar a matriz de rotação R,*

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

Em $\mathbb{Z} \times \mathbb{Z}$ temos,

$$R(x,y) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} . \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -y \\ x \end{pmatrix}.$$

Agora, em $(\mathbb{Z} \times \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$, temos que nos elementos da base a rotação age da seguinte forma,

$$R((1,0) \otimes 1) = (0,1) \otimes 1,$$

$$R((0,1) \otimes 1) = (-1,0) \otimes 1.$$

Veja que o autovalor de R é i e os autovetores são da forma $v = (x,0) \otimes i + (0,y) \otimes 1$ para $x, y \in \mathbb{Z}$, isso nos mostra que

$$Rv = iv$$

para todo $(x,y) \in \mathbb{Z} \times \mathbb{Z}$, isto é, a rotação age como uma transformação escalar em $(\mathbb{Z} \times \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$.

Agora enunciaremos uma propriedade bem conhecida sobre produto tensorial.

Lema 1.1.18 (Propriedade Fundamental do Produto Tensorial)**.** *Um mapeamento $\phi : A \times B \to C$ induz um homomorfismo do R-módulo $A \otimes_R B$ para o R-módulo C pela regra $a \otimes b \mapsto (a,b)^{\phi}$, se e somente se, as seguintes igualdades valem.*

1. $(ra_1, b_1)^\phi = (a_1, rb_1)^\phi = r(a_1, b_1)^\phi$;

2. $(a_1, b_1 + b_2)^\phi = (a_1, b_1)^\phi + (a_1, b_2)^\phi$;

3. $(a_1 + a_2, b_1)^\phi = (a_1, b_1)^\phi + (a_2, b_1)^\phi$.

Para $r \in R$, $a_1, a_2 \in A$ e $b_1, b_2 \in B$.

Com o conhecimento do produto tensorial, estudaremos propriedades importantes da série central inferior de um grupo G. O resultado abaixo também pode ser visto em 1.2 de [13].

Teorema 1.1.19 (Robinson)**.** *Suponha que G é um grupo e defina $F_i = \gamma_i(G)/\gamma_{i+1}(G)$. Então o mapeamento*

$$a(\gamma_{i+1}(G)) \otimes gG' \mapsto [a, g]\gamma_{i+2}(G),$$

com $a \in \gamma_i(G)$ e $g \in G$ determina um homomorfismo sobrejetivo bem definido de $F_i \otimes_{\mathbb{Z}} G_{ab}$ para F_{i+1}.

Demonstração. Se $g \in G$ e $a \in G_i$, onde $G_i = \gamma_i(G)$, considere o mapeamento

$$(aG_{i+1}, gG') \mapsto [a, g]G_{i+2}.$$

Esse mapeamento é bem definido pois, se $x \in G'$, então

$$[a, gx] = [a, x][a, g]^x \equiv [a, g] \bmod G_{i+2}$$

já que $[G_i, G'] \leq G_{i+2}$. Da mesma forma, se $y \in G_{i+1}$, temos que

$$[ay, g] = [a, g]^y[y, g] \equiv [a, g] \bmod G_{i+2}.$$

O mapeamento é bilinear, pois para $[a_1a_2, g] = [a_1, g][a_1, g, a_2][a_2, g]$ e $[a_1, g, a_2] \in G_{i+2}$, então

$$[a_1, g, a_2] \equiv [a_1, g][a_2, g] \bmod G_{i+2}.$$

Da mesma forma, $[a, g_1g_2] \equiv [a, g_1][a, g_2] \bmod G_{i+2}$.

Pela propriedade fundamental do produto tensorial (sobre $\mathbb{Z}$), existe um homomorfismo induzido,

$$\begin{aligned} \varepsilon_i : (G_i/G_{i+1}) \otimes_{\mathbb{Z}} G_{ab} &\to G_{i+1}/G_{i+2} \\ aG_{i+1} \otimes gG' &\mapsto [a, g]G_{i+2} \end{aligned}$$

onde $a \in G_i$ e $g \in G$. Veja que ε_i é sobrejetivo pois $G_{i+1} = [G_i, G]$. □

Teorema 1.1.20. *Seja $\mathfrak{P}$ um propriedade teórica de grupos que é preservada por imagens de produtos tensoriais e suponha que G é um grupo tal que G_{ab} possui $\mathfrak{P}$. Então $\gamma_i(G)/\gamma_{i+1}(G)$ possui $\mathfrak{P}$ para $i = 2, 3, ...$*

Demonstração. Suponha que $F_i = \gamma_i(G)/\gamma_{i+1}(G)$ possua $\mathfrak{P}$, então como F_{i+1} é a imagem de $F_i \otimes_{\mathbb{Z}} G_{ab}$, F_{i+1} possui $\mathfrak{P}$ e então cada fator da série central inferior possui $\mathfrak{P}$. □

A combinação desses dois teoremas acima será chamado posteriormente de Argumento do Produto Tensorial.

1.1.3 Álgebra Linear

A seguir enunciaremos o Teorema da Decomposição Cíclica, que será um resultado importante para concluir o Teorema D. Os resultados sobre álgebra linear deste capítulo baseiam-se principalmente em [8].

Se V é um espaço vetorial de dimensão finita sobre o corpo F, T um operador linear fixo(mas arbitrário) de V, α um vetor qualquer sobre V, então existe um menor subespaço de V que é invariante por T e contém α. Assim, podemos considerar W um subespaço arbitrário de V que seja invariante por T e contenha α, então certamente deve conter os vetores α^T, α^{T^2}, α^{T^3}, e assim por diante. A saber, W deve conter $\alpha^{g(T)}$, para todo polinômio $g(X)$ em $F[X]$.

Definição 1.1.21. *Se a é um vetor qualquer em V, o subespaço T-cíclico gerado por α é o subespaço $Z(\alpha; T)$ dos vetores da forma $\alpha^{g(T)}$, onde $g(X)$ em $F[X]$. Se $Z(\alpha; T) = V$, então α é denominado um vetor cíclico de T.*

Teorema 1.1.22. *Sejam α um vetor não nulo arbitrário em V e p_α o vetor unitário que gera o ideal em $F[X]$ formado pelos polinômios que, aplicados em T, se anulam. Se o grau de p_α é k, então os vetores α, α^T ..., $\alpha^{T^{k-1}}$ formam uma base para $Z(\alpha; T)$.*

Considere um operador linear T sobre um epaço W de dimensão k que possua um vetor cíclico α. Pelo Teorema anterior, os vetores α, ..., $\alpha^{T^{k-1}}$ formam uma base do espaço W e o anulador p_α de α é o polinômio minimal de T. Se fizermos $\alpha_i = \alpha^{T^{i-1}}$, $1 \leq i \leq k$, então a ação de T sobre a base ordenada $\mathcal{B} = \{\alpha_1, ..., \alpha_k\}$ é

$$\alpha_k^T = -c_0\alpha_1 - c_1\alpha_2 - ... - c_{k-1}\alpha_k,$$

onde $p_\alpha = c_0 + c_1 x + ... + c_{k-1}x^{k-1} + x^k$. Isto diz que a matriz de T em relação a base ordenada $\mathcal{B}$ é

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{pmatrix}.$$

Definição 1.1.23. *A matriz acima é denominada matriz associada ao polinômio p.*

Definição 1.1.24. *Sejam T um operador linear sobre um espaço vetorial V e W um subespaço de V. Dizemos que W é T-admissível se*

1. *W é invariante sob T;*
2. *se $\beta^{f(T)}$ está em W, existe um vetor γ em W tal que $\beta^{f(T)} = \gamma^{f(T)}$.*

onde f é um polinômio sobre o corpo de escalares e β é um vetor.

A seguir temos o famoso Teorema da Decomposição Cíclica. Uma demonstração pode ser encontrada em 7.2.3 de [8].

Teorema 1.1.25 (Teorema da Decomposição Cíclica)**.** *Sejam T um operador linear sobre um espaço vetorial V de dimensão finita e W_0 um subespaço próprio T-admissível de V. Então existem vetores não-nulos $\alpha_1, .., \alpha_r$ em V com respectivos T-anuladores $p_1, ..., p_r$ tais que*

1. *$V = W_0 \oplus Z(\alpha_1; T) \oplus ... \oplus Z(\alpha_r; T)$;*
2. *p_k divide p_{k-1}, $k = 2, .., r$.*

Além disso, o inteiro r e os anuladores $p_1, ..., p_k$, são determinados de modo único por 1, 2 e pelo fato de que nenhum α_k é nulo.

1.2 Representações de Grupos

Nessa seção vamos estabelecer os resultados envolvendo Representações de Grupos que precisaremos posteriormente, mas que não dependem de Teoria de Caracteres.

Seja π uma representação permutacional de um grupo G em um conjunto X. Podemos considerar os elementos de X como base de um espaço vetorial V sobre um corpo F arbitrário e, assim, representar os elementos de $(G)\pi$ como transformações lineares de V representadas por matrizes apropriadas em relação a uma dada base.

Dessa forma, π induz um homomorfismo de G no grupo dos operadores lineares (não singulares) de V sobre F. Ou equivalentemente, no grupo das matrizes $n \times n$ (não singulares) com coeficientes em F. Denotaremos o grupo dos operadores lineares (não singulares) de V sobre F por $GL(V, F)$. E o grupo das matrizes $n \times n$ (não singulares) com coeficientes em F por $GL(n, F)$, onde n é a dimensão do espaço vetorial V sobre F. Para cada base $\mathcal{B} = \{v_i, ..., v_n\}$ de V sobre F, associamos para cada T em $GL(V, F)$ a matriz $T_{\mathcal{B}}$ de T em relação a base dada. O mapeamento $\alpha_{\mathcal{B}} : T \to T_{\mathcal{B}}$ é um isomorfismo de $GL(V, F)$ em $GL(n, F)$.

Definição 1.2.1. *Um homomorfismo ϕ de um grupo G para o grupo $GL(V, F)$ é chamado de representação de G. V é denominado espaço de representação ou módulo de representação. Podemos dizer que ϕ é uma representação de G em F.*

Definição 1.2.2. *O núcleo K de ϕ é chamado de núcleo da representação de G em V sobre F. Onde*

$$K = \{g \in G | g^{\phi} = 1_{GL(V,F)}\}.$$

Se ϕ é injetiva, G é mapeado isomorficamente em $GL(V)$ e o núcleo da representação K é trivial, nesse caso, diremos que ϕ é uma representação fiel.

Definição 1.2.3. *Se $G = K$, então a representação é chamada trivial.*

Definição 1.2.4. *A dimensão de V sobre $F (dim_F(V))$ é dita grau de ϕ. As representações de grau 1 são chamadas representações lineares.*

Exemplo 1.2.1. *Seja $G = D_8 = \langle a, b | a^4 = b^2 = 1, bab = a^{-1} \rangle$ o grupo diedral de ordem 8. Defina as matrizes A e B por,*

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

e veja que

$$A^4 = B^2 = I, B^{-1}AB = A^{-1}.$$

A função $\rho : G \to GL(2, \mathbb{R})$ dada por $a^i b^j \mapsto A^i B^j$ onde $0 \leq i \leq 3$ e $j = 0, 1$ é uma representação de D_8 sobre $\mathbb{R}$ de grau 2. Explicitando o mapeamento dos elementos g do grupo D_8 em matrizes, temos,

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, (a)\rho = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$(a^2)\rho = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, (a^3)\rho = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$(b)\rho = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, (ab)\rho = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix},$$

$$(a^2b)\rho = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, (a^3b)\rho = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Definição 1.2.5. *Considere ϕ uma representação de G em V sobre F, W um subespaço de V invariante por $(G)\phi$ e ψ um homomorfismo natural de V em V/W, a composição $\phi\psi$ é um homomorfismo de G em $GL(V/W, F)$ que é dito representação quociente de G em V/W induzida por ϕ.*

Definição 1.2.6. *Uma representação ϕ de um grupo G em um espaço vetorial V sobre um corpo F é dita irredutível se 0 e V são os únicos subespaços $(G)\phi$-invariantes de V. Caso contrário, ϕ é dito redutível.*

Definição 1.2.7. *A representação ϕ é indecomponível se não é possível escrever V como soma direta de dois subespaços não triviais $(G)\phi$-invariantes. Caso contrário, ϕ é decomponível.*

Definição 1.2.8. *Dizemos que uma representação ϕ de G em V sobre F é completamente redutível se existe a decomposição*

$$V = V_1 \oplus ... \oplus V_r,$$

onde V_i é um subespaço $(G)\phi$-invariante de V e $\phi|_{V_i}$ é irredutível, para $1 \leq i \leq r$.

Sejam ϕ uma representação de G em V sobre F e $(v), (v')$ duas bases de V sobre F. Então para $x \in G$, temos que

$$(x\phi)_{(v')} = P^{-1}(x\phi)_{(v)}P,$$

onde P é a matriz mudança de base de (v) em (v'). Assim uma dada representação de ϕ determina representações matriciais de G. Também podemos considerar duas representações ϕ e ϕ' de G nos espaços vetoriais V e V' sobre F, P é uma matriz de um isomorfismo ψ de V em V' mapeando os elementos de (v) no correspondentes em (v') em para cada $x \in G$ temos

$$(x\phi')_{(v')} = P^{-1}(x\phi)_{(v)}P.$$

Definição 1.2.9. *Duas representações ϕ e ϕ' de G nos espaços vetoriais V e V' respectivamente sobre F são equivalentes se existe um isomorfismo ψ de V em V' em que*

$$u\psi(x\phi') = u(x\phi)\psi \qquad\qquad \forall x \in G, u \in V.$$

Lema 1.2.10. *([6] Lema 3.1.1) Sejam ϕ uma representação de G em V sobre F e U e W subespaços de V que são $(G)\phi$-invariantes tal que $U \cap W = 0$. Sejam $\bar{\phi}$ a representação quociente de G em $\bar{V} = V/W$ e $\bar{U}$ a imagem de U em $\bar{V}$. Então $\bar{U}$ é $(G)\bar{\phi}$-invariante e $\phi|_U$ é equivalente a $\bar{\phi}_{\bar{U}}$.*

Definição 1.2.11. *Sejam V um espaço vetorial sobre o corpo F e G um grupo. Então V é um FG-módulo se a multiplicação vg está bem definida para todo $v \in V$ e $g \in G$, satisfazendo as seguintes condições para $u, v \in V$, $\lambda \in F$ e $g, h \in G$,*

1. *$vg \in V$;*
2. *$v(gh) = (vg)h$;*
3. *$v1 = v$;*
4. *$(\lambda v)g = \lambda(vg)$;*
5. *$(u + v)g = ug + vg$.*

Exemplo 1.2.2. *Sejam $D_8 = \langle a, b | a^4 = b^2 = 1, ab = a^{-1} \rangle$ e $\rho : D_8 \to GL(2, \mathbb{R})$ a representação como foi dada anteriormente. Tomando o espaço vetorial $\mathbb{R}^2$ sobre o corpo $\mathbb{R}$ e G a imagem de ρ, temos que $\mathbb{R}^2$ é um FG-módulo.*

O próximo conceito envolve estender o corpo base. Considere V um FG-módulo e $|G| = m$. Então cada elementos de x em G determina uma transformação linear T_x de V de ordem dividindo m, tal que T_x satisfaz o polinômio $X^m - 1$. Então para cada x em G, as raízes características de T_x são raízes m-ésimas da unidade sobre F. Podemos considerar que a extensão $F(\omega)$ contém todas essas raízes da unidade, onde ω é uma m-ésima raiz da unidade. Em várias circunstâncias a análise se torna mais simples de

o corpo F contém uma m-ésima raiz primitiva da unidade ou é algebricamente fechado. Caso isso não ocorra será necessário substituir V por um espaço vetorial apropriado sobre a extensão L de F.

Para descrever esse processo, sejam V um espaço vetorial sobre F e L uma extensão de F. Podemos construir o produto tensorial $V_L = V \otimes_F L$, que é um espaço vetorial sobre L.

Uma vez que um espaço vetorial é visto como FG-módulo, as definições que foram apresentadas anteriormente para módulos e representações podem ser interpretadas no contexto de FG-módulos. Tais noções são equivalentes.

Agora vamos estudar algumas propriedades de representações de grupos abelianos. Tais resultados ajudarão a demonstrar um dos teoremas principais sobre classificação de grupos com uma quantidade finita de órbitas por automorfismos.

Lema 1.2.12. *Seja V um FG-módulo irredutível. Se $z \in Z(G)$ tem raiz característica λ em F, então $vz = \lambda v$, para todo $v \in V$. Em particular, se V é um FG-módulo fiel, $z = 1$ ou $\lambda \neq 1$.*

Demonstração. Seja $W = \{w \in W | wz = \lambda w\}$, tal que por hipótese $W \neq 0$. W é um subespaço de V. Além disso, se $x \in G$ e $w \in W$, temos

$$(wx)z = w(xz) = w(zx) = (wz)x = (\lambda w)x = \lambda(wx)$$

pois $z \in Z(G)$. Assim, $wx \in W$ e consequentemente W é um G-invariante. Mas pela irredutibilidade de G em V, temos que $W = V$, onde $vz = \lambda v$ para todo $v \in V$. Além disso, se G age fielmente em V e $z \neq 1$, então z não induz a transformação linear identidade em V, então $\lambda \neq 1$.

□

Para mais detalhes sobre os sguintes resultados confira [6].

Teorema 1.2.13. *([6] Teorema 3.2.2) Se G possui uma representação irredutível fiel, então $Z(G)$ é cíclico.*

Teorema 1.2.14. *([6] Teorema 3.2.3) Se ϕ é uma representação de um grupo abeliano G com núcleo K, então G/K é cíclico. Em particular, um grupo abeliano não cíclico não possui uma representação fiel irredutível.*

Teorema 1.2.15. *([6] Teorema 3.2.4) Sejam G um grupo abeliano de ordem n e F um corpo que contém uma n-ésima raiz primitiva da unidade. Então toda representação de G sobre F é linear.*

Teorema 1.2.16. *([6] Teorema 3.2.5) Se ϕ é uma representação linear de G, então G/K é cíclico, onde K é o núcleo de ϕ. Em particular, um grupo não cíclico não possui representação fiel de grau 1.*

Agora, vamos estabelecer critérios suficientes para que uma certa representação seja completamente redutível.

Teorema 1.2.17 (Maschke)**.** *([6] Teorema 3.3.1) Seja ϕ uma representação de G em V/F e suponha que F tem característica 0, ou tem característica coprima com $|G|$. Então ϕ é completamente redutível.*

A seguir apresentamos uma aplicação do Teorema de Maschke.

Teorema 1.2.18. *Sejam P um p-grupo abeliano elementar e Q um q-subgrupo abeliano não cíclico de $Aut(P)$, com q um primo distinto de p. Então,*

$$P = \prod_{x \in Q^*} C_P(x).$$

Em particular, P é gerado por seus subgrupos $C_P(x)$ com x em Q^*.

Demonstração. Considere P um espaço vetorial sobre $\mathbb{Z}_p$ e P com um Q-módulo. Como $p \neq q$, o Teorema de Maschke afirma que P é um Q-módulo completamente redutível. Por isso,

$$P = P_1 \oplus ... \oplus P_n$$

onde P_i é um Q-módulo irredutível de P, $1 \leq i \leq n$. Como Q é abeliano, sabemos que Q/Q_i é cíclico, onde Q_i denota o núcleo da representação de Q em P_i. Mas Q é não cíclico, então isso mostra que $Q_i \neq 1$, $1 \leq i \leq n$. Escolhendo x_i em Q_i^* temos que $P_i \subseteq C_P(x_i)$, donde,

$$P = \sum_{i=1}^{n} C_P(x_i) \subseteq \sum_{x \in Q^*} C_P(x).$$

Voltando para a notação multiplicativa, o teorema segue. □

Podemos generalizar esse teorema considerando um espaço vetorial de dimensão finita e obtemos,

Teorema 1.2.19. *Sejam V um espaço vetorial de dimensão finita sobre um corpo F e Q um q-subgrupo abeliano não cíclico de $Aut(V)$, com q um primo distinto da característica de F. Então,*

$$V = \prod_{x \in Q^*} C_V(x).$$

Em particular, V é gerado por seus subgrupos $C_V(x)$ com x em Q^*.

Se existe uma representação irredutível de G em V/F e H é um subgrupo normal de G, é possível determinar como o espaço V se decompõe sobre a ação de H. Essa questão é abordada no teorema a seguir. Encerraremos a seção com a abordagem dessa questão no teorema a seguir. A demonstração também pode ser encontrada em 4.4.1 de [6].

Teorema 1.2.20 (Clifford)**.** *Sejam G um grupo, F um corpo e V um FG-módulo irredutível com dimensão finita sobre F. Considere H um subgrupo normal de G. Então V é a soma direta de subespaços H-invariantes V_i, $1 \leq i \leq r$, que satisfazem:*

1. *$V_i = X_{i1} \oplus ... \oplus X_{it}$, onde cada X_{ij} é um FH-submódulo irredutível, $1 \leq i \leq r$, t é independente de i, e X_{ij}, $X_{i'j'}$ são FH-submódulos irredutíveis se e somente se $i = i'$.*

2. *Para qualquer FH-submódulo U de V, temos que $U = U_1 \oplus ... \oplus U_r$, onde $U_i = U \cap V_i$, $1 \leq i \leq r$. Em particular, se U é irredutível, então U está contido em algum dos V_i.*

3. *Se $x \in G$, o mapeamento $(x)\pi : V_i \to V_i x$, $1 \leq i \leq r$ é uma permutação do conjunto $S = \{V_1, ..., V_r\}$ e π induz uma representação permutacional transitiva de G em S. Além disso, $HC_G(H)$ está contido no núcleo de π.*

Demonstração. Primeiramente, vamos mostrar que V é a soma direta de FH-submódulos irredutíveis. Seja W um FH-submódulo de V. Se $x \in G$, considere $W^x = \{wx | w \in W\}$. Veja que W^x é um subespaço de V, além disso,

$$(wx)h = w(xh) = w(xhx^{-1}x) = w(h^{x^{-1}}x) = (wh^{x^{-1}})x$$

onde $wx \in W^x$, $h \in H$, temos que $(wx)h \in W^x$ pois H é um subgrupo normal de G. Então W^x é um FH-submódulo de V, que não necessariamente é isomorfo a W. Por outro lado, o mapeamento $U \mapsto U^x$ determina uma correspondência injetiva entre os FH-submódulos de W e os FH-submódulos de W^x, pois $W = (W^x)^{x^{-1}}$. Em particular, W^x é irredutível se, e somente se, W é simples. Além disso, se Y é um H-submódulo de V que é isomorfo a W sobre um FH-isomorfismo θ podemos verificar que W^x e Y^x são FH-módulos isomorfos em relação ao H-isomorfismo $x^{-1}\theta x$.

$$(wx)x^{-1}\theta x = w\theta x = yx$$

Agora seja $W = W_1 \oplus ... \oplus W_s$ onde W_i são FH-submódulos irredutíveis de V e $1 \leq i \leq s$, onde s é escolhido como maximal. Suponha que $W_i^x \not\subseteq W$, para algum

i e x em G. Então $W_i^x \cap W$ é um FH-submódulo próprio de W_i^x, e pela simplicidade, $W_i^x \cap W = 0$. Então $W_i^x + W = W_i^x \oplus W$, o que contradiz a escolha de s maximal. Portanto, $W_i^x \subseteq W$ para todo i e x, donde W é G-invariante. Como V é um FG-módulo irredutível, concluímos que $W = V$. Assim, V é a soma direta de FH-submódulos irredutíveis.

Renomeando W_i por X_{ij} tal que X_{ij} e $X_{i'j'}$ são isomorfos se e somente se $i = i'$ e $V_i = X_{i1} \oplus ... \oplus X_{it_i}$, $1 \leq i \leq r$. Como V é a soma direta de FH-submódulos irredutíveis, segue que $V = V_1 \oplus ... \oplus V_r$. Mas ainda não sabemos que t_i é independente de i, isso será provado posteriormente.

Agora, vamos mostrar *2.*, seja U um FH-submódulo de V. Pela irredutibilidade de W_j, a suposição que algum $W_{j_1} \not\subseteq U$ implica que $U \cap W_{j_1} = 0$ e então $U + W_{j_1} = U \oplus W_{j_1}$. Repetindo esse argumento, existe j_k, $1 \leq k \leq e$, tal que

$$V^* = U \oplus W_{j_1} \oplus W_{j_2} \oplus ... \oplus W_{j_e}$$

é uma soma direta e que $W_j \subseteq V^*$ para todo $1 \leq k \leq s$. Mas V é a soma direta de W_j, isso mostra que $V = V^*$. Nomeando V' como a soma direta de W_{j_k}, $1 \leq k \leq e$, e V'' a soma direta de W_j, obtemos que

$$V = U \oplus V' \text{ e } V = V'' \oplus V'$$

Mas pelo Lema 1.2.10 tanto U quanto V'' são FH-módulos isomorfos a V/V' e consequentemente, U é um FH-módulo isomorfo a V''. Segue que qualquer FH-submódulo U de V é a soma direta de FH-submódulos irredutíveis. Se *2.* vale para esses submódulos irredutíveis, então vale para U, portanto, é suficiente provar *2.* para quando U é um FH-submódulo irredutível.

Seja $W'_m = W_1 \oplus ... \oplus W_m$ e escolha m maximal tal que $U \not\subseteq W'_m$. Como $W'_s = V$, $1 \leq m < s$. Além disso, $U \subseteq W'_{m+1} = W'_m \oplus W_{m+1}$. U é irredutível, logo $U \cap W'_m = 0$, então $W'_m + U = W'_m \oplus U \subseteq W'_m \oplus W_{m+1}$. Mas U é isomorfo a um FH-submódulo irredutível não trivial de W'_{m+1}/W'_m que é isomorfo a W_{m+1}. Concluímos que U e W_{m+1} são FH-módulos isomorfos. Suponha que $W_{m+1} \subseteq V_i$, vamos mostrar que $U \subseteq V_i$.

Se $U \not\subseteq V_i$, então U é mapeado isomorficamente em um submódulo irredutível de V/V_i. Mas V/V_i é isomorfo a soma direta aos W_j que não são isomorfos a W_{m+1} e então não é isomorfo a U. Por outro lado, o argumento anterior pode ser repetido em V/V_i para imagem de U, para mostrar que essa imagem e também U é isomorfa a algum W_j que sobrou, uma contradição. Então $U \subseteq V_i$ e então *2.* vale.

Agora, seja $x \in G$, mostramos que X_{ij}^x é um FH-submódulo irredutível e então isomorfo a $X_{i'j'}$ para algum i' e j'. Sabemos que X_{ij}^x e X_{ik}^x são FH-módulos isomorfos para

todo j, k, $1 \leq j,k \leq t_i$. Então i' depende apenas de i e não da escolha de j. Segue que $V_i^x \subseteq V_{i'}$. Além disso, como V é um FG-módulo irredutível, devemos ter $V = \langle V_i^x | x \in G \rangle$ para todo i, $1 \leq i \leq r$. Isso significa que para cada escolha de i, i', $1 \leq i,i' \leq r$, existe um elemento $x_{ii'}$ em G tal que $V_i^{x_{ii'}} \subseteq V_{i'}$. Em particular, $dim_F V_i \leq dim_F V_{i'}$ para todo i, i', donde $dim_F V_i = dim_F V_{i'}$ para todo i e i'. Mas para qualquer i e qualquer $x \in G$, V_i^x tem a mesma dimensão que V_i e $V_i^x \subseteq V_i$ para algum i'. Segue que então que $V_i^x = V_{i'}$. Nós mostramos que o mapeamento $(x)\pi : V_i \to V_i^x = V_i x$ é uma permutação do conjunto $S = \{V_1, ..., V_r\}$. Como $V_i^{xy} = (V_i^x)^y$ para qualquer x e y em G,

$$(x)\pi \circ (y)\pi = (xy)\pi$$

π é um homomorfismo e então é uma representação permutacional de G em S. Além disso, como os elementos $x_{1i'}$, $1 \leq i' \leq r$, mapeiam V_1 em $V_{i'}$, π é transitivo. Ademais, X_{1j} e $X_{1j}^{x_{1i'}}$ tem a mesma dimensão para todo j, $1 \leq j \leq t_1$. Como V_1 e $V_{i'}$ também tem a mesma dimensão, podemos concluir que $t_1 = t_{i'}$ para todo i'. Então t_i é independente de i.

Finalmente, vamos mostrar que $HC_G(H)$ está contido no núcleo de π. Como cada V_i é um FH-módulo, H está contido no núcleo de π. Então precisamos mostrar que $C_G(H)$ está no núcleo de π, ou, equivalentemente, $V_i^x = V_i$ para todo i, $1 \leq i \leq r$, e todo $x \in C_G(H)$. Pelo argumento anterior, o resultado segue se provarmos que se $x \in C_G(H)$ então X_{ij} e X_{ij}^x são FH-módulos isomorfos. Seja ψ_x o isomorfismo de X_{ij} em X_{ij}^x dado por $v\psi_x = vx$ para $v \in X_{ij}$. Como $hx = xh$ para todo $h \in H$, temos que

$$v\psi_x h = vh\psi_x$$

para v em X_{ij}, h em H e x em $C_G(H)$. Agora segue da definição que X_{ij} e X_{ij}^x são FH-módulos isomorfos para todo x em $C_G(H)$ e o teorema está provado.

□

Definição 1.2.21. *Os subespaços V_i, $1 \leq i \leq r$, são chamados de componentes de Wedderburn de V em relação a H.*

1.3 Grupos Lineares

Esta seção tem como objetivo introduzir e estabelecer resultados sobre Grupos Lineares, com o objetivo de demonstrar um dos teoremas de Mal'cev. Para mais detalhes confira [13].

Sejam R um anel comutativo com unidade e $GL(n, R)$ o grupo de todas as matrizes $n \times n$ com entradas em R. Nesse caso para que um elemento seja inversível, é necessário que o determinante da matriz seja uma unidade do anel R.

Definição 1.3.1. *Um grupo G é dito R-linear de grau n se é isomorfo a um subgrupo de $GL(n, R)$.*

Exemplo 1.3.1. *O grupo diedral D_n é $\mathbb{R}$-linear para qualquer n. O grupo tem representação*

$$D_{2n} = \langle a, b | a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle$$

Sejam

$$a = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, b = \begin{pmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & -\cos\frac{2\pi}{n} \end{pmatrix}.$$

O grupo $\langle a, b \rangle$ é um subgrupo de $GL(2, \mathbb{R})$ e satisfaz as condições do grupo diedral.

Exemplo 1.3.2. *O grupo diedral infinito, D_∞ é $\mathbb{Z}$-linear de grau 2. Onde*

$$D_\infty = \langle a, b | a^2 = b^2 = 1 \rangle.$$

Basta considerar

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

o grupo $\langle a, b \rangle$ é um subgrupo de $GL(2, \mathbb{Z})$ e satisfaz as condições do grupo diedral infinito.

Estamos interessados nos casos em que R é um corpo ou $\mathbb{Z}$, portanto se G é um grupo F-linear de grau n e F é um corpo, será dito apenas que G é um grupo linear.

A seguir enunciaremos vários resultados sem a demonstração, como referência temos o Capítulo 3.1 de [13].

Teorema 1.3.2. *Um grupo finito G é R-linear de grau $|G|$ para qualquer anel R com identidade.*

Teorema 1.3.3 (Alternativa de Tits)**.** *Seja G um grupo linear sobre um corpo F.*

1. *Se $char(F) = 0$, então G é virtualmente solúvel ou G possui um subgrupo livre de posto 2;*

2. *Se $char(G) \neq 0$ e G é finitamente gerado, o mesmo resultado segue.*

Teorema 1.3.4. *Um grupo linear finitamente gerado é residualmente finito.*

Definição 1.3.5. *Seja G um grupo R-linear de grau n, onde R é um anel comutativo com unidade. G é dito triangulizável se para algum $g \in GL(n, R)$ o grupo G^g é triangular, ou seja, G é um conjugado de um subgrupo de $T_n(R)$, o grupo das matrizes triangulares (superiores) com unidades na diagonal.*

Definição 1.3.6. *G é dito unitriangulizável se é isomorfo a um subgrupos de $UT_n(R)$, o grupo de matrizes unitriangulares em $GL(n, R)$(ie, matrizes triangulares superiores com 1 na diagonal).*

Definição 1.3.7. *G é dito diagonalizável, se é isomorfo ao grupo de matrizes diagonais em $GL_n(R)$, isto é, um subgrupo de $U(R) \times U(R) \times ... \times U(R)$, com n fatores. Nesse caso, $U(R)$ denota o grupo de unidades de R.*

Com essas definições, temos o seguinte teorema

Teorema 1.3.8. *As seguintes afirmações são verdadeiras,*

1. *Um grupo linear diagonalizável é abeliano.*

2. *Um grupo linear unitriangulizável é nilpotente.*

3. *Um grupo linear triangulizável é nilpotente-por-abeliano.*

Demonstração. 1. Como já foi definido, se G é um grupo linear diagonalizável, então é isomorfo a um subgrupo de $U(R) \times U(R) \times ... \times U(R)$, com n fatores, onde $U(R)$ denota o grupo de unidades de R que por sua vez é abeliano. Assim, o resultado segue.

2. Se E é um anel com identidade e S é um subanel de E, denote por

$$S^i = \left\{ \sum l_{x_1 \ldots x_i} x_1 \ldots x_i | x_j \in S, l_{x_1 \ldots x_i} \in \mathbb{Z} \right\}.$$

Então S^i é um subanel de S. Agora suponha que S é um subanel nilpotente, isto é, $S^n = 0$ para algum $n > 0$ e defina $U = \{1 + x | x \in S\}$. Então, vamos provar que U é nilpotente de classe no máximo $n - 1$, onde

$$1 = U_n \lhd U_{n-1} \lhd ... \lhd U_1 = U$$

é a série central e $U_i = \{1 + x | x \in S^i\}$. Primeiramente, veja que U é um grupo com a multiplicação, pois $1 \in U$ e a U é fechado em relação a multiplicação. A existência do elemento neutro vem do fato que $S^n = 0$ e

$$1 = 1 - x^n = (1 + x)(1 - x + x^2 - ... + (-1)^{n-1}x^{n-1}).$$

Para provar a nilpotência, suponha que $x \in S^i$ e $y \in S^j$, então

$$\begin{aligned}[1 + x, 1 + y] &= (1 + x)^{-1}(1 + y)^{-1}(1 + x)(1 + y) \\ &= ((1 + y)(1 + x))^{-1}(1 + x)(1 + y) \\ &= (1 + y + x + yx)^{-1}(1 + x + y + xy).\end{aligned}$$

Agora, defina $u = x + y + xy$ e $v = y + x + yx$. Então,

$$\begin{aligned}[1 + x, 1 + y] &= (1 + v)^{-1}(1 + u) \\ &= (1 - v + v^2 - ... + (-1)^{n-1}v^{n-1})(1 + u) \\ &= 1 + (1 - v + ... + (-1)^{n-2}v^{n-2})(u - v) + (-1)^{n-1}v^{n-1}u.\end{aligned}$$

Como $u - v = xy - yx \in S^{i=j}$ e $v^{n-1}u \in S^n = 0$ temos que $[1 + x, 1 + y] \in 1 + S^{i=j}$ segue que $[U_i, U_j] \leq U_{i+j}$, em particular, $[U_i, U] \leq U_{i+1}$ e a série de U_i's formam uma série central, como queríamos.

Tomando E como sendo o anel de todas as matrizes $n \times n$ sobre um anel comutativo R com unidade, e S o subanel de todas as matrizes com 0's nas diagonais e abaixo delas,

$$\begin{pmatrix} 0 & x_{12} & x_{13} & \dots & x_{1n} \\ 0 & 0 & x_{23} & \dots & x_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Contas básicas de multiplicação de matriz nos mostram que S^i, definido anteriormente, aplicado nesse caso, nos dá um conjunto de matrizes cujas $i - 1$ primeiras superdiagonais são 0, de tal forma que $S^n = 0$. As superdiagonais as quais estamos nos referindo são enumeradas conforme sua posição em relação a diagonal principal.

Assim, o grupo U definido anteriormente, é exatamente o grupo de matrizes unitriangulares, então segue que U é nilpotente e tem classe de nilpotência no máximo $n - 1$.

3. Seja G um grupo triangulizável. Então é isomorfo a um subgrupo H de $T_n(R)$. O

mapeamento de cada matriz triangular em sua diagonal, nos dá um homomorfismo

$$\varphi : T_n(R) \to U(R) \times U(R) \times ... \times U(R)$$

cujo núcleo é o grupo nilpotente $U_n(R)$. Pelo Teorema do Homomorfismo, segue que $G/U_n(R)$ é isomorfo a um subgrupo de $U(R) \times U(R) \times ... \times U(R)$, que por sua vez é abeliano. E o resultado segue.

□

Suponha que $V = V_1 \oplus ... \oplus V_k$ é a decomposição de m FG-módulo V em submódulos, e suponha que V tem dimensão finita sobre F. Sejam ϕ e ϕ_i a representação de G nos módulos V e V_i, respectivamente. Então ϕ é a soma direta das representações ϕ_i

$$\phi = \phi_1 \oplus ... \oplus \phi_k.$$

Escolhendo uma base para cada V_i, ao tomar a união formamos uma base para V a representação matricial fica

$$x^{\phi *} = \begin{pmatrix} x^{\phi_1 *} & & & 0 \\ & x^{\phi_2 *} & & \\ & & \ddots & \\ 0 & & & x^{\phi_k *} \end{pmatrix}.$$

O objetivo principal desta seção será provar o seguinte teorema,

Teorema 1.3.9 (Mal'cev 1951)**.** *Sejam V um espaço vetorial de dimensão finita n sobre um corpo algebricamente fechado F e G um subgrupo solúvel de $GL(V, F)$.*

1. *Se G é irredutível, então G possui um subgrupo normal diagonalizável D tal que $|G : D| \leq g(n)$ para alguma função g;*

2. *Em geral, G possui um subgrupo normal triangulizável T tal que $|G : T| \leq f(n)$ para alguma função f.*

Antes de apresentar a demonstração, iremos provar certos fatos que ajudarão na demonstração. O próximo lema foi tirado do livro [5](5.2 Exercício 14).

Lema 1.3.10. *Sejam G um grupo finito abeliano e F um corpo algebricamente fechado. Denotando por F^* o grupo multiplicativo de F, então $G \cong Hom(G, F^*)$.*

Demonstração. Primeiramente, vamos mostrar que $Hom(G, F^*)$ é um grupo abeliano. Considere $\chi, \psi \in Hom(G, F^*)$, definimos a operação $\chi\psi$ se $(g)\chi\psi = (g)\chi(g)\psi$, para

todo $g \in G$. Seja $id \in Hom(G, F^*)$ dada por $(g)id = 1$, para todo $g \in G$, tome $\chi \in Hom(G, F^*)$, como $(g)id\chi = (g)id(g)\chi = (g)\chi$, temos que $id\chi = \chi$. Dado $\chi \in Hom(G, F^*)$ note que o mapeamento χ^{-1} dado por $g \mapsto (g)\chi^{-1}$ é um homomorfismo tal que $(g)\chi(g)\chi^{-1} = 1$. $Hom(G, F^*)$ é um grupo abeliano, pois F^* é abeliano.

Como G é abeliano podemos escrevê-lo como o produto de cíclicos $\langle x_1\rangle \times ... \times \langle x_r\rangle$, onde $|\langle x_i\rangle| = n_i$, $1 \leq i \leq r$. Defina o homomorfismo χ_i de G para F^* que mapeia x_i para uma n_i-ésima raiz da unidade e mapeia x_j para 1, quando $j \neq i$.

Veja que χ_i tem ordem n_i em $Hom(G, F^*)$, pois n_i é o menor natural tal que $((g)\chi_i)^{n_i} = 1$ para todo $g \in G$. Agora, vamos mostrar que $Hom(G, F^*) = \langle\chi_1\rangle \times ... \times \langle\chi_r\rangle$. Se $\psi \in Hom(G, F^*)$, pelo Teorema do Homomorfismo, $G/ker(\psi) \cong Im(\psi) \leq F^*$. Segue que $G/ker(\psi)$ é cíclico pois todo subgrupo finito de um corpo é cíclico. Com isso podemos concluir que $\psi \in \langle\chi_1\rangle \times ... \times \langle\chi_r\rangle$.

□

Definição 1.3.11. *Sejam V um espaço vetorial de dimensão finita sobre um corpo F e G um grupo de $GL(n, V)$. G é chamado imprimitivo se existe uma decomposição*

$$V = V_1 \oplus ... \oplus V_k$$

com $k > 1$, tal que os elementos de G permutam os subespaços V_i. G é chamado primitivo se não é imprimitivo.

O teorema abaixo será a base para a demonstração do Teorema de Mal'cev.

Teorema 1.3.12. *Sejam V um espaço vetorial de dimensão finita n sobre um corpo algebricamente fechado F e G um subgrupo solúvel de $GL(V, F)$. Se G é primitivo e irredutível, então existe um subgrupo escalar S tal que $|G : S| \leq n^2h(n^2)$, onde $h(m)$ é o número máximo de automorfismos de um grupo abeliano de ordem no máximo m.*

Demonstração. Seja A um subgrupo normal e abeliano de G. Pelo Teorema de Clifford, V é um FA-módulo totalmente redutível, visto que G é irredutível. Também pelo Teorema de Clifford, segue que $V = V_1 \oplus ... \oplus V_k$ onde V_i é a soma de todos os FA-submódulos irredutíveis dado um certo tipo de isomorfismo. Além disso, os elementos de G permutam os V_i's. Mas como G é primitivo, segue que $k = 1$, isto é, V é soma direta de FA-módulos irredutíveis e isomorfos.

Por hipótese, F é um corpo algebricamente fechado, então todo elemento de G possui uma raiz característica λ em F e portanto, existe um autovalor e um autovetor que gera um autoespaço irredutível. Assim, um FG-módulo irredutível tem dimensão 1.

Consequentemente, A é escalar e $A \leq Z(G)$. Com isso, concluímos que todo subgrupo abeliano normal é central.

Agora seja B/C um subgrupo normal maximal e abeliano de G/C, onde $C = Z(G)$. Queremos mostrar que

$$|B : C| \leq n^2 \text{ e } C_G(B/C) = B.$$

Daí segue que,

$$|G : B| = |G : C_G(B/C)| \leq |Aut(B/C)| \leq f(n^2)$$

e então $|G : C| \leq n^2 f(n^2)$. Como C é escalar, o resultado segue.

Primeiro suponha que $C_G(B) \neq C$. Então $C_G(B)/C$ contém um subgrupo normal abeliano não-trivial D/C de G/C. Como $[B, D] = 1$, segue que BD/C é abeliano, e pela maximalidade de B/C inferimos que $D \leq B$. Dessa forma $D \leq Z(B)$ e D é abeliano. Já foi mostrado que todo subgrupo abeliano normal é central, logo, $D \leq C$, uma contradição. Então $C_G(B) = C$.

Agora, vamos mostrar que $|B : C| \leq n^2$. Escolha elementos $b_1, b_2, ..., b_r$ de classes laterais diferentes de C em B e suponha que os b_i são linearmente dependentes no espaço vetorial $End_F(V)$. Então existe uma relação não trivial da forma $\sum_{i=1}^{s} f_i b_i = 0$, onde $0 \neq f_i \in F$ com o menor caminho $s \leq r$. Agora, $b_1 b_2^{-1} \notin C$, então $[b_1 b_2^{-1}, x] \neq 1$ para algum x em B; logo $[b_1, x] \neq [b_2, x]$. Como $[b_i, x]$ está em C, é escalar, digamos igual a t_i. Então $t_1 \neq t_2$ e

$$x^{-1} b_i x = b_i b_i^{-1} x^{-1} b_i x = b_i [b_i, x] = t_i b_i.$$

Segue que

$$\begin{aligned} 0 &= t_1 \left(\sum_{i=1}^{s} f_i b_i \right) - x^{-1} \left(\sum_{i=1}^{s} f_i b_i \right) x \\ &= t_1 \left(\sum_{i=1}^{s} f_i b_i \right) - \sum_{i=1}^{s} f_i t_i b_i \\ &= \sum_{i=2}^{s} (t_1 - t_i) f_i b_i. \end{aligned}$$

Pela minimalidade de s deduzimos que $(t_1 - t_2) f_2 = 0$ e $f_2 = 0$, uma contradição. Então b_i são linearmente independentes e $r \leq dim_F(End_F(V)) = n^2$. Portanto, $|B : C| \leq n^2$.

Falta mostrar que $K := C_B(B/C) = B$. Veja que, $B \leq K$ porque B/C é abeliano. Se

$k \in K$, o mapeamento abaixo é um homomorfismo bem definido

$$\begin{aligned} \theta_k : B/C &\to C \\ bC &\mapsto [b,k] \end{aligned}$$

Além disso, o mapeamento

$$\begin{aligned} \theta : K &\to Hom(B/C, C) \\ k &\mapsto \theta_k \end{aligned}$$

determina um homomorfismo de K para $H \coloneqq Hom(B/C, C)$ com núcleo $C_K(B) = C$. Dessa forma, K/C é isomorfo a um subgrupo de H. Mas C é escalar, então temos que $|H| \leq |Hom(B/C, F^*)|$, onde $F^* = U(F)$. Por outro lado, os subgrupo finitos de $U(F)$ são cíclicos, então $|Hom(B/C, F^*)| \leq |B/C|$. Finalmente, $|K : C| \leq |B : C|$ e $|K| \leq |B|$, tal que $K = B$ e a prova está completa.

□

Agora, segue a demonstração do Teorema 1.3.9.

Demonstração. 1. Se G é primitivo, então o resultado segue do Teorema anterior. Então vamos assumir que G é não-primitivo. Existe uma decomposição $V = V_1 \oplus ... \oplus V_k$ onde $k > 1$ e os elementos de G permutam os subespaços V_i. Se $g \in G$, então $V_g = V_{i'}$, onde $g^\pi : i \mapsto i'$ é uma permutação de $\{1, 2, ..., k\}$. Agora $\pi : G \to Sym(k)$ é um homomorfismo e, se seu núcleo é K, então $|G : K| \leq k! \leq n!$. Vamos por indução em n, como base de indução, temos $n = 1$. Nesse caso, temos apenas dois subespaços vetoriais em V. Segue da demonstração do teorema anterior.

Suponha que vale para os espaços vetoriais de dimensão menor que n.

Vamos mostrar que vale para o espaço vetorial de dimensão n. K age sobre cada subespaço V_i como um grupo linear. Como $n_i = dim(V_i) < n$, pela hipótese de indução, $K/C_K(V_i)$ possui um subgrupo normal triangulável $D_1/C_K(V_i)$ tal que $|K : D_i| \leq g(n_i)$. Tomando $D^* = D_1 \cap D_2 \cap ... \cap D_k$, vemos que D^* age diagonalmente em cada V_i, e por isso, age também em V. Ademais,

$$|K : D^*| \leq \prod_{i=1}^{k} g(n_i) \leq \bar{g}(n)^n$$

onde $\bar{g}(n) = max\{g(i) | i < n\}$. Então $|G : D^*| \leq \bar{g}(n)n!$, digamos que $\bar{g}(n)n! = m$. Utilizando o coração normal de D^* obtemos um subgrupo diagonalizável normal D.

2. No caso geral, formamos um série de composição no módulo V, digamos

$$0 = V_0 < V_1 < ... < V_r = V$$

e seja $m_i = dim(V_{i+1}/V_i)$. Como G age como um grupo linear irredutível em V_{i+1}/V_i por 1. existe um subgrupo normal diagonalizável $D_i/C_G(V_{i+1}/V_i)$ tal que $|G : D_i| \leq g(m_i)$. Considere $T = D_1 \cap D_2 \cap ... \cap D_r$. Então T é triangularizável e

$$|G : T| \leq \prod_{i=1}^{r} g(m_i) \leq \bar{g}(n)^n$$

onde $\bar{g}(n) = max\{g(i)|i < n\}$.

□

Teorema 1.3.13. *Seja G um grupo solúvel linear. Então G é nilpotente-por-abeliano-por-finito. E se G é irredutível, então é abeliano-por-finito.*

Demonstração. Como G é um grupo linear, G age em um espaço vetorial V sobre um corpo F. Suponha que $\bar{F}$ é o fecho algébrico de F. Então pelo Teorema de Mal'cev, segue que existe um subgrupo normal T em G que é triangulizável que tem índice finito. Já mostramos que T é nilpotente-por-abeliano. Logo G é nilpotente-por-abeliano-por-finito.

Se G é irredutível e age em um espaço vetorial V sobre um corpo F. Considerando $\bar{F}$ o fecho algébrico desse corpo, e o espaço vetorial $\bar{V} = V \otimes_F \bar{F}$. Temos pelo Teorema de Mal'cev que existe um subgrupo T de G que é triangulizável e de índice finito. Veja que T' age de forma unitriangular em $\bar{V}$ e também em V. Mas o subgrupo $[V, T'] = \langle -v + v^t | v \in V, t \in T' \rangle$ gerado por $v(-1 + t)$ com $v \in V$ e $t \in T'$. Seja $g \in G$ e note que,

$$(v(-1 + t))^g = (-v + v^t)^g = -v^g + v^{tg} = -v^g + v^{gt[t,g]}.$$

Pela normalidade de T' em G, temos que $[V, T']$ é um subespaço de V G-invariante. Pela irredutibilidade de V, temos que $[V, T'] = 0$ e $T' = 1$, o que mostra que G é abeliano-por-finito.

□

Para entender melhor a demonstração do próximo Lema, iremos enunciar o Teorema de Cernikov que apresenta argumentos semelhantes ao do Lema que estamos interessados. Uma demosntração do seguinte teorema pode ser encontrado em 1.4.1 de [13].

Teorema 1.3.14 (Cernikov)**.** *Todo grupo solúvel que satisfaz a condição minimal é uma extensão finita do produto direto de um número finito de grupos quasicíclicos.*

Existe uma caracterização interessante envolvendo grupos solúveis de posto finito, que será usado posteriormente para a demonstração do *Teorema D.*. Confira também 5.3.6 de [13].

Teorema 1.3.15. *Seja G um grupo solúvel de posto finito. Então as seguintes afirmações são equivalentes:*

1. *G não possui subgrupos próprios de índice finito;*
2. *$G = G^m$ para todo $m > 0$;*
3. *G é radicável e nilpotente.*

Demonstração. (1) $\implies$ (2) Suponha que G não possui subgrupos de índice finito, como G/G^m para todo $m > 0$ tem índice finito, $G = G^m$.

(2) $\implies$ (1) Suponha, por absurdo, que H é um subgrupo de índice finito n em G, então $|G : H| = n$. Dessa forma, $G/Cor_G(H)$ é um subgrupo de S_n, então $Cor_G(H)$ é um subgrupo normal de G e tem índice finito, digamos k. Seja $x \in G \setminus Cor_G(H)$, por hipótese, $G = G^m$ para todo $m > 0$, então existe $y \in G$ tal que $y^k = x$. Olhando para o grupo quociente $G/Cor_G(H)$, temos que $x \in Cor_G(H)$, uma contradição.

(3) $\implies$ (1) Se H é um subgrupo de índice finito n em G, então $|G : H|$ divide $n!$. Dessa forma, para todo $g \in G$ temos que existe k inteiro positivo, tal que $g^k \in H$. Suponha, por absurdo que H é um subgrupo próprio de G, tomando um elemento $u \in G - H$, pela radicalidade de G, existe $v \in G$ tal que $v^k = u$. O que é uma contradição.

(1) $\implies$ (3) Suponha que G não possui subgrupos de índice finito. Considere uma série normal em G

$$G = G_n \trianglerighteq G_{n-1} \trianglerighteq ... \trianglerighteq G_1 \trianglerighteq G_0 = \{1\}$$

Em que cada fator pode ser um dos abaixo:

- Abeliano, livre de torção e irredutível (sobre os racionais) em relação a G;
- Produto direto de p-grupos abelianos de posto finito.

Queremos mostrar que G é nilpotente, para isso, vamos mostrar existe uma série central em G. Seja F um fator dessa série, vamos mostrar que F é central em G. Se provarmos que G age trivialmente em F, então teremos que F é central. Portanto, o nosso objetivo é mostrar que a ação de G em F é trivial.

Primeiramente, suponha que F é de torção. Então, todos os elementos de F tem ordem finita. Para cada $m > 0$, os elementos de F com ordem dividindo m formam um subgrupo

H finito G-invariante. Temos então um subgrupo finito e normal, veja que $G/C_G(H)$ está imerso no grupo dos automorfismos $Aut(H)$ que é finito. Então $G = C_G(H)$ pois G não possui subgrupos finitos. Assim, pela arbitrariedade de m, podemos percorrer todos os elementos de F e concluir que G age trivialmente em F.

Agora, suponha que F é livre de torção. Como $G/C_G(F)$ está imerso no grupo de automorfismos de F, temos que $G/C_G(F)$ é $\mathbb{Q}$-linear irredutível, pois está imerso em $F \otimes_{\mathbb{Z}} \mathbb{Q}$. Pelo Teorema de Mal'cev, seque que $G/C_G(F)$ é abeliano-por-finito. Seja $\bar{A} \lhd G/C_G(F)$ um subgrupo abeliano de índice finito. Assim, pelo Teorema de Clifford, $\bar{F} = F \otimes_{\mathbb{Z}} \mathbb{Q}$ é um $\mathbb{Q}\bar{A}$-módulo completamente redutível. Se $\bar{S}$ é uma $\mathbb{Q}\bar{A}$-parcela direta simples de $\bar{F}$, então $\bar{S} \cong_{\mathbb{Q}\bar{A}} \mathbb{Q}\bar{A}/I$, onde I é um ideal maximal de $\mathbb{Q}\bar{A}$. Além disso, o mapeamento $x \mapsto x + I$ determina uma imersão de $\bar{A}_S = \bar{A}/C_{\bar{A}}(S)$ no grupo multiplicativo do corpo algébrico multiplicativo $\mathbb{Q}\bar{A}/I$. Mas o grupo multiplicativo de um corpo algébrico multiplicativo é o produto direto de um grupo abeliano livre com um grupo cíclico. Como G tem posto finito, $\bar{A}_S$ é finitamente gerado para todo S. Existe uma quantidade finita de S, pois G tem posto finito, então podemos construir um homomorfismo de $\bar{A}$ no produto cartesiano $\prod_S \bar{A}_S$ que mapeia $a \in \bar{A}$ em cada classe lateral. O núcleo de tal homomorfismo é trivial, então $\bar{A}$ é isomorfo a um subgrupo de $\prod_S \bar{A}_S$. Como $\bar{A}$ é abeliano, segue que $\bar{A}$ é finitamente gerado. Então, $\bar{G}$ é finitamente gerado.

Portanto, $G/C_G(F)$ é residualmente finito, então $G = C_G(F)$. Assim, G age trivialmente em F. Portanto, G é nilpotente.

Seja $G_{ab} = G/G'$, como G_{ab} é abeliano e não tem subgrupos de índice finito, temos que G_{ab} é radicável. Pelo argumento do produto tensorial, temos que todos os fatores da série central inferior são radicáveis,

$$G \trianglerighteq G' \trianglerighteq [G', G] \trianglerighteq ... \trianglerighteq \{1\}$$

ou com uma notação diferente,

$$G = \gamma_0(G) \trianglerighteq \gamma_1(G) \trianglerighteq \gamma_2(G) \trianglerighteq ... \trianglerighteq \gamma_c(G) = \{1\}.$$

Vamos por indução tamanho da serie central inferior. Como base de indução, temos o caso em que $G' = \{1\}$. Já vimos que G_{ab} é radicável, então o resultado vale.

Suponha que todos os grupos que tenham série central inferior de tamanho menor que c e satisfazem as hipóteses estabelecidas anteriormente são radicáveis.

Como isso, suponha que o tamanho da serie central inferior de G é c. Sejam $x \in G$ e $m > 0$. $G/\gamma_c(G)$ é radicável, então $x\gamma_c(G) = g^m\gamma_c(G)$, ou seja, $x = g^m c_1$, para algum $g \in G$ e $c_1 \in \gamma_c(G)$. Como $\gamma_c(G)$ é radicável, existe $c_2 \in \gamma_c(G)$ tal que $c_1 = c_2^m$, assim,

$$x = g^m c_2^m = (gc_2)^m.$$

Segue que G é radicável.

Agora vamos mostrar que se G é um grupo nilpotente radicável, os elementos de ordem finita estão no centro. De fato, considere $g \in Z_2(G)$(segundo termo da série central superior) de ordem m. Se x é qualquer elemento de G, escrevemos $x = y^m$, onde $y \in G$. Então

$$[x, g] = [y^m, g] = [y, g^m] = 1.$$

Assim, $g \in Z(G)$. Logo o subgrupo de torção está contido em $Z(G)$ e a afirmação segue.

□

1.4 Grupos de Frobenius e Automorfismos Livres de Pontos Fixos

Nesta seção iremos estudar brevemente os Grupos de Frobenius assim como apresentar algumas de suas propriedades. Em seguida, vamos estudar automorfismos livres de pontos fixos com o objetivo de provar o Teorema de Thompson que será importante para a demonstração do Teorema B. Essa seção foi baseada principalmente em [6].

Definição 1.4.1 (Grupo de Frobenius)**.** *Um grupo finito G é um grupo de Frobenius quando em sua representação por permutações G é transitivo, há um subgrupo não-trivial H que fixa um elemento e apenas a identidade fixa mais de um elemento. Tal subgrupo H é chamado complemento de Frobenius.*

Frobenius descobriu uma propriedade muito importante sobre essa classe de grupos. Segue o enunciado dessa propriedade, mas sem demonstração, pois envolve Teoria de Caracteres que não é o foco desse trabalho. Para uma demonstração do teorema abaixo confira 5.5.1 de [6].

Teorema 1.4.2 (Frobenius)**.** *Sejam G um grupo de Frobenius e H um subgrupo fixando um elemento. Então o subconjunto de G que consiste da identidade mais os elementos que não fixam nenhuma letra é um subgrupo normal K de G de ordem $[G : H]$.*

Vamos nos referir a esse subgrupo normal K como o *núcleo de Frobenius* de G. E o subgrupo que fixa um elemento será chamado de *complemento de Frobenius*. A seguir temos uma consequência do Teorema 1.4.2, a demonstração se encontra em 2.7.5 de [6].

Teorema 1.4.3. *Seja G um grupo de Frobenius com complemento H e núcleo K. Então,*

1. *$G = HK$, com $H \cap K = 1$, de forma que G é o produto semidireto de K por H;*
2. *$|H|$ divide $|K| - 1$;*
3. *Todo elemento de H^* induz por conjugação um automorfismo livre de pontos fixos sobre K;*
4. *$C_G(y) \leq K$, $\forall y \in K^*$.*

A seguir, veremos um caso importante envolvendo grupos de Frobenius no contexto de representações de grupos.

Teorema 1.4.4. *Seja $G = HA$ um grupo de Frobenius em que o kernel H é um q-subgrupo abeliano elementar para algum primo q cujo complemento A é cíclico. Suponha que G é representado de forma irredutível e fiel em V sobre F, onde F contém uma raiz q-ésima da unidade. Então o número de componentes de Wedderburn de V em relação a H é exatamente $|A|$.*

Demonstração. Pelo Teorema 1.4.3, o fato de G ser um grupo de Frobenius com núcleo de Frobenius H e complemento de Frobenius A é equivalente a $C_H(u) = 1$ para todo u em A^*.

Seja V_i, $1 \leq i \leq r$, os componentes de Wedderburn de V em relação a H e suponha por contradição que $r < |A|$. Como H não varia V_i, o Teorema 1.2.20 implica que A permuta os V_i transitivamente. Como o número de V_i é menor que $|A|$, o subgrupo A_1 de A que fixa V_1 é não trivial. Sejam $G_1 = HA_1$ e N_1 o núcleo da representação de G_1 em V_1. Se x_i, $1 \leq i \leq r$, são os elementos de A tais que $V_1 x_i = V_i$, então $N_1^{x_i}$ é o núcleo da representação de $G_1^{x_i}$ em V_i. Como A é abeliano, $A_1 \cap N_1 \subseteq N_1^{x_i}$ para todo i. Mas a representação de G em V é fiel, então $A_1 \cap N_1 = 1$. O mesmo vale para qualquer conjugado de A_1 em G_1. No entanto, G é um grupo de Frobenius, qualquer elemento de G_1 que não está em um conjugado de A_1 pertence a H. Logo, $N_1 \subseteq H$. Como $H^{x_i} = H$, concluímos que $N_1 \subset H$.

Agora seja $\bar{G_1} = G_1/N_1 = \bar{H}\bar{A}_1$, tal que $\bar{G_1}$ é fielmente representado em V_1 e V_1 é a soma direta de FH-submódulos isomorfos X_i, $1 \leq i \leq t$. Como $\bar{H}$ é abeliano e F contém um q-ésima raiz primitiva da unidade, os Teoremas 1.2.14 e 1.2.15 implicam que $\bar{H} = \langle \bar{y} \rangle$ é cíclico. E também $\bar{y}$ age em cada X_i, os quais tem dimensão 1 sobre F, como transformação escalar. Como os X_i são FQ-módulos isomorfos , $\bar{y}$ age em V_1 como transformação escalar e então $\bar{y}$ comuta com a ação $\bar{A}_1$ em V_1. Como a representação de $\bar{G_1}$ em V_1 é fiel, concluímos que $\bar{H} \subseteq Z(\bar{G_1})$.

Assim, tomando H como um espaço vetorial sobre $\mathbb{Z}_q$. Temos que $\bar{A}_1$ centraliza $\bar{H} = H/N_1$ e consequentemente qualquer elemento u de A_1^* tem 1 como raiz característica em H. Logo, $C_H(u) \neq 1$, uma contradição já que G é um grupo de Frobenius.

□

O próximo resultado será uma aplicação do teorema acima.

Teorema 1.4.5. *Seja $G = QP$, onde Q é um q-subgrupo normal abeliano elementar de G e $|P| = p$, onde p e q são primos distintos. Suponha que $C_G(Q) = Q$ e que Q é um subgrupo normal minimal de G. Então se V é um FG-módulo fiel em que F não tem característica p ou q, temos que $C_V(P) \neq 0$.*

Demonstração. Visto que $|P| = p$, considere $P = \langle x \rangle$. Basta mostrar que 1 é uma raiz característica de x em V. É suficiente mostrar isso em V_L, onde L é uma extensão do

corpo F. Como V_L também é um FG-módulo simples, temos que é suficiente mostrar que F contém uma q-ésima raiz da unidade.

Veja que F não tem característica p ou q, segue pelo Teorema 1.2.17 que V é um FG-módulo completamente redutível. A representação de Q é fiel em V, logo existe um FG-submódulo de V irredutível U, no qual a ação de Q é não trivial. Considere K o núcleo da representação de G em U. Como $K \cap Q \lhd G$ e Q é um subgrupo minimal de G, temos que $K \cap Q = 1$, o que implica que K é um p-grupo. Mas se $K \neq 1$, $K = P$ é um p-Sylow de G. Nesse caso, $[Q, P] \subseteq Q \cap P = 1$. Logo, P centraliza Q e $C_G(Q) = G$, contrariando a hipótese. Então $K = 1$ e U é um FG-módulo fiel. Se $U \subset V$, então x tem raiz característica 1em U por indução em $\dim_F V$ e o Teorema segue. Podemos assumir que G é irredutível em V.

Agora, $C_Q(x) = 1$, caso contrário, x iria centralizar Q já que Q é um subgrupo normal minimal de G. Portanto, cada elemento de P^* induz por conjugação um automorfismo de Q que apenas fixa a identidade. Assim, G é um grupo de Frobenius com núcleo de Frobenius Q e complemento de Frobenius P. Dessa forma, pelo teorema anterior, V possui $p = |P|$ componentes de Wedderburn V_i, $1 \leq i \leq p$, em relação a Q.

Mas se v_1 é um vetor não nulo de V_1, então os vetores $v_1 x^{i-1}$ pertence a V_i, $1 \leq i \leq r$, e são linearmente independentes como V é a soma direta de V_i. Deste modo, o vetor

$$v = v_1 + v_1 x + ... + v_1 x^{p-1} \neq 0.$$

Por outro lado, é imediato que $vx = v$ pois $x^p = 1$. Assim, 1 é a raiz característica de x em V e o teorema está provado. □

Esse resultado será utilizado no estudo de grupos de automorfismos regulares, que são definidos da seguinte forma,

Definição 1.4.6. *Um grupo não trivial de automorfismos A de um grupo G é dito um grupo de automorfismos regulares quando cada elemento de A^* fixa apenas a identidade em G. Isto é, $C_G(\phi) = 1$, para todo $\phi \in A^*$.*

Com base nessa definição, a seguir veremos alguns resultados importantes.

Teorema 1.4.7. *Seja A um grupo de automorfismos regulares de um p-grupo P. Então A não possui subgrupos abelianos não cíclicos.*

Demonstração. Suponha que C é um subgrupo não cíclico abeliano de A. Então algum q-Sylow de C é não cíclico. Mas então $V = \langle C_V(\phi) | \phi \in Q^* \rangle$ pelo teorema passado. Como $V = \Omega_1(Z(P)) \neq 1$, isto mostra que $C_V(\phi) \neq 1$ para algum ϕ em Q^*, contrariando a regularidade de A. □

Teorema 1.4.8. *([6] Teorema 5.4.10.(ii)) Se P é um p-grupo em que todo subgrupo abeliano é cíclicos, então P é cíclico ou $p = 2$ e P é isomorfo ao quatérnio generalizado.*

Teorema 1.4.9. *([6] Teorema 5.4.11)*

Seja A um grupo de automorfismos regulares de um p-grupo P. Então os q-Sylows de A são cíclicos quando q é ímpar ou são cíclicos ou quaternios generalizados quando $p = 2$.

Automorfismos livres de pontos fixos

Agora vamos ao estudo dos automorfismos livres de pontos fixos. O resultado mais importante sobre o assunto é o Teorema de Thompson sobre a nilpotencia de grupos que admitem automorfismo de ordem prima.

Definição 1.4.10 (Automorfismos Livres de Pontos Fixos)**.** *Um automorfismo ϕ de um grupo G é dito livre de pontos fixos se $C_G(\phi) = 1$, ou seja, se fixa apenas o elemento neutro. Um grupo de automorfismos A de G é livre de pontos fixos se $C_G(A) = 1$, ie. se fixa apenas o elemento neutro, onde*

$$C_G(\phi) = \{x \in G | x^\phi = x\}$$

A seguir, enunciaremos alguns fatos que diferenciam essas definições,

1. ϕ é livre de pontos fixos se e somente se $\langle\phi\rangle$ é livre de pontos fixos;
2. Um grupo regular de automorfismos é livre de pontos fixos;
3. Em um grupo regular cada um de seus elementos não triviais são livres de pontos fixos;
4. Ser grupo livre de pontos fixos, não implica ser grupo regular de automorfismos.
5. Seja ϕ de ordem prima, ϕ é livre de pontos fixos se somente se $\langle\phi\rangle$ é grupo regular de automorfismos.

Agora, vamos estabelecer propriedades de automorfismos livres de pontos fixos.

Lema 1.4.11. *Sejam G um grupo finito e ϕ um automorfismo de G livre de pontos fixos. Se n é a ordem de ϕ, então*

1. *Todo elemento de G pode ser expresso na forma $x^{-1}(x\phi)$ e $(x\phi)x^{-1}$ para certos $x \in G$;*

2. Para todo $x \in G$, temos que

$$x(x\phi)...(x\phi^{n-1}) = (x\phi^{n-1})...(x\phi)x = 1.$$

Demonstração. Se $x^{-1}(x\phi) = y^{-1}(y\phi)$ com x, y em G, então transpondo obtemos que $xy^{-1} = (xy^{-1})\phi$. Mas então $xy^{-1} = 1$ e $x = y$, pois ϕ é livre de pontos fixos. Assim, o número de elementos distintos em G da forma $x^{-1}(x\phi)$ é o mesmo que o número de elementos x em G. Logo todo elemento pode ser expresso na forma $(x\phi)x^{-1}$. Portanto, *1.* está provado.

Agora vamos provar *2.*. Se $x \in G$, então pelo parágrafo anterior, $x = y^{-1}(y\phi)$ para algum y em G. Donde

$$\begin{aligned} x(x\phi)...(x\phi^{n-1}) &= y^{-1}(y\phi)(y^{-1}(y\phi)\phi)...(y^{-1}(y\phi)\phi^{n-1}) \\ &= y^{-1}(y\phi^n) = y^{-1}y = 1. \end{aligned}$$

A outra igualdade pode ser provada de maneira análoga. □

Teorema 1.4.12. *([6] Teorema 10.1.2) Se ϕ é um automorfismo livre de pontos fixos de G, então ϕ deixa invariante um único p-Sylow de G para cada p em $\pi(G)$. Além disso, P contém todo p-subgrupo ϕ-invariante de G.*

Lema 1.4.13. *Sejam ϕ um automorfismo livre de pontos fixos de G e H um subgrupo normal de G ϕ-invariante. Então ϕ induz um automorfismo livre de pontos fixos em G/H.*

Demonstração. Seja $\bar{G} = G/H$ e suponha que $\bar{x}\phi = \bar{x}$ para algum $\bar{x}$ em $\bar{G}$. Então $\bar{x}^{-1}(\bar{x}\phi) = \bar{1}$ então $y = x^{-1}(x\phi) \in H$ para algum representante x de $\bar{x}$ em G. Como ϕ induz um automorfismo livre de pontos fixos de H, temos que $y = z^{-1}(z\phi)$ para algum z em H e segue que $x = z$. Logo $x \in H$ e então $\bar{x} = \bar{1}$. Assim, ϕ induz um automorfismo livre de pontos fixos de $\bar{G}$. □

Exemplo 1.4.1. *Considere o $G = \mathbb{Z}$, já sabemos que $Aut(G) \cong C_2$, onde um automorfismo é a identidade e o outro automorfismo, digamos ϕ, é dado por $\phi(1) = -1$. Note que $\mathbb{Z}$ é um grupo abeliano que admite um automorfismo livre de pontos fixos de ordem 2.*

Teorema 1.4.14. *Se ϕ é um automorfismo livre de pontos fixos de G de ordem 2, então G é abeliano e $x\phi = x^{-1}$, para todo x em G.*

Demonstração. Pelo Lema 1.4.11, temos que $x(x\phi) = 1$, donde $x\phi = x^{-1}$ para todo x em G. Mas se x, $y \in G$, temos que

$$(xy)^{-1} = (xy)\phi = (x\phi)(y\phi) = x^{-1}y^{-1}.$$

Isto mostra que $1 = (xy)^{-1}xy = x^{-1}y^{-1}xy$, ou seja, $xy = yx$. □

A seguir temos um exemplo de um grupo não abeliano que admite automorfismo livre de pontos fixos de ordem 3.

Exemplo 1.4.2. *Seja $F = \mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$, visto como corpo finito com 7 elementos. Então o grupo*

$$UT_3(7) := \left\{ m(a,b,c) := \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c \in F \right\}$$

é não abeliano de ordem 7^3, mas sabemos que o grupo é nilpotente de classe 2. O inverso de um elemento $m(a,b,c)$ em $UT_3(7)$ é dado por $m(a,b,c)^{-1} = m(-a,-b,-c+ab)$. Além disso o centro e o subgrupo derivado de $UT_3(7)$ coincidem e são

$$Z(UT_3(7)) = UT_3(7)' = \{z \in UT_3(7) | z^7 = 1\} = \{m(0,0,c) | c \in F\}.$$

Para $f \in F \setminus \{0\}$, vejamos que o mapeamento definido por,

$$\lambda_f : m(x,y,z) \mapsto m(fx, fy, f^2z)$$

é um automorfismo de $UT_3(7)$. Tomando o grupo multiplicativo de $\mathbb{Z}/7\mathbb{Z}$, existe um subgrupo de ordem 3, digamos $S = \{\bar{1}, \bar{2}, \bar{4}\}$. Então $\{\lambda_f | f \in S\}$ é um grupo cíclico de automorfismos livres de pontos fixos de ordem 3 em $UT_3(7)$. De fato, suponha que λ_f tenha um ponto fixo, isto é, existem $a,b,c \in F$ tal que $m(a,b,c)^{\lambda_f} = m(a,b,c)$. Se $f \neq \bar{1}$, então $a = b = 0$ e $f^2c = c$. Como f tem ordem 3, temos que $f^2 \neq \bar{1}$ e também $c = 0$.

Teorema 1.4.15. *Se ϕ é um automorfismo livre de pontos fixos de G de ordem 3, então G é nilpotente e x comuta com $x\phi$ para todo x em G.*

Demonstração. Pelo Lema 1.4.11 *(2.)*, $x(x\phi)(x\phi^2) = (x\phi^2)(x\phi)x = 1$, então temos que

$$x(x\phi) = (x\phi)x = (x\phi^2)^{-1}$$

então x comuta com $x\phi$ para todo x em G.

Agora seja P o único p-Sylow ϕ-invariante de G para qualquer primo p em $\pi(G)$. Vamos mostrar que $P \lhd G$. Suponha falso, nesse caso existe um p-Sylow Q de G tal que $P \neq Q$. Sejam x em Q tal que $x \notin P$ e $H = \langle x, x\phi \rangle$. Já mostramos que $x(x\phi) = (x\phi)x$, então H é abeliano. Como x é um elemento de ordem potência de p, temos que $x\phi$

também tem ordem potência de p. Dessa forma, H é um p-grupo. Por outro lado, como $x\phi^2 = (x(x\phi))^{-1}$, ϕ transforma os geradores de H em elementos de H, então deixa H invariante. Logo, H é um p-subgrupo de G ϕ-invariante e $H \subseteq P$, pelo Teorema 1.4.12. Uma contradição. pois $x \in H$ e $x \notin P$.

Com isso, pela arbitrariedade de P, provamos que todo subgrupo de Sylow é normal em G. Pelos Lemas 1.1.10 e 1.1.10, temos que G é nilpotente.

□

Exemplo 1.4.3. *Sejam $|G| = 7^2 \cdot 3$ e $|\phi| = 4$, onde*

$$G = \langle x_1, x_2, y | x_1^7 = x_2^7 = y^3 = 1, x_1x_2 = x_2x_1, x_1^y = x_1^2, x_2^y = x_2^4 \rangle.$$

G é o produto semidireto interno do grupo abeliano $\langle x_1, x_2 \rangle$ de ordem 49 e do grupo cíclico $\langle y \rangle$ de ordem 3. Assim G é um grupo de ordem $7^2 \cdot 3$ cujos elementos são $x_1^i x_2^j y^k$, $0 \leq i \leq 6$, $0 \leq j \leq 6$, $0 \leq k \leq 2$. Como o 3-Sylow de G não é normal, G não é nilpotente. Mas G é solúvel pelo Teorema 1.1.15.

Se definirmos ϕ pela regra

$$(x_1^i x_2^j y^k)\phi = x_1^{-j} x_2^i y^{-k}$$

Veja que $(x_1)\phi = x_2$, $(x_2)\phi = x_1^{-1}$ e $y\phi = y^{-1}$. Observe que ϕ é um automorfismo livre de pontos fixos de ordem 4.

Com esse exemplo segue o seguinte teorema.

Teorema 1.4.16. *Existem grupos solúveis não-nilpotentes admitindo automorfismos livres de pontos fixos de ordem composta.*

Já mostramos que grupos que admitem automorfismos de ordem 2 e 3 são nilpotentes. Thompson provou que todo grupo que admite um automorfismo livre de pontos fixos de ordem prima é nilpotente. Afim de demonstrar esse resultado, vamos enunciar definições e um teorema que ajudará em parte da demonstração.

Definição 1.4.17 (p-complemento normal)**.** *Sejam G um grupo e $P \in Syl_p(G)$. Se $G = PO_{p'}(G)$ então dizemos que G tem um p-complemento normal. Visto que $O_{p'}(G) \triangleleft G$ e $P \cap O_{p'}(G) = 1$*

Definição 1.4.18. *Seja P um p-grupo, definimos $A(P)$ como o conjunto de todos os subgrupos de P que tem ordem máxima. Definimos também*

$$J(P) = \langle A | A \in A(P) \rangle.$$

$J(P)$ é chamado o subgrupo de Thompson de P.

A seguir enunciamos um famoso teorema atribuído a Glauberman e Thompson, para conferir a demonstração veja 8.3.1 de [6].

Teorema 1.4.19 (Glauberman-Thompson)**.** *Se P é um p-subgrupo de G, para p ímpar, e se $N_G(Z(J(P)))$ possui um p-complemento normal, então G também possui.*

O Teorema a seguir foi primeiramente provado por Thompson em sua tese de doutorado. Tal Teorema apresenta um resultado muito importante sobre automorfismos livres de pontos fixos.

Teorema 1.4.20 (Thompson)**.** *Seja G um grupo finito. Se G admite um automorfismo livre de pontos fixos de ordem prima, então G é nilpotente.*

Demonstração. Suponha, por contradição, que G é menor o grupo admitindo um automorfismo livre de pontos fixos de ordem prima mas que não é nilpotente. Seja ϕ o automorfismo livre de pontos fixos com ordem prima r. Separamos a demonstração em dois casos.

Se G é solúvel, vamos reduzir o problema ao Teorema 1.4.5.

Primeiramente, vamos mostrar que G não possui dois subgrupos normais não triviais H_1, H_2 que são ϕ-invariantes e tal que $H_1 \cap H_2 = 1$. Por contradição, suponha que G possua tais subgrupos. Podemos considerar o produto direto, $G/H_1 \times G/H_2$. Veja que G/H_1 e G/H_2 são nilpotentes pela minimalidade de G. Assim, a aplicação,

$$\begin{aligned} \psi : G &\to G/H_1 \times G/H_2 \\ g &\mapsto (H_1x, H_2x) \end{aligned}$$

define um homomorfismo de G para $G/H_1 \times G/H_2$. Agora, veja que $(H_1x, H_2x) = (H_1, H_2)$ se $x \in H_1 \cap H_2$. Mas $H_1 \cap H_2 = 1$, então ψ é injetiva. Com isso, G é isomorfo a um subgrupo de $G/H_1 \times G/H_2$. Ou seja, G é nilpotente, contrariando a escolha inicial de G. Logo, G não possui tais subgrupos H_1 e H_2.

Seja N um subgrupo normal minimal ϕ-invariante de G. Como G é solúvel, N é um p-subgrupo abeliano elementar de G. Além disso, ϕ induz um automorfismo livre de pontos fixos no grupo quociente $\bar{G} = G/N$ cuja ordem preservada, pelo Lema 1.4.13. Pela minimalidade de G, segue que G/N é nilpotente. Observe que $\bar{G}$ não é p-grupo, pois G não é nilpotente. Sejam $\bar{Q}$ um q-Sylow de $\bar{G}$ com $q \neq p$ e $\bar{M}$ um subgrupo minimal ϕ-invariante de $\Omega_1(Z(\bar{Q}))$. Sabemos que $\bar{M}$ é normal em $\bar{G}$ e como $\bar{G}$ é nilpotente, $Z(\bar{Q}) < Z(\bar{G})$.

Assim, $\bar{M} \neq 1$ e $\bar{M} \lhd \bar{G}$. Denote por H a imagem inversa de $\bar{M}$ em G, temos que $H = NM$, onde M é um q-grupo abeliano elementar, $M \neq 1$, $H \lhd G$ e H é ϕ-invariante. Podemos assumir que M é ϕ-invariante, e então pela escolha minimal de M, segue que ϕ é irredutível em M.

Se $H \subset G$, então H é nilpotente. Donde M char $H \lhd G$ e então M e N são dois subgrupos normais de G ϕ-invariantes tais que $M \cap N = 1$, o que não pode ocorrer. Então $G = H = NM$. Ademais, $C_M(N)$ é ϕ-invariante e como ϕ é irredutível em M, $C_M(N) = 1$ ou $C_M(N) = M$. Se ocorrer $C_M(N) = M$, G seria nilpotente, o que não ocorre. Então $C_M(N) = 1$.

Agora, se G^* denota o produto semidireto de M por $\langle\phi\rangle$, G^* é irredutível em N como um espaço vetorial sobre $\mathbb{Z}_p$ e a representação é fiel visto que $C_M(N) = 1$ e ϕ é livre de pontos fixos em N. Mas $G^* = M\langle\phi\rangle$ é um p'-grupo, $C_{G^*}(M) = M$, e G^*/M tem ordem prima. Então $C_N(\phi) \neq 1$ pelo Teorema 1.4.5. Essa contradição prova essa parte do teorema.

Agora, vamos ao caso em que G não é solúvel. Se G possui um subgrupo normal H próprio não trivial ϕ-invariante, então H é nilpotente, pela minimalidade de G. Além disso, ϕ induz um automorfismo livre de pontos fixos no grupo quociente G/H. Como r é um primo, temos que ϕ induzido em G/H tem ordem r. Pela minimalidade de G, temos que G/H é nilpotente. Assim, G é solúvel.

Portanto, suponhamos que G não possui um subgrupo normal próprio não trivial ϕ-invariante. Seja $P \in Syl_p(G)$, tal que P é o único Sylow ϕ-invariante, para p um primo ímpar. Note que tal primo p existe, pois G não é um 2-grupo, caso fosse, seria nilpotente. Seja $N = N_G(Z(J(P)))$. Como $Z(J(P))$ char P, N é ϕ-invariante e consequentemente $N \subset G$. Pela minimalidade de G, temos que N é nilpotente. Então N possui um p-complemento normal. Como p é ímpar, pelo Teorema de Glauberman-Thompson, temos que G tem um p-complemento normal K. Como K char G, K é ϕ invariante e então $K = 1$, pela suposição que G não é solúvel. Assim, $G = P$, e G é nilpotente, o que não ocorre. Logo G é solúvel.

□

Se G é um grupo de Frobenius com núcleo de Frobenius K e complemento de Frobenius A, então A induz um grupo regular de automorfismos de K. A possui um elemento x de ordem prima r e então x induz um automorfismo (por conjugação) livre de pontos fixos em K de ordem r. Assim, K é nilpotente pelo Teorema 1.4.2.

Como corolário do Teorema 1.4.20 temos que o núcleo de Frobenius é necessariamente nilpotente. Para mais detalhes confira 10.3.1 de [6].

Teorema 1.4.21. *Se G é um grupo de Frobenius com núcleo de Frobenius K e complemento de Frobenius A, então as seguintes condições valem*

1. *A induz um grupo regular de automorfismo em K;*
2. *$|A|$ divide $|K| - 1$;*
3. *K é nilpotente e é abeliano se $|A|$ é par;*
4. *Os p-Sylows de A são cíclicos para p ímpar e para p par os p-Sylows de A são quatérnios generalizados;*
5. *Os subgrupos de A de ordem pq, com p e q primos, é cíclico;*
6. *Se $|A|$ é ímpar, A é metacíclico. Se $|A|$ é par, A possui uma involução única contida em $Z(A)$.*

Capítulo

2

Grupos finitos com 3 órbitas por automorfismos

2.1 Conceitos Elementares

Sejam G um grupo e $Aut(G)$ seu grupo de automorfismos. Dado $g \in G$, as órbitas por automorfismos de G são definidas por

$$Orb_{Aut(G)}(g) = \{h \in G \mid \exists \alpha \in Aut(G) \text{ e } h = g^{\alpha}\} = \{g^{\alpha} \mid \alpha \in Aut(G)\}.$$

Note que G é particionado pelas órbitas de automorfismos. O número de órbitas é denotado por $\omega(G)$. Se $\omega(G)$ é finito, dizemos que G tem uma quantidade finita de órbitas por automorfismos.

Exemplo 2.1.1. *Vejamos o grupo dos quatérnios de ordem 8,*

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\},$$

onde, $(-1)^2 = 1$ *e* $i^2 = j^2 = k^2 = ijk = -1$. *Como os automorfismos preservam a ordem dos elementos, temos uma órbita para o elemento neutro,*

$$Orb_{Aut(Q_8)}(1) = \{1\}.$$

Note que -1 *é o único elemento de ordem 2. Então,*

$$Orb_{Aut(Q_8)}(-1) = \{-1\}.$$

Agora, tomemos um elemento de ordem 4, digamos i. A aplicação dada por

$$\begin{aligned} \phi : Q_8 &\to Q_8 \\ i &\mapsto j \\ j &\mapsto i \\ k &\mapsto -k \end{aligned}$$

define um automorfismo de Q_8 e nos mostra que $j \in Orb_{Aut(Q_8)}(i)$. Da mesma forma, o automorfismo

$$\begin{aligned} \psi : Q_8 &\to Q_8 \\ j &\mapsto k \\ k &\mapsto j \\ i &\mapsto -i \end{aligned}$$

nos informa que $k, -i, -k \in Orb_{Aut(Q_8)}(i)$. Similarmente, podemos concluir que $-j \in Orb_{Aut(Q_8)}(i)$. E então,

$$Orb_{Aut(Q_8)}(i) = \{i, -i, j, -j, k, -k\}.$$

Temos que $\omega(Q_8) = 3$, isto é, Q_8 é particionado em 3 órbitas por automorfismo, são elas

$$Q_8 = \{1\} \cup \{-1\} \cup \{i, -i, j, -j, k, -k\}.$$

Uma motivação para o estudo de órbitas por automorfismos está no contexto de grupos topológicos. Estamos interessados em saber o quanto um grupo topológico é homogêneo e como os automorfismo são objetos que preservam com muito rigor a estrutura de um grupo, quanto menos órbitas, mais homogêneo será o grupo.

Definição 2.1.1. *Seja G um grupo. Se $\omega(G) = 2$, então dizemos que G é um grupo homogêneo.*

Para isso, vamos classificar grupos baseados apenas no número $\omega(G)$. Isto é, dado um número de órbitas de automorfismos, podemos encontrar propriedades de grupos que caracterizam tais grupos?

Para o caso em que $\omega(G) = 1$, G é o grupo trivial, pois a órbita do elemento neutro só possui um elemento. E analogamente, se G é o grupo trivial, então o grupo de automorfismo é trivial, então existe uma única órbita, $\omega(G) = 1$.

Para o caso em que $\omega(G) = 2$ e G é finito, temos uma órbita para o elemento neutro $Orb_G(1)$, e outra órbita $Orb_G(g)$ para os elementos $g \in G^* = G \setminus \{1\}$. Dessa forma, para dois elementos quaisquer $x, y \in G^*$ existe um automorfismo φ tal que $x^\varphi = y$, ou seja, a ação é transitiva. Segue que todos elementos tem a mesma ordem, supondo que p é um primo que divide a ordem de G, pelo Teorema de Cauchy, existe um elemento de ordem p em G. Assim, todos os elementos em G^* tem ordem prima p e G é um p grupo. O centro $Z(G)$ de um p grupo é um subgrupo característico e não trivial, logo, como a ação é transitiva, segue que G é abeliano. Portanto, G é um grupo abeliano elementar. Analogamente, se G é um grupo abeliano elementar então seu grupo de automorfismos é $Aut(G) = GL(n, GF(p))$, e sabemos que $GL(n, GF(p))$ age transitivamente em G, logo $\omega(G) = 2$.

Conforme mencionado, grupos abelianos elementares também podem ser vistos como espaços vetoriais sobre um corpo de característica prima. Essa observação será relevante em outras classificações de grupos com uma quantidade finita de órbitas por automorfismos.

Com isso, temos uma classificação simples para grupos finitos com $\omega(G) = 2$. Por outro lado, considerando grupos com $\omega(G) = 2$ e livres de torção (onde os elementos não têm ordem finita), não existe uma "classificação"com propriedades bem detalhadas. Por exemplo, em 6.4.6 de [15], temos um grupo construído por G. Higman, B. Neumann e H. Neumann, que é simples livre de torção não abeliano e com todos os elementos não triviais conjugados. Ou seja, com duas órbitas por automorfismos.

No entanto, para o caso particular em que o grupo é solúvel, temos

Lema 2.1.2. *Se $\omega(G) = 2$ e G é solúvel livre de torção, então G é abeliano e $G = \oplus\mathbb{Q}$.*

Nesse caso, como $G = \oplus\mathbb{Q}$, G pode ser visto como um espaço vetorial sobre o corpo $\mathbb{Q}$. Assim, podemos fazer um paralelo com a classificação de grupos finitos com $\omega(G) = 2$, onde mencionamos que esses grupos também podem ser vistos como espaços vetoriais.

A seguir temos dois fatos simples e bem conhecidos sobre grupos com uma quantidade finita de órbitas por automorfismos.

Definição 2.1.3. *Em um grupo finito G, o menor número natural n tal que $g^n = 1$, para todo $g \in G$ é chamado de expoente de G.*

Lema 2.1.4. *Se G é um grupo de torção e $\omega(G) < \infty$, então G tem expoente limitado.*

Demonstração. Seja $\omega(G) = n$, para algum inteiro positivo n. Como os automorfismos preservam as ordens dos elementos, podemos tomar $r_1, ..., r_n$ como sendo as ordens dos elementos em cada órbita de automorfismo, com r_i inteiros positivos para $1 \leq i \leq n$.

Por contradição, suponha que G não tem expoente limitado. Então existem elementos de ordens arbitrariamente grandes em G. Contrariando o fato de existirem apenas elementos com as ordens $r_1, ..., r_n$.

□

Lema 2.1.5. *Se $\omega(G) < \infty$, então G tem um número finito de subgrupos característicos.*

Demonstração. Seja $\omega(G) = n$, para algum inteiro positivo n. Podemos tomar $H_1, ..., H_n$ como sendo as distintas órbitas por automorfismo de G, onde $H_1 = 1$. Como os subgrupos característicos são invariantes por automorfismos, todo subgrupo característico será exatamente a união de certas órbitas por automorfismos. Mas como existem finitas, existem finitos subgrupos característicos.

□

Exemplo 2.1.2. *Tome o grupo dos números inteiros $\mathbb{Z}$. Sabemos que $Aut(\mathbb{Z}) \cong C_2$ é o grupo que contém o automorfismo identidade e o automorfismo φ que aplica 1 em -1. Além disso, todo subgrupo de $\mathbb{Z}$ é característico, pois é da forma $n\mathbb{Z}$, para algum n inteiro. Ou seja, temos um grupo que possui infinitos subgrupos característico, logo, não pode ter uma quantidade finita de órbitas por automorfismos.*

Agora, vamos estudar os grupos com 3 órbitas por automorfismos.

Definição 2.1.6. *Um grupo G é chamado quase homogêneo se $\omega(G)$ é no máximo 3.*

Lema 2.1.7. *([14] Lema 1.1) Seja H um subgrupo característico próprio não trivial de um grupo G quase homogêneo. Então H e G/H são homogêneos.*

Demonstração. Como H é um subgrupo característico próprio não trivial, os conjuntos disjuntos $\{1\}$, $H \setminus \{1\}$ e $G \setminus H$ são invariantes por $Aut(G)$. E assim, formam três órbitas. A ação de $Aut(G)$ em G induz uma ação no grupo quociente G/H. Assim, vemos que G/H possui duas órbitas.

□

Lema 2.1.8. *([14] Corolário 1.2) Seja G um grupo quase homogêneo.*

1. *Se G é solúvel mas não abeliano, então o comutador G' e G/G' são grupos homogeneos abelianos. Em particular, o comprimento derivado é no máximo 2 e os grupos G' e G/G' são espaços vetoriais.*

2. *Se G é solúvel e o centro de G é não trivial, então G é nilpotente de classe no máximo 2.*

Uma classe importante de grupos são os p-grupos. Vejamos algumas propriedades de p-grupos no contexto de órbitas por automorfismos.

Exemplo 2.1.3. *Se o grupo G é tal que $|G| = p$, G é abeliano elementar e já vimos que $\omega(G) = 2$.*

Exemplo 2.1.4. *Se $|G| = p^2$ e $G = C_{p^2}$, temos três órbitas por automorfismos: a órbita do elemento neutro, uma órbita contendo os elementos de ordem p e uma órbita contendo os elementos de ordem p^2.*

Exemplo 2.1.5. *Se $|G| = p^3$ e $G = C_p \times C_{p^2}$, temos mais que três órbitas por automorfismos. De fato, 1 ocupa uma órbita e os outros elementos são de ordem p e p^2. O subgrupo $\mho^1(G)$ é característico em G e portanto seus elementos de ordem diferente de 1 formam uma órbita de automorfismo. Além disso, $|\mho^1(G)| = p$. Mas veja que existem elementos de ordem p que não estão em $\mho^1(G)$, logo existe mais de uma órbita por automorfismos com elementos de ordem p. Logo $\omega(G) > 3$.*

Ainda não se conhece a classificação exata de grupos com 3 órbitas por automorfismos. Mas existem resultados que classificam algumas classes de grupos com 3 órbitas. Em [4], os autores Alexander Bors e Stephen P. Glasby classificam 2-grupos que admitem exatamente 3 órbitas por automorfismos. Já em [12], T. Laffey e D. MacHale classificaram grupos finitos com $\omega(G) = 3$ que não são p-grupos. Esta última classificação será o foco da próxima seção.

2.2 Prova do Teorema A

Precisaremos do seguinte lema para nosso resultado Teorema A.

Lema 2.2.1. *([9] II.3.10) Seja V um espaço vetorial de dimensão n sobre o corpo $K = GF(p^f)$ e H um grupo abeliano de mapeamentos K-lineares de V sobre si mesmo e V um módulo H irredutível. Então H é mapeado como grupo de permutação em V, semelhante a um grupo de mapeamentos da forma*

$$x^A = a(A)x, \qquad (a(A) \in GF(p^{nf})),$$

sobre $GF(p^{nf})$. Em particular, H é cíclico, e

$$|H| \mid p^{nf} - 1,$$

onde n é determinado unicamente por $|H|$ como o menor número natural com $p^{nf} - 1 \equiv 0$ mod $(|H|)$. Se $H = \langle A_0 \rangle$, então $GF(p^f)[a(A_0)] = GF(p^{nf})$.

Vamos classificar os grupos quase homogêneos finitos de ordem mista.

Teorema A (Laffey & MacHale (1986))**.** *Seja G um grupo finito que não é p-grupo. As seguintes afirmações são equivalentes:*

1. *$\omega(G) = 3$;*
2. *$|G| = p^n q$, para primos p, q e para um inteiro $n \geq 1$, e G tem um p-subgrupo de Sylow P normal abeliano elementar. Além disso, p é uma raiz primitiva mod q (i.e. $q-1$ é o menor natural tal que $p^{q-1} \equiv 1$ mod q). Seja Q um q-subgrupo de Sylow de G. Então P, visto como $GF(p)Q$-módulo é a soma direta de $t \geq 1$ cópias do único $GF(p)Q$-módulo irredutível de dimensão $q-1$. Em particular, $|P| = p^{t(q-1)}$.*

Demonstração. ($1 \implies 2$) Suponha que $\omega(G) = 3$ e que G não é um p-grupo. Então $|G| = p^a q^b$ para primos p, q e inteiros $a \geq 1$ e $b \geq 1$. Pelo Teorema 1.1.15 (Burnside), segue que G é solúvel. Assim, podemos supor que $O_p(G) \neq 1$. Como $O_p(G)$ char G, temos que $O_p(G)$ ocupa duas órbitas por automorfismo (a órbita do elemento neutro e a órbita dos elementos de ordem p). Ou seja, $P := O_p(G)$ é um p-subgrupo de Sylow de G. Além disso, o subgrupo $\Omega_1(Z(P))$ é característico em $Z(P)$, que por sua vez é característico em G. Pela transitividade da propriedade característica, $\Omega_1(Z(P))$ char G. Como são apenas 3 órbitas de automorfismos, $\Omega_1(Z(P)) = G$. Então P é abeliano elementar.

Seja $Q \in Syl_q(G)$. Observe que G não possui elementos de ordem pq pois $\omega(G) = 3$. Caso a ação de Q em P admita pontos fixos, teríamos que existe $y \in Q$ tal que para todo

$x \in P$, $yxy^{-1} = x$, ou seja, y comuta com todos os elementos de P. Porém ao multiplicar x com y teríamos um elemento xy em G com ordem pq, o que não pode ocorrer. Logo Q age sobre P livre de pontos fixos. Pelo Teorema 1.4.9, temos que Q é cíclico quando q é ímpar ou é o quaternio generalizado. Mas por uma questão de ordem, Q tem expoente q, então, $|Q| = q$.

Agora, veja que P pode ser visto como $GF(p)Q$-módulo. Escreveremos a operação em P como adição e a ação (por conjugação) de Q como multiplicação. Como p e q são distintos, pelo Teorema 1.2.17 (Maschke), $P = P_1 \oplus ... \oplus P_r$, onde P_i, $1 \leq i \leq r$, são $GF(p)Q$-módulos irredutíveis. Pelo Lema 2.2.1, $|P_i| = p^e$, onde e é a ordem de p mod q (i.e. e é o menor natural tal que $p^e \equiv 1 \bmod q$). Se $Q = \langle\alpha\rangle$, escolhemos uma base para P_i em que α é representada pela matriz companheira de seu polinômio minimal $m_i(\lambda)$ em P_i. Então P_i é determinado a menos de isomorfismo pelo polinômio minimal $m_i(\lambda)$. Agora, vamos mostrar que $P_1, ..., P_r$ são todos módulos isomorfos. Suponha que P_1 não é isomorfo a P_2. Então $m_1(\lambda) \neq m_2(\lambda)$. Seja $0 \neq u_i \in P_i$ $(i = 1, 2)$. Como $\omega(G) = 3$, existe $\sigma \in Aut(G)$ onde $u_1^\sigma = u_1 + u_2$. Agora, $\alpha^{\sigma^{-1}} = \alpha^k w$ para algum $w \in P$, e algum $k \geq 1$ com $(k, q) = 1$. Seja $g(\lambda)$ o polinômio minimal de α^k em P_1. Note que $deg(g) = e$. Considere

$$\begin{aligned} u_1^\sigma g(\alpha) &= u_1^\sigma (g(\alpha^{\sigma^{-1}}))^\sigma \\ &= u_1^\sigma (g(\alpha^k w))^\sigma \\ &= u_1^\sigma (g(\alpha^k))^\sigma \\ &= [u_1 g(\alpha^k)]^\sigma = 0 \end{aligned}$$

Então, $(u_1 + u_2)g(\alpha) = 0$. Mas o polinômio minimal de α em $u_1 + u_2$ é $m_1(\lambda)m_2(\lambda)$, pois $m_1 \neq m_2$ implica que $(m_1, m_2) = 1$. Como $degg = degm_i$, temos uma contradição. Então os termos P_i são $GF(p)G$-módulos isomorfos.

Agora, para qualquer i tal que $(i, q) = 1$ existe $\tau \in \mathrm{Aut}(G)$ tal que $\alpha^\tau = \alpha^i$. Seja $0 \neq u \in P$. Então o polinomio minimal $m(\alpha)$ tal que $um(\alpha) = 0$ é o polinomio minimal de α em P. Mas como P é abeliano,

$$0 = um(\alpha) = [um(\alpha)]^\tau = u^\tau m(\alpha^\tau) = u^\tau m(\alpha^i).$$

Assim, $m(\alpha^i) = 0$ e então $m(\lambda)$ divide $m(\lambda^i)$ $(i = 1, ..., q-1)$. Logo, se w é uma raiz de $m(x)$ no fecho algébrico de $GF(p)$, w^i também é. Portanto, $m(\lambda)$ é divisível pelo polinômio ciclotomico $\Phi_{q-1}(\lambda)$. Assim, $e \geq q - 1$, e então $e = q - 1$ e o resultado segue.

($2 \implies 1$) Suponha que G satisfaz *2.* Então Q age livre de pontos fixos em P, assim, G possui apenas elementos de ordem 1, p e q. Primeiramente, vamos mostrar que todos os elementos de ordem p são conjugados. Note que P é um $GF(p)Q$-módulo homogeneo, então se $0 \neq u \in P$, então $P_0 = \{uf(\alpha)|f(x) \in GF(p)[x]\}$ é um $GF(p)Q$-submódulo irredutível de ordem p^{q-1}. Sejam $0 \neq v \in P$ e $P_1 = \{vf(\alpha)|f(x) \in GF(p)[x]\}$. Se $P_0 = P_1$, então podemos escrever $P = P_0 \oplus P_2$ como $GF(p)Q$-módulos. Mas então temos que o mapeamento σ definido por $\alpha^\sigma = \alpha$, $u^\sigma = v$ e $w^\sigma = w (w \in P_2)$ se estende a um automorfismo de G.

Se $P_0 \neq P_1$, então podemos escrever $P = P_0 \oplus P_1 \oplus P_2$ como $GF(p)Q$-módulo. Da mesma forma, o mapeamento τ definido por $\alpha^\tau = \alpha$, $u^\tau = v$, $v^\tau = u$ e $w^\tau = w^\tau (w \in P_2)$ se estende a um automorfismo de G.

Devemos mostrar que os elementos de ordem q formam uma única órbita sobre ação de $\mathrm{Aut}(G)$. Como P permuta os q-Sylows de G de forma transitiva é suficiente mostrar, via teorema de Sylow, que para todo i com $1 \leq i \leq q-1$, existe $\theta \in \mathrm{Aut}(G)$ tal que $\alpha^\theta = \alpha^i$.

Sejam $P = P_0 \oplus ... \oplus P_t$, onde P_i são $GF(p)Q$-módulos irredutíveis, e $0 \neq u_j \in P_j$. Então cada $u \in P_j$ pode ser expresso de maneira única na forma $u_j f(\alpha)$ para algum $f(\lambda) \in GF(p)[\lambda]$ com $\deg f < q-1$. Defina o mapeamento θ por $\alpha^\theta = \alpha^i$, $u_j^\theta = u_j$ e $(u_j f(\alpha))^\theta = u_j f(\alpha^i)$.

Note que se $0 \neq u \in P$ é tal que $ug(\alpha) = 0$ para algum $g(x) \in GF(p)[x]$, então $\Phi_{q-1}(\lambda)$ divide $g(\lambda)$ e então divide $g(\lambda^i)$. Assim, $ug(\alpha^i) = 0$. Isso prova que a extensão natural de θ para P está bem definido. Dessa forma, θ se estende a um automorfismo de G. Completando a demonstração.

□

De maneira geral, a classificação acima nos diz que um grupo finito G que não é um p-grupo, tem a forma

$$G = P \rtimes Q = (C_p \times ... \times C_p) \rtimes C_q,$$

onde $|G| = p^n q$, $P \in Syl_p(G)$ e $Q \in Syl_q(G)$.

A seguir veremos um exemplo simples.

Exemplo 2.2.1. *Considere* $G = S_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. *Temos que* $|G| = 2 \cdot 3$. *Veja que 2 é o menor inteiro positivo tal que* $2^2 \equiv 1 mod 3$. *Automorfismos aplicam geradores em geradores então,* $|Aut(G)| = 6$. *E sabemos que* $G/Z(G)$ *é isomorfo ao subgrupo dos automorfismos internos, mas como o centro é trivial, os automorfismos*

de G são os próprios automorfismos internos. São eles:

$$\varphi_1 : G \to G \qquad x \mapsto x \qquad\qquad \varphi_2 : G \to G \qquad x \mapsto x^{(1,2)}$$

$$\varphi_3 : G \to G \qquad x \mapsto x^{(1,3)} \qquad\qquad \varphi_4 : G \to G \qquad x \mapsto x^{(2,3)}$$

$$\varphi_5 : G \to G \qquad x \mapsto x^{(1,2,3)} \qquad\qquad \varphi_6 : G \to G \qquad x \mapsto x^{(1,3,2)}$$

Agora, analisemos as órbitas de cada um dos elementos.

$$\begin{aligned} Orb_G(1) &= \{1\} \\ Orb_G((1,2)) &= \{(1,2),(2,3),(1,3)\} \\ &= Orb_G((1,3)) \\ &= Orb_G((2,3)) \\ Orb_G((1,2,3)) &= \{(1,2,3),(1,3,2)\} \\ &= Orb_G((1,3,2)) \end{aligned}$$

De fato, são apenas três órbitas por automorfismo.

Exemplo 2.2.2. *Considere $D_5 = \langle a, b | a^5 = 1 = b^2, a^b = a^{-1} \rangle$, com $|D_5| = 2{\cdot}5$. Temos que 5 é raiz primitiva módulo 2, e $\langle a \rangle$ é normal em D_5, então pelo Teorema acima, $\omega(D_5) = 3$. Podemos também analisar os automorfismos, um automorfismo $\varphi \in Aut(D_5)$ é totalmente determinado pela imagem de a e b. Como a^φ tem ordem 5 e todos os elementos fora de $\langle a \rangle$ tem ordem 2, temos que $a^\varphi = a^r$ com $(5, r) = 1$. Então $(\langle a \rangle)^\varphi = \langle a \rangle$. Logo, $b^\varphi \notin \langle a \rangle$, tal que*

$$a^\varphi = a^r \qquad e \qquad b^\varphi = a^s b,$$

onde $r \in (\mathbb{Z}/5\mathbb{Z})^\times$ e $s \in \mathbb{Z}/5\mathbb{Z}$. Assim, vemos que são de fato 3 órbitas por automorfismo.

Baseados nesse exemplo veja que

Corolário 2.2.2. $\omega(D_n) = 3$, *para* n *um número primo ímpar.*

Demonstração. Considerando a representação do grupo diedral

$$D_n = \langle a, b | a^n = 1 = b^2, a^b = a^{-1} \rangle.$$

Temos que $|D_n| = 2 \cdot n$. Também podemos notar que o subgrupo $\langle a \rangle$ é normal em D_n, pois $a^b = a^{-1}$. E é abeliano elementar, visto que $|\langle a \rangle| = n$. Além disso, n é raiz primitiva módulo 2. Assim, aplicando o Teorema acima, o resultado segue.

□

Capítulo

3

Grupos de posto finito com 3 órbitas por automorfismos

Vimos no capítulo anterior que com exceção dos p-grupos, os grupos finitos com $\omega(G) = 3$ foram totalmente classificados. Para grupos infinitos, existem resultados interessantes também. Esses grupos foram estudados em [1].

3.1 Sobre grupos com $\omega(G) < \infty$

Apresentaremos, nessa seção, resultados importantes que ajudam a demonstrar o Teorema C e o Teorema D. Veremos no primeiro lema, um resultado por Schwachhofer-Stroppel [16].

Lema 3.1.1 (Schwachhofer-Stroppel)**.** *Se G é infinito abeliano com $\omega(G) < \infty$ então,*

$$G = Tor(G) \oplus D,$$

onde D é um subgrupo livre de torção, divisível e característico e $Tor(G)$ é o conjunto de todos os elementos de torção.

Definição 3.1.2. *Um subgrupo $K \leq G$ é dito complemento de um subgrupo normal N em G, se $N \cap K = 1$ e $G = NK$.*

Lema 3.1.3 (Schur)**.** *Se G é um grupo finito e N é um subgrupo normal abeliano tal que $(|N|, |G : N|) = 1$, então existe um complemento K de N.*

A seguir mostraremos que esse resultado vale sob hipóteses mais gerais. Confira também [1].

Lema 3.1.4. *Seja A um subgrupo normal abeliano, divisível, livre de torção e de índice finito em G. Então existe um subgrupo H de G tal que $G = A \rtimes H$.*

Demonstração. Queremos construir um subgrupo H tal que $H \cap A = \{1\}$ e $G = HA$.

Como A é normal, então seja $B = G/A$ o grupo quociente. Como A é abeliano, A pode ser visto como B-módulo pela ação $a^{gA} = a^g$, que também pode ser vista como

$$\begin{aligned} \varphi : B &\to Sym(A) \\ gA &\mapsto \varphi(gA), \end{aligned}$$

onde

$$\begin{aligned} \varphi(gA) : A &\to A \\ a &\mapsto \varphi(gA)(a) = a^{gA} = a^g \end{aligned}$$

Tomamos um representante t_x para cada classe lateral x em B, de forma que $T = \{t_x | x \in B\}$ é um transversal de A em G.

Veja que $t_x t_y A = t_{xy} A$, isso significa que ao multiplicar duas classes laterais, temos uma outra classe lateral que seria a multiplicação dessas suas classes. Então existe um elemento $c(x, y)$ de A tal que $t_x t_y = t_{xy} c(x, y)$. Assim,

$$\begin{aligned} (t_x t_y) t_z &= t_{xy} c(x, y) t_z \\ &= t_{xy} t_z t_z^{-1} c(x, y) t_z \\ &= t_{xy} t_z t_z^{-1} a^{-1} a c(x, y) t_z \\ &= t_{xy} t_z t_z^{-1} a^{-1} c(x, y) a t_z \\ &= t_{xy} t_z (a t_z)^{-1} c(x, y) a t_z \\ &= t_{xy} t_z c(x, y)^z \\ &= t_{xyz} c(xy, z) c(x, y)^z \end{aligned}$$

$\forall a \in A$. Por outro lado,

$$t_x (t_y t_z) = t_x t_{yz} c(y, z) = t_{xyz} c(x, yz) c(y, z).$$

Assim, temos que $c(xy,z)c(x,y)^z = c(x,yz)c(y,z)$, para cada $x,y \in B$. Seja $d(y) = \prod_{x\in B} c(x,y) \in A$, isto é, fixando uma classe lateral y tomamos o produto de todos os $c(x,y)$ para toda classe lateral $x \in B$. Como A é abeliano,

$$\begin{aligned} d(z)d(y)^z &= \prod_{x\in B} c(x,z) \prod_{x\in B} c(x,y)^z \\ &= c(x_1,yz)c(y,z) \prod_{x\in B-\{x_1y\}} c(x,z) \prod_{x\in B-\{x_1\}} c(x,y)^z \\ &\ldots \\ &= \prod_{x_i\in B} c(x_i,yz)c(y,z) \\ &= d(yz)c(y,z)^n. \end{aligned}$$

onde $n = |B|$, que é finito por hipótese. Então de $d(z)d(y)^z = d(yz)c(y,z)^n$ e $d(yz)c(y,z)^n = c(y,z)^n d(yz)$ obtemos que $d(yz) = d(y)^z d(z)c(y,z)^{-n}$.

Agora, como A é um subgrupo divisível, existe $e(y) \in A$ tal que $e(y)^n = d(y)^{-1}$ para todo $y \in B$. Logo,

$$\begin{gathered} e(yz)^{-n} = (e(yz)^n)^{-1} = (d(yz)^{-1})^{-1} = ((d(y)^z d(z)c(y,z)^{-n})^{-1})^{-1} = \\ = ((d(y)^z)^{-1} d(z)^{-1} c(y,z)^n)^{-1} = (e(y)^{nz} e(z)^n c(y,z)^n)^{-1} = \\ = (e(y)^z e(z)c(y,z))^{-n}. \end{gathered}$$

A é livre de torção, então $e(yz) = e(y)^z e(z)c(y,z)$. Definimos $s_x = t_x e(x)$, então

$$\begin{aligned} s_y s_z &= t_y e(y) t_z e(z) \\ &= t_y t_z e(y)^z e(z) \\ &= t_{yz} c(y,z) e(y)^z e(z) \\ &= t_{yz} e(y)^z e(z) c(y,z) \\ &= t_{yz} e(yz) \\ &= s_{yz}. \end{aligned}$$

Podemos, pois, definir o homomorfismo

$$\begin{aligned} \phi : B &\to G \\ x &\mapsto s_x = t_x \prod_{y \in B} c(y,x)^{-1}. \end{aligned}$$

Seja $H \leq G$ tal que $H = B^{\phi}$. Se $s_x \in H \cap A$, então $t_x \prod_{y \in B} c(y,x)^{-1} \in A$. Mas $\prod_{y \in B} c(y,x)^{-1} \in A$, então t_x é o representante da classe de A, ou seja, x é o elemento neutro 1_B em B pois $B = G/A$. Pelas propriedades de homomorfismos, $\phi(x) = 1_A$, logo $H \cap A = \{1\}$.

Se $s_x = 1_G$, temos que $t_x \in A$, ou seja, $x = 1_B$. Segue, então que ϕ é injetiva.

Como $n = |B| = |G/A|$ e ϕ é injetiva, $|H| = n$. Pelo segundo teorema de isomorfismo, $HA/A \cong H \cong B = G/A$. E segue que $G = HA$.

□

O próximo teorema é fundamental na teoria de grupos.

Teorema 3.1.5 (Schur-Zassenhaus)**.** *Seja N um subgrupo normal de um grupo finito G. Suponha que $|N| = n$ e $|G : N| = m$ são coprimos. Então G possui subgrupos de ordem m, que são dois a dois conjugados em G.*

Note que esse teorema garante a existência de subgrupos de uma certa ordem. Um resultado similar, no contexto de órbitas por automorfismo, será apresentado a seguir.

Consideraremos grupos com um número finito de órbitas de automorfismo, que possuem um subgrupo livre de torção solúvel, característico e de índice finito. Em particular, a partir de agora todos os grupos serão infinitos.

Lema 3.1.6. *Seja n um inteiro positivo, G um grupo tal que $\omega(G) < \infty$ e A um subgrupo livre de torção, característico, de índice finito n. Se A é solúvel, então existe um subgrupo H de G tal que $G = A \rtimes H$.*

Demonstração. Vamos argumentar por indução no tamanho da série derivada de A. Primeiramente, suponha A abeliano. Temos então que A é um grupo abeliano, com $\omega(A) < \infty$. Pelo resultado de Schwachhöfer-Stroppel mencionado previamente, segue que

$$A = Tor(A) \oplus D,$$

onde D é um subgrupo livre de torção, divisível e característico e $Tor(A)$ é o conjunto de todos os elementos de torção. No caso, $Tor(A) = 1$, então A é divisível. Podemos então aplicar do Lema anterior e o resultado segue.

Suponha que para toda série derivada de tamanho $d-1$ o resultado vale, vamos provar que vale para a série de tamanho d.

Se A é não abeliano, vamos mostrar que $A/A^{(d-1)}$ é livre de torção, onde d é o tamanho da série derivada de A. Veja que $A^{(d-1)}$ é abeliano pois seu comutador é trivial e como é um subgrupo de um grupo livre de torção, $A^{(d-1)}$ é livre de torção. Temos que $A^{(d-1)}$ é infinito abeliano e tal que $\omega(A^{(d-1)}) < \infty$, estamos nas hipóteses do Lema 3.1.1, segue que $A^{(d-1)}$ é divisível. Então, $A^{(d-1)}$ é um subgrupo abeliano, livre de torção e divisível.Suponha, por contradição, que $A/A^{(d-1)}$ não é livre de torção. Então podemos determinar um elemento $a \in A$ tal que o grupo $\langle a, A^{(d-1)} \rangle$ possui um subgrupo que é livre de torção, divisível e de índice finito, então pelo lema anterior o subgrupo $\langle a, A^{(d-1)} \rangle$ possui elementos de ordem finita. Uma contradição, logo, $\langle a, A^{(d-1)} \rangle$ é livre de torção.

Agora seguindo o argumento de indução no tamanho da série derivada de A. Para o quociente $\bar{G} = G/A^{(d-1)}$ e $\bar{A} = A/A^{(d-1)}$, $\bar{A}$ é livre de torção, característico e de índice finito n, segue por hipótese de indução, que existe um subgrupo finito $\bar{B}$ de ordem n em $\bar{G}$, tal que $\bar{G} = \bar{A} \rtimes \bar{B}$.

Seja B a imagem inversa de $\bar{B}$, temos que $A^{(d-1)} \leq B$ e que $A^{(d-1)}$ tem índice finito n em B. Aplicando o Lema 3.1.4 segue que B possui um subgrupo H de ordem n que é o complemento de A em G. Veja que $H \cap A^{(d-1)} = \{1\}$, então $H \cap A = \{1\}$. Além disso, de $\bar{G} = \bar{A}\bar{B}$ e $B = A^{(d-1)}H$, temos que $G = AH$. Portanto, $G = A \rtimes H$.

□

Lema 3.1.7. *Seja G um grupo abeliano de posto finito. Se $\omega(G) < \infty$, então o subgrupo de torção $Tor(G)$ é finito.*

Demonstração. Se G tem um número finito de órbitas de automorfismo, como $Tor(G) \leq G$, temos que $\omega(Tor(G)) < \infty$. Isso no permite concluir que o expoente do subgrupo de torção $exp(Tor(G))$ é limitado.

Como G tem posto finito, os seus subgrupos possuem um número máximo de geradores, logo $Tor(G)$ é finitamente gerado.

Com isso, podemos concluir que não existe elemento de ordem infinita em $Tor(G)$ e também, são finitos geradores, e assim segue que $Tor(G)$ é finito.

□

3.2 Provas dos Teoremas C e D

Definição 3.2.1. *Sejam G um grupo e r um inteiro positivo. Então G tem posto finito r se cada subgrupo finitamente gerado de G pode ser gerado por r ou menos elementos e r é o menor inteiro que satisfaz isso.*

Teorema C. *Seja G um grupo solúvel de posto finito. Se $\omega(G) < \infty$, então G possui um subgrupo K livre de torção, radicável, nilpotente e característico tal que*

$$G = K \rtimes H,$$

onde H é um subgrupo finito.

Demonstração. Como G é solúvel, por indução no tamanho da série derivada de G.

Para o grupo G em que a série derivada tem tamanho 1, $[G, G] = \{1\}$, ou seja, o grupo é abeliano. Pelo resultado de Schwachhofer-Stroppel mencionado anteriormente no Lema 3.1.1,

$$G = Tor(G) \oplus D$$

onde D é um subgrupo livre de torção, divisível e característico e $Tor(G)$ é o conjunto de todos os elementos de torção. Dessa forma, G é um grupo abeliano, de posto finito e tal que $\omega(G) < \infty$, podemos aplicar o Lema 3.1.7 e obter que $Tor(G)$ é um subgrupo finito de G. Assim, para esse caso o resultado segue.

Suponha que o resultado seja válido para grupos G com série derivada de tamanho menor ou igual a $d - 1$.

Vamos provar que vale para grupos G com série derivada de tamanho d. Seja a série derivada,

$$G \geq G^{(1)} \geq G^{(2)} \geq ... \geq G^{(d-1)} \geq G^{(d)} = \{1\}$$

$G^{(d-1)}$ é abeliano, então pelo mesmo argumento

$$G^{(d-1)} = Tor(G^{(d-1)}) \oplus D_1$$

onde D_1 é um subgrupo livre de torção, divisível e característico, $Tor(G^{(d-1)})$ é o conjunto de todos os elementos de torção $G^{(d-1)}$ e $Tor(G^{(d-1)})$ é finito. Podemos então concluir que $Aut(Tor(G^{(d-1)}))$ é finito.

Pela hipótese de indução $G/G^{(d-1)}$ possui um subgrupo $\bar{A}$ livre de torção, radicável, nilpotente e característico tal que $G/G^{(d-1)} = \bar{A} \rtimes \bar{B}$, onde $\bar{B}$ é um subgrupo finito. Como

$\bar{A}$ é radicável e nilpotente, pelo Teorema 1.3.15, temos que $\bar{A} = \bar{A}^n$ para todo $n > 0$.

Por outro lado, como $Tor(G^{(d-1)})$ é normal em $G^{(d-1)}$ que por sua vez é característico em G, temos que o normalizador $N_G(Tor(G^{(d-1)})) = G$. Sabemos que o normalizador age por conjugação no próprio grupo, onde o estabilizador é o centralizador $C_G(Tor(G^{(d-1)}))$. Além disso,

$$\frac{G}{C_G(Tor(G^{(d-1)}))} = \frac{N_G(Tor(G^{(d-1)}))}{C_G(Tor(G^{(d-1)}))} \cong \leq Aut(Tor(G^{(d-1)}))$$

já vimos que $Aut(Tor(G^{(d-1)}))$ é finito, logo, $G/C_G(Tor(G^{(d-1)}))$ é finito.

Seja A a imagem inversa de $\bar{A}$ pelo homomorfismo canônico. Como A age sobre $Tor(G^{(d-1)})$, $\bar{A}$ é livre de torção e $\bar{A}$ não tem subgrupos de índice finito, concluímos que $A \leq C_G(Tor(G^{(d-1)})$. Então $Tor(G^{(d-1)}) \leq Z(A)$ e $Tor(A) = C_G(Tor(G^{(d-1)})$.

Tomando $K = A^e$ onde $e = exp(C_G(Tor(G^{(d-1)}))$, segue que K é livre de torção e tem índice finito em G. Logo, pelo Lema 3.1.6, existe um subgrupo finito H tal que $G = K \rtimes H$ e note que H não possui subgrupos próprios de índice finito. Pelo Lema 3.1.4 temos que K é nilpotente radicável. E a prova está completa.

□

Agora vamos ao Teorema D.

Teorema D. *Seja G um grupo solúvel de ordem mista e de posto finito. $\omega(G) = 3$ se, e somente se, $G = A \rtimes H$ onde $|H| = p$ para algum primo p, H age livre de pontos fixos em A e $A = \mathbb{Q}^n$, onde $n = t(p-1)$ para algum inteiro positivo t.*

Demonstração. Suponha que G é um grupo solúvel de ordem mista e de posto finito tal que $\omega(G) = 3$. Pelo Teorema C, G possui um subgrupo A livre de torção, radicável, nilpotente e característico tal que $G = A \rtimes H$, onde H é um subgrupo finito. O fato de A ser nilpotente nos garante que o centro $Z(A)$ é um subgrupo não trivial, logo como $Z(A)$ é característico, segue que A é abeliano($\mathbb{Q}^n$). Pelo mesmo argumento utilizado na prova para grupos finitos de duas órbitas de automorfismo, H é um p-grupos abeliano elementar.

A é característico, ou seja, invariante por automorfismos, logo, temos que uma das órbitas é ocupada pelos elementos de A, a outra pelos elemento neutro e a última será ocupada pelos elementos em $G \setminus A$. Como o grupo tem ordem mista, todos os elementos

de $G \setminus A$ tem ordem p, e então H age sobre A

$$\begin{aligned} \varphi : H &\to Sym(A) \\ h &\mapsto \varphi(h), \end{aligned}$$

onde

$$\begin{aligned} \varphi(h) : A &\to A \\ a &\mapsto \varphi(h)(a) = hah^{-1}. \end{aligned}$$

A ação de H sobre A é livre de pontos fixos pois, caso haja um ponto fixo, teríamos que existe $a \in A$ tal que para todo $h \in H$, $hah^{-1} = a$, ou seja, a seria central. Mas então como o centro é característico, $A = Z(G)$, porém ao multiplicar a com um elemento em $G \setminus A$ teríamos ordem infinita, o que não pode ocorrer. Logo H age sobre A livre de pontos fixos.

Agora, vamos concluir que H é cíclico. H age sobre $A = \mathbb{Q}^n$, que é um espaço vetorial de dimensão n sobre o corpo $\mathbb{Q}$. Então podemos analisar a representação de H em A, pelo Teorema 1.2.19 temos que H é cíclico.

Agora, veja que A pode ser visto como $\mathbb{Q}H$-módulo. Escreveremos a operação em A como adição e a ação (por conjugação) de H como multiplicação. Como a ordem de H é prima e A é um espaço vetorial sobre um corpo de característica 0, pelo Teorema de Maschke, $A = A_1 \oplus ... \oplus A_r$, onde A_i, $1 \leq i \leq r$, são $\mathbb{Q}H$-módulos irredutíveis. Se $H = \langle \alpha \rangle$ e $|H| = q$, escolhemos uma base para A_i em que α é representada pela matriz companheira de seu polinômio minimal $m_i(\lambda)$ em A_i. Então A_i é determinado a menos de isomorfismo pelo polinômio minimal $m_i(\lambda)$. Agora, vamos mostrar que $A_1, ..., A_r$ são todos módulos isomorfos. Suponha que A_1 não é isomorfo a A_2. Então $m_1(\lambda) \neq m_2(\lambda)$. Seja $0 \neq u_i \in A_i$ $(i = 1, 2)$. Como $\omega(G) = 3$, existe $\sigma \in Aut(G)$ onde $u_1^\sigma = u_1 + u_2$. Agora, $\alpha^{\sigma^{-1}} = \alpha^k w$ para algum $w \in A$, e algum $k \geq 1$ com $(k, q) = 1$. Seja $g(\lambda)$ o polinômio minimal de α^k em A_1. Note que $deg(g) = e$. Considere

$$\begin{aligned} u_1^\sigma g(\alpha) &= u_1^\sigma (g(\alpha^{\sigma^{-1}}))^\sigma \\ &= u_1^\sigma (g(\alpha^k w))^\sigma \\ &= u_1^\sigma (g(\alpha^k))^\sigma \\ &= [u_1 g(\alpha^k)]^\sigma = 0. \end{aligned}$$

Então, $(u_1 + u_2)g(\alpha) = 0$. Mas o polinômio minimal de α em $u_1 + u_2$ é $m_1(\lambda)m_2(\lambda)$, pois $m_1 \neq m_2$ implica que $(m_1, m_2) = 1$. Como $degg = degm_i$, temos uma contradição. Então os termos A_i são $\mathbb{Q}H$-módulos isomorfos.

Reciprocamente, suponha que $G = A \rtimes H$ onde $|H| = p$ para algum primo p, H age de maneira a não deixar pontos fixos em A e $A = \mathbb{Q}^n$ para algum inteiro positivo n. Vamos mostrar que todos os elementos em $G \setminus A$ tem ordem p.

Seja $h \in H$, tal que $H = \langle h \rangle$, como H é cíclico de ordem p, $h^p = 1$. Esse elemento, h, induz um operador linear que iremos definir como, $T_h : \mathbb{Q}^n \to \mathbb{Q}^n$ dado por $a \mapsto a^h$.

Dado que o polinômio minimal divide

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + ... + x + 1)$$

segue que $m_h(x) = x^{p-1} + x^{p-2} + ... + x + 1$, por que h age de maneira a não deixar pontos fixos em A, assim 1 não pode ser autovalor. O que nos mostra que o polinômio minimal não divide $(x-1)$. A seguir provaremos uma identidade importante para concluir a argumentação,

$$\begin{aligned} x^n(y^{x^{n-1}})...y^x y =& x^n(x^{n-1-1}yx^{n-1})...x^{-1}yxy \\ =& xyx^{n-1}...x^{-1}yxy \\ =& xyxy..xy \\ =& (xy)^n. \end{aligned}$$

Com a identidade provada acima, obtemos que

$$(h^j a)^p = h^{jp}(a^{h^{j(p-1)}})...a^{h^j}a = 1.$$

Isso mostra que todos os elementos em $G \setminus A$ tem ordem p.

Agora falta mostrar que são três órbitas de automorfismo. Sejam $b, c \in A \setminus \{1\}$ e $\alpha, \beta \in G \setminus A$. Pelo Teorema 1.1.25 existem $b_1, b_2, ..., b_t, c_1, c_2, ..., c_t$ vetores de A tais que

$$\{b_1, T_\alpha(b_1), ..., T_\alpha^{p-2}(b_1), b_2, ..., T_\alpha(b_2), ..., T_\alpha^{p-2}(b_2), b_t, T_\alpha(b_t), ..., T_\alpha^{p-2}(b_t)\} \tag{3.1}$$

e

$$\{c_1, T_\beta(c_1), ..., T_\beta^{p-2}(c_1), c_2, ..., T_\beta(c_2), ..., T_\beta^{p-2}(c_2), c_t, T_\beta(c_t), ..., T_\beta^{p-2}(c_t)\}$$

formam bases de A. Sem perda de generalidade, podemos supor que $b = b_1$ e $c = c_1$, assim o mapeamento dados por

$$b_i \mapsto c_i \text{ e } \alpha \mapsto \beta$$

se estende a um automorfismo.

Então todo elemento não trivial de A pertence a mesma órbita e todo elemento de $G \setminus A$ pertence a mesma órbita. Como (3.1) é base de A, $A = \mathbb{Q}^n$ se decompõe na soma direta de t subespaços de dimensão $p - 1$ e prova está completa. □

Capítulo

4

Grupos finitos com 4 órbitas por automorfismos

Este capítulo se baseia em [12], onde os autores caracterizam os grupos finitos solúveis com $\omega(G) = 4$. O objetivo é provar o seguinte resultado.

Teorema B [Laffey & MacHale (1986)]**.** *Seja G um grupo finito solúvel de ordem mista tal que $\omega(G) = 4$. Então $|G| = p^a q^b$, para p, q primos distintos. E o grupo G tem um p-subgrupo de Sylow normal $P \in Syl_p(G)$. Seja $Q \in Syl_q(G)$. Então um dos itens vale,*

1. *Q age livre-de-pontos-fixos em P, $|Q| = q$ e $\omega(P) = 2$ ou $\omega(P) = 3$;*
2. *P é abeliano elementar e Q é cíclico de ordem 4 ou o quatérnio de ordem 8;*
3. *$G = P \times Q$, onde P e Q são abelianos elementares.*

Demonstração. Primeiramente, vamos provar que $|\pi(G)| = 2$. G possui 4 órbitas por automorfismo, então $|\pi(G)| \in \{1, 2, 3\}$. Como G não é um p-grupo, não pode ocorrer $|\pi(G)| = 1$. Suponha então que $|\pi(G)| = 3$. Considere $\pi(G) = \{p, q, r\}$, onde p é tal que $O_p(G) \neq 1$. Como G possui exatamente 4 órbitas e $O_p(G)$ char G, temos que $O_p(G) = P$, com $P \in Syl_p(G)$. Ademais, podemos supor que $O_q(G/O_p(G)) \neq 1$, pois G é solúvel. Sejam $Q \in Syl_q(G)$, $R \in Syl_r(G)$ e considere o subgrupo normal $N = QP$. Considere $1 \neq x \in R$, como G admite apenas elementos de ordem p, q e r, temos que x age livre de pontos fixos em N. Assim, N admite um automorfismo livre de pontos fixos de ordem prima r, pelo Teorema 1.4.20 (Thompson), N é nilpotente. N tem elementos de ordem p

e q, assim, sabemos que N, e portanto G, tem ao menos um elemento de ordem pq. Uma contradição. Donde $|\pi(G)| = 2$.

Sejam $\pi(G) = \{p, q\}$ e $P \in Syl_p(G)$. Primeiramente, suponha por absurdo que P não é normal. Como $\Omega_1(Z(O_p(G)))$ char G e $\omega(G) = 4$, $O_p(G)$ ocupa duas órbitas e portanto, $O_p(G)$ é p-abeliano elementar. Além disso, $G/O_p(G)$ é um grupo com três órbitas por automorfismos. Pela classificação de grupos com três órbitas por automorfismos (Teorema A), $G/O_p(G)$ se decompõe como produto semidireto de um p-subgrupo de Sylow com um q-subgrupo de Sylow de $G/O_p(G)$. Como $O_p(G) < P$, $P/O_p(G)$ é um p-subgrupo de Sylow de $G/O_p(G)$ que não é normal. Logo $QO_p(G)/O_p(G)$ é normal em $G/O_p(G)$, para $Q \in Syl_q(G)$. Então, temos que $QO_p(G)$ é normal em G, Q é abeliano elementar de ordem $q^{t(p-1)}$ e $|P/O_p(G)| = p$. Assim, $QO_p(G)$ tem três órbitas e pela classificação de grupos com três órbitas por automorfismos em temos que Q é cíclico de ordem q. Então $t = p - 1 = 1$, tal que $p = 2$ e $G/O_p(G)$ é o grupo diedral de ordem $2q$.

$$\frac{G}{O_p(G)} = \langle aO_p(G), bO_p(G) | a^q O_p(G) = O_p(G) = b^2 O_p(G), a^b O_p(G) = a^{-1} O_p(G) \rangle$$

Analisando as órbitas de automorfismos, temos dois casos,

- $1, 2, q, 2$;
- $1, 2, q, 4$.

onde as órbitas são representadas pela ordem dos elementos de sua respectiva órbita.

Caso ocorresse $1, 2, q, 2$, P seria abeliano e portanto, $P \leq C_G(O_p(G)) = O_p(G)$. Logo, temos as órbitas representadas por $1, 2, q, 4$. E P tem expoente 4. O subgrupo $QO_p(G)$ é característico em G, pois todo elemento em $P \setminus O_p(G)$ tem ordem 4. Pelo Argumento de Frattini, $G = O_p(G)N_G(Q)$. Então $N_G(Q)$ contém um elemento de ordem 2 que não pertence a $O_2(G)$, digamos β. Seja $Q = \langle \alpha \rangle$. Então $[\alpha, \beta^2] \in Q$ e $1 \neq \beta^2 \in O_2(G)$. Assim, $[\alpha, \beta^2] = 1$, e $\alpha\beta^2$ é um elemento de ordem $2q$. Uma contradição, logo P é normal em G.

Em seguida, vamos classificar os grupos. Se P não é abeliano elementar, então P possui exatamente três órbitas por automorfismos, cada órbita com elementos de ordens 1,p e p^2. Tomando um elemento de G que não pertence a P, pelo número restrito de órbitas, concluímos que esse elemento tem ordem q e age livre de pontos fixos em P. Logo, Q é cíclico e $|Q| = q$. Nesse caso, o grupo está descrito em *1.*

Suponha que P é abeliano elementar, isto é, todo elemento de P tem ordem p e portanto, G não possui elementos de ordem potência de p com expoente maior que 1. Analisando as órbitas de automorfismos, temos quatro casos:

- $1, p, p, q$;
- $1, p, q, q$;
- $1, p, q, q^2$;
- $1, p, q, pq$.

Onde as órbitas são representadas pela ordem dos elementos de sua respectiva órbita.

Caso tenhamos os representantes $1, p, p$ e q, sabemos que P ocupa três das quatro órbitas por automorfismo e qualquer elemento que não está em P, tem ordem q. Como já argumentamos, esse representa o caso *1.*

Se as órbitas por automorfismos são representadas por $1, p, q, q$ ou $1, p, q, q^2$, Q age livre de pontos fixos em P. Assim, pelo Teorema 1.4.9 Q é cíclico de ordem q^2 ou é o quatérnio generalizado de ordem $8 (q = 2)$.

Vamos analisar o último caso $1, p, q, pq$. Esse caso nos dá que tanto P quanto Q são abelianos elementares. Para cada subgrupo maximal A de Q, seja $C_P(A)$ o centralizador de A em P.

Supondo que $O_q(G) \neq 1$, temos que $O_p(G) \times O_q(G)$ é um subgrupo característico de G que ocupa 4 órbitas de automorfismos. Então $O_p(G) \times O_q(G) = G$. Nesse caso, temos o grupo descrito em *3.*

Agora, se $O_q(G) = 1$, Q age fielmente em P. Pelo Teorema 1.2.17 (Maschke), P é a soma direta de $GF(p)Q$-módulos irredutíveis, digamos,

$$P = P_1 \oplus ... \oplus P_m.$$

Seja $|Q| = q^b$. Se $b = 1$, então Q é cíclico e temos o grupo descrito em *1.*. Suponha então que $b > 1$, vamos mostrar que existe um elemento $z \in G$, tal que $C_P(z) = 1$, ou seja, z age livre de ponto fixo em P. Como Q é abeliano elementar, Q/Q_i é cíclico, em que Q_i denota o núcleo da representação de Q em P_i, $1 \leq i \leq m$. Mas como $b > 1$, Q é não cíclico, então $Q_i \neq 1$. Escolhendo $y_i \in Q_i^*$, temos $P_i \subseteq C_P(y_i)$, donde

$$P = \sum_{y \in Q^*} C_P(y).$$

Dado $y \in Q$, existe $\bar{y} \in Q$ tal que $\bar{y}$ age livre de pontos fixos em $C_P(y)$. Caso contrário, $C_P(y)$ seria central em G, contrariando $O_q(G) = 1$. Assim, tomando z como sendo o produto dos elementos que agem livres de pontos fixos em cada $C_P(y)$, temos que $C_P(z) = 1$.

Dado $\varphi \in Aut(G)$, provaremos que se $C_P(z) = 1$, então $C_P(z^\varphi)$. Se $[z^\varphi, x] = 1$, para algum $x \in P$, então,

$$\begin{aligned} 1 = [z^\varphi, x]^{\varphi^{-1}} &= ((z^\varphi)^{-1} x^{-1} z^\varphi x)^{\varphi^{-1}} \\ &= ((z^{-1})^\varphi x^{-1} z^\varphi x)^{\varphi^{-1}} \\ &= ((z^{-1})^\varphi)^{\varphi^{-1}} (x^{-1})^{\varphi^{-1}} (z^\varphi)^{\varphi^{-1}} x^{\varphi^{-1}} \\ &= z^{-1} (x^{-1})^{\varphi^{-1}} z x^{\varphi^{-1}} \\ &= [z, x^{\varphi^{-1}}] \end{aligned}$$

mas z age livre de ponto fixo em P e $x^{\varphi^{-1}} \in P$, logo $x = 1$. Isso mostra que existe pelo menos uma órbita para elementos que agem livre de pontos fixos em P. No entanto, como existem elementos de ordem pq em G, existe outra órbita para elementos de fixam ao menos um ponto em P. Logo $\omega(G) > 4$. Assim, o caso $b > 1$ não ocorre e o teorema está provado.

□

Capítulo

5

Considerações finais

Ao longo deste trabalho, classificamos grupos finitos (não p-grupos) com $\omega(G) = 3$, grupos de ordem mista com posto finito e $\omega(G) = 3$ e grupos finitos solúveis com $\omega(G) = 4$. Apresentamos a seguir alguns resultados.

Em [14], Maurer e Stroppel, classificaram grupos abelianos com no máximo 3 órbitas,

Teorema 5.1. *Um grupo abeliano é quase homogêneo se e somente se é um grupo aditivo de um módulo livre sobre R, onde $R = \mathbb{Q}$ ou $R \in \{\mathbb{Z}(p), \mathbb{Z}(p^2)\}$ para algum primo p.*

Os autores Laffey e MacHale, em [12], classificaram grupos não solúveis com 4 órbitas por automorfismos,

Teorema 5.2. *Seja G um grupo finito não solúvel, com $\omega(G) \leq 4$, então G é isomorfo a $PSL(2, \mathbb{F}_4)$.*

Além disso, em [3], Bastos, Dantas e Garonzi provaram,

Teorema 5.3. *Seja G um grupo finito não solúvel com $\omega(G) \leq 6$. Então G é isomorfo a $PSL(2, \mathbb{F}_4)$, $PSL(2, \mathbb{F}_7)$, $PSL(2, \mathbb{F}_8)$, $PSL(2, \mathbb{F}_9)$, $PSL(3, \mathbb{F}_4)$ ou $ASL(2, \mathbb{F}_9)$. Ademais, $\omega(PSL(2, \mathbb{F}_4)) = 4$, $\omega(PSL(2, \mathbb{F}_7)) = 5$, $\omega(PSL(2, \mathbb{F}_8)) = 5$, $\omega(PSL(2, \mathbb{F}_9)) = 5$, $\omega(PSL(3, \mathbb{F}_4)) = 6$ e $\omega(ASL(2, \mathbb{F}_4)) = 6$.*

Por fim, em [2], os autores provaram que se G é um grupo virtualmente nilpotente com $\omega(G) < \infty$, então o grupo admite uma escrita $G = K \rtimes H$, onde H é um subgrupo de torção e K é um subgrupo livre de torção característico, nilpotente e radicável. Além disso, $G' = D \times Tor(G')$ onde D é um subgrupo livre de torção nilpotente, característico e radicável.

Referências Bibliográficas

[1] R. Bastos, A.C. Dantas, and E. de Melo. Soluble groups with few orbits under automorphisms. *Geometriae Dedicata*, 209(1):119–123, Mar 2020.

[2] R. Bastos, A.C. Dantas, and E. de Melo. Virtually nilpotent groups with finitely many orbits under automorphisms. *Archiv der Mathematik*, 116(3):261–270, Feb 2021.

[3] R. Bastos, A.C. Dantas, and M. Garonzi. Finite groups with six or seven automorphism orbits. *Journal of Group Theory*, 21:945–954, Jan 2017.

[4] A. Bors and S.P. Glasby. Finite 2-groups with exactly three automorphism orbits, 2020.

[5] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.

[6] D. Gorenstein. *Finite Groups*. Chelsea Publishing Company, New York, N.Y., 2nd edition, 1980.

[7] M. Hall. *Theory of Groups*. The Macmillan Company, New York, 1963.

[8] K. Hoffman and R.A. Kunze. *Linear Algebra*. PHI Learning, second edition, 2004.

[9] B. Huppert. *Endliche Gruppen I*. Springer-Verlag, 1967.

[10] E.I. Khukhro. *P-Automorphisms of finite p-groups*. Clarendon Press, Oxford, 2004.

[11] E.I. Khukhro. *Nilpotent groups and their Automorphism*. De Gruyter,, 2011.

[12] Thomas J. Laffey and D. MacHale. Automorphism orbits of finite groups. *Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics*, 40(2):253–260, 1986.

[13] J.C. Lennox and D.J.S. Robinson. *The Theory of Infinite Soluble Groups*. Clarendon Press, Oxford, 2004.

[14] H. Mäurer and M. Stroppel. Groups that are almost homogeneous. *Geometriae Dedicata*, 68:229–243, 1997.

[15] D.J.S. Robinson. *A Course in the Theory of Groups*. Springer, Berlin, 1996.

[16] M. Schwachhöfer and M. Stroppel. Finding representatives for the orbits under the automorphism group of a bounded abelian group. *J. Algebra*, 221:225–239, 1999.