Universidade de Brasília

Automorfismos Involutivos Quase Regulares de Grupos Unicamente 2-Divisíveis

Samuel Terto de Sousa Rodrigues

Orientador: Prof. Dr. Pavel Shumyatsky

Departamento de Matemática
Universidade de Brasília

Dissertação apresentada como requisito parcial para obtenção do grau de
Mestre em Matemática

Brasília, 28 de Março de 2025

À minha família.

Agradecimentos

Agradeço primeiramente a Deus pelo Seu cuidado!

À minha família, à minha mãe Edilene, ao meu pai Antônio e a minha irmã Jaciara, pelo apoio incondicional em todas as circunstâncias enfrentadas.

Ao meu orientador Prof. Dr. Pavel Shumyatsky pela paciência, disponibilidade e atenção dedicada neste período.

Aos professores Emerson de Melo, Jhone Caldeira e Igor Lima pelo aceite em integrar a banca de avaliação desta dissertação.

Aos professores do Programa de Pós-graduação em Matemática da UnB, em especial Manuela Resende, Luciana Ávila, Sheila Chagas, Maurício Ayala, Raimundo Bastos, Noraí Rocco e Ma To Fu, pela contribuição na minha formação.

A todos os meus professores da graduação na Universidade Federal do Acre, especialmente os professores Ivan Ramos, Sérgio Brazil, Sandro Ricardo, Marcos Aurélio, Lidermir Arruda, Simone Chalub, Salete Chalub, Altemir Braga, Daiana Viana e José Ronaldo, pelos ensinamentos e incentivos para ingresso em um curso de mestrado.

Aos funcionários do Departamento de Matemática da UnB, que de muitas formas me ajudaram a chegar neste momento.

Aos meus amigos e colegas do MAT-UnB: Ângelo Machado, Fabiane Soares, Thafne Sirqueira, Paul Vilca, Ronaldo Murakami, Thais Marçal, Daniel Abreu, Débora Senise, Vítor Machado, Pako, Guilherme, Valdemir, Josy, Tharles Araújo, Mateus Figueiredo, Jonatas Peralta, Talita Matias, Vitória Henryla, Emanuelle Ortega, Gabriela Ferreira, Gabriella Cristina, Alexandre Oliveira, Santiago Benites, Juan Suasnanbar e Eduardo Freire, pelo apoio e a amizade construída durante o curso.

Aos meus amigos e colegas de graduação: Iglesson Menezes, Henrique Oliveira, Gustavo Mapeano, Andréia Freitas, Bruno Rodrigues, Wesley Bezerra, Weslley Rodrigues, Francisco Sampaio, Francisco Nunes e Paula Vitória, pelos incentivos.

Ao CNPq pelo apoio financeiro durante a elaboração deste trabalho, sem o qual não seria possível a realização deste curso de mestrado.

Resumo

Este trabalho fornece uma demonstração detalhada de um teorema devido a Yoav Segev, onde se consideram grupos G nos quais, para todo elemento $x \in G$, existe um único elemento $y \in G$ tal que $y^2 = x$. Supondo que G admita um automorfismo involutivo quase regular, Segev prova que G é solúvel. Este resultado complementa, de certa forma, o teorema de Shunkov, que afirma que um grupo periódico G admitindo um automorfismo involutivo quase regular é virtualmente solúvel.

Palavras chave: Automorfismos involutivos quase regulares, grupos unicamente 2-divisíveis, grupos solúveis.

Abstract

This work provides a detailed proof of a theorem due to Yoav Segev, which considers groups G where, for every element $x \in G$, there exists a unique element $y \in G$ such that $y^2 = x$. Assuming that G admits an almost regular involutory automorphism, Segev proves that G is solvable. This result complements, in a certain sense, Shunkov's theorem saying that a periodic group G admitting an almost regular involutory automorphism is virtually solvable.

Keywords: Almost regular involutory automorphisms, uniquely 2-divisible groups, solvable groups.

Conteúdo

Lista de Símbolos

$C_G(X)$	Centralizador do conjunto X no grupo G;
$C_G(\varphi)$	Centralizador do automorfismo φ em G;
G'	Subgrupo derivado de G;
$G \cong H$	G é isomorfo a H;
$H \trianglelefteq G$	H é subgrupo normal em G;
$Z(G)$	Centro do grupo G;
$\dot{\bigcup}$	União disjunta;
$\mathrm{Im}\varphi$	Imagem da aplicação φ;
$\ker\varphi$	Núcleo da aplicação φ;
$\prod_{i=1}^{n} x_i$	Produto dos elementos x_i com $i = 1, 2, \ldots, n$;
g^h	Conjugação de g por h, isto é, $h^{-1}gh$;
xH	Classe lateral à esquerda de H;
x^f	Imagem de x pela aplicação f;
$\square$	Indica o fim de uma demonstração.

Introdução

Seja φ um automorfismo de um grupo G. Dizemos que φ é um automorfismo involutivo se $\varphi \neq Id$ e $\varphi^2 = Id$, ou seja, se φ é um elemento de ordem dois no grupo de automorfismos de G. Chamamos de centralizador do automorfismo φ em G o subgrupo dos pontos fixos de φ dado por

$$C_G(\varphi) := \{g \in G \mid \varphi(g) = g\}.$$

Se $C_G(\varphi)$ for finito, dizemos que φ é um automorfismo quase regular. Quando $C_G(\varphi) = \{1\}$, dizemos que φ é um automorfismo regular ou livre de pontos fixos.

Ao longo do século passado, alguns matemáticos como W. Burnside, B. H. Neumann, J. G. Thompson, G. Higman e outros perceberam que o subgrupo $C_G(\varphi)$ tem forte relação com a estrutura do grupo G. Veja, por exemplo, os seguintes teoremas de W. Burnside [1] de 1911:

Teorema. *Sejam G um grupo finito e φ um automorfismo de G que possui ordem m. Então, a ordem do centralizador de φ em G é congruente à ordem de G módulo m. Em símbolos,*

$$|C_G(\varphi)| \equiv |G| \pmod{m}.$$

Teorema. *Se G é um grupo finito que admite um automorfismo de ordem 2 livre de pontos fixos, então G é abeliano.*

O trabalho de Burnside nesse campo contribuiu para dar início a uma abordagem sistemática que consiste em compreender grupos através do estudo de seus automorfismos e simetrias. A partir daí, muitos avanços foram possíveis em Teoria de Grupos. Em 1956, B. H. Neumann [5] provou que, se um grupo finito admite um automorfismo de ordem 3 livre de pontos fixos, então o grupo é nilpotente de classe no máximo 2. Nesse sentido, um teorema mais geral é obtido a partir da junção dos teoremas de Higman [4] e Thompson [11]:

Teorema. *Se G é um grupo finito que admite um automorfismo livre de pontos fixos, cuja ordem é um primo p, então, G é um grupo nilpotente e sua classe de nilpotência é limitada por uma função $h(p)$, que depende apenas de p.*

Em 1974, V. P. Shunkov [10] provou que em um grupo periódico G, que admite um automorfismo de ordem 2 com o centralizador finito, todo subgrupo finitamente gerado de G é finito, e mais, G possui um subgrupo solúvel de índice finito. Em outras palavras, temos o seguinte teorema:

Teorema. *Se um grupo periódico G possui um automorfismo involutivo quase regular, então G é localmente finito e virtualmente solúvel.*

Inspirado pelas técnicas introduzidas por Shunkov no artigo [10], Y. Segev [9] provou o Teorema A, abaixo, que é o assunto central desta dissertação. Antes de enunciá-lo, precisamos esclarecer o que é um grupo unicamente 2-divisível: denominamos dessa forma os grupos G nos quais para cada $x \in G$ existe um único elemento $y \in G$ tal que $y^2 = x$.

Teorema A. *Seja U um grupo unicamente 2-divisível. Se U admite um automorfismo involutivo quase regular, então U é solúvel.*

Observe que tanto este teorema como aquele provado por Shunkov também ressaltam uma relação entre o centralizador do automorfismo do grupo e a estrutura desse grupo e, neste caso, a propriedade em questão é a solubilidade. Em seu artigo, Segev escreveu que a sua maior motivação para este teorema vem de questões sobre os grupos radicais de conjuntos especiais de Moufang que, segundo ele, tendem a ser grupos unicamente 2-divisíveis; este assunto não será abordado neste trabalho, porém pode ser encontrado em [8].

Nesta dissertação, objetivamos apresentar a prova do Teorema A, obtido em 2011 por Segev em [9]. Faremos isto buscando usar apenas conceitos elementares da Teoria de Grupos.

O texto está organizado da seguinte maneira: no primeiro capítulo, intitulado "Noções Preliminares" discorremos sobre alguns conceitos fundamentais da Teoria de Grupos, como automorfismos, ações de grupos, produto semidireto e grupos solúveis. Estes assuntos são necessários para atingir a compreensão dos resultados e demonstrações que estão ao longo do texto. O segundo capítulo trata dos grupos unicamente 2-divisíveis; vamos defini-los e apresentar algumas de suas propriedades, como a sua caracterização no contexto de grupos finitos e quando essa propriedade é herdada por subgrupos. O terceiro e último capítulo, que foi chamado de "A prova do Teorema A" enuncia e demonstra todos os resultados auxiliares e fundamentais para a prova do teorema de Segev.

Capítulo 1

Noções Preliminares

Vamos assumir que o leitor possui domínio sobre os conceitos mais básicos da Teoria de Grupos. Sendo assim, no que se segue, iremos percorrer um caminho que objetiva somente alcançar a compreensão dos resultados aos quais se dedica esta dissertação. As principais referências bibliográficas utilizadas para a construção deste capítulo foram os livros de A. Garcia e Y. Lequain [3] e de D. J. Robinson [7].

1.1 Grupos e Subgrupos

Nesta seção abordaremos alguns conceitos importantes, tais como grupos quocientes, subgrupos gerados por subconjuntos, grupos finitamente gerados, centralizadores, subgrupos derivados, etc. Em seguida, também trataremos a respeito de alguns teoremas que são fundamentais para os resultados dos próximos capítulos.

Começamos definindo grupo quociente. Considere G um grupo e H um subgrupo fixado de G. Podemos definir a seguinte relação de equivalência sobre G: dados $x, y \in G$, $y \sim_H x$ se, e somente se, $y = xh$ para algum $h \in H$. A classe de equivalência que contém x é o subconjunto de G denotado por xH e definido por

$$xH = \{xh \mid \ h \in H\}.$$

Este será chamado de *classe lateral à esquerda* de H em G. Analogamente, podemos definir a *classe lateral à direita* de H em G. Note que dizer que $x \in H$ é equivalente a dizer que $xH = H$. Pelas propriedades de relações de equivalência, para $x, y \in G$ vale que:

(1) se $xH \neq yH$, então $xH \cap yH = \varnothing$;

(2) $xH = yH$ se, e somente se, $x^{-1}y \in H$;

(3) $\bigcup_{x\in G} xH = G$.

Chamamos de índice de H em G, e denotamos por $|G:H|$, o número de classes laterais à esquerda (ou à direita) de H em G.

Se tomamos um representante para cada classe lateral à esquerda de H em G, pelo Axioma da Escolha, obtemos um conjunto T formado por esses representantes. Podemos então escrever G como a seguinte união disjunta:

$$G = \dot{\bigcup}_{t\in T} tH.$$

Assim, todos os elementos de G poderão ser escritos de forma única como o produto th, com $t \in T$ e $h \in H$. Chamaremos o conjunto T de *transversal à esquerda* de H em G. De maneira análoga, definimos *transversal à direita*. A cardinalidade de T é igual ao índice de H em G. Vejamos agora alguns resultados sobre índices.

Teorema 1.1.1. *Sejam G um grupo, H um subgrupo de G e K um subgrupo de H. Sejam T um transversal à esquerda de H em G e U um transversal à esquerda de K em H, então $TU = \{tu \mid t \in T, u \in U\}$ é um transversal à esquerda de K em G. Além disso, $|G:K| = |G:H| \cdot |H:K|$.*

Demonstração. Temos que $G = \dot{\bigcup}_{t\in T} tH$ e $H = \dot{\bigcup}_{u\in U} uK$. Substituindo H obtemos que $G = \dot{\bigcup}_{t\in T, u\in U} tuK$. Agora, resta mostrar que todas as classes laterais tuK são distintas. Suponha que $t_1u_1K = t_2u_2K$ com $t_1, t_2 \in T$ e $u_1, u_2 \in U$. Então, $t_1u_1 \in t_2u_2K$ e podemos escrever $t_1u_1 = t_2u_2k$, com $k \in K$, assim, temos $t_2^{-1}t_1 = u_2ku_1^{-1} \in H$. Logo, $t_1H = t_2H$, como T é um transversal, segue que $t_1 = t_2$. Portanto, $u_1K = u_2K$, donde $u_1 = u_2$ pois U é um transversal. Concluímos então que TU é um transversal à esquerda de H em G. Veja ainda que, como a cardinalidade de TU é igual ao produto das cardinalidades de T e U, temos que $|G:K| = |G:H| \cdot |H:K|$. □

Teorema 1.1.2. *(Poincaré) A interseção de um conjunto finito de subgrupos, cada um dos quais com índice finito, também tem índice finito.*

Demonstração. Sejam G um grupo e $H_1, H_2, ..., H_n$ subgrupos de G. Defina $H = \bigcap_{i=1}^{n} H_i$. Basta demonstrar que $|G:H| \leq |G:H_1| \cdot |G:H_2| \cdot ... \cdot |G:H_n|$.

Para cada $x \in G$ associamos a n-úpla de classes laterais à esquerda $(xH_1, xH_2, ..., xH_n)$. Veja que para $x, y \in G$ temos $(xH_1, xH_2, ..., xH_n) = (yH_1, yH_2, ..., yH_n)$ se, e somente se, $xH_i = yH_i$, para $i = 1, 2, ..., n$, e isso equivale a $x^{-1}y \in H_i$ para $i = 1, 2, ..., n$, de onde obtemos que $x^{-1}y \in H$. Sendo assim, temos que $xH = yH$. Portanto, a aplicação $xH \mapsto (xH_1, xH_2, ..., xH_n)$

é injetiva, e por isso, vale a desigualdade acima. Então, como $|G : H_i|$ é finito para $i = 1,2,...,n$, segue que $|G : H|$ é finito. □

O conjunto das classe laterais à esquerda $G/\sim_H = \{xH \mid x \in G\}$ possui uma operação induzida pela operação de G, dada por

$$(xH, yH) \mapsto xyH.$$

Tal operação está bem definida quando H é um subgrupo normal em G, pois independe dos representantes das classes. Isto, nos leva a seguinte

Definição 1.1.3. Sejam G um grupo e H um subgrupo normal em G. O grupo de suas classes laterais, com a operação induzida de G, é chamado de *grupo quociente* de G por H. Ele será denotado por G/H.

Agora, vamos definir alguns subgrupos importantes.

Definição 1.1.4. Seja X subconjunto não vazio de um grupo G. Definimos o subgrupo gerado por X como a interseção de todos os subgrupos de G que contém X, e o denotamos por $\langle X \rangle$. Também podemos entendê-lo como o menor subgrupo de G que contém X, isto é, se $X \subseteq S \leq G$, então $\langle X \rangle \subseteq S$.

Para descrever os elementos de um subgrupo gerado por um subconjunto temos a seguinte

Proposição 1.1.5. *Se X é um subconjunto não vazio de um grupo G, então $\langle X \rangle$ é o conjunto de todos os elementos da forma $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$, onde $\alpha_i = \pm 1$, $x_i \in X$ e $k \geq 0$ (quando $k = 0$, este produto é interpretado como* 1*).*

Dizemos que G é um *grupo finitamente gerado* se G pode ser gerado por um subconjunto com um número finito de elementos.

Definição 1.1.6. Sejam G um grupo e X um subconjunto não vazio de G. Chamamos de *centralizador de X em G*, e denotamos por $C_G(X)$, o conjunto de todos os elementos $g \in G$ tais que $gx = xg$, para todo elemento $x \in X$. Quando $X = G$ o centralizador $C_G(X)$ será chamado de *centro de G* e denotado por $Z(G)$.

Naturalmente, $C_G(X)$ é um subgrupo de G, pois $1_G \in C_G(X)$ e para quaisquer $a, b \in C_G(X)$ temos que $ab^{-1} \in C_G(X)$.

Outra observação interessante é que, se H é um subgrupo finitamente gerado de G, isto é, se $H = \langle g_1, g_2, \ldots, g_n \rangle$ onde cada $g_i \in G$ com $i = 1,2,\ldots,n$, então

$$C_G(H) = \bigcap_{i=1}^{n} C_G(g_i).$$

Para verificar isto, perceba que $C_G(H)$ está contido em $\bigcap_{i=1}^{n} C_G(g_i)$, pois dado $x \in C_G(H)$ temos que x centraliza qualquer elemento de H, inclusive seus geradores, então $x \in \bigcap_{i=1}^{n} C_G(g_i)$. Por outro lado, se $x \in \bigcap_{i=1}^{n} C_G(g_i)$, temos que x centraliza cada g_i e, consequentemente, x centraliza qualquer produto entre $g_1, g_2, \ldots, g_n$; ou seja, x centraliza os elementos de H. Logo, $x \in C_G(H)$ e, portanto, a inclusão contrária é válida. Daí, verifica-se a igualdade.

Antes de expor o próximo subgrupo, precisamos definir o comutador de dois elementos de um grupo.

Definição 1.1.7. Sejam x e y elementos de um grupo G. O comutador de x e y, nesta ordem, é o elemento de G dado por $x^{-1}y^{-1}xy$ e denotado por $[x,y]$.

Proposição 1.1.8. *Sejam x, y e z elementos quaisquer em G. Os comutadores desses elementos possuem as seguintes propriedades:*

(1) $[x,y] = 1$ *se, e somente se,* $xy = yx$;

(2) $[x,y] = [y,x]^{-1}$;

(3) $[x,y]^z = [x^z, y^z]$;

(4) $[x,yz] = [x,z][x,y]^z$;

(5) $[xy,z] = [x,z]^y[y,z]$;

(6) $[x,y^{-1}] = ([x,y]^{y^{-1}})^{-1}$;

(7) $[x^{-1},y] = ([x,y]^{x^{-1}})^{-1}$.

Demonstração. (1) A equação $[x,y] = 1$ é equivalente a $x^{-1}y^{-1}xy = 1$, o que acontece se, e somente se, $xy = yx$;

(2)

$$[x,y] = x^{-1}y^{-1}xy = (y^{-1}x^{-1}yx)^{-1} = [y,x]^{-1};$$

(3)

$$\begin{aligned}[x,y]^z &= (x^{-1}y^{-1}xy)^z \\ &= z^{-1}x^{-1}y^{-1}xyz \\ &= z^{-1}x^{-1}(zz^{-1})y^{-1}(zz^{-1})x(zz^{-1})yz \\ &= (z^{-1}x^{-1}z)(z^{-1}y^{-1}z)(z^{-1}xz)(z^{-1}yz) \\ &= (z^{-1}xz)^{-1}(z^{-1}yz)^{-1}z^{-1}xzz^{-1}yz \\ &= (x^z)^{-1}(y^z)^{-1}x^zy^z = [x^z,y^z];\end{aligned}$$

(4)

$$\begin{aligned}[x,yz] &= x^{-1}(yz)^{-1}xyz \\ &= x^{-1}z^{-1}y^{-1}xyz \\ &= x^{-1}z^{-1}(xzz^{-1}x^{-1})y^{-1}xyz \\ &= x^{-1}z^{-1}xzz^{-1}(x^{-1}y^{-1}xy)z \\ &= x^{-1}z^{-1}xz(x^{-1}y^{-1}xy)^z = [x,z][x,y]^z;\end{aligned}$$

(5)

$$\begin{aligned}[xy,z] &= (xy)^{-1}z^{-1}(xy)z \\ &= y^{-1}x^{-1}z^{-1}xyz \\ &= y^{-1}x^{-1}z^{-1}x(zyy^{-1}z^{-1})yz \\ &= y^{-1}(x^{-1}z^{-1}xz)yy^{-1}z^{-1}yz \\ &= (x^{-1}z^{-1}xz)^yy^{-1}z^{-1}yz = [x,z]^y[y,z];\end{aligned}$$

(6)

$$\begin{aligned}[x,y^{-1}] &= x^{-1}yxy^{-1} \\ &= yy^{-1}x^{-1}yxy^{-1} \\ &= (yx^{-1}y^{-1}xyy^{-1})^{-1} \\ &= ((x^{-1}y^{-1}xy)^{y^{-1}})^{-1} = ([x,y]^{y^{-1}})^{-1};\end{aligned}$$

(7)

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

□

Agora, podemos fazer a

Definição 1.1.9. Sejam X e Y subconjuntos não vazios de um grupo G. Definimos

$$[X,Y] = \langle [x,y] \mid \ x \in X \text{ e } y \in Y \rangle.$$

Quando $X = Y = G$, chamamos $[G,G]$ de *subgrupo derivado* ou *subgrupo comutador de* G e o denotamos por G'.

Agora, veremos alguns resultados importantes sobre grupos.

Proposição 1.1.10. *Seja G um grupo. O subgrupo derivado G' é normal em G.*

Demonstração. Considere $g \in G$ e $\alpha = [x_1,y_1][x_2,y_3]\dots[x_n,y_n] \in G'$. Tendo em vista a propriedade *(3)* da Proposição 1.1.8, obtemos que

$$\begin{aligned}\alpha^g &= ([x_1,y_1][x_2,y_3]\dots[x_n,y_n])^g \\ &= [x_1,y_1]^g[x_2,y_3]^g\dots[x_n,y_n]^g \\ &= [x_1^g,y_1^g][x_2^g,y_3^g]\dots[x_n^g,y_n^g] \in G'.\end{aligned}$$

Sendo assim, qualquer que seja $\alpha \in G'$, temos que $\alpha^g \in G'$, para todo $g \in G$. Logo, G' é normal em G. □

Proposição 1.1.11. *Seja N um subgrupo normal de um grupo G. Então o grupo quociente G/N é abeliano se, e somente se, $G' \leq N$. Em particular, G/G' é abeliano.*

Demonstração. Sejam xN e yN elementos de G/N. Suponha que G/N é abeliano. Então, temos

$$xyN = xNyN = yNxN = yxN.$$

E isto implica que $x^{-1}y^{-1}xyN = N$, isto é, $x^{-1}y^{-1}xy = [x,y] \in N$. Da arbitrariedade de x e y segue que $G' \leq N$.

Agora, por outro lado, suponha que $G' \leq N$. Então,

$$xNyN = xyN = yx[x,y]N = yxN = yNxN.$$

Logo, G/N é abeliano. □

Por fim, enunciamos um resultado atribuído a Issai Schur, que relaciona o centro de um grupo com o subgrupo derivado. Sua demonstração pode ser encontrada em [7].

Teorema 1.1.12. *(Schur). Seja G um grupo. Se $|G : Z(G)|$ é finito, então o subgrupo derivado G' é finito.*

1.2 Automorfismos

A partir desta seção, usaremos a notação exponencial para aplicações. Isto significa que, se temos uma aplicação $f : X \to Y$ e $x \in X$, denotaremos por x^f a imagem x pela aplicação f.

Definição 1.2.1. Dados dois grupos $(G,\cdot)$ e $(H,*)$ um *homomorfismo* $\varphi : G \to H$ é uma aplicação que satisfaz

$$(a \cdot b)^\varphi = a^\varphi * b^\varphi,$$

para quaisquer $a,b \in G$. Além disso, chamamos de *núcleo* e *imagem* de φ, respectivamente, os conjuntos

$$\ker\varphi = \{g \in G \mid g^\varphi = 1_H\}$$

e

$$\mathrm{Im}\varphi = \{g^\varphi \mid g \in G\}.$$

Decorre desta definição a

Proposição 1.2.2. *Seja $\varphi\colon G \to H$ um homomorfismo de grupos. Para quaisquer $n \in \mathbb{Z}$ e $g \in G$ temos que*

$$(g^n)^\varphi = (g^\varphi)^n.$$

Quando $n = 0$ e $n = -1$, vemos que φ preserva elemento neutro e inverso:

$$(1_G)^\varphi = 1_H \quad e \quad (g^{-1})^\varphi = (g^\varphi)^{-1}.$$

Dado um homomorfismo de grupos $\varphi\colon G \to H$, pode-se verificar que $\mathrm{Im}\varphi$ é subgrupo de H, que $\ker\varphi$ é subgrupo de G e mais, $\ker\varphi$ é normal em G. Veja: se $x \in G$ e $g \in \ker\varphi$ temos que $g^x \in \ker\varphi$, pois $(g^x)^\varphi = (x^{-1}gx)^\varphi = (x^{-1})^\varphi(g)^\varphi(x)^\varphi = (x^\varphi)^{-1}1_H(x)^\varphi = 1_H$.

Um homomorfismo injetivo é chamado de *monomorfismo* e um homomorfismo sobrejetivo é chamado de *epimorfismo*. Quando o homomorfismo é simultaneamente injetivo e sobrejetivo, ou seja, bijetivo, o chamamos de *isomorfismo*. O resultado a seguir estabelece critérios para verificarmos essas propriedades.

Proposição 1.2.3. *Seja $\varphi\colon G \to H$ um homomorfismo.*

(1) φ é um monomorfismo se, e somente se, $\ker\varphi = \{1_G\}$*;*

(2) φ é um epimorfismo se, e somente se, $\mathrm{Im}\varphi = H$*;*

(3) φ é um isomorfismo se, e somente se, $\ker\varphi = \{1_G\}$ *e* $\mathrm{Im}\varphi = H$.

Demonstração. (1) Se φ é um monomorfismo e $x \in \ker\varphi$, temos que $x^\varphi = 1_H = (1_G)^\varphi$, mas como φ é injetiva obtemos $x = 1_G$. Então, $\ker\varphi = \{1_G\}$.

Por outro lado, se $\ker\varphi = \{1_G\}$ e $x, y \in G$ temos que $x^\varphi = y^\varphi$, donde $x^\varphi (y^\varphi)^{-1} = 1_H$ e ainda $(xy^{-1})^\varphi = 1_H$. Sendo assim, $xy^{-1} \in \ker\varphi$. Logo, $xy^{-1} = 1_H$ e, portanto, $x = y$. Então, concluímos que φ é injetiva, isto é, um monomorfismo.

(2) Segue diretamente da definição de aplicação sobrejetiva.

(3) Segue de dos itens anteriores. □

Os teoremas a seguir estabelecem relações interessantes entre grupos quocientes e homomorfismos.

Teorema 1.2.4. *(Primeiro Teorema do Isomorfismo)*

(1) Se $\alpha : G \to H$ é um homomorfismo de grupos, a aplicação

$$\begin{aligned} \theta \;:\; & \frac{G}{\ker\alpha} \to \mathrm{Im}\alpha \\ & x(\ker\alpha) \mapsto x^\alpha \end{aligned}$$

é um isomorfismo.

(2) Se N é um subgrupo normal de um grupo G, a aplicação

$$\begin{aligned} \varphi \;:\; & G \to \frac{G}{N} \\ & x \mapsto xN \end{aligned}$$

é um epimorfismo, com $\ker\varphi = N$.

Demonstração. (1) Sabemos que $\ker\alpha$ é normal em G. Note que se $xk \in x(\ker\alpha)$ temos que $(xk)^\alpha = x^\alpha k^\alpha = x^\alpha 1_H = x^\alpha$, isto é, a imagem de xk não depende de k, então a aplicação θ está bem definida. Claramente θ é um epimorfismo, pois $\mathrm{Im}\theta = \mathrm{Im}\alpha$. Agora, observe que $x(\ker\alpha) \in \ker\theta$ se, e somente se, $x \in \ker\alpha$, ou seja, $\ker\theta = \{\ker\alpha\} = \{1_{G/\ker\alpha}\}$. Logo, θ é um isomorfismo.

(2) A aplicação φ é um isomorfismo, pois $(xy)^\varphi = xyN = xNyN = x^\varphi y^\varphi$ para quaisquer $x, y \in G$. E como $\mathrm{Im}\varphi = G/N$, concluímos que φ é um epimorfismo. □

Teorema 1.2.5. *(Segundo Teorema do Isomorfismo) Sejam G um grupo, N e H subgrupos de G, com N normal em G. Então, $N \cap H \trianglelefteq H$ e*

$$\begin{aligned}\theta \;:\; \frac{H}{H\cap N} &\to \frac{NH}{N}\\ x(H\cap N) &\mapsto xN\end{aligned}$$

é um isomorfismo.

Demonstração. A aplicação $\alpha : H \to NH/N$, que $x \mapsto xN$, é claramente um epimorfismo. Observe que $\ker\alpha = \{x \in H \mid x^\alpha = N\} = \{x \in H \mid xN = N\} = \{x \in H \mid x \in N\} = H \cap N$ e, por isso, $H \cap N \trianglelefteq H$. Agora, usando o Primeiro Teorema do Isomorfismo item *(1)*, temos que o epimorfismo α induz o seguinte isomorfismo:

$$\begin{aligned}\theta \;:\; \frac{H}{H\cap N} &\to \frac{NH}{N}\\ x(H\cap N) &\mapsto x^\alpha = xN.\end{aligned}$$

□

Teorema 1.2.6. *(Terceiro Teorema do Isomorfismo) Sejam M e N subgrupos normais de um grupo G e seja $N \leq M$. Então, $M/N \triangleleft G/N$ e $\dfrac{(G/N)}{(M/N)}$ é isomorfo a G/M.*

Demonstração. Defina a aplicação $\alpha : G/N \to G/M$, que $xN \mapsto xM$. Observe que $\mathrm{Im}\alpha = G/M$, então α é um epimorfismo. Agora, note que $(xN)^\alpha = M$ se, e somente se, $x \in M$. Sendo assim, $\ker\alpha = M/N$ e, consequentemente, $M/N \triangleleft G/N$. Por fim, segue do item *(1)* do Primeiro Teorema do Isomorfismo que o epimorfismo α induz o isomorfismo

$$\begin{aligned}\theta \;:\; \frac{G/N}{M/N} &\to \frac{G}{M}\\ xN(M/N) &\mapsto (xN)^\alpha = xM.\end{aligned}$$

□

Para finalizar esta seção, apresentaremos a seguir o conceito de automorfismos de grupos e algumas de suas propriedades que são peças centrais desta dissertação.

Definição 1.2.7. Seja G um grupo. Um *automorfismo* de G é um isomorfismo $\varphi : G \to G$. O conjunto de todos os automorfismos de G é denotado por $\mathrm{Aut}(G)$.

Observe que $\mathrm{Aut}(G)$ é um grupo com a operação de composição de aplicações.

Um automorfismo $\varphi \in \mathrm{Aut}(G)$ é dito *involutivo* se $\varphi \neq Id$ e $\varphi^2 = Id$, isto é, se φ é uma *involução* no grupo $\mathrm{Aut}(G)$. A saber, em um grupo qualquer, um elemento diferente da identidade que possui ordem 2 é chamado de *involução*.

Podemos pensar em um automorfismo de um grupo G como uma permutação dos elementos G que mantém a estrutura de grupo inalterada. Alguns automorfismos fixam elementos do grupo. Chamamos estes elementos de pontos fixos do automorfismo, e denotamos por $C_G(\varphi)$ o conjunto de pontos fixos de um automorfismo φ. Em símbolos,

$$C_G(\varphi) = \{g \in G \mid g^{\varphi} = g\}.$$

Quando $C_G(\varphi)$ é finito, dizemos que φ é um automorfismo *quase regular*. E quando $C_G(\varphi) = \{1\}$, dizemos que φ é um automorfismo *livre de pontos fixos*.

Note que $C_G(\varphi)$ é um subgrupo de G, pois 1_G é fixado por φ, o produto de dois elementos fixados por φ é fixado por φ e se um elemento é fixado por φ, o seu inverso também é.

Como exemplo do que acabamos de definir, consideremos o grupo $(\mathbb{R} \setminus \{0\}, \cdot)$ e a aplicação $\varphi : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ definida por $x^{\varphi} = x^{-1}$ para todo $x \in \mathbb{R} \setminus \{0\}$. Observe que φ é um automorfismo involutivo quase regular, uma vez que satisfaz o seguinte:

(1) $\varphi \in \mathrm{Aut}(\mathbb{R} \setminus \{0\})$;

(2) $\varphi \neq Id$ e $\varphi^2 = Id$;

(3) o centralizador de φ, dado por $C_{\mathbb{R}\setminus\{0\}}(\varphi) = \{-1, 1\}$, é finito.

1.3 Ações de Grupos

Grupos podem "agir" sobre um conjunto de elementos. Por exemplo, os elementos do grupo simétrico agem sobre os elementos de um conjunto qualquer, permutando-os; os elementos do grupo diedral agem sobre os vértices de um polígono regular, refletindo-o e rotacionando-o. Grupos abstratos também podem agir sobre um conjunto, como veremos a seguir.

Definição 1.3.1. Sejam G um grupo e X um conjunto não vazio. Dizemos que G age sobre X quando existe uma aplicação $\sigma : G \times X \to X$ definida por $(g,x)^\sigma = x^g$, que para $x \in X$ e $g,h \in G$ satisfaz o seguinte:

(1) $x^1 = x$;

(2) $x^{gh} = (x^g)^h$.

Se um grupo G age sobre um conjunto X, a aplicação φ_g que associa cada $x \in X$ a $x^g \in X$ é uma bijeção, que induz o homomorfismo $\varphi : G \to \mathrm{Sym}(X)$ que associa cada $g \in G$ à permutação φ_g de X. Por outro lado, se temos um homomorfismo φ de G em $\mathrm{Sym}(X)$, então $x^{g^\varphi} := x^g$ define uma ação de G sobre X. Sendo assim, podemos dizer que uma ação do grupo G sobre o conjunto X determina e é determinada por um homomorfismo de G em $\mathrm{Sym}(X)$.

Sabemos que se X é um grupo, $\mathrm{Aut}(X) \leq \mathrm{Sym}(X)$. Quando $\mathrm{Im}(\varphi) \subseteq \mathrm{Aut}(X)$ dizemos que G age sobre X por automorfismos.

Usando a definição de ação de um grupo G sobre um conjunto X, podemos definir, e denotar por $\mathcal{O}_x$, a *órbita* de um elemento $x \in X$ como sendo o conjunto

$$\mathcal{O}_x := \{x^g \mid g \in G\} \subseteq X.$$

Observe que duas órbitas $\mathcal{O}_x$ e $\mathcal{O}_y$, com $x,y \in X$, são disjuntas ou coincidem: supondo que $\mathcal{O}_x \cap \mathcal{O}_y \neq \varnothing$, tome $s \in \mathcal{O}_x \cap \mathcal{O}_y$. Sabemos que $s = x^g = y^h$ para $g,h \in G$. Daí, vem que $x = (y^h)^{g^{-1}} = y^{hg^{-1}}$, e isto significa que $x \in \mathcal{O}_y$. Sendo assim, qualquer elemento em $\mathcal{O}_x$ pode ser escrito como elemento de $\mathcal{O}_y$. Logo, $\mathcal{O}_x \subseteq \mathcal{O}_y$. Analogamente, podemos concluir que vale a inclusão contrária e, consequentemente, a igualdade. Portanto, se duas órbitas não são disjuntas, elas coincidem. Além disso, o conjunto X pode ser dado como a união das órbitas de seus elementos, já que $x \in \mathcal{O}_x$. Então, as órbitas dos elementos de X formam uma partição de X.

Definimos como *estabilizador* do elemento $x \in X$ o subconjunto dos elementos de G que fixam x. Em símbolos,

$$G_x := \{g \in G \mid x^g = x\}.$$

Observe que G_x é um subgrupo de G, pois produtos e inversos de elementos de G_x também fixam x.

Dizemos que G age *transitivamente* sobre X quando, para quaisquer $x,y \in X$, existe $g \in G$ tal que $x^g = y$ ou, equivalentemente, quando $\mathcal{O}_x = X$ para algum $x \in X$.

Agora, vamos deduzir a *equação das órbitas*. Considere que G é um grupo finito agindo sobre um conjunto finito X. Note que quando qualquer elemento da classe lateral $G_x g$ age em x obtemos o elemento x^g da órbita de x. Isto motiva uma função α definida por $G_x g \mapsto x^g$. Tal função é injetiva. Veja: se $G_x g$ e $G_x h$ são duas classes laterais do estabilizador de x tais que $(G_x g)^\alpha = (G_x h)^\alpha$, temos que $x^g = x^h$; de onde concluímos que $x^{gh^{-1}} = x$, isto é, $gh^{-1} \in G_x$, então podemos escrever que $G_x g h^{-1} = G_x$ e daí obtemos que $G_x g = G_x h$. Como o domínio e o contradomínio de α são finitos, a função é, na realidade, uma bijeção. Sendo assim, podemos afirmar que o conjunto das classes laterais à direita de G_x em G tem a mesma cardinalidade que $\mathcal{O}_x$, ou seja, $|G : G_x| = |\mathcal{O}_x|$. Como sabemos X é a união disjunta das órbitas da ação de G sobre X, então se $\mathcal{O}_{x_1}, \mathcal{O}_{x_2}, \ldots, \mathcal{O}_{x_n}$ são suas órbitas, temos que

$$|X| = |\mathcal{O}_{x_1} \cup \mathcal{O}_{x_2} \cup \cdots \cup \mathcal{O}_{x_n}| = \sum_{i=1}^{t} |\mathcal{O}_{x_i}| = \sum_{i=1}^{t} |G : G_{x_i}|.$$

Esta equação é chamada de equação das órbitas. Vamos usá-la para o que pretendemos a seguir.

A partir de agora, aproveitaremos este contexto de ações de grupos para abordar um lema atribuído a Cauchy que será essencial para o estudo dos grupos finitos que são unicamente 2-divisíveis.

Lema 1.3.2. *(Cauchy) Se um primo p divide a ordem de um grupo finito, então esse grupo contém um elemento de ordem p.*

Demonstração. Seja G um grupo finito e seja $G^P = G \times \cdots \times G$ (p vezes). Considere o conjunto

$$X = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \ldots g_p = 1\}.$$

Para encontrar $|X|$ podemos usar o seguinte raciocínio: seja $(g_1, g_2, \ldots, g_p)$ uma p-upla qualquer em X. Se $g_1 \ldots g_{p-1} g_p = 1$, devemos ter que $g_p = (g_1 \ldots g_{p-1})^{-1}$. Sendo assim, na contagem dos elementos de X temos que considerar um total de $|G|$ possibilidades de elementos de G para cada entrada de uma p-upla, exceto para a última entrada que possui um elemento fixo associado a cada uma das entradas anteriores. Logo, $|X| = |G|^{p-1}$. Observe que não houve perda de generalidade, pois o mesmo raciocínio pode ser feito com qualquer entrada de uma p-upla.

Considere o grupo $C = C_p = \langle \sigma \rangle$, onde σ é uma aplicação que leva $(g_1, g_2, \ldots, g_p)$ em $(g_2, \ldots, g_p, g_1)$. Podemos definir uma ação de C sobre X através da posição $x^{\sigma^i} := (x^\sigma)^{\sigma_{i-1}}$, $x \in X$. Note que esta é uma ação bem definida, pois se $x = (g_1, g_2, \ldots, g_p) \in X$ então

$x^\sigma = (g_2, \ldots, g_p, g_1) \in X$, já que

$$g_2 \ldots g_p g_1 = g_1^{-1} g_1 g_2 \ldots g_p g_1 = g_1^{-1} g_1 = 1.$$

Agora, observe que o elemento $\sigma \in C$ fixa o elemento $(g_1, g_2, \ldots, g_{p-1}, g_p) \in X$ se, e somente se, $g_1 = g_2 = \cdots = g_{p-1} = g_p = g$, e neste caso temos que $g^p = 1$, isto é, a ordem de g é p. Sendo assim, para concluir a demonstração basta verificar que existe pelo menos um elemento $x \in X$, diferente da identidade, tal que $x^\sigma = x$. Então, considere o subconjunto $Y = \{(g_1, g_2, \ldots, g_p) \in X \mid g_1 = g_2 = \cdots = g_p\}$. Queremos mostrar que $|Y| > 1$.

Observe que a cardinalidade da órbita de um elemento que não é fixado pela a aplicação σ é $|C : C_x| = p$, já que p é primo. Considerando que k é o número de órbitas com p elementos, pela equação das órbitas temos que $|X| = |Y| + kp$, daí $|G|^{p-1} = |Y| + kp$ e como p divide $|G|$ segue que p divide $|G|^{p-1}$, e portanto, p divide $|Y| + kp$, donde concluímos que p divide $|Y|$. Logo, $|Y| > 1$ e a identidade de G^p não é o único elemento de Y. Consequentemente, existe um elemento $(g_1, g_2, \ldots, g_p) \in X$, com $g_1 = g_2 = \cdots = g_p = g \neq 1$, tal que $g^p = 1$. □

1.4 Produto Semidireto

Nesta seção trataremos sobre produtos semidiretos. Esta é uma ferramenta importante para o estudo de um grupo a partir de seus automorfismos. Começaremos com a seguinte definição.

Definição 1.4.1. Sejam H e N subgrupos de um grupo G, com N normal em G. Dizemos que G é um *produto semidireto (interno)* de N por H, quando $G = HN$ e $H \cap N = \{1\}$. Em símbolos, $G = N \rtimes H$.

Cada elemento $g \in G$ pode ser escrito de maneira única na forma $g = hn$, onde $h \in H$ e $n \in N$. De fato, se g é o produto hn e se também pode ser escrito como o produto $h_1 n_1$, com $n, n_1 \in N$ e $h, h_1 \in H$, teremos $hn = h_1 n_1$ e, consequentemente, $h_1^{-1} h = n_1 n^{-1} \in N \cap H = \{1\}$. Logo, $h_1^{-1} h = n_1 n^{-1} = 1$ e segue que $h_1 = h$ e $n_1 = n$. Portanto, temos a unicidade anunciada.

A operação de G, funciona da seguinte forma: dados os elementos $g = hn$ e $g_1 = h_1 n_1$ em G temos que

$$hnh_1 n_1 = hh_1 nn^{-1} h_1^{-1} nh_1 = hh_1 n^{h_1} n_1 \in G,$$

pois $hh_1 \in H$ e $n^{h_1} n_1 \in N$.

Observe que, a conjugação em N por $h \in H$ produz, para cada h, um automorfismo α_h de N, dado por $n^{\alpha_h} = n^h = h^{-1}nh$. Sendo assim, podemos escrever

$$hnh_1n_1 = hh_1n^{\alpha_{h_1}}n_1.$$

A aplicação $h \mapsto \alpha_h$ é um homomorfismo $\alpha : H \to \mathrm{Aut}(N)$. Veja: dados $h, h_1 \in H$ e $n \in N$,

$$(hh_1)^\alpha = n^{\alpha_{hh_1}} = h_1^{-1}h^{-1}nhh_1 = (h_1^{-1}nh)^{\alpha_{h_1}} = (n^{\alpha_h})^{\alpha_{h_1}} = n^{\alpha_h\alpha_{h_1}} = h^\alpha h_1^\alpha.$$

E isto determina uma ação de H sobre N por automorfismos.

Com isto em vista, vamos definir agora uma maneira de construir um novo grupo a partir de dois grupos dados e uma ação por automorfismos.

Sejam H e N grupos, não necessariamente subgrupos de um grupo dado. Suponha que H aja sobre N por automorfismos, isto é, existe um homomorfismo $\varphi : H \to \mathrm{Aut}(N)$ dado por $n^{h^\varphi} = n^h$. O conjunto $G = \{(h,n) \mid h \in H, n \in N\}$ forma um grupo quando munido da seguinte operação $*$: para (h,n) e (h_1,n_1) em G,

$$(h,n) * (h_1,n_1) = (hh_1, n^{h_1^\varphi}n_1) = (hh_1, n^{h_1}n_1) \in G.$$

A operação $*$ está bem definida. A associatividade vale, pois para quaisquer (h,n), (h_1,n_1) e (h_2,n_2) em G, temos

$$\begin{aligned}((h,n) * (h_1,n_1)) * (h_2,n_2) &= (hh_1, n^{h_1}n_1)(h_2,n_2)\\ &= ((hh_1)h_2, (n^{h_1}n_1)^{h_2}n_2)\\ &= (h(h_1h_2), n^{h_1h_2}n_1^{h_2}n_2)\\ &= (h,n)(h_1h_2, n_1^{h_2}n_2)\\ &= (h,n) * ((h_1,n_1) * (h_2,n_2)).\end{aligned}$$

O elemento neutro de G é o par ordenado $(1_H, 1_N)$ e o elemento inverso do par (h,n) é $(h^{-1}, (n^{-1})^{h^{-1}})$.

Definição 1.4.2. Sejam H e N grupos e suponha que H aja sobre N com ação σ. O grupo G definido acima é chamado de *produto semidireto (externo)* de N por H com ação σ, e denotado por $G = N \rtimes_\sigma H$.

Sejam $H^* := \{(h, 1_N) \mid h \in H\}$ e $N^* := \{(1_H, n) \mid n \in N\}$. Ao considerarmos a aplicação $f_1 : H \to H^*$ que $h \mapsto (h, 1_N)$, podemos perceber que H^* é um subgrupo de G isomorfo a H,

e ao considerarmos $f_2 : N \to N^*$ que $n \mapsto (1_H, n)$, podemos perceber que N^* é um subgrupo normal de G isomorfo a N. Para verificar que N^* é normal em G, basta conjugar $(1_H, n) \in N^*$ por um elemento arbitrário $(h, n_1) \in G$ e constatar que o conjugado está em N^*:

$$\begin{aligned}(1_H, n)^{(h,n_1)} &= (h, n_1)^{-1} * (1_H, n) * (h, n_1) \\ &= (h^{-1}, (n_1^{-1})^{h^{-1}}) * (1_H, n) * (h, n_1) \\ &= (h^{-1}, (n_1^{-1})^{h^{-1}} n) * (h, n_1) \\ &= (1_H, ((n_1^{-1})^{h^{-1}} n)^h n_1) \\ &= (1_H, n_1^{-1} n^h n_1) \in N^*.\end{aligned}$$

Além disso, observe que $H^* \cap K^* = \{(1_H, 1_N)\}$ e que $G = H^* N^*$, pois $(h, 1_N)(1_H, n) = (h, n)$. Estes resultados nos permitem identificar G como o produto semidireto interno de N^* por H^*. Para simplificar as notações dos elementos de G usaremos justaposição e escreveremos hn no lugar do par ordenado (h, n). Assim, o produto $(h, n) * (h_1, n_1)$ será escrito como hnh_1n_1.

Uma observação importante é que quando consideramos um grupo H e o homomorfismo identidade $\mathcal{I} : \mathrm{Aut}(H) \to \mathrm{Aut}(H)$, o produto semidireto $G = \mathrm{Aut}(H) \ltimes_{\mathcal{I}} H$ é chamado de *produto holomorfo* de H. No último capítulo, estudaremos um subgrupo de um produto holomorfo.

1.5 Grupos Solúveis

Nesta seção definiremos grupos solúveis e apresentaremos alguns resultados sobre solubilidade que contribuirão para a demonstração do Teorema A.

Definição 1.5.1. Um grupo G é dito *solúvel* se existe uma cadeia de subgrupos

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

onde cada termo G_i é normal em G_{i+1} e cada fator G_{i+1}/G_i é abeliano. Uma cadeia com tal descrição é chamada de cadeia abeliana ou série abeliana.

Decorre naturalmente desta definição que todo grupo abeliano é solúvel.

Proposição 1.5.2. *Seja G um grupo e $N, H \leq G$, com N normal em G. Vale que:*

(1) Se G é solúvel, então H é solúvel;

(2) Se G é solúvel, então G/N é solúvel.

(3) Se N e G/N são solúveis, então G é solúvel;

(4) Se N e H são solúveis, então NH é solúvel.

Demonstração. (1) Como G é solúvel, considere a seguinte cadeia de subgrupos de G:

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

onde $G_i \trianglelefteq G_{i+1}$ e G_{i+1}/G_i é abeliano.

Seja $K_i := G_i \cap H$, com $i = 0, 1, ..., n$, uma cadeia finita de subgrupos de H. Primeiro, vamos mostrar que $K_i \trianglelefteq K_{i+1}$: sejam $g \in K_{i+1}$ e $k \in K_i$, temos que $g^{-1}kg \in H$, pois $g, k \in H$. Como $G_i \trianglelefteq G_{i+1}$, $k \in G_i$ e $g \in G_{i+1}$ segue que $g^{-1}kg \in G_i$. Portanto, $g^{-1}kg \in K_i$.

Agora vamos mostrar que K_{i+1}/K_i é abeliano. Observe que $K_{i+1}/K_i = K_{i+1}/(K_{i+1} \cap G_i)$. Pelo segundo Teorema do Isomorfismo 1.2.5, este último quociente é isomorfo a $K_{i+1}G_i/G_i$, que é subgrupo de G_{i+1}/G_i e, portanto, abeliano. Isso prova que H é solúvel.

(2) Vamos mostrar que G/N possui uma cadeia abeliana. Como G é solúvel, considere a mesma cadeia de subgrupos de G dada no item anterior. Seja $\{NG_i/N\}_{i=0}^n$ uma cadeia de subgrupos de G/N. Pelo Terceiro Teorema do Isomorfismo

$$\frac{NG_{i+1}/N}{NG_i/N} \cong \frac{NG_{i+1}}{NG_i}.$$

Sendo assim, temos que $NG_i \trianglelefteq NG_{i+1}$. Agora, observe que

$$\frac{NG_{i+1}}{NG_i} = \frac{(NG_{i+1})G_i}{NG_i} = \frac{(NG_i)G_{i+1}}{NG_i} \cong \frac{G_{i+1}}{NG_i \cap NG_i} \cong \frac{\dfrac{G_{i+1}}{G_i}}{\dfrac{NG_i \cap NG_i}{G_i}}.$$

Como, por hipótese, $\dfrac{G_{i+1}}{G_i}$ é abeliano, o último quociente da equação acima também é. Logo, os fatores da cadeia $\{NG_i/N\}_{i=0}^n$ são abelianos, e portanto, G/N é solúvel.

(3) Suponhamos que N e G/N são solúveis. Vamos mostrar que existe uma cadeia finita de subgrupos de G que satisfaz as propriedades da definição. Para N e G/N considere as cadeias de subgrupos $\{N_i\}_{i=0}^r$ e $\{H_i/N\}_{i=0}^s$, respectivamente. Como N e G/N são solúveis, temos que $N_i \trianglelefteq N_{i+1}$ e que N_{i+1}/N é abeliano, também, $H_i/N \trianglelefteq H_{i+1}/N$ e o fator $\dfrac{H_{i+1}/N}{H_i/N}$ é abeliano. Pelo Terceiro Teorema do Isomorfismo,

$$\frac{H_{i+1}/N}{H_i/N} \cong \frac{H_{i+1}}{H_i}.$$

Logo, H_{i+1}/H_i é abeliano. Agora, note que $H_0 = N$. Então, temos a cadeia

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = N = H_0 \trianglelefteq H_1 \trianglelefteq \ldots H_s = G$$

satisfazendo as propriedades. Portanto, G é solúvel.

(4) Sem nenhuma perda de generalidade, podemos considerar $G = NH$. Note que, pelo Segundo Teorema do Isomorfismo,

$$\frac{G}{N} = \frac{HN}{N} \cong \frac{H}{N \cap H}.$$

Usando o item *(2)* concluímos que este último grupo quociente é solúvel. Logo, G/N é solúvel. Por fim, usando o item *(3)*, obtemos que $G = NH$ é solúvel. □

Um famoso e importante resultado, obtido por W. Feit e J. G. Thompson em [2], é o seguinte

Teorema 1.5.3. *Todos os grupos finitos de ordem ímpar são solúveis.*

Este teorema tem fundamental importância na demonstração do Teorema A.

Antes do próximo resultado, vamos definir o que chamamos de grupo periódico ou grupo de torção. Para tanto, relembramos a definição de *ordem de um elemento*: dado um grupo G e $g \in G$, a ordem do elemento g é o menor inteiro positivo n tal que $g^n = 1$. Se tal inteiro não existir, dizemos que a ordem do elemento g é infinita.

Definição 1.5.4. Seja G um grupo. Quando todos os elementos de G têm ordem finita, dizemos que G é um *grupo periódico*.

Ademais, outros conceitos que precisaremos são os de grupo virtualmente e localmente solúvel: dizemos que um grupo G é *virtualmente solúvel* quando G possui um subgrupo de índice finito que é solúvel. E dizemos que G é *localmente solúvel* quando todos os seus subgrupos finitamente gerados são solúveis. De modo geral usamos essa terminologia para qualquer propriedade de um grupo, por exemplo, finitude; como veremos a seguir. Antes, é necessário comentar que, dado um elemento de um grupo, o chamamos de *involução quase regular* quando esse elemento possui ordem dois e seu centralizador é finito.

Em 1974, V. P. Shunkov provou o

Teorema 1.5.5. *Se um grupo G é periódico e possui uma involução quase regular, então G é localmente finito e virtualmente solúvel.*

A demonstração deste teorema se encontra em [10]. Como sua consequência, temos o

Corolário 1.5.6. *Se um grupo periódico G possui um automorfismo involutivo quase regular, então G é localmente finito e virtualmente solúvel.*

Demonstração. Seja G um grupo periódico que possui um automorfismo α que é involutivo e quase regular. Dentro do produto holomorfo de G tome o subgrupo $L \coloneqq \langle \alpha \rangle \ltimes_{\mathcal{I}} G$. Observe que L é periódico e possui a involução quase regular α, então ao aplicar o Teorema 1.5.5 de Shunkov obtemos que L é localmente finito e virtualmente solúvel.

Como L é localmente finito, todos os subgrupos finitamente gerados de L são finitos. Sendo assim, os subgrupos finitamente gerados da cópia de G em L também são. Logo, podemos afirmar que G é localmente finito.

Agora vamos mostrar que G é virtualmente solúvel. Como L é virtualmente solúvel, existe $K \leq L$ de índice finito e solúvel. Sendo G normal em L podemos tomar o subgrupo GK e, usando o Teorema 1.1.1, escrever

$$|GK : G \cap K| = |GK : G||G : G \cap K| = |GK : K||K : G \cap K|.$$

Ademais, sabemos, pelo Segundo Teorema do Isomorfismo, que $|GK : G| = |K : G \cap K|$. Então, segue que $|G : G \cap K| = |GK : K| < \infty$. Além disso, $G \cap K$ é solúvel, pois K é solúvel. Portanto, G é virtualmente solúvel. □

Agora, vamos introduzir um conceito necessário para a demonstração da próxima proposição. Sejam G um grupo e H um subgrupo de G, defina $H_G = \bigcap_{g \in G} g^{-1}Hg$. Este é um subgrupo normal de G que está contido em H. Observe que H é normal em G se, e somente se, $H = H_G$. Vamos chamar H_G de *núcleo normal* de H em G.

Proposição 1.5.7. *Se G é um grupo localmente solúvel e virtualmente solúvel, então G é solúvel.*

Demonstração. Como G é virtualmente solúvel, existe $H \leq G$ de índice finito que é solúvel. Tome o núcleo normal H_G. Sabemos que H_G é solúvel, pois é subgrupo de H, e também que $|G : H_G|$ é finito, considere-o igual a n. Agora, seja $T = \{t_1, t_2, ..., t_n\} \subseteq G$ um transversal de H_G em G. Assim, temos que

$$\begin{aligned} G &= t_1 H_G \dot{\cup} t_2 H_G \dot{\cup} ... \dot{\cup} t_n H_G \\ &= \langle t_1, t_2, ..., t_n, H_G \rangle \\ &= \langle t_1, t_2, ..., t_n \rangle H_G. \end{aligned}$$

Já que G é localmente solúvel, o subgrupo $\langle t_1, t_2, ..., t_n \rangle$ é solúvel. Portanto, usando a Proposição 1.5.2 item *(2)*, concluímos que G é solúvel. □

Capítulo 2

Grupos Unicamente 2-divisíveis

2.1 Caracterização e Propriedades

Neste capítulo estudaremos os grupos 2-divisíveis na direção de obter resultados para a demonstração do Teorema A. Veremos quando essa propriedade é herdada por subgrupos e também quando grupos finitos são 2-divisíveis. Vamos começar com a seguinte

Definição 2.1.1. Um grupo G é 2-divisível se para cada elemento $x \in G$ existe um elemento $y \in G$ tal que $y^2 = x$. Se o elemento y é único, dizemos que G é um grupo unicamente 2-divisível.

Uma observação importante é que um grupo G unicamente 2-divisível não possui involuções, isto é, elementos de ordem 2. Caso contrário, se existisse $g \in G$ tal que a ordem g é 2, teríamos que $g^2 = 1$ e $(1)^2 = 1$. Mas, isto contradiz a unicidade.

Em geral, não podemos dizer que grupos 2-divisíveis não possuem involuções. Por exemplo, o grupo multiplicativo dos números complexos $(\mathbb{C} \setminus \{0\}, \cdot)$ é 2-divisível, pois todos os seus elementos têm duas raízes quadradas, mas este grupo possui a involução -1.

A afirmação é válida, porém, para grupos finitos 2-divisíveis. Antes de verificar isso, vejamos a

Proposição 2.1.2. *Seja G um grupo finito. G é 2-divisível se, e somente se, a ordem de G é ímpar.*

Demonstração. Primeiro, vamos mostrar que se G é 2-divisível, então a ordem de G é ímpar.

Suponha, por contradição, que a ordem de G seja par. Pelo Lema 1.3.2 para $p = 2$, existe $g_1 \in G$ tal que a ordem de g_1 é 2. Então, a aplicação $\varphi : G \to G$, dada por $g^{\varphi} = g^2$, não é injetiva pois $g_1^{\varphi} = 1 = 1^{\varphi}$. Como uma aplicação com domínio e contradomínio finitos e de mesma cardinalidade é injetiva se, e somente se, é sobrejetiva, segue que φ não é sobrejetiva.

Isto significa que existe $g \in G$ para o qual não existe $h \in G$ tal que $h^2 = g$. Mas, isto contradiz a hipótese de que G é 2-divisível. Logo, a ordem de G deve ser ímpar.

Resta mostrar que se $|G|$ é ímpar, então G é 2-divisível.

Seja $|G| = n$, com n ímpar, e considere a mesma aplicação $\varphi : G \to G$, dada por $g^\varphi = g^2$. Observe que para todo $g \in G$, o elemento $g^{\frac{n+1}{2}} \in G$ satisfaz

$$(g^{\frac{n+1}{2}})^\varphi = (g^{\frac{n+1}{2}})^2 = g^{n+1} = g^n g = g.$$

Portanto, φ é sobrejetiva. Assim, para cada $g \in G$ existe $h \in G$ tal que $h^2 = g$. Logo, G é 2-divisível. □

Agora, sabemos que um grupo G finito e 2-divisível possui ordem ímpar. Sendo assim, 2 não divide a ordem de G. Logo, pelo Teorema 1.3.2 segue que G não possui elemento de ordem 2.

Em relação aos subgrupos, temos o seguinte: para grupos infinitos 2-divisíveis, em geral, não vale que seus subgrupos são 2-divisíveis. Veja o exemplo: o grupo $(\mathbb{R}_+ \setminus \{0\}, \cdot)$ é 2-divisível, porém, o subgrupo $(\mathbb{Q}_+ \setminus \{0\}, \cdot)$ não é, pois não existe elemento neste subgrupo cujo quadrado é 2. Todavia, para grupos finitos vale a seguinte:

Proposição 2.1.3. *Seja G um grupo finito 2-divisível. Se H é subgrupo de G, então H também é 2-divisível.*

Demonstração. Sabemos que $|G|$ é ímpar. Do Teorema de Lagrange sabemos que $|H|$ divide $|G|$. Logo, $|H|$ é ímpar. Portanto, segue do resultado anterior que H é 2-divisível. □

Tanto para grupos finitos como para grupos infinitos, vale a

Proposição 2.1.4. *Em um grupo unicamente 2-divisível, a interseção finita de subgrupos 2-divisíveis é um subgrupo 2-divisível.*

Demonstração. Seja G o referido grupo e sejam $H_1, H_2, ..., H_n$ subgrupos 2-divisíveis de G. Tome o subgrupo $H := \bigcap_{i=1}^{n} H_i$. Veja que se $x \in H$, então x está em cada H_i. Sabemos que existe um único elemento $y \in G$ tal que $y^2 = x$. Note que esse elemento y também pertence a cada H_i, pois estes são subgrupos 2-divisíveis. Então, $y \in H$ e, portanto, H é 2-divisível. □

A propriedade de um grupo ser unicamente 2-divisível é herdada por centralizadores. Veja:

Proposição 2.1.5. *Seja G um grupo unicamente 2-divisível. Se T é um subconjunto não vazio de G, então $C_G(T)$ é um subgrupo unicamente 2-divisível de G.*

Demonstração. Já sabemos que centralizadores são sempre subgrupos. Por isso, precisamos apenas mostrar que $C_G(T)$ é unicamente 2-divisível.

Tomando $x \in C_G(T)$, temos que $xt = tx$ para todo $t \in T$. Sabemos que existe um único $y \in G$ tal que $y^2 = x$. Então, para verificar o fato acima, precisamos mostrar que $y \in C_G(T)$, isto é, que $yt = ty$ para todo $t \in T$. Veja que

$$(t^{-1}yt)^2 = t^{-1}ytt^{-1}yt = t^{-1}y^2t = t^{-1}xt = t^{-1}tx = x.$$

Daí, pela unicidade do elemento cujo quadrado é igual a x, segue que $t^{-1}yt = y$, assim, obtemos que $yt = ty$ para todo $t \in T$. Logo, $y \in C_G(T)$ e, portanto, $C_G(T)$ é unicamente 2-divisível. □

O resultado abaixo será muito útil na conclusão da demonstração do Teorema A.

Proposição 2.1.6. *Seja G um grupo unicamente 2-divisível. Se φ é um automorfismo de G, então $C_G(\varphi)$ é um subgrupo unicamente 2-divisível de G.*

Demonstração. Já sabemos que $C_G(\varphi)$ é um subgrupo de G. Temos apenas que mostrar que para todo $x \in C_G(\varphi)$ existe um único $y \in C_G(\varphi)$ tal que $y^2 = x$.

Tome $x \in C_G(\varphi)$. Pela hipótese, existe um único $y \in G$ tal que $y^2 = x$. Veja que $(y^2)^\varphi = x^\varphi = x = y^2$. Daí, $(y^\varphi)^2 = y^2$. Como G é unicamente 2-divisível, segue da última igualdade que $y^\varphi = y$. Portanto, $y \in C_G(\varphi)$. □

Capítulo 3

A prova do Teorema A

Os esforços realizados neste capítulo têm como objetivo fornecer a demonstração do Teorema A.

Agora, vamos obter alguns resultados. Começaremos estabelecendo notações fixas para as próximas seções:

(1) salvo menção em contrário, U denotará um grupo infinito unicamente 2-divisível. O elemento $v \in \mathrm{Aut}(U)$ será um automorfismo involutivo quase regular;

(2) G denotará o produto semidireto de U pelo $\langle v \rangle$, identificando U e $\langle v \rangle$ com as suas imagens em G. A notação $\mathrm{Inv}(G)$ se referirá ao conjunto das involuções do grupo G;

(3) definimos $S := \{x \in U \,|\, x^v = x^{-1}\}$;

(4) a letra A simbolizará um subgrupo fixado de U, que é infinito, maximal (com respeito à inclusão) abeliano e é invertido por v (i.e. todos os seus elementos são invertidos por v). A existência de A será demonstrada na seção 3.2, através do Lema de Zorn e do item *(2)* do Lema 3.2.2;

(5) para cada $u \in U$ denotaremos por A_u o maior subgrupo de A invertido pelo elemento uvu^{-1} de G.

3.1 Resultados Auxiliares

Primeiro, vamos verificar que os subgrupos A e A_u são unicamente 2-divisíveis.

Lema 3.1.1. *O subgrupo A é unicamente 2-divisível. E também, para qualquer $u \in U$, o subgrupo A_u é unicamente 2-divisível.*

Demonstração. Seja $a \in A$ um elemento qualquer. Sabemos que existe um único elemento $x \in U$ tal que $x^2 = a$. Queremos mostrar que $x \in A$.

Como A é invertido por ν, temos $a^\nu = a^{-1}$. Então, $(x^2)^\nu = (x^2)^{-1}$, e daí $(x^\nu)^2 = (x^{-1})^2$. Já que U é unicamente 2-divisível, vale que $x^\nu = x^{-1}$, ou seja, ν inverte x. Além disso, x comuta com qualquer elemento de A. De fato, ao tomarmos um elemento arbitrário $b \in A$, temos que

$$(b^{-1}xb)^2 = b^{-1}x^2b = b^{-1}ab = b^{-1}ba = a.$$

Assim, pela unicidade do elemento cujo quadrado é igual a a, vale que $b^{-1}xb = x$, ou seja, x comuta com b. Consequentemente, como A é abeliano, segue que o subgrupo $\langle x, A\rangle$ é abeliano. Agora, veja que para qualquer $b \in A$,

$$(xb)^\nu = x^\nu b^\nu = x^{-1}b^{-1} = b^{-1}x^{-1} = (xb)^{-1}. \tag{3.1.1}$$

Com isto, concluímos que qualquer elemento do subgrupo $\langle x, A\rangle$ é invertido por ν. Sendo assim, como $\langle x, A\rangle$ contém A, que por hipótese é maximal, temos que $\langle x, A\rangle = A$, e portanto, $x \in A$. Logo, A é unicamente 2-divisível.

Para mostrar que o subgrupo A_u é unicamente 2-divisível, procedemos analogamente. Para qualquer elemento $a \in A_u$, sabemos que existe um único elemento $x \in A$ tal que $x^2 = a$, e queremos mostrar que $x \in A_u$.

De fato, como A_u é invertido por $u\nu u^{-1}$, temos que $a^{u\nu u^{-1}} = a^{-1}$. Então, vale que $(x^2)^{u\nu u^{-1}} = (x^2)^{-1}$, e daí $(x^{u\nu u^{-1}})^2 = (x^{-1})^2$. Já que A é unicamente 2-divisível, segue que $x^{u\nu u^{-1}} = x^{-1}$. Como A é abeliano, o subgrupo $\langle x, A_u\rangle$ é abeliano. Para verificar que os elementos de $\langle x, A_u\rangle$ são invertidos por $u\nu u^{-1}$ basta repetir a equação (3.1.1) trocando ν por $u\nu u^{-1}$ e considerando que b é um elemento qualquer de A_u. Agora, temos que o subgrupo $\langle x, A_u\rangle$ contém A_u, mas A_u é o maior subgrupo de A invertido por $u\nu u^{-1}$, então segue que $\langle x, A_u\rangle = A_u$. Logo, $x \in A_u$, e portanto, A_u é unicamente 2-divisível. □

No próximo lema vamos ver o conjunto S, definido acima, como um subconjunto do grupo G.

Lema 3.1.2. *Seja* $S := \{x \in U \mid x^\nu = x^{-1}\}$. *Podemos reescrevê-lo como* $S = \{\nu\nu^x \mid x \in U\}$.

Demonstração. Seja $y \in S$. Existe um único elemento $x_0 \in U$ tal que $x_0^2 = y$. Como $y^\nu = y^{-1}$, temos que $(x_0^2)^\nu = x_0^{-2}$ e daí $(x_0^\nu)^2 = (x_0^{-1})^2$. Sendo U um grupo unicamente 2-divisível, vale que $x_0^\nu = x_0^{-1}$, ou seja, $\nu x_0 \nu = x_0^{-1}$. Multiplicando esta última equação à esquerda por x_0^{-1}, temos $x_0^{-1}\nu x_0 \nu = x_0^{-2}$, o que é equivalente a $\nu^{x_0}\nu = x_0^{-2}$. Ao inverter ambos os lados desta, obtemos que $\nu\nu^{x_0} = x_0^2 = y$. Logo, $y \in \{\nu\nu^x \mid x \in U\}$ e, consequentemente, $S \subseteq \{\nu\nu^x \mid x \in U\}$.

Por outro lado, tomando $z \in \{vv^x | x \in U\}$, temos que $z = vv^{x_0}$ para algum $x_0 \in U$ e

$$z^v = vzv = vvv^{x_0}v = v^{x_0}v = z^{-1}.$$

Logo, $z \in S$; assim, $\{vv^x | x \in U\} \subseteq S$. Portanto, $S = \{vv^x | x \in U\}$. □

A demonstração do próximo lema se encontra em [6].

Lema 3.1.3. *Seja H um grupo formado pela união finita de n classes laterais dos subgrupos $C_1, C_2, ..., C_n$ de H:*

$$H = \bigcup_{i=1}^{n} C_i g_i.$$

Então o índice (de pelo menos) um desses subgrupos em H não excede n.

Consequência deste lema é o

Corolário 3.1.4. *Seja H um grupo formado pela união finita de n subconjuntos $S_1, S_2, ..., S_n$ de H:*

$$H = \bigcup_{i=1}^{n} S_i.$$

Para cada i definimos $C_i := \langle ab^{-1} | a, b \in S_i \rangle$. Então, o índice (de pelo menos) um dos subgrupos $C_1, C_2, ..., C_n$ em H não excede n.

Demonstração. Para cada $i = 1, 2, ..., n$, tome $g_i \in S_i$. Vamos mostrar que $S_i \subseteq C_i g_i$ para todo i=1, 2, ..., n, onde $C_i g_i = \langle ab^{-1} | a, b \in S_i \rangle g_i$.

Note que em $C_i g_i$ há um elemento da forma $ab^{-1}g_i$. E podemos escrever qualquer elemento $x \in S_i$, inclusive g_i, como $x = xg_i^{-1}g_i$, ao considerarmos $a = x$ e $b = g_i$. Logo $x \in C_i g_i$, e portanto, $S_i \subseteq C_i g_i$. Agora, temos que $H = \bigcup_{i=1}^{n} S_i \subseteq \bigcup_{i=1}^{n} C_i g_i$. E por outro lado, temos que $C_i g_i \subseteq H$ e $\bigcup_{i=1}^{n} C_i g_i \subseteq H$. Assim, concluímos que $H = \bigcup_{i=1}^{n} C_i g_i$. Por fim, aplicando o Lema 3.1.3, segue que o índice de (pelo menos) um dos C_i em H não excede n. □

No próximo lema, mostraremos que as involuções do grupo G são conjugadas. E, em seguida, usaremos esse resultado para expressar os elementos de S em termos das involuções de G.

Lema 3.1.5. *(1) Todas as involuções em G são conjugados;*

(2) $S = \{v\tau | \tau \in \mathrm{Inv}(G)\}$.

Demonstração. (1) Como G é um produto semidireto de U por $\langle \nu \rangle$, qualquer elemento $g \in G$ é um produto da forma $g = xy$, com $x \in U$ e $y \in \langle \nu \rangle$. Mas, necessariamente, $y = \nu$ ou $y = id$, então $g = x\nu$ ou $g = x \in U$. Sendo assim, se $g \in \mathrm{Inv}(G)$, isto é, se g é uma involução em G, então g possui a forma $g = x\nu$, pois U não admite involuções.

Seja $\tau \in \mathrm{Inv}(G)$. Então, $\tau = x\nu$ para algum $x \in U$. Como τ é uma involução, $x \in S$. De fato, $\tau^2 = 1_G$ e isto implica que $(x\nu)^2 = 1_G$, assim, $x\nu x\nu = 1_G$ e reescrevendo isto temos que $xx^\nu = 1_G$, o que nos dá $x^\nu = x^{-1}$. Logo, $x \in S$.

Agora, seja $y \in U$ o único elemento tal que $y^2 = x$. Então, temos que $(y^2)^\nu = (y^2)^{-1}$ e, equivalentemente, $(y^\nu)^2 = (y^{-1})^2$. Como U é unicamente 2-divisível, vale que $y^\nu = y^{-1}$. Logo, $y \in S$. Daí, como $\nu y \nu = y^{-1}$ tem-se que $y\nu = \nu y^{-1}$. Multiplicando esta última equação à esquerda por y, temos $y^2\nu = y\nu y^{-1}$ e, como $y^2 = x$, obtemos $x\nu = y\nu y^{-1}$, isto é, $\tau = y\nu y^{-1}$. Portanto, a involução τ é um conjugado de ν.

(2) Segue do Lema 3.1.2. □

A seguir, vamos obter alguns resultados que envolvem um subgrupo abeliano 2-divisível de U.

Lema 3.1.6. *Seja D um subgrupo abeliano 2-divisível de U. Então, vale o seguinte:*

(1) $C_U(D)/D$ é um grupo unicamente 2-divisível.

(2) se D é invertido por ν, então νD é um automorfismo involutivo quase regular de $C_U(D)/D$.

(3) assuma que D é invertido por ν e seja E/D um subgrupo de $C_U(D)/D$ que é invertido por νD. Então, E é invertido por ν, e em particular, E é abeliano.

Demonstração. (1) Primeiro, observamos que como D é abeliano, $D \leq C_U(D)$. E mais, se $c \in C_U(D)$, temos $cx = xc$, para todo $x \in D$, daí $cD = Dc$. Logo, $D \trianglelefteq C_U(D)$. Portanto, $C_U(D)/D$ é um grupo.

Agora, defina $C := C_U(D)$. Assuma para $a, b \in C$ que $a^2D = b^2D$. Sejam $x, y \in D$ com $a^2x = b^2y$, e como D é unicamente 2-divisível considere $u, w \in D$ tais que $u^2 = x$ e $w^2 = y$. Sendo assim, temos que $a^2u^2 = b^2w^2$, e como a e b comutam com qualquer elemento de D, obtemos que $(au)^2 = (bw)^2$. Portanto, como C é unicamente 2-divisível pela Proposição 2.1.5, segue que $au = bw$. Consequentemente, $auD = bwD$, o que nos permite concluir que $aD = bD$.

Além disso, mostremos também que para todo $aD \in C/D$ existe $bD \in C/D$ tal que $(bD)^2 = aD$. Seja aD um elemento qualquer em C/D e seja $b \in U$ tal que $b^2 = a \in C$. Então,

como C é unicamente 2-divisível, $b \in C$, e portanto, $bD \in C/D$. Agora, veja que

$$(bD)^2 = bDbD = b^2D = aD.$$

Assim, concluímos que $C_U(D)/D$ é um grupo unicamente 2-divisível.

(2) Seja a aplicação $\nu D : C/D \to C/D$, definida por $(xD)^{\nu D} = x^{\nu}D$. A bijetividade de νD segue da bijetividade de ν, assim como o fato de νD ser um automorfismo: dados $aD, bD \in C/D$, temos

$$\begin{aligned}(aDbD)^{\nu D} &= (abD)^{\nu D} \\ &= (ab)^{\nu}D \\ &= a^{\nu}b^{\nu}D \\ &= a^{\nu}Db^{\nu}D \\ &= (aD)^{\nu D}(bD)^{\nu D}.\end{aligned}$$

E também,

$$(\nu D)^2 = \nu D\nu D = \nu^2 D = IdD.$$

Portanto, νD é um automorfismo involutivo.

Agora, tome $aD \in C_{C/D}(\nu D)$, isto é, suponha que aD centraliza νD. Assim, temos $\nu D = a^{-1}D\nu DaD$, donde vem que $\nu D = a^{-1}\nu aD$, reescrevendo, obtemos $\nu D = \nu^a D$. Logo, $\nu^a = \nu d$ para algum $d \in D$. Tome $x \in D$ com $x^2 = d$. Como ν inverte x, temos que $\nu x = x^{-1}\nu$. Então,

$$\nu^a = \nu x^2 = \nu xx = x^{-1}\nu x = \nu^x.$$

Daí, $a^{-1}\nu a = x^{-1}\nu x$, e isto implica que $ax^{-1}\nu = \nu ax^{-1}$. Logo, $ax^{-1} \in C_C(\nu) \subseteq C_U(\nu)$. Podemos escrever, $a = ax^{-1}x$, assim, $aD = ax^{-1}xD$ e, equivalentemente, $aD = ax^{-1}D$. Então, vale a igualdade:

$$C_{C/D}(\nu D) = C_C(\nu)D/D,$$

onde $C_C(\nu)D/D = \{adD \,|\, ad \in C_C(\nu),\ d \in D\}$. Logo, como ν é quase regular, o $C_C(\nu)$ é finito e o $C_C(\nu)D/D$ também o é. Portanto, νD é quase regular.

(3) Para provar este item, basta mostrar que qualquer elemento $y \in E$ é invertido por ν e também que os elementos de E comutam entre si.

Seja $xD \in C/D$ um elemento invertido por νD. Então, aplicando νD em xD, temos $x^{\nu}D = x^{-1}D$, daí $x^{\nu} = x^{-1}d$, para algum $d \in D$. Conjugando esta última igualdade por ν obtemos que $x = x^{-\nu}d^{-1}$, assim, também temos que $x^{\nu} = x^{-1}d^{-1}$. Comparando as duas expressões de x^{ν}, concluímos que $d = 1$.

Agora, seja y um elemento qualquer em E. Por hipótese, $yD \in E/D$ é invertido por νD. Daí, sabendo que $d = 1$ para um elemento qualquer $x \in C$, inclusive para $x = y$, obtemos que $y^\nu = y^{-1}d = y^{-1}$. Logo, E é invertido por ν. E para concluir que E é abeliano, tome elementos quaisquer $y_1, y_2 \in E$ e veja que

$$y_1y_2 = (y_1^{-1})^\nu(y_2^{-1})^\nu = (y_1^{-1}y_2^{-1})^\nu = ((y_2y_1)^{-1})^\nu = y_2y_1. \qquad \square$$

3.2 Resultados Principais

No início deste capítulo, fixamos a notação A para um subgrupo maximal de U, que é infinito, abeliano e invertido por ν. Nesta seção, iniciaremos demonstrando o resultado que assegura a existência de tal subgrupo. Porém, antes disso, precisamos relembrar o Lema de Zorn.

Lema 3.2.1. *(Zorn) Se, em um conjunto não vazio e parcialmente ordenado, todo subconjunto totalmente ordenado possui uma cota superior, então esse conjunto possui um elemento maximal.*

No nosso contexto, a relação de ordem considerada é a inclusão e o conjunto em questão é o conjunto de subgrupos de U com alguma propriedade. Observe que a família dos subgrupos de U que são abelianos possui uma cota superior, pois qualquer cadeia de subgrupos abelianos tem como cota superior a união dos subgrupos da cadeia. Logo, pelo Lema de Zorn, existe um subgrupo abeliano maximal em U. Analogamente, podemos argumentar para a família dos subgrupos de U que são invertidos por ν. Portanto, U possui um subgrupo maximal abeliano que é invertido por ν. No próximo lema, provaremos a infinitude desse subgrupo.

Lema 3.2.2. *Seja D um subgrupo abeliano de U (admitimos $D = \{1\}$) tal que D é invertido por ν e $C_U(D)$ é infinito. Assuma que*

$$(S \cap C_U(D)) \setminus D \neq \varnothing.$$

Então, vale o seguinte:

(1) Existe um elemento $w \in C_U(D) \setminus D$ que é invertido por ν e tal que $C_U(\langle D, w\rangle)$ é infinito.

(2) Existe um subgrupo de U infinito e abeliano que é invertido por ν.

Demonstração. (1) Seja $V := C_U(D)$. Da Proposição 2.1.5, sabemos que V é um grupo infinito unicamente 2-divisível. Observe que ν também é um automorfismo para V. Com

efeito, dado $u \in V$, temos que $u^\nu \in V$, pois, se $d \in D$ ocorre que u^ν centraliza d. Veja:

$$u^\nu d = u^\nu (d^{-1})^\nu = (ud^{-1})^\nu = (d^{-1}u)^\nu = (d^{-1})^\nu u^\nu = du^\nu.$$

Sendo assim, como V é um grupo infinito unicamente 2-divisível e ν é um automorfismo involutivo quase regular para V, sem perda de generalidade, podemos assumir que $U = V$, e ainda, que $D \leq Z(U)$, pois $D \leq Z(V)$.

Do fato de que a $(S \cap C_U(D)) \subset S$, decorre que $(S \cap C_U(D)) \setminus D \subset S \setminus D$. Logo, pelo que assumimos como hipótese, segue que $S \setminus D \neq \varnothing$. Sendo assim, tome $b \in S \setminus D$, e escreva $b = \nu\tau$ com $\tau \in \mathrm{Inv}(G)$. Seja

$$u \in U \text{ tal que } u^{-2} = \nu\tau.$$

Veja que ao conjugar por τ ambos os lados desta última equação obtemos que $\tau\nu = (u^{-2})^\tau$, mas $\tau\nu = u^2$, então $u^2 = (u^{-2})^\tau$. Conjugando por τ novamente, temos que $(u^2)^\tau = u^{-2}$, reescrevendo obtemos $(u^\tau)^2 = (u^{-1})^2$. Como U é unicamente 2-divisível, concluímos que $u^\tau = u^{-1}$. Usando um argumento análogo, também constatamos que $u^\nu = u^{-1}$. Sendo assim, da igualdade $\nu\tau = u^{-2}$ vem que

$$\nu = u^{-1}u^{-1}\tau = u^{-1}\tau\tau u^{-1}\tau = u^{-1}\tau(u^{-1})^\tau = u^{-1}\tau u = \tau^u.$$

Agora, afirmamos que existe $h \in C_U(\tau)$ tal que hu é invertido por um número infinito de involuções de G. Suponha por um momento que essa afirmação vale.

Observação: Para todo $h \in C_U(\tau)$, temos que $hu \notin D$.

De fato, se $h = 1$ obtemos $hu = u$, e como $b = u^{-2} \notin D$, decorre que $u \notin D$. Caso contrário, se $hu \in D$ e $h \neq 1$, então como a involução τ inverte hu temos que

$$u^{-1}h^{-1} = (hu)^\tau = h^\tau u^\tau = hu^{-1}.$$

Isso significa que u inverte h. Mas, isto não é possível em U. Se fosse possível, da equação acima, teríamos que $uhu^{-1} = h^{-1}$, donde decorre que

$$uhu^{-1}h = 1, \tag{3.2.1}$$

mas, como $D \leq Z(U)$, temos que $huu = uhu$, e isso implica que $hu = uh$. Daí, comutando u com h na equação (3.2.1), temos $huu^{-1}h = 1$, o que leva a $h^2 = 1$. Mas, isto não ocorre em um grupo unicamente 2-divisível quando $h \neq 1$. Portanto, a observação vale.

Como todas as involuções em G são conjugadas, ao conjugar hu por um elemento apropriado de $C_U(hu)$, podemos assumir que ν inverte hu. Veja: se $x^{-1} \in C_U(hu)$, vale que

$$hu = (hu)^{x^{-1}}.$$

Como a involução τ inverte hu, temos $(hu)^\tau = (hu)^{-1}$, substituindo hu do lado esquerdo desta equação por $(hu)^{x^{-1}}$, vem que $((hu)^{x^{-1}})^\tau = (hu)^{x^{-1}\tau} = (hu)^{-1}$. Como $\nu = x^{-1}\tau$, obtemos que $(hu)^\nu = (hu)^{-1}$. Agora, perceba que como hu é invertido por um número infinito de involuções, podemos concluir que $C_U(hu)$ é infinito.

Portanto, tomando $w = hu$, e sabendo que $C_U(w) \subset U = C_U(D)$, podemos deduzir que $C_U(\langle D, w\rangle) = C_U(D) \cap C_U(w) = C_U(w)$ é infinito. Então, de fato, existe $w \in C_U(D) \setminus D$ que é invertido por ν e tal que o $C_U(\langle D, w\rangle)$ é infinito.

Porém, resta demonstrar a existência de h. Façamos isso.

Para cada $a \in S$, seja

$$s_a := \nu\tau^a.$$

Como τ^a é uma involução de G, temos que $s_a \in S$. Então, seja $l_a \in U$ tal que

$$l_a^{-2} = s_a.$$

Veja que

$$(l_a^{-2})^\nu = (s_a)^\nu = (\nu\tau^a)^\nu = \nu\nu\tau^a\nu = \tau^a\nu = (\nu\tau^a)^{-1} = s_a^{-1} = l_a^2.$$

Conjugando por ν ambos os lados da equação $(l_a^{-2})^\nu = l_a^2$, decorre que $(l_a^2)^\nu = l_a^{-2}$, equivalentemente, $(l_a^\nu)^2 = (l_a^{-1})^2$. Logo, $l_a^\nu = l_a^{-1}$.

Por cálculos análogos, podemos concluir também que $l_a^{\tau^a} = l_a^{-1}$. Partindo do fato de que l_a é invertido por ν, temos

$$l_a^\nu l_a^{-1} = l_a^{-2} = s_a = \nu\tau^a,$$

daí $\nu l_a \nu l_a^{-1} = \nu\tau^a$ e, pela lei do cancelamento à esquerda, temos $l_a\nu l_a^{-1} = \tau^a$, ou seja, $\nu = \tau^{al_a}$. Daí, como ν também é igual a τ^u, segue que $\tau^{al_a} = \tau^u$. Logo, obtemos

$$al_au^{-1}\tau = \tau al_au^{-1},$$

isto é, $al_au^{-1} \in C_U(\tau)$.

Defina $h_a := al_au^{-1}$, assim, $l_a = a^{-1}h_au$. Como l_a e a são invertidos por ν, ao conjugar a última igualdade por ν, obtemos

$$a(h_au)^\nu = l_a^{-1} = l_a^{-1}a^{-1}a = (al_a)^{-1}a = (al_au^{-1}u)^{-1}a = (h_au)^{-1}a,$$

donde, $a(h_au)^\nu a^{-1} = (h_au)^{-1}$, e ainda, $a\nu h_au\nu a^{-1} = a\nu h_au(a\nu)^{-1} = (h_au)^{-1}$. Observe que $a\nu$ é uma involução de G, pois $(a\nu)^2 = a\nu a\nu = aa^\nu = aa^{-1} = 1_G$. Então, podemos escrever

$$(h_au)^{a\nu} = (h_au)^{-1}.$$

Agora, observe que $C_U(\tau)$ é finito pois τ é um conjugado de ν e, por hipótese, $C_U(\nu)$ é finito. Sendo assim, o conjunto $\{h_a \mid a \in S\}$ é finito, pois está contido em $C_U(\tau)$. Além disso, o conjunto S é infinito, pois existem infinitas involuções em G. Isto significa que o conjunto das involuções $\{a\nu \mid a \in S\}$ é infinito. Portanto, existe $h = h_a \in C_U(\tau)$ para o qual existem infinitas involuções $a\nu \in G$, com $a \in S$, que invertem hu. E assim, terminamos a demonstração de *(1)*.

(2) Pelo Lema de Zorn, existe um subgrupo D_0 de U que é maximal, abeliano e que é invertido por ν. Suponha que $C_U(D_0)$ é infinito. Note que se D_0 é infinito, o resultado vale.

Vamos supor, por contradição, que D_0 seja finito. Sabemos que ν age sobre $C_U(D_0)$. Observe que se $x \in C_U(D_0)$, então $\nu\nu^x \in S$ e $\nu\nu^x = \nu x^{-1}\nu x = (x^{-1})^\nu x \in C_U(D_0)$. Como podemos tomar infinitos x em $C_U(D_0)$, segue que $S \cap C_U(D_0)$ é infinito. Então, $(S \cap C_U(D_0)) \setminus D_0 \neq \varnothing$. Pelo item *(1)* existe $w \in C_U(D_0) \setminus D_0$ que é invertido por ν. Sendo assim, o subgrupo $\langle D_0, w\rangle$ é abeliano e invertido por ν (observe que, como este subgrupo é abeliano, o produto de dois elementos que são invertidos por ν também é invertido por ν). Mas, como D_0 é maximal segue que $D_0 = \langle D_0, w\rangle$, e isto implica que $w \in D_0$, uma contradição. □

Agora, vamos provar o seguinte lema técnico.

Lema 3.2.3. *Seja $x \in U$, e seja $s \in U$ o único elemento tal que $s^{-2} = \nu x^{-1}\nu x$. Então, $xs \in C_U(\nu)$.*

Demonstração. Afirmamos que ν inverte s. De fato, ao conjugar por ν ambos os lados da equação $s^{-2} = \nu\nu^x$, temos que $(s^{-2})^\nu = \nu^x\nu$. Mas, $\nu^x\nu = s^2$. Então, $(s^{-2})^\nu = s^2$. Conjugando por ν novamente, obtemos $(s^2)^\nu = s^{-2}$. E reescrevendo, $(s^\nu)^2 = (s^{-1})^2$. Portanto, como U é unicamente 2-divisível vale que $s^\nu = s^{-1}$.

De maneira inteiramente análoga, também concluímos que ν^x inverte s. Usando estes dois fatos, temos

$$1 = s^2\nu\nu^x = \nu\nu s^2\nu\nu^x = \nu s^{-2}\nu^x = \nu s^{-1}\nu^x\nu^x s^{-1}\nu^x = \nu s^{-1}\nu^x s = \nu s^{-1}x^{-1}\nu xs,$$

e isto implica que $xs\nu = \nu xs$. Portanto, $xs \in C_U(\nu)$. □

Lembramos que fixamos a notação A_u, com $u \in U$, para denotar o maior subgrupo de A que é invertido por $u\nu u^{-1}$. Tal subgrupo possui índice finito em A. Veja:

Proposição 3.2.4. *O índice $|A : A_u|$ é finito.*

Demonstração. Para cada elemento $a \in A$ e considere o elemento

$$\nu\nu^{au}.$$

Como $\nu\nu^{au} = \nu(au)^{-1}\nu au = ((au)^{-1})^{\nu}au$, podemos ver que $\nu\nu^{au} \in U$. Sendo assim, seja $s_a \in U$ tal que $s_a^{-2} = \nu\nu^{au}$. Pelo Lema 3.2.3 obtemos que

$$w_a \coloneqq aus_a \in C_U(\nu). \tag{3.2.2}$$

Agora, defina

$$\mathcal{M}_a \coloneqq \{b \in A \mid w_b = w_a\}.$$

Para cada $w_c \in C_U(\nu)$, podemos construir um conjunto $\mathcal{M}_c$, e como $C_U(\nu)$ é finito,

$$\text{o conjunto } \{\mathcal{M}_c \mid c \in A\} \text{ também é finito.} \tag{3.2.3}$$

Além disso, observe que se $x \in A$, então x está em algum $\mathcal{M}_c$ em que $w_x = w_c$, e como consequência, $x \in \bigcup_{c\in A} \mathcal{M}_c$. Logo, $A \subseteq \bigcup_{c\in A} \mathcal{M}_c$. Por outro lado, se $x \in \bigcup_{c\in A} \mathcal{M}_c$, então x está em algum $\mathcal{M}_c$, que por sua vez está contido em A, assim, $x \in A$. Logo, $\bigcup_{c\in A} \mathcal{M}_c \subseteq A$, e portanto,

$$A = \bigcup_{c\in A} \mathcal{M}_c. \tag{3.2.4}$$

Agora, com raciocínio análogo ao que usamos na demonstração do lema anterior concluímos que ν inverte s_a. Além disso, ν inverte $a \in A$ e ν centraliza w_a.

De (3.2.2) temos que $s_a^{-1} = w_a^{-1}au$. Conjugando por ν ambos os lados desta equação, obtemos $\nu s_a^{-1}\nu = \nu w_a^{-1}au\nu$. Daí, $s_a^{-1} = \nu\nu w_a^{-1}au\nu\nu$. Comutando ν com w_a^{-1}, temos que $s_a^{-1} = \nu w_a^{-1}\nu au$. Como $w_a^{-1} = s_a^{-1}u^{-1}a^{-1}$, vem que $s_a^{-1} = (s_a^{-1}u^{-1}a^{-1})^{\nu}au$. Já que ν inverte a e s_a, reescrevemos $s_a^{-1} = s_a u^{-\nu}aau$, donde segue que $s_a^{-2} = u^{-\nu}aau$. Portanto, $s_a^{-1} = u^{-\nu}aaus_a = u^{-\nu}aw_a$.

Então, obtemos a igualdade $w_a^{-1}au = u^{-\nu}aw_a$. Tendo em vista que $bus_b = aus_a$, para todo $b \in \mathcal{M}_a$, temos $w_a^{-1}bu = \nu u^{-1}\nu bw_a$, então $\nu w_a^{-1}bu = u^{-1}\nu bw_a$, assim

$$\nu w_a^{-1}b = u^{-1}\nu bw_a u^{-1}. \tag{3.2.5}$$

Seja $c \in \mathcal{M}_a$. Da equação (3.2.5), também temos que $\nu w_a^{-1}c = u^{-1}\nu cw_a u^{-1}$. Como $c^{-1} = uw_a^{-1}c^{-1}\nu u\nu w_a^{-1}$ e $b = w_a\nu u^{-1}\nu bw_a u^{-1}$, segue que

$$c^{-1}b = uw_a^{-1}c^{-1}\nu u\nu w_a^{-1}w_a\nu u^{-1}\nu bw_a u^{-1} = uw_a^{-1}c^{-1}bw_a u^{-1},$$

para todo $b, c \in \mathcal{M}_a$.

Agora,vamos mostrar que $uw_a^{-1}\nu w_a u^{-1}$ inverte $c^{-1}b$ usando esta última equação e o fato de que ν inverte $c^{-1}b$:

$$\begin{aligned} uw_a^{-1}\nu w_a u^{-1}c^{-1}buw_a^{-1}\nu w_a u^{-1} &= uw_a^{-1}\nu c^{-1}b\nu w_a u^{-1} \\ &= uw_a^{-1}b^{-1}cw_a u^{-1} \\ &= (uw_a^{-1}c^{-1}bw_a u^{-1})^{-1} \\ &= (c^{-1}b)^{-1}. \end{aligned}$$

Mas, $uw_a^{-1}\nu w_a u^{-1} = uw_a^{-1}w_a\nu u^{-1} = u\nu u^{-1}$, então $u\nu u^{-1}$ inverte $c^{-1}b$ e também seu inverso. Logo, podemos concluir que

$$u\nu u^{-1} \text{ inverte } \langle b^{-1}c \mid b, c \in \mathcal{M}_a\rangle, \text{para todo } a \in A.$$

Por (3.2.3), pela equação (3.2.4) e pelo Corolário 3.1.4, um dos subgrupos

$$\langle b^{-1}c \mid b, c \in \mathcal{M}_a\rangle$$

têm índice finito em A, então $|A : A_u| < \infty$. □

Lema 3.2.5. *Seja B um subgrupo abeliano finitamente gerado de U que é invertido por ν. Então, A contém um subgrupo A_1 de índice finito tal que $\langle A_1, B\rangle$ é abeliano.*

Demonstração. Lembre-se da definição de A, que fixamos no início do capítulo no item (4), e considere para $b \in B$ a definição de A_u, com $u = b$, estabelecida no item (5). Seja

$\mathcal{B} = \{b_1, b_2, ..., b_n\}$ o conjunto de geradores de B e seja

$$A_1 := \bigcap_{i=1}^{n} A_{b_i}.$$

Pela Proposição 3.2.4, $|A : A_{b_i}|$ é finito; e pelo Teorema 1.1.2 de Poincaré, temos que $|A : A_1|$ é finito. Além disso, como $A_1 \leq A_{b_i}$ e $b_i v b_i^{-1}$ inverte A_{b_i}, vale que $b_i v b_i^{-1}$ também inverte A_1 para todo $b_i \in \mathcal{B}$; e ainda, como A_1 é subgrupo de A, sabemos que v inverte A_1, assim, para todo $a \in A_1$ temos $a^{b_i v b_i^{-1}} = a^{-1}$ e $a^v = a^{-1}$. Então, $a^{b_i v b_i^{-1}} = a^v$. Daí, $v b_i v b_i^{-1} a b_i v b_i^{-1} v = a$. Lembrando que v inverte b_i, obtemos que $b_i^{-2} a b_i^2 = a$. Logo, $b_i^2 a = a b_i^2$. Portanto, $b_i^2 \in C_U(A_1)$. Pela Proposição 2.1.5, $C_U(A_1)$ é unicamente 2-divisível, então $b_i \in C_U(A_1)$. Logo, todos os geradores de B comutam com todos os elementos de A_1, e isto significa que, todos os elementos de B comutam com todos os elementos de A_1; ademais B é abeliano e $A_1 \leq A$ é abeliano, então concluímos que $\langle A_1, B \rangle$ é abeliano. □

Lema 3.2.6. *Seja D um subgrupo 2-divisível de A com índice finito. Então, $C_U(D)/D$ é finito e solúvel.*

Demonstração. Seja $C := C_U(D)$ e $\overline{C} := C/D$. Suponha por contradição que $\overline{C}$ é infinito. Do Lema 3.1.6 item *(1)*, $\overline{C}$ é unicamente 2-divisível. E como, por hipótese, $|A : D|$ é finito e $A \leq C$, temos que $\overline{A} := A/D$ é um subgrupo finito de $\overline{C}$.

Observe que, por hipótese, D é unicamente 2-divisível, é abeliano e é invertido por v. Então, podemos aplicar o Lema 3.1.6, item *(2)*, e concluir que vD é um automorfismo involutivo quase regular de $\overline{C}$. Agora, aplicando o Lema 3.2.2 item *(2)* (com $\overline{C}$ no lugar de U e vD no lugar de v), concluímos que existe um subgrupo de $\overline{C}$ infinito e abeliano que é invertido por vD, e é maximal. Vamos denotá-lo por $\overline{E}$.

Agora, note que $\overline{A}$ é abeliano, finitamente gerado e é invertido por vD. Aplicando o Lema 3.2.5 temos que $\overline{E}$ contém um subgrupo $\overline{E_1}$ de índice finito tal que $\overline{E_2} := \langle \overline{E_1}, \overline{A} \rangle$ é abeliano. Sendo assim, $\overline{E_2}$ é invertido por vD pois seus geradores o são. Então, aplicando o Lema 3.1.6, item *(3)*, obtemos que E_2 em C é invertido por v e é abeliano. Como E_2 é gerado por E_1 e A, segue que E_2 contém A propriamente. Mas, isto contradiz a maximalidade de A e mostra que $\overline{C}$ é finito.

Por fim, como $\overline{C}$ é finito e unicamente 2-divisível, a Proposição 2.1.2 garante que $\overline{C}$ possui ordem ímpar. Pelo Teorema 1.5.3 de Feit-Thompson, concluímos que $\overline{C}$ é solúvel. □

Lema 3.2.7. *Seja $R := \langle S \rangle$. Se H é um subgrupo finitamente gerado de R, então H é solúvel e $H/Z(H)$ é finito.*

Demonstração. Seja h um elemento qualquer em R. Como $S = \{v v^u \mid u \in U\}$, temos que

$$h = \prod_{i=1}^{n} (v u_i v u_i^{-1})^{\alpha_i},$$

onde $u_i \in U$ e $\alpha_i = \pm 1$, com $i = 1, 2, ..., n$.

Seja $D := \bigcap_{i=1}^{n} A_{u_i}$, onde A_{u_i} é o subgrupo de A estabelecido no início do capítulo. Da Proposição 3.2.4, temos que o índice $|A : A_{u_i}|$ é finito, com isso, segue do Teorema 1.1.2 (Teorema de Poincaré) que o índice $|A : D|$ é finito. Além disso, pelo Lema 3.1.1, temos que A_{u_i} é 2-divisível, e como em um grupo unicamente 2-divisível, a interseção finita de subgrupos 2-divisíveis também é um subgrupo 2-divisível, segue que D é 2-divisível. Então, podemos aplicar o Lema 3.2.6 e concluir que $C_U(D)/D$ é finito e solúvel.

Como A_{u_i} é o maior subgrupo de A invertido por $u_i v u_i^{-1}$, podemos concluir que D também é invertido por v e por $u_1 v u_1^{-1}, u_2 v u_2^{-1}, ..., u_n v u_n^{-1}$. Assim, para qualquer elemento $d \in D$, temos

$$u_i v u_i^{-1} d u_i v u_i^{-1} = d^{-1}.$$

Conjugando por v ambos os lados desta equação, obtemos

$$v u_i v u_i^{-1} d u_i v u_i^{-1} v = v d^{-1} v = d.$$

Daí, temos que $v u_i v u_i^{-1} d = d v u_i v u_i^{-1}$. Logo, $(v u_i v u_i^{-1})^{\alpha_i} \in C_U(D)$, com $i = 1, 2, ..., n$. Portanto, como h é o produto dos elementos da forma $(v u_i v u_i^{-1})^{\alpha_i}$, segue que $h \in C_U(D)$ ou, equivalentemente, $D \subseteq C_U(h)$.

Seja H um subgrupo finitamente gerado de R. Então $H = \langle h_1, h_2, \ldots, h_s \rangle$ para alguns $h_1, h_2, \ldots, h_s \in R$. Dessa forma, temos que $C_U(H) = \bigcap_{i=1}^{s} C_U(h_i)$. Como $D \subseteq C_U(h_i)$, com $i = 1, 2, \ldots, s$, segue que $D \subseteq C_U(H)$ ou, equivalentemente, $H \subseteq C_U(D)$. Sendo assim,

$$\frac{HD}{D} \leq \frac{C_U(D)}{D}$$

e, portanto, HD/D é finito e solúvel. Pelo Segundo Teorema do Isomorfismo, $H/H \cap D$ também é finito e solúvel. Como D é abeliano, $H \cap D$ é solúvel. Então, do item *(2)* da Proposição 1.5.2, segue que H é solúvel.

Por fim, como $H \cap D \leq Z(H)$ e $|H : H \cap D|$ é finito, temos que $|H : Z(H)|$ também é finito, assim, $H/Z(H)$ é finito. □

Proposição 3.2.8. *Seja $R = \langle S \rangle$. Então:*

(1) R' é um grupo periódico;

(2) R é solúvel.

Demonstração. (1) Sejam $g \in R'$ e $a_1, \ldots, a_n, b_1, \ldots, b_n \in R$ tais que

$$g = \prod_{i=1}^{n} [a_i, b_i].$$

Considere $X = \{a_i, b_i \mid i = 1, ..., n\}$ e $H = \langle X \rangle$. Como $X \subseteq H$ temos que $g \in H'$. Observe que H é finitamente gerado, logo, pelo Lema 3.2.7, segue que $H/Z(H)$ é finito. Aplicando o Teorema 1.1.12, devido a Schur, podemos concluir que H' é finito. Sendo assim, g possui ordem finita, e portanto, R' é periódico.

(2) Observe que S é ν-invariante, então R também é. Logo, ν é um automorfismo involutivo quase regular para R' e como, do item anterior, sabemos que R' é um grupo periódico, podemos aplicar o Corolário 1.5.6 e concluir que R' é virtualmente solúvel. E ainda, pelo Lema 3.2.7, R é localmente solúvel, então R' também é localmente solúvel. Logo, pela Proposição 1.5.7, temos que R' é solúvel. E como R/R' é abeliano, segue que R é solúvel. □

No lema a seguir, veremos que é possível escrever o grupo U como um produto dos subgrupos $R = \langle S \rangle$ e $C_U(\nu)$.

Lema 3.2.9. *(1) Cada elemento $u \in U$ pode ser escrito de forma única como um produto $u = cs$, com $c \in C_U(\nu)$ e $s \in S$;*

(2) O subgrupo $\langle S \rangle$ é normal em U.

Demonstração. (1) Para $x \in U$ vamos denotar por $x^{\frac{1}{2}}$ o único elemento de U cujo quadrado é x. Seja $u \in U$. Suponha que $u = cs$, com $c \in C_U(\nu)$ e $s \in S$. Então, temos que

$$\begin{aligned} u(u^{-1}u^{\nu})^{\frac{1}{2}} &= cs((cs)^{-1}(cs)^{\nu})^{\frac{1}{2}} \\ &= cs(s^{-1}c^{-1}cs^{-1})^{\frac{1}{2}} \\ &= cs(s^{-2})^{\frac{1}{2}} \\ &= css^{-1} = c. \end{aligned}$$

Logo, c é unicamente determinado por u e, consequentemente, como $s = c^{-1}u = (u^{-\nu}u)^{\frac{1}{2}}$, o elemento s também é unicamente determinado por u.

Agora, seja $u \in U$ um elemento arbitrário. Veja que v fixa $u(u^{-1}u^v)^{\frac{1}{2}}$ e que v inverte $(u^{-v}u)^{\frac{1}{2}}$:

$$\begin{aligned}(u(u^{-1}u^v)^{\frac{1}{2}})^v &= u^v((u^{-1}u^v)^{\frac{1}{2}})^v \\ &= u^v((u^{-1}u^v)^v)^{\frac{1}{2}} \\ &= u^v(u^{-v}u)^{\frac{1}{2}} \\ &= u^v(u^{-v}u)(u^{-v}u)^{-1}(u^{-v}u)^{\frac{1}{2}} \\ &= u(u^{-v}u)^{-1}(u^{-v}u)^{\frac{1}{2}} \\ &= u(u^{-v}u)^{-\frac{1}{2}} \\ &= u((u^{-v}u)^{-1})^{\frac{1}{2}} \\ &= u(u^{-1}u^v)^{\frac{1}{2}}\end{aligned}$$

e

$$\begin{aligned}((u^{-v}u)^{\frac{1}{2}})^v &= ((u^{-v}u)^v)^{\frac{1}{2}} \\ &= (u^{-1}u^v)^{\frac{1}{2}} \\ &= ((u^{-v}u)^{-1})^{\frac{1}{2}} \\ &= ((u^{-v}u)^{\frac{1}{2}})^{-1}.\end{aligned}$$

Portanto, $c := u(u^{-1}u^v)^{\frac{1}{2}} \in C_U(v)$ e $s = c^{-1}u = (u^{-v}u)^{\frac{1}{2}} \in S$.

(2) Sejam $c \in C_U(v)$ e $s \in S$. Observe que $s^c \in S$, pois $(s^c)^v = (s^v)^c = (s^{-1})^c = (s^c)^{-1}$. Isto significa que $C_U(v)$ normaliza $\langle S \rangle$. Como de *(1)* temos que $U = \langle S \rangle C_U(v)$, segue que $\langle S \rangle \trianglelefteq U$. □

Finalmente, estamos em condições de demonstrar o

Teorema A. *Seja U um grupo unicamente 2-divisível. Se U admite um automorfismo involutivo quase regular, então U é solúvel.*

Demonstração. Caso em que U é um grupo finito: como U é um grupo finito unicamente 2-divisível, pela Proposição 2.1.2, U possui ordem ímpar. Então, segue do Teorema de Feit-Thompson que U é solúvel.

Caso em que U é um grupo infinito: pela Proposição 3.2.8, $\langle S \rangle$ é solúvel. Do Lema 3.2.9, $U = C_U(v)\langle S \rangle$ e $\langle S \rangle \trianglelefteq U$. Observe que $C_U(v)$ é um subgrupo finito unicamente 2-divisível e, por isso, possui ordem ímpar. Logo, pelo Teorema 1.5.3 de Feit-Thompson, $C_U(v)$ é solúvel. Sendo assim, pela Proposição 1.5.2 item *(3)*, U é solúvel. □

Bibliografia

[1] Burnside, W. (1911). *Theory of groups of finite order*. Cambridge University Press.

[2] Feit, W. and Thompson, J. G. (1963). Solvability of groups of odd order. *Pacific Journal of Mathematics*.

[3] Garcia, A. and Lequain, Y. (2006). *Elementos de álgebra*. Instituto de Matemática Pura e Aplicada.

[4] Higman, G. (1957). Groups and rings having automorphisms without non-trivial fixed elements. *Journal of the London Mathematical Society*, 1(3):321–334.

[5] Neumann, B. (1956). Groups with automorphisms that leave only the neutral element fixed. *Archiv der Mathematik*, 7(1):1–5.

[6] Neumann, B. H. (1954). Groups covered by permutable subsets. *J. London Math. Soc.*, 29:236–248.

[7] Robinson, D. J. (2012). *A Course in the Theory of Groups*, volume 80. Springer Science & Business Media.

[8] Segev, Y. (2010). Toward the abelian root groups conjecture for special Moufang sets. *Adv. Math.*, 223(5):1545–1554.

[9] Segev, Y. (2011). Almost regular involutory automorphisms of uniquely 2-divisible groups. *Proceedings of the American Mathematical Society*, pages 3445–3450.

[10] Shunkov, V. P. (1974). Periodic groups with an almost regular involution. *Algebra and Logic*, pages 260–272.

[11] Thompson, J. (1959). Finite groups with fixed-point-free automorphisms of prime order. *Proceedings of the National Academy of Sciences*, 45(4):578–581.