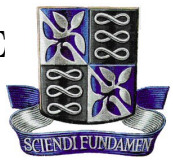
Universidade Federal da Bahia - UFBA
Instituto de Matemática e Estatística - IME
Programa de Pós-Graduação em Matemática - PGMAT
Mestrado em Matemática



CIT-GRUPOS E CN-GRUPOS E SEUS ANÉIS DE GRUPO INTEGRAIS

VANDERLEI LOPES DE JESUS

Salvador-Bahia
Abril de 2017

CIT-GRUPOS E CN-GRUPOS E SEUS ANÉIS DE GRUPO INTEGRAIS

VANDERLEI LOPES DE JESUS

Dissertação de Mestrado apresentada ao colegiado do curso de Pós-Graduação em Matemática da Universidade Federal da Bahia, como requisito parcial para obtenção do Título de Mestre em Matemática.

Orientador: Prof. Dr. Thierry Corrêa Petit Lobão.

Salvador-Bahia
Abril de 2017

Jesus, Vanderlei Lopes.

CIT-grupos e CN-grupos e seus anéis de grupo integrais / Vanderlei Lopes de Jesus. – Salvador: UFBA, 2017.

v, 75 f.

Orientador: Prof. Dr. Thierry Corrêa Petit Lobão.

Dissertação (mestrado) – Universidade Federal da Bahia, Instituto de Matemática e Estatística, Programa de Pós-graduação em Matemática, 2017.

Referências bibliográficas.

1. Anéis (Álgebra). 2. Anéis de Grupo. 3. Teoria de Grupos. I. Petit Lobão, Thierry. II. Universidade Federal da Bahia, Instituto de Matemática. III. Título.

CDU : 512.55

CIT-GRUPOS E CN-GRUPOS E SEUS ANÉIS DE GRUPO INTEGRAIS

Vanderlei Lopes de Jesus

Dissertação de Mestrado apresentada ao Colegiado do Curso de Pós-graduação em Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do título de Mestre em Matemática, em 27 de Abril de 2017.

Banca examinadora:

Prof. Dr. Thierry Corrêa Petit Lobão (Orientador)
UFBA

Prof[a]. Dr[a]. Manuela da Silva Souza
UFBA

Prof. Dr. Osnel Broche Cristo
UFLA

Agradecimentos

Agradecer a Deus por ser minha fortaleza dia a dia. Um muito obrigado a minha amada família, pelo apoio irrepreensível em toda essa caminhada. Um agradecimento especial a minha flor Solange, pelo amor, incentivo e compreensão nesse período em que estivemos distantes, mas nunca separados.

Agradeço a meu orientador Thierry Petit Lobão pela orientação, pelo incentivo e motivação, mesmo com muitos orientandos sempre esteve disposto e atencioso quando precisei.

Agradeço aos professores Manuela da Silva Souza e Osnel Broche Cristo, pela honra de tê-los na banca examinadora de minha dissertação.

Agradeço a todos meus professores do Instituto de Matemática e Estatística da UFBA, por terem contribuído à minha formação.

Agradeço a todos os meus amigos do mestrado, pela amizade e pelos momentos que compartilhamos nesse período.

Um agradecimento muito especial a Gideone e Genildo, pelo laço de amizade e confiança que semeamos nesses dois anos em que moramos e estudamos juntos. Amizades que levarei para a vida.

"Entrega o teu caminho ao Senhor,
cofia nele, e o mais ele fará."
Salmos 37.5

Resumo

Neste trabalho, discutiremos o Problema do Isomorfismo (Iso) e a Propriedade do Normalizador (Nor), duas questões de destaque na teoria de anéis de grupo integrais. Investigaremos estas questões em duas classes de grupos finitos determinadas por centralizadores, a saber, os CN-grupos e os CIT-grupos.

Estes grupos além de serem estruturalmente conectados são historicamente importantes, pelo papel fundamental que desempenharam no esforço que desenvolveu-se em boa parte do século passado na classificação dos grupos simples.

A propriedade do normalizador obteve resposta positiva em várias classes de grupos. Nesse trabalho, vamos mostrar que esta questão tem resposta positiva para a classe dos CIT-grupos e como consequência, concluiremos que a classe dos CN-grupos também é uma solução a questão. Ademais, apresentaremos nossas considerações quanto ao isomorfismo nessas classes de grupos.

Palavras-chave: Anéis de Grupo Integrais; Problema do Isomorfismo; Propriedade do Normalizador; CIT-Grupos; CN-Grupos.

Abstract

In this work, we will discuss the isomorphism problem (Iso) and the normalizer property (Nor), two central questions in theory of integral group rings. We will investigate these questions in two classes of finite groups determined by centralizers, namely the CN-groups and the CIT-groups.

These groups in addition to being structurally connected, are historically important because of the fundamental role they played in the effort that was developed in much of the last century in the classification of simple groups.

The normalizer property obtained positive response in several classes of groups. In this work, we will show that this question has positive response to the class of CIT-groups and as a consequence, we will conclude that the CN-groups class is also a solution to the question. Besides, we will present our considerations regarding isomorphism in these classes of groups.

Keywords: Integral Group Rings; Isomorphism Problem; Normalizer Property; CIT-Groups; CN-Groups.

Sumário

Capítulo 1

Introdução

A dissertação ora apresentada investiga dois temas de grande importância na teoria dos anéis de grupo, o Problema do Isomorfismo (Iso) e a Propriedade do Normalizador (Nor).

Dados um grupo G (não necessariamente finito) e R um anel comutativo com identidade, determinamos um novo anel chamado anel de grupo e denotado por RG, o qual consiste de um módulo livre tendo os elementos do grupo G como base e os elementos do anel R como coeficientes, além de ter a operação multiplicação entre seus elementos, que é definida a partir da propriedade de distributividade. Neste trabalho, G denotará um grupo finito e R um anel com identidade (a menos de casos explícitos) e $\mathbb{Z}G$ denotará os chamados anéis de grupo integrais, isto é, em que o anel de coeficientes considerado é o dos inteiros.

O Conceito de Anel de Grupo apareceu implicitamente no artigo de A. Cayley [Cay54]. Em torno à pesquisa acerca da estrutura das álgebras e da representação de grupos, ganhou destaque notadamente em meados do século XX, tornando-se uma importante área de pesquisa em álgebra. Situando-se na fronteira entre a Teoria dos Grupos e a Teoria dos Anéis, o estudo dos anéis de grupo tem, a cada dia, ganhado mais atenção, em muito, por suas aplicações práticas, como é o caso do uso em Teoria de Códigos de Erro.

Dentre as muitas questões importantes em teoria de anéis de grupo, uma questão central é o *Problema do Isomorfismo*, conhecido como (ISO), que consiste em verificar quando um grupo é determinado pelo seu anel de grupo, ou seja, dados dois grupos G e H e um anel com identidade R, será que a existência de um isomorfismo $RG \simeq RH$ implica em $G \simeq H$? Desde 1940, esta questão vem sendo discutida, a partir dos trabalhos de G. Higman com diversos anéis de coeficientes, entretanto, vários resultados relevan-

tes foram obtidos utilizando-se o anel dos inteiros, e assim, a questão do isomorfismo tornou-se uma conjectura para anéis de grupo integrais:

Conjectura (Iso): *Os grupos finitos são determinados via isomorfismo pelos seus anéis de grupo integrais, isto é, se G é um grupo finito então*

$$\mathbb{Z}G \simeq \mathbb{Z}H \Longrightarrow G \simeq H.$$

Na teoria de anéis de grupo, uma questão de destaque é a chamada *Propriedade do Normalizador*, conhecida como (Nor). Denotamos por $U = U(\mathbb{Z}G)$ o grupo das unidades do anel de grupo integral $\mathbb{Z}G$, por $Z(U(\mathbb{Z}G))$ o centro de tal grupo e por $N_U(G)$ o normalizador de G no grupo das unidades de $\mathbb{Z}G$. Claro que G e $Z(U(\mathbb{Z}G))$ estão contidos em $N_U(G)$, e portanto o produto $G \cdot Z(U(\mathbb{Z}G))$ está contido em $N_U(G)$. Dizemos que um grupo G satisfaz a propriedade do normalizador quando o normalizador de G no grupo das unidades de seu anel de grupo integral $\mathbb{Z}G$ é o menor possível, isto é, o produto de G pelo centro do grupo das unidades de seu anel de grupo integral,

$$N_U(G) = G \cdot Z(U(\mathbb{Z}G)).$$

Inicialmente, (Nor) foi apresentada como conjectura:

Conjectura (Nor): *Seja G um grupo finito. Então*

$$N_U(G) = G \cdot Z(U(\mathbb{Z}G)).$$

Nesse sentido, D. Coleman [Co64], em 1964, mostrou que os p-grupos satisfazem (Nor) e, consequentemente, estendeu esse resultado para os grupos nilpotentes. Posteriormente, S. Jackowski e Z. Marciniak [JaM87], em 1987, mostraram que os grupos que possuem um 2-subgrupo de Sylow normal satisfazem (Nor), e assim concluíram que (Nor) é valida para grupos de ordem ímpar, direcionando, a partir daí, os rumos de investigação de (Nor) para grupos de ordem par.

M. Manzur [Ma95], em 1995, revelou uma relação entre o problema do isomorfismo e a propriedade do normalizador no que diz respeito a algumas extensões infinitas de grupos finitos, como segue no teorema abaixo:

Teorema 1.0.1 *(Manzur, [Ma95]) Se G é um grupo finito e C^∞ representa um grupo cíclico infinito, então o problema do isomorfismo para $\mathbb{Z}(G \times C^\infty)$ tem resposta afirmativa se, e somente se, tem resposta afirmativa para G e vale a conjectura do normalizador em G.*

O resultado de Manzur deu ainda mais relevância a (Nor) e percebeu-se que, no contexto dos grupos infinitos, encontrando-se um contraexemplo para (Nor) era possível obter um contraexemplo para (Iso). Nesse sentido, em 2001, M. Hertweck [Her01], conseguiu uma generalização do resultado de Manzur, para extensões finitas de G e, então, fazendo uso de tal generalização, apresentou um contraexemplo para as duas questões. Sendo assim, ambas as questões perdem o status de conjectura, porém, não a relevância, porque, a partir de então, o objetivo desta linha de pesquisa tornou-se a busca das classes de grupos que satisfazem (Nor) e/ou são determinados pelos seus anéis de grupo integral, satisfazendo (Iso).

Um grupo finito G é chamado *CN-grupo* se o centralizador em G de todo elemento não identidade é um subgrupo nilpotente. Os CN-grupos são completamente classificados e formam uma classe de grupos importante historicamente, em especial, por terem desempenhado papel decisivo no processo de construção da prova do *Teorema da Ordem Ímpar: todo grupo de ordem ímpar é solúvel*; e de classificação dos grupos simples. Um dos maiores trabalhos nesse sentido foi feito, em 1960, por W. Feit, M. Hall e J. Thompson [FHT60], quando eles estabeleceram a solubilidade de todos os CN-grupos de ordem ímpar. Outro trabalho de destaque foi feito por M. Suzuki [Su61], em 1961, ao determinar completamente todos os CN-grupos não solúveis e, ao faze-lô, descobriu uma família de grupos simples que leva seu nome, os chamados *Grupos de Suzuki*.

Um grupo finito de ordem par G é dito *CIT-grupo* se o centralizador em G de toda involução é um 2-grupo. Os CIT-grupos também se destacaram na classificação dos grupos simples, onde foram estudados e classificados por M. Suzuki em [Su61] e [Suz61]. M. Suzuki mostrou que um grupo não solúvel G é um CN-grupo se, e somente se, é um CIT-grupo. Daí, a existência de uma interseção entre estas duas classes de grupos.

Um grupo finito G que contém um subgrupo não trivial H tal que $H \cap x^{-1}Hx = 1$, para todo $x \in G \setminus H$ é chamado grupo de Frobenius. Petit Lobão [Pe01], em 2001, teve sucesso em mostrar que a classe dos grupos de Frobenius é uma solução para (Iso). Em 2002, Petit Lobão e Polcino Milies [PeP02], mostraram que os grupos de Frobenius também satisfazem a (Nor). Esta classe de grupos tem um papel relevante na teoria geral de grupos e representam uma subclasse da imensa variedade de grupos de permutação transitivos. Não existe uma conexão aparente de CN-grupos e CIT-grupos com os grupos de Frobenius, mas os grupos de Frobenius aparecem internamente na estrutura destes grupos. Assim, é natural buscar estender as investigações do Isomorfismo e do Normalizador aos CN-grupos e aos CIT-grupos.

Nesse trabalho, vamos utilizar as técnicas empregadas por Petit Lobão e Polcino

Milies para mostrar que os CIT-grupos constituem uma solução a (Nor). Como consequência, obteremos que os CN-grupos também são uma solução à questão. Além disso, vamos expor nossas considerações quanto à investigação de (Iso) nestas classes de grupos.

Nosso trabalho está organizado da seguinte forma: No segundo capítulo, faremos uma exposição preliminar de definições e resultados de teoria dos grupos, destacaremos alguns grupos de permutação necessários ao corpo desse trabalho e faremos uma revisão de literatura dos conceitos, das propriedades e dos resultados que dizem respeito aos CN-grupos e aos CIT-grupos que são de nosso interesse. Nesse capítulo preliminar, os resultados são apresentados sem demonstração.

No terceiro capítulo, introduziremos definições e resultados iniciais da teoria de anéis de grupo, apresentaremos o grupo das unidades triviais do anel de grupo integral, a propriedade do normalizador, bem como os resultados fundamentais desta questão que são importantes à teoria e ao nosso trabalho. Por fim, abordaremos o problema do isomorfismo apresentando conceitos, propriedades, uma lista de grupos que satisfazem a questão e abordaremos as conjecturas de Zassenhaus.

Finalmente, o quarto capítulo, parte principal de nosso trabalho, é direcionado a investigar a propriedade do normalizador e o problema do isomorfismo para as classes dos CIT-grupos e dos CN-grupos. Mostraremos que estas duas classes de grupos são soluções à questão do normalizador e faremos nossas considerações quanto ao isomorfismo.

Capítulo 2

Preliminares

2.1 Grupos

Apresentaremos nesta sessão definições e resultados importantes da teoria dos grupos que são relevantes no corpo deste trabalho. Para nossos fins G denotará sempre um grupo finito. Para uma leitura aprofundada veja [Rot95], [Sc64] e [Go80].

Definição 2.1.1 *Dados dois elementos g e h de um grupo G, o **comutador** de g e h é o elemento*

$$[g,h] = g^{-1}h^{-1}gh \in G.$$

*Chamamos **subgrupo derivado** de G ao subgrupo gerado*

$$G' = [G,G] = \langle [g,h] \ : \ g,h \in G \rangle.$$

O lema seguinte, diz que G' é o menor subgrupo normal de G tal que o quociente é abeliano.

Lema 2.1.1 *Sejam G um grupo e $H \trianglelefteq G$. Então:*

(i) $G' \trianglelefteq G$;

(ii) $\frac{G}{G'}$ *é abeliano;*

(iii) $\frac{G}{H}$ *é abeliano se, e somente se,* $G' \leq H$.

Se X e Y são subconjuntos de um grupo G escrevemos XY para o subconjunto constituído de todos os produtos xy com $x \in X$ e $y \in Y$. Assim,

$$XY = \{xy \ : \ x \in X, y \in Y\}.$$

Se $X_i, 1 \leq i \leq n$ são subconjuntos de G, definimos o subconjunto $X_1 \cdots X_n$ de modo análogo ao caso $n = 2$. Uma propriedade importante é que $XY = YX$ se, e somente se, XY é um subgrupo de G. Se G é gerado por X e Y, então escrevemos $G = \langle X, Y \rangle$ ou simplesmente $G = XY$.

Definição 2.1.2 *Sejam $G_1, \ldots, G_n$ grupos. Considere o conjunto*

$$G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) \ : \ g_i \in G_i, \ 1 \leq i \leq n\},$$

Com a multiplicação coordenada

$$(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) = (g_1 \cdot h_1, \ldots, g_n \cdot h_n).$$

Este conjunto, munido desta operação assim definida, é um grupo, chamado ***produto direto externo*** *dos grupos $G_1, \ldots, G_n$.*

Definição 2.1.3 *Sejam H e K dois subgrupos de um grupo finito G. Dizemos que G é o* ***produto direto interno*** *de H e K, e escrevemos $G = H \times K$, se as seguintes condições valem:*

(i) $G = HK$;

(ii) $H \cap K = \{1\}$;

(iii) $H \lhd G$ *e* $K \lhd G$.

De modo intuitivo, se $\{H_i\}_{i \in I}$ é uma família de subgrupos normais de um grupo G, então G é chamado produto direto interno dos subgrupos $\{H_i\}_{i \in I}$ e escrevemos $G = \prod_{i \in I} H_i$, se as seguintes condições são satisfeitas:

(i) $G = \langle H_i \ : \ i \in I \rangle$; isto é, todo elemento $g \in G$ pode ser escrito como o produto de um número finito de elementos dos subgrupos $\{H_i\}_{i \in I}$;

(ii) $H_i \cap \langle H_j \ : \ j \in I, \ j \neq i \rangle = \{1\}$ para todo índice $i \in I$.

Teorema 2.1.1 *Sejam K e H subgrupos de um grupo finito G. Então*

(i) $K \times H$ *é abeliano se, e somente se, K e H são abelianos;*

(ii) $K \times H$ *é isomorfo a* $H \times K$;

(iii) Se K e H são grupos cíclicos com ordens relativamente primas então $K \times H$ é cíclico.

Definição 2.1.4 *Sejam G um grupo, $N \trianglelefteq G$ e $H \leq G$. Dizemos que G é o* ***produto semidireto*** *de N por H e escrevemos $G = N \rtimes H$ se valem:*

(i) $G = NH$;

(ii) $\forall\ g \in G,\ g = nh$ *para únicos* $n \in N,\ h \in H$;

(iii) $N \cap H = \{1\}$.

Se $G = N \rtimes H$ então $H \simeq \frac{G}{N}$. Além disso, H é chamado complemento de N e se G é finito então $|G| = |N|[G : N] = |N||H|$.

Definição 2.1.5 *Sejam G um grupo, $N \trianglelefteq G$ e H um grupo. Dizemos que G é o* ***produto semidireto externo*** *de N por H e escrevemos $G \simeq N \rtimes H$ se existe H_1 subgrupo de G tal que $H_1 \simeq H$ e $G = N \rtimes H_1$.*

Definição 2.1.6 *Um subgrupo H de um grupo G diz-se um* ***subgrupo característico*** *se $\phi(H) = H$, para todo automorfismo $\phi : G \to G$. Para indicar que H é um subgrupo característico de G escrevemos $HcarG$.*

Sejam G um grupo e $HcarG$. Restringindo os automorfismos internos de G a H, vemos que H é um subgrupo normal. Segue-se que todo subgrupo característico é normal.

Definição 2.1.7 *Um subgrupo N de um grupo G é dito* ***subgrupo de Hall*** *se sua ordem e índice em G são relativamente primos, isto é, $mdc\big(|N|\ ,\ [G : N]\big) = 1$.*

O próximo resultado garante que se um grupo G contém um subgrupo de Hall normal N, então G decompõe-se em um produto semidireto $G = N \rtimes H$, para algum $H \leq G$.

Proposição 2.1.1 (Schur-Zassenhaus) *Sejam G um grupo e N um subgrupo de Hall normal de G. Então existe um subgrupo H de G tal que $G = N \rtimes H$.*

Definição 2.1.8 *Um subgrupo G é chamado* ***metacíclico*** *se contém um subgrupo normal A tal que A e $\frac{G}{A}$ são cíclicos.*

Definição 2.1.9 *Um grupo G dado pela relação:*

$$G = \langle h, k,\ |\ h^{2^{a-1}} = k^2 = m,\ m^2 = 1,\ k^{-1}hk = h^{-1} \rangle$$

é chamado ***grupo de quatérnios generalizado****. No caso em que $a = 2$ $(|G| = 8)$ ele é chamado grupo de quatérnios.*

Definição 2.1.10 *Seja G um grupo. Um elemento $G \ni x \neq 1$ é dito uma* ***involução*** *se $x^2 = 1$.*

Definição 2.1.11 *Dado um subgrupo H de um grupo G, chama-se* ***normalizador*** *de H em G ao conjunto*

$$N_G(H) = \{g \in G \ : \ H^g = g^{-1}Hg = H\}.$$

O normalizador de H em G é o maior subgrupo de G em que H é normal.

Definição 2.1.12 *Dado um subgrupo H de um grupo G, chama-se* ***centralizador*** *de H em G ao conjunto*

$$C_G(H) = \{g \in G \ : \ gh = hg \ \forall h \in H\}.$$

Em particular,

$$C_G(x) = \{g \in G \ : \ gx = xg\}, \ \forall x \in G.$$

Definição 2.1.13 *Seja G um grupo. O conjunto*

$$Z(G) = \{g \in G \ : \ gx = xg, \ \forall x \in G\}$$

chama-se ***centro*** *de G.*

O centro de G é um subgrupo característico de G que goza da seguinte propriedade:

$$Z(G) = \bigcap_{x \in G} C_G(x).$$

Definição 2.1.14 *Dado $g \in G$, chama-se* ***classe de conjugação*** *de g em G ao conjunto*

$$C_g \ = \ \{x^{-1}gx = g^x \ : \ x \in G\}.$$

Dados $g_1, g_2 \in G$ dizemos que g_1 é **conjugado** de g_2 em G ou que g_1 e g_2 estão na mesma classe de conjugação em G e escrevemos $g_1 \sim g_2$ se, existir $x \in G$ tal que $g_1 = g_2^x$. Por outro lado, dois elementos distintos $a, b \in G$ definem o mesmo conjugado de $g \in G$ se, e somente se,

$$\begin{aligned} a^{-1}ga = b^{-1}gb \ &\Leftrightarrow \ g = ab^{-1}gba^{-1} = (ba^{-1})^{-1}g(ba^{-1}) \\ &\Leftrightarrow \ ba^{-1} \in C_G(g). \end{aligned}$$

Assim, temos que

$$|C_g| = \frac{|G|}{|C_G(g)|} = [G : C_G(g)].$$

Sejam $x_1, x_2, \ldots, x_t$ os representantes de todas as classes de conjugação de G e seja $n_i = |C_{x_i}|$. Como estas classes formam um recobrimento disjunto de G, temos a seguinte **equação das classes**:

$$|G| = n_1 + n_2 + \ldots + n_t. \tag{2.1}$$

Note que um elemento $x_i \in G$ é central se, e somente se, sua classe de conjugação C_{x_i}, consiste de um único elemento, ele próprio, de modo que o número de inteiros n_i que são iguais a 1 na equação 2.1 é precisamente igual a $|Z(G)|$. Assim, também podemos escrever a equação 2.1 da seguinte forma:

$$|G| = |Z(G)| + \sum_{n_i > 1} n_i. \tag{2.2}$$

Definição 2.1.15 *Seja G um grupo e $a \in G$. Dizemos que a é um* ***elemento de torção*** *de G se existir $n \in \mathbb{N}$ tal que $a^n = 1$. O conjunto*

$$T(G) = \{a \in G \ : \ o(a) < +\infty\}$$

é um subgrupo chamado ***subgrupo de torção*** *de G. Se $T(G) = \{1\}$ então G é dito* ***grupo livre de torção****.*

Seja p um inteiro primo. Um grupo finito G diz-se um p**-grupo** se sua ordem é uma potência de p e um elemento $g \in G$ diz-se um p**-elemento** se sua ordem $o(g)$ é uma potência de p. Em um p-grupo todo elemento é um p-elemento. Seja G um grupo finito de ordem $|G| = p^n m$, onde p denota um inteiro primo e $m, n \in \mathbb{N}$ com m não divisível por p. Como a ordem de um subgrupo divide a ordem do grupo, um p-subgrupo de G não pode ter ordem maior que p^n. Assim, um subgrupo de ordem p^n deve ser maximal no conjunto dos p-subgrupos de G.

Definição 2.1.16 *Seja G um grupo de ordem $|G| = p^n m$, em que $p \nmid m$ é um inteiro primo. Um subgrupo de G de ordem p^n chama-se um p-**subgrupo de Sylow** de G.*

O próximo teorema apresenta uma caracterização dos p-subgrupos de Sylow de um grupo G.

Teorema 2.1.2 *Seja G um grupo de ordem $|G| = p^n m$, em que p é um inteiro primo*

que não divide m. Então:

(i) G tem ao menos um p-subgrupo de Sylow;

(ii) Se n_p denota o número de p-subgrupos de Sylow de G então

$$n_p \equiv 1 \ (mod\ p) \ e \ n_p \mid m;$$

(iii) Todo p-subgrupo de G está contido em um p-subgrupo de Sylow de G;

(iv) Todos os p-subgrupos de Sylow de G são conjugados.

Definição 2.1.17 *Um grupo G é dito **solúvel** se contém uma série de subgrupos distintos*

$$1 = H_0 \leq H_1 \leq \ldots \leq H_n = G$$

*tal que, cada subgrupo H_{i-1} é normal em H_i e os grupos quocientes $\frac{H_i}{H_{i-1}}$, $1 \leq i \leq n$, são abelianos. Tal série de subgrupos de G é chamada **série subnormal abeliana** de G.*

Teorema 2.1.3 *Seja H um subgrupo normal de G. Se H e $\frac{G}{H}$ são solúveis, então G é solúvel.*

Definição 2.1.18 *Um grupo G diz-se **nilpotente** se contém uma série de subgrupos distintos*

$$1 = H_0 \leq H_1 \leq \ldots \leq H_n = G$$

tal que cada subgrupo H_i é normal em G e cada quociente $\frac{H_i}{H_{i-1}}$ está contido no centro de $\frac{G}{H_{i-1}}$, $1 \leq i \leq n$.

Uma tal série de subgrupos de G diz-se uma **série central** de G. O menor número natural $n \in \mathbb{N}$ tal que $H_n = G$ chama-se **classe de nilpotência** de G. Um fato importante é que subgrupos e grupos quocientes de grupos nilpotentes são nilpotentes. Além disso, todo p-grupo finito e todos os produtos diretos finitos de grupos nilpotentes são nilpotentes.

Definição 2.1.19 *O subgrupo gerado por todos os subgrupos normais nilpotentes de um grupo G é chamado **subgrupo Fitting** de G e denotado por $Fitt(G)$.*

Uma característica importante e particular dos grupos nilpotentes é que, todo subgrupo de Sylow de um grupo nilpotente é normal, além disso, todo grupo nilpotente

decompõe-se em produto direto de seus subgrupos de Sylow. Apresentamos esta caracterização dos grupos nilpotentes no próximo teorema.

Teorema 2.1.4 *Seja G um grupo finito. Então as seguintes condições são equivalentes:*

(i) G é nilpotente;

(ii) Todo subgrupo de Sylow de G é normal;

(iii) G é produto direto dos seus subgrupos de Sylow.

Definição 2.1.20 *Sejam G um grupo e X um conjunto não vazio. Dizemos que G **age** sobre X se existir uma aplicação $\tau : G \times X \to X$, com $\tau(g, x) = gx$, atendendo as condições:*

1. $1x = x,\ \forall x \in X.$
2. $g_1(g_2x) = (g_1g_2)x,\ \forall g_1, g_2 \in G,\ x \in X.$

*A aplicação τ é chamada **ação** de G sobre X e X é chamado G**-conjunto**. Se $n = |X|$, então n é chamado o **grau** do G-conjunto X. Se X for infinito então ele é um G-conjunto de grau infinito. O grau de um G-conjunto também é o chamado **grau do grupo** G.*

Sejam G um grupo, X um G-conjunto e um elemento $x \in X$. Chamamos de **estabilizador** de x em G e denotamos por $stb_G(x)$, ao conjunto de todos os elementos de G que fixam x, isto é,

$$stab_G(x) = \{g \in G \ : gx = x\}.$$

O $stab_G(x)$ é um subgrupo de G. Para cada $x \in X$, chamamos de **órbita** de x ao conjunto

$$orb(x) = \{gx \ : g \in G\}.$$

Exemplo 2.1.1 *A aplicação $f : G \times G \to G$ definida por*

$$(g, x) \mapsto g^x = x^{-1}gx,$$

*é uma ação, chamada **Ação Conjugação**. Veja que, para todo $x \in G$ temos*

$$stab_G(x) = C_G(x) \text{ e } orb(x) = \{g^x \ : \ g \in G\}.$$

Dados um grupo G e um G-conjunto X, existe uma relação entre o estabilizador e a órbita de um elemento $x \in X$. O Teorema da órbita e do estabilizador garante que o tamanho da orbita de x é o índice de seu estabilizador no grupo G.

Teorema 2.1.5 (Teorema da órbita e do estabilizador) *Sejam G um grupo e X um G-conjunto. Então para cada $x \in X$,*

$$|orb(x)| = [G : stab_G(x)].$$

2.2 Grupos de Permutação

Nesta seção faremos uma breve abordagem sobre os grupos de permutação, apresentando alguns grupos e resultados, sem demonstração, necessários ao desenvolvimento do trabalho.

Definição 2.2.1 *Uma **permutação** de um conjunto não vazio X é uma bijeção $\pi : X \to X$. O conjunto $S(X) = \{\pi : X \to X,$ todas as permutações de $X\}$ munido da composição de funções é um grupo, chamado **grupo de permutações** de X.*

Se $\pi, \rho \in S(X)$, escrevemos a composição $\pi \circ \rho$ simplesmente pela justaposição $\pi\rho$. Se X é finito, com n elementos, então escrevemos $S(X) = S_n$.

Definição 2.2.2 *Uma permutação $\pi \in S_n$ é dita um **r-ciclo** se existem elementos distintos $a_1, \ldots, a_r \in \{1, \ldots, n\}$ tais que*

$$\pi(a_1) = a_2,\ \pi(a_2) = a_3, \ldots,\ \pi(a_{r-1}) = a_r,\ \pi(a_r) = a_1,$$

e tais que

$$\pi(j) = j,\ \forall j \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_r\},$$

*tal r-ciclo é denotado por $(a_1 \ldots a_r)$ e o número r é chamado o comprimento do ciclo. Os 2-ciclos são também chamados **transposições**.*

Uma propriedade importante é que, todo elemento de S_n pode ser expresso por um produto de transposições (esta escrita não é necessariamente única), isto é, $S_n = \langle\{\text{transposições}\}\rangle$.

Definição 2.2.3 *Um elemento $\pi \in S_n$ é uma **permutação par** quando π se escreve como um produto de um número par de transposições. Analogamente, um elemento*

*$\pi \in S_n$ é uma **permutação ímpar** quando π se escreve como um produto de um número ímpar de transposições.*

Definição 2.2.4 *Seja S_n um grupo de permutação. Seja*

$$A_n = \{\sigma \in S_n \mid \sigma \text{ é permutação par}\}.$$

*Temos que A_n é um subgrupo de S_n de índice 2 denominado **grupo alternado** ou **grupo das permutações pares**.*

Uma característica importante dos grupos alternados A_n, é que eles são simples para $n \geq 5$. Como A_2 e A_3 são trivialmente simples, temos que A_n é simples para $n \neq 4$.

Seja G um grupo de permutação e X um G-conjunto. Dizemos que G **age transitivamente** sobre X ou, simplesmente, que G é um **grupo transitivo** se, para quaisquer $x, y \in X$, existir $g \in G$ com $gx = y$ ou, equivalentemente, se

$$X = orb(x), \forall\ x \in X.$$

Dizemos que G é um **grupo semitransitivo** se todas as órbitas têm o mesmo comprimento. Ainda, se $stab_G(x) = \{1\}$ para todo $x \in X$ então G é dito **grupo semirregular**. Se G é semirregular e transitivo então G é dito **grupo regular**.

Dizemos que um grupo de permutação G agindo sobre um G-conjunto X é **k-transitivo** se, dadas duas sequências $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k)$ arbitrárias de elementos de X, existir um elemento $\sigma \in G$ tal que

$$\sigma x_i = y_i,\ \forall\ i = 1, \ldots, k.$$

2.2.1 Grupos de Zassenhaus

Os **grupos de Zassenhaus**, em homenagem a Hans Zassenhaus, constituem uma classe de grupos de permutação 2-transitivos, historicamente importantes por conter famílias infinitas de grupos simples. Os grupos de Zassenhaus contribuíram para a classificação dos grupos cujos 2-subgrupos de Sylow são diedrais, os grupos com 2-subgrupo de Sylow abelianos e os grupos cujo centralizador de todo elemento não-identidade é nilpotente. Graças a Hans Zassenhaus, M. Suzuki e W. Feit, os grupos de Zassenhaus são completamente classificados, como podemos ver em [HuB82] Capítulo XI. e [Go80] Capítulo $XIII$.

Definição 2.2.5 *Um grupo de permutação G agindo sobre um conjunto finito X é dito ser um grupo de Zassenhaus se as seguintes condições são satisfeitas:*

1. *G é 2-transitivo;*
2. *Todo $1 \neq g \in G$ fixa no máximo 2 pontos de X;*
3. *G não tem subgrupo normal regular.*

Exemplo 2.2.1 *Em geral, obter exemplos de grupos de Zassenhaus não é uma tarefa fácil, mas encontramos uma infinidade de grupos de Zassenhaus quando analisamos os grupos alternados simples, por exemplo, A_5 e A_6 são grupos de Zassenhaus.*

Observação 2.2.1 *Os grupos de Zassenhaus são chamados Z-grupos. Seja G um grupo de Zassenhaus agindo sobre um conjunto de $n+1$ elementos X. Se n é par então G é dito um grupo de Zassenhaus de grau ímpar ou simplesmente um ZT-grupo. Nesse caso, em 1961, M. Suzuki, a saber [[Su61] Parte I Teorema 1], mostrou que G é um grupo simples cujo centralizador de toda involução é um 2-grupo.*

2.2.2 Grupos de Frobenius

Um **grupo de Frobenius** é um grupo de permutação transitivo G que não é regular, isto é, o estabilizador em G, de todo elemento de um G-conjunto é não trivial. Assim como os grupos de Zassenhaus, os grupos de Frobenius representarem uma classe de grupos de permutação transitivos relevante em teoria dos grupos. Uma leitura aprofundada sobre os grupos de Frobenius pode ser feita em [Go80] e [Sc64].

Uma definição alternativa para grupos de Frobenius é a seguinte:

Definição 2.2.6 *Um grupo finito G é chamado grupo de Frobenius se contém um subgrupo não trivial H tal que $H \cap H^x = 1$, para todo $x \in G \setminus H$, onde*

$$H^x = \{x^{-1}hx \ : \ x \in G \setminus H, \ h \in H\}.$$

Uma observação importante é que nenhum grupo abeliano G é um grupo de Frobenius, pois nesse caso $H \cap H^x = H$, qualquer que seja H subgrupo de G e x em G. Ademais, o subgrupo H da Definição 2.2.6 não é normal. Uma caracterização dos grupos de Frobenius é apresentada no teorema seguinte e sua demonstração encontra-se em [Go80] Teorema 7.6.

Teorema 2.2.1 *Sejam G um grupo de Frobenius e H um subgrupo tal que $H \cap H^g = 1$, para todo $g \in G \setminus H$. Escreva $H^* = H \setminus \{1\}$. Então:*

(i) $K = G \setminus (\bigcup_{x \in G} (H^*)^x)$ *é um subgrupo característico de G, $mdc(|K|, |H|) = 1$ e $G = K \rtimes H$.*

(ii) K *é nilpotente.*

(iii) Se $|H|$ é par, então existe um único elemento z de ordem 2 em H, este elemento é central em H e $z^{-1}kz = k^{-1}$, para todo $k \in K$. Ademais, K é abeliano.

(iv) Se $h^{-1}kh = k$, para $h \in H^*$ e $k \in K$, então $k = 1$. Isto é, a ação de H^* em K é livre de ponto fixo.

O subgrupo K do Teorema 2.2.1 é unicamente determinado e é chamado **núcleo de Frobenius** de G. Um subgrupo H tal que $G = K \rtimes H$ é chamado **complemento de Frobenius** de G.

Exemplo 2.2.2 *O grupo alternado A_4 é um grupo de Frobenius. Com efeito, A_4 é um grupo de ordem 12 cujo único subgrupo normal não trivial é o subgrupo*

$$K = \{1, (12)(34), (13)(24), (14)(23)\},$$

que é isomorfo ao grupo de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$. O grupo A_4 possui exatamente quatro subgrupos de ordem 3 todos eles conjugados entre si. Além disso, A_4 possui três subgrupos de ordem 2 todos eles conjugados entre si, mas A_4 não possui subgrupos de ordem 6. Temos que a permutação $(123) \in A_4$ gera o subgrupo

$$\langle (123) \rangle = \{1, (123), (132)\}.$$

Ademais, $K \cap \langle (123) \rangle = \{1\}$ e $A_4 = K \rtimes \langle (123) \rangle$ é um grupo de Frobenius com núcleo de Frobenius K e complementar de Frobenius $\langle (123) \rangle$.

2.2.3 Grupos de Camina

Agora faremos uma exposição, de forma sucinta, dos **grupos de Camina**. Estes grupos, constituem uma generalização dos grupos de Frobenius e foram introduzidos por A. R. Camina, em 1978, [Ca78]. Os grupos de Camina apresentam uma estrutura peculiar: toda classe lateral não trivial do subgrupo derivado consiste de elementos conjugados.

Definição 2.2.7 *Um* ***núcleo de Camina*** *em um grupo finito G é um subgrupo normal próprio K tal que se $g \in G \setminus K$ então g é conjugado a gk em G, para todo $k \in K$. Em outras palavras, a classe lateral gK de todo elemento $g \in G \setminus K$ é uma classe de conjugação.*

Sejam K_1 e K_2 núcleos de Camina de um grupo G e fixemos $g \in G - \{K_1 \cup K_2\}$. Dado $k_1 \in K_1$ temos que g é conjugado a gk_1 em G. Logo, existe $x \in G$ tal que $gk_1 = g^x$. Mas, desde que K_2 é o núcleo de Camina de G, existe $k_2 \in K_2$ tal que $g^x = gk_2$. Daí, obtemos que,

$$gk_1 = g^x = gk_2 \;\Leftrightarrow\; k_1 = k_2.$$

Portanto, $K_1 \subseteq K_2$. De modo análogo, $K_2 \subseteq K_1$, e portanto $K_1 = K_2$. Logo, o núcleo de Camina de um grupo finito G é único.

Se K é o núcleo de Camina de um grupo finito G, então para todo $k \in K$ e $g \in G \setminus K$, tem-se que g é conjugado a gk em G. Logo, existe $x \in G$ tal que

$$gk = g^x = x^{-1}gx \;\Rightarrow\; k = g^{-1}x^{-1}gx = [g, x] \in G'.$$

Portanto, $K \subseteq G'$. Se G' é o núcleo de Camina de G, então dizemos que G é um grupo de Camina

Exemplo 2.2.3 *Considere o grupo dos quatérnios de ordem* 8

$$Q_8 = \langle i, j, k \;:\; i^2 = j^2 = k^2 = -1 = ijk \rangle$$

de subgrupos:
$H_1 = Q_8$, $H_2 = \{1\}$, $H_3 = \{1, -1\}$, $H_4 = \{1, -1, i, -i\}$, $H_5 = \{1, -1, j, -j\}$ *e* $H_6 = \{1, -1, k, -k\}$.
As classes de conjugação em Q_8 são:

$$C_1 = \{1\},\; C_{-1} = \{-1\},\; C_i = \{i, -i\},\; C_j = \{j, -j\} \text{ e } C_k = \{k, -k\}.$$

Agora veja que $Q_8' = \{1, -1\}$. Logo, se $g \in Q_8 \setminus Q_8'$, então $C_g = gQ_8'$. Portanto, Q_8 é um grupo de Camina.

Exemplo 2.2.4 *Considere o grupo diedral de ordem* 8

$$D_4 = \langle a, b \;:\; a^4 = 1 = b^2,\; bab = a^{-1} \rangle$$

de subgrupos:
$H_1 = D_4$, $H_2 = \{1\}$, $H_3 = \{1, a, a^2, a^3\}$, $H_4 = \{1, b\}$, $H_5 = \{1, ab\}$, $H_6 = \{1, a^2b\}$, $H_7 = \{1, a^3b\}$ *e* $H_8 = \{1, a^2\}$.
as classes de conjugação em D_4 *são:*

$$C_1 = \{1\},\ C_a = \{a, a^3\},\ C_{a^2} = \{a^2\},\ C_b = \{b, ab\},\ C_{a^2b} = \{a^2b, a^3b\}.$$

Temos que $D_4' = \{1, a^2\}$. *Note que, para todo* $g \in D_4 \setminus D_4'$, *tem-se* $C_g = gD_4'$. *Portanto,* D_4 *é um grupo de Camina.*

Observe que, na Definição 2.2.7, o núcleo de Camina K de um grupo finito G é sempre um subgrupo próprio normal de G. Assim, grupos abelianos e grupos simples nunca podem ser grupos de Camina, uma vez que grupos abelianos têm subgrupos derivados triviais $\{1\}$ e grupos simples não têm subgrupos normais próprios. Uma caracterização dos grupos de Camina segue no próximo teorema.

Teorema 2.2.2 *(Teorema 2, [Ca78]) Seja* G *um grupo finito com a propriedade de ter um núcleo de Camina* K. *Então uma das seguintes afirmações é verdadeira:*

(i) G *é um grupo de Frobenius com núcleo de Frobenius* K.

(ii) K *é um* p*-grupo para algum primo* p.

(iii) $\frac{G}{K}$ *é um* p*-grupo para algum primo* p.

Em 1996, os autores Rex Dark e Carlo M. Scoppola, [DaS96], provaram que p-grupos de Camina têm classe de nilpotência limitada por três. E, fazendo uso deste resultado, obtiveram o seguinte corolário:

Corolário 2.2.1 *(Corolário, [DaS96]) Seja* G *um grupo finito com núcleo de Camina* K *e seja* $\frac{G}{K}$ *um* p*-grupo abeliano. Se* G *não é um* p*-grupo nem um grupo de Frobenius com núcleo de Frobenius* K, *então* $p = 2$, G *é um grupo de Frobenius com complementar de Frobenius isomorfo ao* Q_8 *e* K *é um subgrupo de índice* 4.

Interpretando o Teorema 2.2.2 e o Corolário 2.2.1, vemos que grupos de Camina são essencialmente, grupos de Frobenius finitos ou grupos de Camina com núcleo de Camina G' um p-grupo. Mas, David Chillag e Marcel Herzog, em 2008, [ChH08], utilizando uma generalização de núcleo de Camina, mostraram que se, G é um grupo de Camina, então G é um p-grupo, um grupo de Frobenius com núcleo G' ou $\frac{G}{G'}$ é um p-grupo. Aliando este resultado ao Corolário 2.2.1, obtemos que grupos de Camina consistem de grupos de Frobenius e p-grupos.

Observação 2.2.2 *Quando iniciamos as discussões referentes a elaboração deste trabalho, tínhamos como meta investigar as questões do isomorfismo e do normalizador no anel de grupo integral sobre grupos de Camina. Após nos familiarizarmos com esses grupos, percebemos que eles são soluções triviais às duas questões, uma vez que, consistem de p-grupos e grupos de Frobenius, grupos estes que são soluções a ambas questões, como veremos no decorrer deste trabalho.*

2.2.4 Grupo Linear Especial Projetivo

O grupo das matrizes não singulares (determinante não nulo) são um objeto de estudo natural como grupos de permutação. Uma investigação na estrutura desses grupos nos permite conhecer uma família de grupos simples. Nesta subseção, iremos resumidamente, descrever as propriedades e os resultados dos grupos lineares especiais projetivos, que são relevantes no desenvolvimento deste trabalho. Para uma leitura aprofundada veja [Go80], [GrS12], [HuB82], [Rot95] e [Sc64].

Definição 2.2.8 *Seja K um corpo. O **Grupo Linear Geral** $GL(m, K)$ é o grupo multiplicativo de todas as matrizes $m \times m$ não singulares sobre K. Se $K = \mathbb{F}_q$ é um corpo finito com q elementos, então denotamos este grupo por $GL(m, q)$.*

O conjunto de todas as matrizes $m \times m$ sobre um corpo K que possuem determinante 1 é um subgrupo de $GL(m, K)$, denotado por $SL(m, K)$ e chamado **Grupo Linear Especial**. Se $K = \mathbb{F}_q$ é um corpo finito com q elementos, então denotamos este grupo por $SL(m, q)$.

Denote por $Z(m, K)$ o centro do grupo $GL(m, K)$. O **Grupo Linear Geral Projetivo** sobre K é o grupo quociente

$$PGL(m, K) = \frac{GL(m, K)}{Z(m, K)}.$$

Ademais, se $SZ(m, K)$ denota o centro do grupo $SL(m, K)$, então o **Grupo Linear Especial Projetivo** sobre K é o grupo quociente

$$PSL(m, K) = \frac{SL(m, K)}{SZ(m, K)}.$$

Como antes, se $K = \mathbb{F}_q$ é um corpo finito com q elementos, então escrevemos $PGL(m, q)$ e $PSL(m, q)$ para denotar o grupo linear geral projetivo e o grupo linear especial projetivo respectivamente.

Seja V um espaço vetorial de dimensão finita m sobre um corpo K e seja $GL(V)$ o grupo de automorfismos de V. Então cada elemento de $GL(m, K)$ corresponde naturalmente um automorfismo linear de V. Consequentemente,

$$GL(m, K) \simeq GL(V).$$

Seja $SL(V)$ o grupo dos automorfismos de V cuja representação matricial tem determinante 1. Como o determinante de uma matriz não depende da base escolhida, temos que

$$SL(m, K) \simeq SL(V).$$

Assim, se $Z(V)$ e $SZ(V)$ denotam os centro de $GL(V)$ e $SL(V)$, respectivamente, então temos os isomorfismos $Z(m, K) \simeq Z(V)$ e $SZ(m, K) \simeq SZ(V)$. Segue que

$$PGL(m, K) \simeq PGL(V) \text{ e } PSL(m, K) \simeq PSL(V).$$

Seja $V_{n+1}(K)$ um espaço vetorial de dimensão $n+1$ sobre um corpo K. Definimos uma relação de equivalência sobre $V_{n+1}(K)$ da seguinte forma

$$\alpha \equiv \beta \text{ se } \exists\ k \in K - \{0\} \text{ tal que } k\alpha = \beta.$$

Denote a classe de equivalência de α por $[\alpha]$. Definimos o **Espaço Projetivo** n-dimensional $\mathbb{P}_n(K)$ sobre o corpo K como o conjunto de todas as classes de equivalência $[\alpha]$, onde $\alpha \neq 0$. Se $K = \mathbb{F}_q$ é um corpo com q elementos, então denotamos este espaço projetivo por $\mathbb{P}_n(q)$.

Uma demonstração do próximo teorema pode ser encontrada nas Proposições 1.26 e 1.27 de [GrS12].

Teorema 2.2.3 *Fixemos $m = 2$ e $K = \mathbb{F}_q$ um corpo finito com q elementos. Seja $V_2(\mathbb{F}_q)$ um espaço vetorial bidimensional sobre $\mathbb{F}_q$ e seja $\mathbb{P}_1(q)$ o respectivo espaço projetivo unidimensional. Então*

(i) $PGL(2, q)$ agindo sobre $\mathbb{P}_1(q)$ é um grupo de Zassenhaus para $q > 3$;

(ii) $PSL(2, q)$ agindo sobre $\mathbb{P}_1(q)$ é um grupo de Zassenhaus para $q > 3$ ímpar.

Uma demonstração do próximo teorema pode ser encontrada no Teorema 9.46 de [Rot95].

Teorema 2.2.4 *Os grupos $PSL(m, K)$ são simples para $m \geq 3$ e todo corpo K. Ademais, os grupos $PSL(2, q)$ são simples para $q > 3$.*

O Teorema 2.2.3, mostra que os grupos projetivos $PGL(2, q)$ e $PSL(2, q)$ para $q > 3$ e $q > 3$ ímpar, respectivamente, constituem uma infinidade de exemplos de grupos de Zassenhaus. Por outro lado, o Teorema 2.2.4 apresenta o critério para simplicidade dos grupos projetivos $PSL(m, K)$, assim obtemos uma família infinita de grupos de simples.

Observação 2.2.3 *Os grupos projetivos especiais e os grupos alternados A_n, representam uma infinidade de grupos simples e são estruturalmente relacionados. Descrevemos alguns casos, que podem sem verificados em [Rot95].*

(i) O grupo $PSL(2, 9)$ é de ordem 360 e é isomorfo ao grupo Alternado A_6.

(ii) O grupo $PSL(2, 3)$ é de ordem 12 e é isomorfo ao grupo Alternado A_4, que é um grupo de Frobenius.

(iii) Os grupos $PSL(3, 4)$ e A_8 são grupos simples de mesma ordem, mas não são isomorfos.

2.3 CN-Grupos

2.3.1 Grupos de Suzuki

Os **grupos de Suzuki** foram introduzidos em 1960 por Michio Suzuki, [Su60]. Estes grupos constituem uma família infinita de grupos simples e foram descobertos por Suzuki quando ele classificou todos os grupos finitos não solúveis cujo centralizador de todo elemento não identidade é nilpotente. Suzuki construiu esses grupos como um subgrupo do grupo linear especial $SL(4, q)$ gerado por certas três matizes explícitas 4×4 sobre um corpo finito. Faremos nessa subseção a construção feita por Suzuki e sua caracterização. Para uma leitura aprofundada sobre os grupos de Suzuki recomendamos [Su60], [HuB82] e [GrS12].

Construção do grupo de Suzuki:

Seja q uma potência de 2 com expoente ímpar: $q = 2^{2n+1}$, $n \in \mathbb{Z}_{\geq 0}$. Escrevemos $q = 2r^2$ com $r = 2^n$. Seja $K = \mathbb{F}_q$ um corpo finito com q elementos e seja θ o automorfismo de K que mapeia cada elemento a sua r-ésima potência, isto é, $\theta(\alpha) = \alpha^r$,

para todo $\alpha \in K$. Para um par de elementos $\alpha, \beta \in K$, denotamos por $S(\alpha, \beta)$ a seguinte matriz triangular inferior:

$$S(\alpha,\beta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha^r & 1 & 0 & 0 \\ \beta & \alpha & 1 & 0 \\ \alpha^{2r+1} + \alpha^r\beta + \beta^{2r} & \alpha^{r+1} + \beta & \alpha^r & 1 \end{pmatrix}.$$

Agora, para cada $\lambda \in K - \{0\}$, seja $M(\lambda)$ a seguinte matriz diagonal:

$$M(\lambda) = \begin{pmatrix} \lambda^r & 0 & 0 & 0 \\ 0 & \lambda^{1-r} & 0 & 0 \\ 0 & 0 & \lambda^{r-1} & 0 \\ 0 & 0 & 0 & \lambda^{-r} \end{pmatrix}.$$

Por fim, denote por T a seguinte matriz não singular:

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

O grupo gerado por estas três matrizes quadradas 4×4 é um subgrupo de $SL(4, q)$, chamado **grupo de Suzuki** e denotado por $Suz(q)$, isto é,

$$Suz(q) = \big\langle S(\alpha,\beta), M(\lambda), T \mid \alpha, \beta \in K,\ \lambda \in K \setminus \{0\} \big\rangle.$$

O próximo teorema caracteriza os grupos de Suzuki e sua demonstração pode ser encontrada em [HuB82] Capítulo XI Seção 3 e em [GrS12].

Teorema 2.3.1 *Seja $Suz(q)$ um grupo de Suzuki com $q = 2^{2n+1}$ e $n \in \mathbb{Z}_{\geq 0}$. Então*

(i) $|Suz(q)| = (q-1)q^2(q^2+1)$ *se* $K = \mathbb{F}_q$;

(ii) $Suz(q)$ *é um grupo de Zassenhaus se* $q > 2$;

(iii) $Suz(q)$ *é simples se* $q > 2$;

(iv) $Suz(2) = \langle\ \alpha, \beta \mid \alpha^5 = 1 = \beta^4,\ \alpha\beta = \beta\alpha^2\ \rangle = \mathbb{Z}_5 \rtimes \mathbb{Z}_4$ *é o grupo de Frobenius de ordem* 20*, com núcleo de Frobenius isomorfo ao grupo cíclico* $\mathbb{Z}_5$ *e complementar de Frobenius isomorfo ao grupo cíclico* $\mathbb{Z}_4$;

(vi) Se $q > 2$, então para todo $g \in Suz(q)$, $g \neq 1$, tem-se que $C_G(g)$ é nilpotente.

Pelo Teorema 2.3.1, se G denota um grupo de Suzuki, então G é um grupo de Zassenhaus simples cujo centralizador de todo elemento não identidade é nilpotente ou G é um grupo de Frobenius de ordem 20 com núcleo isomorfo ao grupo cíclico $\mathbb{Z}_5$ e complementar isomorfo ao grupo cíclico $\mathbb{Z}_4$.

2.3.2 CA-Grupos

Um grupo finito G diz-se **CA-grupo** se, o centralizador de todo elemento não identidade é um subgrupo abeliano, isto é, para todo $1 \neq x \in G$, o subgrupo $C_G(x)$ é abeliano.

Exemplo 2.3.1 *Todo grupo abeliano é um CA-grupo. Um fato interessante é que se, G não tem centro trivial, então G é um CA-grupo se, e somente se, G é um grupo abeliano. Com efeito, se $Z(G) \neq \{1\}$, então existe $1 \neq g \in Z(G)$. Como g é um elemento central, segue que $C_G(g) = G$. Assumindo que G é um CA-grupo, temos que $C_G(g) = G$ é abeliano. Concluímos que um CA-grupo G é um grupo abeliano ou tem centro trivial.*

Os CA-grupos foram estudados primeiramente por Louis Weisner em 1925, [We25]. Ele provou que tais grupos finitos são solúveis ou simples. No entanto, existe um erro em sua prova. Mas, Yu-Fen Wu em 1998, [YFW98], apresentou uma prova correta para o resultado de Weisner.

Em 1957, Michio Suzuki, a saber [Su57], mostrou que CA-grupos de ordem ímpar consistem de grupos de Frobenius e grupos abelianos. No ano seguinte, R. Brauer, Suzuki e G. Wall, [BrSW58], provaram que CA-grupos de ordem par são grupos de Frobenius, grupos abelianos ou isomorfos ao grupo simples $PSL(2, 2^m)$ para $m \geq 2$. Unindo esses resultados temos o seguinte teorema:

Teorema 2.3.2 *Seja G um CA-grupo. Se a ordem de G é ímpar, então*

(i) G é um grupo de Frobenius; ou

(ii) G é um grupo abeliano.

Se a ordem de G é par, então

(i) G é um grupo de Frobenius;

(ii) G *é um grupo abeniano; ou*

(iii) G *é isomorfo ao* $PSL(2, 2^m)$ *para* $m \geq 2$.

2.3.3 CN-Grupos

Agora abordaremos os grupos finitos cujo centralizador de todo elemento não identidade é um subgrupo nilpotente. Estes grupos são chamados **CN-grupos**. Os matemáticos W. Feit, M. Hall e J. Thompson em [FHT60], empenhados em mostrar que todo grupo de ordem ímpar é solúvel e em classificar os grupos simples, estabeleceram a solubilidade de todos os CN-grupos de ordem ímpar. Estes grupos englobam os grupos nilpotentes, a família dos CA-grupos e como podemos observar no Teorema 2.3.1, a família dos grupos de Suzuki simples. Uma analise completa sobre essa classe de grupos pode ser feita consultando [Go80], [Su61] e [FHT60].

Para analisar os CN-grupos solúveis, precisamos do conceito de **grupo de 3-passos**. Seja G um grupo finito e p um número primo fixado divisor da ordem de G. O subgrupo gerado por todos os p-subgrupos normais de G é um p-subgrupo normal de G e, em particular, é o único p-subgrupo normal maximal de G. Denotamos tal subgrupo por $O_p(G)$. Seja $\bar{G} = \frac{G}{O_p(G)}$. Em $\bar{G}$ consideremos o único p'-subgrupo normal maximal $O_{p'}(\bar{G})$. Denote por $O_{p,p'}(G)$ sua imagem inversa em G. Temos que $O_{p,p'}(G)$ é um subgrupo normal de G que contém $O_p(G)$. Similarmente, definimos $O_{p,p',p}(G)$ como a imagem inversa em G de $O_p(\frac{G}{O_{p,p'}(G)})$. Continuando a definição de maneira análoga, obtemos uma série de subgrupos característicos de G:

$$1 \lhd O_p(G) \lhd O_{p,p'}(G) \lhd O_{p,p',p}(G) \lhd \ldots \text{ série superior de } G.$$

$$1 \lhd O_{p'}(\bar{G}) \lhd O_{p',p}(\bar{G}) \lhd O_{p',p,p'}(\bar{G}) \lhd \ldots \text{ série inferior de } G.$$

Definição 2.3.1 *Dizemos que um grupo* G *é um grupo de* 3*-passos (com respeito ao primo* p*) quando*

(i) $O_{p,p'}(G)$ *é um grupo de Frobenius com núcleo de Frobenius* $O_p(G)$ *e complementar de Frobenius cíclico de ordem ímpar. Isso implica que* $p = 2$ *ou* G *é um grupo de ordem ímpar;*

(ii) $G = O_{p,p',p}(G)$ *e* $O_{p,p'}(G) \lhd G$;

(iii) $\frac{G}{O_p(G)}$ *é um grupo de Frobenius com núcleo de Frobenius* $\frac{O_{p,p'}(G)}{O_p(G)}$.

Lema 2.3.1 *Seja G um grupo de 3-passos com respeito a um primo p. Então G é um CN-grupo solúvel.*

Observação 2.3.1 *A demonstração do lema encontra-se em [[Go80], Lema 1.4, p. 401] e consiste em mostrar que, se G é um grupo de 3-passos com respeito a um primo p, então dado P, um p-subgrupo de Sylow de G, existe $A \simeq \frac{O_{p,p'}(G)}{O_p(G)}$, um subgrupo cíclico de G com ordem relativamente prima com p, tal que G é gerado por P e por A; isto é, cada elemento $g \in G$ pode ser expresso de modo único como $g = xy$ com $x \in P$ e $y \in A$, e assim escrevemos $G = PA$. Daí, para concluir que G é um CN-grupo, basta mostrar que $C_G(x)$ é nilpotente para todo $x \in P$ e que $C_G(y)$ é nilpotente para todo $y \in A$. Para tanto, mostra-se que $C_G(x)$ é um p-grupo para todo $x \in P$ e que $C_G(y) = A$ para todo $x \in A$. Como p-grupos e grupos abelianos são grupos nilpotentes, o resultado segue.*

Concluímos da demonstração do lema que, se G é um grupo de 3-passos com respeito a um primo p, então dado P um p-subgrupo de Sylow de G, existe $A \simeq \frac{O_{p,p'}(G)}{O_p(G)}$, um subgrupo cíclico de G com ordem relativamente prima com p, tal que G é gerado por P e por A, isto é, $G = PA$. Ademais, $C_G(x)$ é um p-grupo para todo $x \in P$ e $C_G(y) = A$ para todo $y \in A$

Exemplo 2.3.2 *O grupo de permutação S_4 é um exemplo de um grupo de 3-passos. Com efeito, para $p = 2$ temos que*

$$O_2(S_4) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \quad e \quad O_{2,3}(S_4) = A_4.$$

Como $\frac{S_4}{A_4} \simeq \mathbb{Z}_2$ temos que S_4 é um grupo de 3-passos com respeito a $p = 2$ e com série superior

$$1 \lhd Z_2 \times \mathbb{Z}_2 \lhd A_4 \lhd S_4.$$

Se P denota um 2-subgrupo de Sylow de S_4, então P tem ordem 8 e é isomorfo ao grupo diedral D_4. Segue que $S_4 = PA$, onde $A \simeq \mathbb{Z}_3$.

O próximo teorema caracteriza os CN-grupos solúveis e sua demonstração encontra-se em [[Go80], Teorema 1.5, p. 402].

Teorema 2.3.3 *(Feit, Hall e Thompson) Seja G um CN-grupo solúvel. Então uma das afirmações é verdadeira:*

(i) G é nilpotente;

(ii) G é um grupo de Frobenius com complementar cíclico ou produto direto de um cíclico de ordem ímpar por um grupo de quatérnios generalizado;

(iii) G é um grupo de 3-passos.

Como observa Daniel Gorenstein em [Go80] página 416, no caso em que um CN-grupo G não é solúvel, Suzuki [Su61], provou que G é um grupo de Zassenhaus de grau ímpar, o qual é simples, pela Observação 2.2.1, ou G é isomorfo a um dos seguintes grupos lineares especiais projetivos:

(i) $PSL(2,q)$, onde q é um número de Fermat ($q = 2^{2^n} + 1,\ n \in \mathbb{Z}_{\geq 0}$) ou um número de Mersenne primo ($q = 2^n - 1,\ n \in \mathbb{Z}_{\geq 2}$);

(ii) $PSL(2,9)$;

(iii) $PSL(3,4)$.

Temos pela Observação 2.2.3 que se G é isomorfo a $PSL(2,9)$ ou a $PSL(3,4)$, então é um grupo simples. Se G é isomorfo a $PSL(2,q)$ onde $q = 2^{2^n} + 1$, é um número de Fermat, então para $q = 3$ $(n = 0)$ tem-se $PSL(2,q) = PSL(2,3) \simeq A_4$ é um grupo de Frobenius. Para $q > 3$ $(n > 0)$ tem-se que $PSL(2,q)$ é simples, pelo Teorema 2.2.4. No caso em que G é isomorfo a $PSL(2,q)$, com $q = 2^n - 1$ um número de Mersenner primo, temos, para $q = 3,\ (n = 2)$ que $PSL(2,q) = PSL(2,3)$ é um grupo de Frobenius e, para $q > 3,\ (n > 2)$ que $PSL(2,q)$ é um grupo simples.

Pelo Teorema 2.2.3, temos que os grupos $PSL(2,q)$ são grupos de Zassenhaus para $q > 3$ ímpar. Assim, o resultado de Suzuki é resumido no seguinte teorema:

Teorema 2.3.4 *Seja G um CN-grupo não solúvel. Então vale uma das seguintes afirmações:*

(i) G é um grupo de Zassenhaus simples;

(ii) G é isomorfo ao grupo simples $PSL(3,4)$;

(iii) G é isomorfo ao grupo alternado A_4, que é um grupo de Frobenius de ordem 12.

Observe que, tanto no caso solúvel quanto no caso não solúvel, os CN-grupos intersectam estruturalmente os grupos de Frobenius. Na próxima seção, veremos que CN-grupos e grupos de Frobenius também então relacionados com os CIT-grupos.

2.4 CIT-Grupos

Com a noção de CN-grupos podemos considerar grupos de ordem par e focar nossa atenção no centralizador de involuções. Os grupos de ordem par cujo centralizador de involuções é um 2-grupo foram estudados e classificados por M. Suzuki em [Su61] e [Suz61]. Reuniremos nesta sessão os principais resultados e propriedades dos CIT-grupos que serão importantes no decorrer do nosso trabalho.

Lema 2.4.1 *Todo grupo de ordem par possui pelo menos uma involução.*

Demonstração: Seja G um grupo finito tal que $|G| = 2m$. Logo o número de elementos não triviais de G é $2m-1$ que é ímpar. Suponhamos por absurdo que G não possui uma involução, isto é, todo elemento $G \ni x \neq 1$ é diferente de seu inverso. Assim, os elementos de G e seus inversos podem ser listados aos pares:

$$(x_1, x_1^{-1}),\ (x_2, x_2^{-1}),\ \ldots,\ (x_n, x_n^{-1}).$$

Admitindo que $x_1 = 1$, os elementos restantes são de um total par, um absurdo, pois o número de elementos não triviais de G é ímpar. Portanto, para algum $G \ni x \neq 1$, devemos ter $x = x^{-1}$, isto é, x é uma involução.

■

Definição 2.4.1 *Um grupo G de ordem par é dito **CIT-grupo** se o centralizador em G de toda involução é um 2-grupo.*

Note que pela Observação 2.2.1, os grupos de Zassenhaus simples constituem um importante exemplo de CIT-grupos.

Exemplo 2.4.1 *O grupo diedral de ordem 8, $D_4 = \langle a, b \ : a^4 = 1,\ b^2 = 1,\ bab = a^{-1} \rangle$ possui 5 involuções, a saber, $a^2,\ b,\ ab,\ a^2b,$ e a^3b, com centralizadores*

$$C_G(a^2) = D_4,\ C_G(b) = C_G(ab) = \{1, a^2, b, ab\} \text{ e } C_G(a^2b) = C_G(a^3b) = \{1, a^2, a^2b, a^3b\}.$$

Logo, o centralizador em D_4 de toda involução é um 2-grupo, e portanto D_4 é um CIT-grupo.

Exemplo 2.4.2 *Em geral, todo 2-grupo finito G é um CIT-grupo. Com efeito, G possui pelo menos uma involução x e temos que $C_G(x) \leq G$. Pelo Teorema de Lagrange,*

a ordem de um subgrupo divide a ordem do grupo. Como G é um 2-grupo temos que $C_G(x)$ é um 2-grupo. Daí, todo 2-grupo finito é um CIT-grupo.

Exemplo 2.4.3 *Seja $S_3 = \langle a, b \ : \ a^3 = 1, b^2 = 1, \ baba = 1\rangle$ o grupo de permutação de três pontos. Temos que b, ab, e a^2b são as involuções em S_3, com centralizadores*

$$C_G(b) = \{1, b\}, \ C_G(ab) = \{1, ab\} \ e \ C_G(a^2b) = \{1, a^2b\}.$$

Assim, o centralizador em S_3 de toda involução é um 2-grupo, e portanto S_3 é um CIT-grupo.

Em 1961, Suzuki [Su61] mostrou, no Teorema 4, que os CN-grupos não solúveis são CIT-grupos, mas não conseguiu naquele momento determinar se CIT-grupos eram CN-grupos. Contudo, em [Suz61] Teorema 14, ele concluiu que CIT-grupos não solúveis são CN-grupos. Daí segue o Teorema:

Teorema 2.4.1 *(Suzuki) Um grupo finito não solúvel G é um CN-grupo se, e somente se, é um CIT-grupo.*

Como, por definição, CIT-grupos são de ordem par, vemos que o resultado de Suzuki garante que todo CN-grupo não solúvel é de ordem par. Sabemos que todo CN-grupo de ordem ímpar é solúvel, pois todo grupo de ordem ímpar é solúvel, mas veja que isso não impede a existência de CN-grupos solúveis de ordem par. Como os CN-grupos não solúveis são conhecidos pela sessão anterior, focaremos agora nossa atenção na estrutura dos CIT-grupos solúveis.

Teorema 2.4.2 *(Suzuki, [Su61] Parte II Teorema 1) Seja G um CIT-grupo. Assuma que G contêm um subgrupo normal próprio de ordem ímpar. Então G é um grupo solúvel. Neste caso, G contém um subgrupo normal abeliano A de ordem ímpar tal que $G = A \rtimes S$, para um 2-subgrupo de Sylow S de G e nenhum elemento não identidade de A comuta com um elemento não identidade de S. Em particular, G é um grupo de Frobenius.*

Este último teorema diz que se G é um CIT-grupo solúvel e contém um subgrupo normal próprio normal de ordem ímpar, então G é um grupo de Frobenius com complementar um 2-subgrupo de Sylow e núcleo abeliano. Vejamos agora o caso em que G é um CIT-grupo solúvel, mas não contém um subgrupo normal próprio de ordem ímpar.

Teorema 2.4.3 *(Suzuki, [Su61] Parte II Teorema 2) Seja G um CIT-grupo solúvel. Se G não contém um subgrupo normal próprio de ordem ímpar, então G possui uma série de subgrupos normais de ordem par*

$$G \rhd L \rhd N \rhd 1$$

tal que $\frac{G}{L}$ e $\frac{L}{N}$ são cíclicos de ordens relativamente primas, N é um 2-grupo e a extensão de G sobre N é disjunta, isto é, $G = N \rtimes K$ com $N \cap K = \{1\}$. Se além disso, $\frac{G}{N}$ é de ordem par, então o grupo $\frac{G}{L}$ é isomorfo a um 2-subgrupo de $\frac{G}{N}$, que induz um automorfismo de $\frac{L}{N}$ livre de pontos fixos, isto é, $\frac{G}{N} \simeq \frac{L}{N} \rtimes \frac{G}{L}$ é um grupo de Frobenius.

Observação 2.4.1 *Na demonstração do teorema Suzuki, mostra que, se $\frac{G}{N}$ é um grupo de ordem par, então $\frac{G}{N}$ é um grupo de Frobenius. Veja que se $\frac{G}{N}$ é de ordem ímpar, então N é um subgrupo de Hall de G, e portanto pelo Teorema de Schur-Zassenhaus, existe um subgrupo K de G de ordem ímpar igual a $|\frac{G}{N}|$ tal que $G = N \rtimes K$. Uma propriedade interessante revelada por Suzuki nessa demonstração é que se, $\frac{G}{N}$ é de ordem ímpar e P é um p-subgrupo de Sylow de G com p primo ímpar, então P é cíclico e $N \rtimes P$ é um grupo de Frobenius.*

No caso de $\frac{G}{N}$ ter ordem par, Suzuki mostra que $\frac{L}{N}$ é de ordem ímpar, e assim N é um subgrupo de Hall de L, donde, pelo Teorema de Schur-Zassenhaus, existe um subgrupo H de L de ordem ímpar igual a $|\frac{L}{N}|$ tal que $L = N \rtimes H$. No final da prova, Suzuki mostra que, se $K = N_G(H)$, então $G = N \rtimes K$. Além disso, $K \simeq \frac{G}{N}$ é um grupo de Frobenius com núcleo $\frac{L}{N}$ e complementar isomorfo a $\frac{G}{L}$.

Em todo caso, independentemente da ordem de $\frac{G}{N}$, como $\frac{L}{N}$ é um subgrupo normal de $\frac{G}{N}$, temos o seguinte isomorfismo no produto semidireto externo

$$K \simeq \frac{G}{N} \simeq \frac{L}{N} \rtimes \frac{G}{L}.$$

Como $\frac{L}{N}$ e $\frac{G}{L}$ são cíclicos de ordens relativamente primas, segue que K é um grupo metacíclico.

Decorre que, se G é um CIT-grupo solúvel e não contém um subgrupo normal próprio de ordem ímpar, então G pode ser decomposto em um produto semidireto $G = N \rtimes K$, de um 2-grupo normal N por um grupo metacíclico K.

Capítulo 3

Anéis de Grupo

Neste capítulo, faremos uma exposição de conceitos e resultados importantes que são necessários para estudos na teoria de anéis de grupo e que estão presentes na literatura. Apresentaremos o grupo das unidades triviais de um anel de grupo integral e abordaremos a propriedade do normalizador e o problema do isomorfismo. Para uma leitura aprofundada da teoria de anéis de grupo veja [PoS02] e [Se93].

Definição 3.0.1 *Sejam G um grupo (não necessariamente finito) e R um anel com identidade. Denotamos por RG o conjunto de todas as combinações lineares formais da forma*

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

em que $a_g \in R$ e $(a_g)_{g \in G}$ é uma sequência quase nula, isto é, apenas um número finito de termos é diferente de zero. A tripla $(RG, +, \cdot)$, ou simplesmente RG, com as operações de adição e multiplicação definidas da seguinte forma:

(i) soma de dois elementos:

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

(ii) produto de dois elementos:

$$\big(\sum_{g \in G} a_g g\big) \cdot \big(\sum_{h \in G} b_h h\big) = \sum_{g,h \in G} (a_g b_h)(gh),$$

é um anel chamado ***anel de grupo de*** G ***sobre*** R.

Note que RG possui elemento identidade $1_{RG} = 1_R 1_G$, ou seja, RG é um anel com identidade. Também, $0_{RG} = \sum_{g\in G} 0_R g$. Definindo o produto de um elemento $\sum_{g\in G} a_g g$ de RG por escalar λ de R da seguinte forma:

$$\lambda \cdot \big(\sum_{g\in G} a_g g\big) = \sum_{g\in G} (\lambda a_g) g,$$

verifica-se que RG é um R-módulo, e, se R é comutativo segue-se que RG é uma álgebra sobre R. Anéis de grupo em que o anel considerado é o dos inteiros, $\mathbb{Z}$, são chamados **anéis de grupo integrais**.

Exemplo 3.0.1 *Sejam $C_2 = \langle g \ : \ g^2 = 1_{C_2}\rangle$ o grupo cíclico de ordem 2 e $\mathbb{Z}_3$ o corpo dos números inteiros módulo 3. O anel de grupo de C_2 sobre $\mathbb{Z}_3$ é o conjunto*

$$\mathbb{Z}_3 C_2 = \{a \cdot 1_{C_2} + b \cdot g \ : \ a, b \in \mathbb{Z}_3\} = \{0, 1, 2, g, 2g, 1+g, 1+2g, 2+g, 2+2g\}.$$

Lema 3.0.1 *Sejam R um anel finito de ordem m e G um grupo finito de ordem n. Então o anel de grupo RG é um anel finito de ordem $|R|^{|G|} = m^n$.*

De agora em diate, denotaremos tanto a identidade de RG quanto a identidade de G por 1, a menos de casos explícitos.

Definição 3.0.2 *A função $\varepsilon : RG \to R$ definida por*

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

que é um epimorfismo de anéis, chama-se ***função de aumento*** *de RG.*

Para ver que ε é um epimorfismo de anéis, considere elementos quaisquer $\alpha = \sum_{g\in G} a_g g$, $\beta = \sum_{g\in G} b_g g \in RG$. Então, para a soma temos que:

$$\begin{aligned}
\varepsilon(\alpha+\beta) &= \varepsilon\Big(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\Big) = \varepsilon\Big(\sum_{g\in G} (a_g + b_g) g\Big) \\
&= \sum_{g\in G} (a_g + b_g) = \sum_{g\in G} a_g + \sum_{g\in G} b_g \\
&= \varepsilon\Big(\sum_{g\in G} a_g g\Big) + \varepsilon\Big(\sum_{g\in G} b_g g\Big).
\end{aligned}$$

Para o produto, temos que:

$$\begin{aligned}\varepsilon(\alpha\cdot\beta) &= \varepsilon\Big(\sum_{g\in G}a_g g\cdot\sum_{h\in G}b_h h\Big)=\varepsilon\Big(\sum_{g,h\in G}(a_g b_h)(gh)\Big)\\ &= \sum_{g,h\in G}a_g b_h=\sum_{g\in G}a_g\cdot\sum_{h\in G}b_h\\ &= \varepsilon\Big(\sum_{g\in G}a_g g\Big)\cdot\varepsilon\Big(\sum_{h\in G}b_h h\Big).\end{aligned}$$

Veja que ε é sobrejetor, pois dado um elemento $r\in R$ tem-se que $r=\varepsilon(r1)$. Portanto, ε é um epimorfismo de anéis.

O núcleo da função de aumento ε é denotado por $\Delta_R(G)$ e o chamaremos de **ideal de aumento** de RG. Note que se $\alpha=\sum_{g\in G}a_g g\in\Delta_R(G)$ então

$$\varepsilon(\alpha)=\varepsilon\Big(\sum_{g\in G}a_g g\Big)=\sum_{g\in G}a_g=0.$$

Assim, temos que

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

Desde que os elementos da forma $g-1\in\Delta_R(G)$, onde $g\in G$, segue-se que $\{g-1\ :\ g\in G,\ g\neq 1\}$ é um conjunto gerador de $\Delta_R(G)$ sobre R. Como também é claramente linearmente independente sobre R, temos que esse conjunto constitui uma base de $\Delta_R(G)$ sobre o anel R.

Segue que podemos escrever

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

Seja N um subgrupo normal de G. Então a função $\varphi: RG\to R(\frac{G}{N})$ definida por

$$\varphi(\alpha)=\varphi\Big(\sum_{g\in G}a_g g\Big)=\sum_{g\in G}a_g gN$$

é um epimorfismo de anéis com

$$\Delta_R(G,N)=ker\varphi=\Big\{\sum_{g\in G}a_g g\in RG\ :\ \sum_{g\in G}a_g gN=0\Big\}.$$

Como $G = \bigcup_{i=1}^{k} g_i N$, onde $k = [G : N]$ é o índice de N em G, temos que

$$\alpha = \sum_{g \in G} a_g g = \sum_{i=1}^{k} \sum_{n \in N} a_{(g_i n)} g_i n = \sum_{i=1}^{k} g_i \Big(\sum_{n \in N} a_{(g_i n)} n \Big).$$

Note que

$$\begin{aligned} \alpha \in \Delta_R(G,N) &\Leftrightarrow \varphi(\alpha) = 0 \\ &\Leftrightarrow \sum_{i=1}^{k} \sum_{n \in N} a_{(g_i n)} \varphi(g_i)\varphi(n) = 0 \\ &\Leftrightarrow \sum_{i=1}^{k} \Big(\sum_{n \in N} a_{(g_i n)} \Big) \varphi(g_i) = 0 \\ &\Leftrightarrow \sum_{n \in N} a_{(g_i n)} = 0, \ \forall i. \end{aligned}$$

Portanto,

$$\begin{aligned} \alpha &= \sum_{i=1}^{k} g_i \Big(\sum_{n \in N} a_{(g_i n)} n \Big) = \sum_{i=1}^{k} g_i \Big(\sum_{n \in N} a_{(g_i n)} n - \sum_{n \in N} a_{(g_i n)} \Big) \\ &= \sum_{i=1}^{k} g_i \sum_{n \in N} a_{(g_i n)} (n-1) \in \langle x - 1 \ : \ x \in N \rangle_{RG}. \end{aligned}$$

Daí, segue que

$$\Delta_R(G,N) = \Big\{ \sum_{n \in N} a_n (n-1) \ : \ a_n \in RG \Big\}.$$

Em particular, $\Delta_R(G) = \Delta_R(G,G)$.

Definição 3.0.3 *Dado $\alpha = \sum_{g \in G} a_g g \in RG$, definimos o **suporte** de α como o conjunto dos elementos $g \in G$ que aparecem na composição de α de forma não trivial. Em símbolos,*

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

Dados um grupo G e um anel R, podemos considerar $\{C_i\}_{i \in I}$ o conjunto das classe de conjugação de G que possuem um número finito de elementos. Assim, para cada $i \in I$, temos os elementos chamados de **somas de classes** de G sobre R, denotadas

por $\hat{C}_g$, descritos da seguinte forma:

$$\hat{C}_g = \sum_{x \in C_g} x = \sum_{x \sim g} x.$$

Dados dois elementos x e y de um anel R, o **comutador de Lie** de x e y é o elemento

$$(x, y) = xy - yx.$$

O conjunto gerado

$$(R, R) = \langle (x, y) \ : \ x, y \in R \rangle$$

é um subgrupo aditivo de R gerado por todos os comutadores de Lie (x, y), com $x, y \in R$. Em particular,

$$(RG, RG) = \langle (\alpha, \beta) \ : \ \alpha, \beta \in RG \rangle$$

é um R-módulo com multiplicação por escalar definida por:

$$r(x, y) = (rx, y), \ \forall x, y \in G \text{ e } r \in R.$$

Para $\alpha = \sum_{g \in G} a_g g \in RG$, definimos

$$\tilde{\alpha}_g = \sum_{h \sim g} a_h,$$

onde $\sim$ denota a conjugação em G, isto é, $\tilde{\alpha}_g$ é a soma dos coeficientes de α na classe de conjugação de g.

Lema 3.0.2 *Dado o anel de grupo RG temos:*

(i) $(RG, RG) = \left\{ \sum_{i=1}^{n} r_i(g_i, h_i) \ : \ n \in \mathbb{N}; \ g_i, h_i \in G \ e \ r_i \in R \right\}$

(ii) se $\alpha \in (RG, RG)$*, então* $\tilde{\alpha}_g = 0$*, para todo* $g \in G$*.*

Demonstração:

(i) Sejam $\alpha = \sum_{g \in G} a_g g, \ \beta = \sum_{h \in G} b_h h \in RG$. Temos

$$\begin{aligned} (\alpha, \beta) &= \left(\sum_{g \in G} a_g g, \sum_{h \in G} b_h h \right) = \sum_{g,h \in G} (a_g b_h)(gh) - \sum_{g,h \in G} (b_h a_g)(hg) \\ &= \sum_{g,h \in G} r_{g,h}(gh - hg) = \sum_{g,h \in G} r_{g,h}(g, h). \end{aligned}$$

Portanto $(RG, RG) \subseteq \left\{ \sum_{i=1}^{n} r_i(g_i, h_i) \ : \ n \in \mathbb{N};\ g_i, h_i \in G \text{ e } r_i \in R \right\}$. Como a inclusão contraria é óbvia pela multiplicação por escalar, $r(x, y) = (rx, y)$, $\forall x, y \in G$ e $r \in R$, temos a igualdade.

(ii) Sejam $\sum_{g\in G} a_g g,\ \sum_{h\in G} b_h h$ elementos arbitrários de RG, tais que

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

Como $(g, h) = gh - hg = gh - h(gh)h^{-1}$, uma vez que gh e hg são conjugados em G, temos

$$\begin{aligned} \alpha &= \sum_{g,h\in G} r_{g,h}(g, h) = \sum_{g,h\in G} r_{g,h}(gh - hg) = \sum_{g,h\in G} r_{g,h}(gh - h(gh)h^{-1}) \\ &= \underbrace{\sum_{g,h\in G} r_{g,h}(gh)}_{\alpha_1} - \underbrace{\sum_{g,h\in G} r_{g,h} h(gh)h^{-1}}_{\alpha_2}. \end{aligned}$$

Assim, para cada somando do coeficiente de gh em α_1 temos um somando do coeficiente de $h(gh)h^{-1}$ em α_2, o qual será o seu simétrico aditivo, com g e h percorrendo G. Portanto, $\tilde{\alpha}_x = 0\ \forall x \in G$.

■

3.1 Unidades Triviais

Definição 3.1.1 *Seja R um anel. Denotamos por $U(R)$ o* ***grupo multiplicativo das unidades*** *de R, isto é,*

$$U(R) = \{x \in R \ : \ (\exists y \in R)\ xy = yx = 1\}.$$

Dado o anel de grupo RG, chamamos de **unidades triviais** os elementos da forma $ug \in RG$ em que $u \in U(R)$ e $g \in G$. Assim, em particular, as únicas unidades triviais do anel de grupo integral $\mathbb{Z}G$ são $\pm g$.

Note que a função de aumento ε é tal que $\varepsilon(\alpha) \in U(R)$ para todo $\alpha \in U(RG)$, pois

se $\alpha = \sum_{g\in G} a_g g \in U(RG)$, então existe $\beta = \sum_{h\in G} b_h h \in RG$ tal que

$$\alpha \cdot \beta = \left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} (a_g b_h)(gh) = 1_R 1_G = 1.$$

Portanto,

$$\left(\sum_{g\in G} a_g\right) \cdot \left(\sum_{h\in G} b_h\right) = 1_R$$

donde $\varepsilon(\alpha) = \sum_{g\in G} a_g \in U(R)$. Denotamos por

$$U_1(RG) = \{\alpha \in U(RG) \ : \ \varepsilon(\alpha) = 1\},$$

o **subgrupo das unidades normalizadas** de RG, ou **subgrupo das unidades de aumento 1** em $U(RG)$.

Seja $u \in U(\mathbb{Z}G)$, como $U(\mathbb{Z}) = \pm 1$ temos que $\varepsilon(u) = \pm 1$. Portanto, podemos escrever $U(\mathbb{Z}G) = \pm U_1(\mathbb{Z}G)$.

Definição 3.1.2 *A aplicação* $* : \mathbb{Z}G \to \mathbb{Z}G$ *definida por*

$$*\left(\sum_{g\in G} a_g g\right) = \left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1},$$

que satisfaz as seguintes propriedades:

(i) $*(\alpha + \beta) = \alpha^* + \beta^*$;

(ii) $*(\alpha\beta) = \beta^*\alpha^*$;

(ii) $*(*(\alpha)) = \alpha^{**} = \alpha$.

Recebe o nome de involução canônica, ou clássica, de $\mathbb{Z}G$.

Esta aplicação representa uma ferramenta importante nos estudos de anéis de grupo integral, como podemos observar no próximo resultado.

Proposição 3.1.1 *Para* $\gamma \in \mathbb{Z}G$, $\gamma\gamma^* = 1$ *se, e somente se,* $\gamma = \pm g$, *para algum* $g \in G$.

Demonstração: Por um lado, suponha que $\gamma = \sum_{g\in G} a_g g$, $\gamma^* = \sum_{g\in G} a_g g^{-1}$ e $\gamma\gamma^* = 1$. Então,

$$1 = \gamma\gamma^* = \left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} a_g g^{-1}\right) = \sum_{g\in G} a_g^2 \cdot 1 + \sum_{g\neq 1} a_g g.$$

Logo, $\sum_{g\in G} a_g^2 = 1$, implicando existir único $g_0 \in G$ tal que $a_{g_0} = \pm 1$. Assim,

$$\gamma = \sum_{g\in G} a_g g = a_{g_0} g_0 + \sum_{g\neq g_0} a_g g,$$

e portanto

$$\begin{aligned} 1 = \gamma\gamma^* &= \big(a_{g_0} g_0 + \sum_{g\neq g_0} a_g g\big) \cdot \big(a_{g_0} g_0^{-1} + \sum_{g\neq g_0} a_g g^{-1}\big) \\ &= a_{g_0}^2 \cdot 1 + \sum_{g\neq g_0} (a_{g_0} a_g)(g_0 g^{-1}) + \sum_{g\neq g_0} (a_g a_{g_0})(g g_0^{-1}) + \sum_{g\neq g_0} a_g g \cdot \sum_{g\neq g_0} a_g g^{-1} \\ &= 1 + a_{g_0} \cdot \sum_{g\neq g_0} a_g (g_0 g^{-1}) + a_{g_0} \cdot \sum_{g\neq g_0} a_g (g g_0^{-1}) + \sum_{g\neq g_0} a_g g \cdot \sum_{g\neq g_0} a_g g^{-1}. \end{aligned}$$

Assim,

$$a_{g_0} \cdot \sum_{g\neq g_0} a_g (g_0 g^{-1}) + a_{g_0} \cdot \sum_{g\neq g_0} a_g (g g_0^{-1}) + \sum_{g\neq g_0} a_g g \cdot \sum_{g\neq g_0} a_g g^{-1} = 0,$$

isto é, $\sum_{g\neq g_0} a_g = 0$, onde concluímos que $\sum_{g\neq g_0} a_g g = 0$, e assim $\gamma = a_{g_0} g_0 = \pm g_0$.

Reciprocamente, se $\gamma = \pm g$ para algum $g \in G$, então $\gamma^* = \pm g^{-1}$ e claramente $\gamma\gamma^* = 1$.

■

Proposição 3.1.2 (Berman - Higman) *Sejam G um grupo finito e um elemento $\gamma = \sum_{g\in G} a_g g \in \mathbb{Z}G$ tal que $\gamma^m = 1$. Se $a_1 \neq 0$, então $\gamma = \pm 1$.*

Demonstração: Ver [Proposição 1.4, [Se93]].

■

Corolário 3.1.1 *Sejam G um grupo finito e $\gamma = \sum_{g\in G} a_g g \in Z(U(\mathbb{Z}G))$, uma unidade central de ordem finita. Então γ é da forma $\pm g$, com $g \in Z(G)$. Em particular,*

$$T(Z(U(\mathbb{Z}G))) = Z(G).$$

Demonstração: Se $\gamma = \sum_{g\in G} a_g g$ é um elemento central de ordem finita no grupo das unidades de $\mathbb{Z}G$, então, para algum $g_0 \in Z(G)$ temos $a_{g_0} \neq 0$. Logo, $\gamma \cdot g_0^{-1}$ também é uma unidade de ordem finita em $\mathbb{Z}G$. Além disso, o coeficiente de 1 na expressão $\gamma \cdot g_0^{-1}$ é $a_{g_0} \neq 0$. Pela Proposição 3.1.2 temos que $\gamma \cdot g_0^{-1} = \pm 1$, e portanto $\gamma = \pm g_0$. Em particular, $g_0 \in Z(G)$ então $\gamma = \pm g_0 \in (\pm)Z(G)$. Como G é um grupo finito logo é um grupo de torção, e portanto $T(Z(U(\mathbb{Z}G))) = Z(G)$. ■

Corolário 3.1.2 *Suponha que $\gamma \in \mathbb{Z}G$ seja tal que $\gamma\gamma^* = \gamma^*\gamma$. Se γ é uma unidade de ordem finita n, então $\gamma = \pm g_0$, para algum $g_0 \in G$.*

Demonstração: Digamos que $\gamma = \sum_{g\in G} a_g g$. Como $\gamma\gamma^* = \gamma^*\gamma$ e γ tem ordem finita n, temos que $(\gamma\gamma^*)^n = 1$. Além disso,

$$\gamma\gamma^* = \sum_{g\in G} a_g^2 \cdot 1 + \sum_{g\neq 1} a_g g,$$

e portanto $\sum_{g\in G} a_g^2 \neq 0$. Pela Proposição 3.1.2, temos que $\gamma\gamma^* = \pm 1$. Consequentemente, $\sum_{g\in G} a_g^2 = 1$. Assim, $\gamma\gamma^* = 1$. Segue que existe um único $a_{g_0} = \pm 1$ e concluímos que $\gamma = \pm g_0$, para algum $g_0 \in G$.

■

3.2 A Propriedade do Normalizador

A **Propriedade do Normalizador** (Nor) é uma questão de destaque na teoria dos anéis de grupo integrais sobre grupos finitos. Dizemos que um grupo finito G satisfaz a propriedade do normalizador quando

$$N_U(G) = G \cdot Z(U(\mathbb{Z}G)).$$

Isto é, quando o normalizador de G no grupo das unidades de $\mathbb{Z}G$ é o menor possível, ou seja, é o produto do grupo G pelo centro do grupo de unidades. Como $U(\mathbb{Z}G) = \pm U_1(\mathbb{Z}G)$, a propriedade do normalizador, também, pode ser interpretada por

$$N_{U_1}(G) = G \cdot Z(U_1(\mathbb{Z}G)).$$

Dado $u \in N_U(G)$, denotamos por $\varphi_u : G \to G$ o automorfismo $\varphi_u(g) = u^{-1}gu$, e por $Aut_U(G)$ o grupo formado por tais automorfismos. Temos que $Inn(G) \subseteq Aut_U(G)$, em que $Inn(G)$ consiste nos automorfismos internos de G. Assim, (Nor) é válida se, e somente se,

$$\forall u \in N_U(G),\ u = g_0 \cdot z,\ \text{com } g_0 \in G \text{ e } z \in Z(U(\mathbb{Z}G)).$$

Logo,

$$u^{-1}gu = \varphi_u(g) = z^{-1}g_0^{-1}gg_0z = g_0^{-1}gg_0,$$

que equivale a afirmar que φ_u é um automorfismo interno de G, ou seja, vale a inclusão $Aut_U(G) \subseteq Inn(G)$. Portanto, a propriedade do normalizador pode ser reformulada como a seguinte questão, para um grupo finito G:

$$Aut_U(G) = Inn(G)?$$

A propriedade do normalizador é uma questão para grupos finitos, mas também pode ser investigada no campo dos grupos infinitos. Neste trabalho, nos restringiremos a analisar a questão no campo dos grupos finitos. Inicialmente (Nor) foi apresentada como uma conjectura, porém, em 2001, M. Hertweck [Her01], apresentou um contraexemplo para (Nor), e assim esse problema perdeu o status de conjectura, mas não sua importância, buscando-se então conhecer as classes de grupos que são soluções para (Nor). Na subseção seguinte apresentaremos uma série de resultados fundamentais à propriedade do normalizador que estão presentes na literatura.

3.2.1 Resultados Fundamentais

O primeiro resultado a seguir, é uma versão pontual de (Nor), pois garante que todo grupo satisfaz a propriedade do normalizador pontualmente.

Proposição 3.2.1 *(Lema 1, [PeS03]) Seja $u \in N_U(G)$. Então $\varphi_u(g)$ é conjugado a g em G para todo $g \in G$.*

Demonstração: Primeiramente, veja que

$$\varphi_u(g) - g = u^{-1}gu - g = (u^{-1}, gu) \in (\mathbb{Z}G, \mathbb{Z}G).$$

Agora, coloquemos $\varphi_u(g) = h \in G$ e consideremos $\alpha = h - g$. Então, pelo Lema 3.0.2 tem-se $\tilde{\alpha}(x) = 0$, para todo $x \in G$. Em particular, $\tilde{\alpha}(g) = 0$. Como g é trivialmente conjugado a si próprio, seu coeficiente -1 aparece como uma das parcelas de $\tilde{\alpha}(g)$. Como este se anula, a soma das demais parcelas em $\tilde{\alpha}(g)$ é igual a 1 e corresponderá ao coeficiente de h, pois $supp(\alpha) = \{h, g\}$. Portanto, h e g são conjugados, isto é, $\varphi_u(g)$ e g são conjugados.

■

A Proposição 3.2.1 além de garantir a validade de (Nor) pontualmente, assegura que os automorfismos de um grupo G induzidos por unidades $u \in N_U(G)$ preservam classes de conjugação. Ademais, veja que, se G é abeliano, então φ_u é o automorfismo

identidade em G, e portanto é interno, isto é, (Nor) vale trivialmente para grupos abelianos finitos. O próximo teorema é uma versão local de (Nor), mostrando que a propriedade é satisfeita pelos p-subgrupos de um grupo finito.

Teorema 3.2.1 (Coleman) *Sejam P um p-subgrupo de um grupo finito G e $u \in N_U(G)$. Então existe $y \in G$ tal que $u^{-1}gu = y^{-1}gy$ para todo $g \in P$.*

Demonstração: Dado $g \in G$, temos que $\varphi_u(g) = u^{-1}gu \in G$, e assim $u = g^{-1}u\varphi_u(g)$. Escrevendo $u = \sum_{x\in G} a_x x$ temos

$$\sum_{x\in G} a_x x = \sum_{x\in G} a_x g^{-1} x \varphi_u(g).$$

Assim, g age sobre G com a ação

$$g \cdot x = \sigma_g(x) = g^{-1}x\varphi_u(g)$$

e a função $a : G \to \mathbb{Z}$, dada por $x \mapsto a_x$, é constante nas órbitas dessa ação, isto é,

$$a(\sigma_g(x)) = a(g^{-1}x\varphi_u(g)) = a_x, \ \forall x \in G.$$

Restringindo a a P, as órbitas dessa ação têm como comprimento uma potência de p, pois P é um p-subgrupo e pelo Teorema da Órbita e do Estabilizador, Teorema 2.1.5,

$$|Orb(x)| = [P : stab_P(x)],$$

donde $|Orb(x)|$ divide $|P|$. Agora veja que a função de aumento ε, aplicada em u é tal que

$$\pm 1 = \varepsilon(u) = \sum_{x\in G} a_x = \sum_{x\in G} a(\sigma_g(x)).$$

Segue que existe uma órbita de comprimento 1, pois caso contrário, não poderíamos ter $\pm 1 = \varepsilon(u)$, ou seja, existe $x \in G$ tal que $\sigma_g(x) = x$ para todo $g \in P$, uma vez que x pertence a sua órbita. Daí,

$$g^{-1}x\varphi_u(g) = x \ \Rightarrow \ \varphi_u(g) = x^{-1}gx, \ \forall g \in P.$$

Portanto $\varphi_u \in Inn(G)$.

■

Corolário 3.2.1 *Seja G um grupo nilpotente finito. Então vale (Nor) para G.*

Demonstração: Como G é nilpotente, podemos escreve-lo como produto direto de seus p-subgrupos de Sylow, $G = P_1 \times \cdots \times P_n$. Sejam $g \in G$ e $u \in N_U(G)$. Podemos escrever $g = g_1 \dots g_n$, com cada $g_i \in P_i$. Pelo Teorema 3.2.1, para cada P_i, existe $y_i \in G$ tal que $u^{-1}x_iu = y_i^{-1}x_iy_i$ para todo $x_i \in P_i$. Considere $y_i = y_{i1} \dots y_{in}$, em que $y_{ij} \in P_j$. Na ação de y_i em P_i, é relevante a coordenadas y_{ii}, isto é, $y_i^{-1}x_iy_i = y_{ii}^{-1}x_iy_{ii}$, pois as outras coordenadas comutam já que encontram-se em subgrupos de Sylow distintos. Sendo assim,

$$\begin{aligned} u^{-1}gu &= u^{-1}(g_1 \dots g_n)u \\ &= (u^{-1}g_1u) \dots (u^{-1}g_nu) \\ &= (y_1^{-1}g_1y_1) \dots (y_n^{-1}g_ny_n) \\ &= (y_{11}^{-1}g_1y_{11}) \dots (y_{nn}^{-1}g_ny_{nn}) \\ &= (y_{nn}^{-1} \dots y_{11}^{-1})(g_1 \dots g_n)(y_{11} \dots y_{nn}) \\ &= (y_{11} \dots y_{nn})^{-1}(g_1 \dots g_n)(y_{11} \dots y_{nn}) \\ &= y^{-1}gy, \end{aligned}$$

para $y = y_{11} \dots y_{nn} \in G$, sendo que y_{ii} comuta com y_{jj} e g_j, sempre que $i \neq j$. Assim, para todo $g \in G$ temos que $u^{-1}gu = y^{-1}gy$. ∎

O próximo resultado é um lema auxiliar, necessário a demonstração dos próximos resultados.

Lema 3.2.1 *Sejam G um grupo e $u \in U(\mathbb{Z}G)$. Então*

$$u \in N_U(G) \;\Leftrightarrow\; uu^* \in Z(\mathbb{Z}G).$$

Demonstração: Sejam $u \in N_U(G)$ e $\varphi_u \in Aut_U(G)$ tal que $\varphi_u(g) = u^{-1}gu$ para todo $g \in G$. Aplicando a involução $*$, em ambos os lados da última igualdade, temos

$$(\varphi_u(g))^* = (u^{-1}gu)^* = u^*g^{-1}(u^{-1})^*.$$

Assim, substituindo g por g^{-1}, obtemos

$$(\varphi_u(g^{-1}))^* = (u^{-1}g^{-1}u)^* = u^*g(u^{-1})^* = (\varphi_u^{-1}(g))^*.$$

Como $u \in N_U(G)$ temos que $\varphi_u(g) \in G$ donde $\varphi_u^{-1}(g) \in G$, e portanto

$$(\varphi_u^{-1}(g))^* = \varphi_u(g).$$

Daí,

$$\begin{aligned}(\varphi_u^{-1}(g))^* &= u^*g(u^{-1})^* = \varphi_u(g)\\ &\Leftrightarrow (u^{-1})^*\varphi_u(g)u^* = g\\ &\Leftrightarrow (u^{-1})^*(u^{-1}gu)u^* = g\\ &\Leftrightarrow (uu^*)^{-1}g(uu^*) = g\\ &\Leftrightarrow uu^* \in Z(\mathbb{Z}G).\end{aligned}$$

Além disso,

$$u(uu^*) = (uu^*)u = u(u^*u) \;\Rightarrow\; uu^* = u^*u \in Z(\mathbb{Z}G).$$

Reciprocamente, suponhamos que $uu^* \in Z(\mathbb{Z}G)$. Então, para $g \in G$ arbitrário, temos

$$\begin{aligned}(u^{-1}gu)(u^{-1}gu)^* &= (u^{-1}gu)(u^*g^{-1}(u^{-1})^*)\\ &= u^{-1}g(uu^*)g^{-1}(u^{-1})^*\\ &= u^{-1}(uu^*)gg^{-1}(u^{-1})^*\\ &= u^*(u^{-1})^*\\ &= 1.\end{aligned}$$

Pela Proposição 3.1.1, existe $g_0 \in G$ tal que $u^{-1}gu = \pm g_0$. Como g percorre todo G temos que $u \in N_U(G)$.

■

Proposição 3.2.2 (Krempa) *Seja $u \in U(\mathbb{Z}G)$. Se $u \in N_U(G)$, então*

$$u^2 \in G \cdot Z(\mathbb{Z}G).$$

Em particular, $u^2 = g_0(u^*u)$ para algum $g_0 \in G$.

Demonstração: Suponhamos que $u \in N_U(G)$ e consideremos a unidade

$$v = u^*u^{-1} \in U(\mathbb{Z}G).$$

Pelo Lema 3.2.1, temos

$$vv^* = u^*u^{-1}(u^{-1})^*u = u^*(u^*u)^{-1}u = (u^*u)^{-1}u^*u = 1.$$

Pela proposição 3.1.1, existe $g \in G$ tal que $v = \pm g$. Como $\varepsilon(v) = \varepsilon(u^*)\varepsilon(u^{-1}) = 1$, vemos que $v = g$. Consequentemente,

$$v = g = u^*u^{-1} \Leftrightarrow gu = u^* \Leftrightarrow gu^2 = u^*u \Leftrightarrow u^2 = g^{-1}(u^*u),$$

e portanto $u^2 \in G \cdot Z(\mathbb{Z}G)$, como queríamos.

■

Como consequência imediata do resultado de Krempa, segue o corolário:

Corolário 3.2.2 *Sejam $u \in N_U(G)$ e $\varphi_u \in Aut_U(G)$. Então $\varphi_{u^2} \in Inn(G)$.*

Agora enunciaremos um lema técnico, fundamental à prova que a propriedade do normalizador é válida para grupos de ordem ímpar.

Lema 3.2.2 *Seja $\varphi_u \in Aut_U(G)$. Então a ordem de φ_u é divisível apenas pelos primos que dividem a ordem de G.*

Demonstração: Ver [Lema 9.3, [Se93]].

■

Agora apresentaremos três resultados sob a propriedade do normalizador, apresentados por Jackowski e Marciniak em 1987, que representaram um marco na teoria de anéis de grupo, por estabelecerem uma direção de pesquisa contundente na busca por uma solução geral da questão do normalizador para grupos finitos. Esses resultados contribuíram para a afirmação de (Nor) como uma conjectura. Bem verdade, que o contraexemplo apresentado por Hertweck em 2001, tira de (Nor) o status de conjectura mas, ainda hoje, os resultados de Jackowski e Marciniak são de fundamental importância na busca de classe de grupos que são soluções para (Nor).

O primeiro resultado garante a validade da propriedade do normalizador para todo grupo de ordem ímpar.

Teorema 3.2.2 *(Teorema 3.4, [JaM87]) A propriedade do normalizador vale para grupos de ordem ímpar.*

Demonstração: Sejam G um grupo de ordem ímpar, $u \in N_U(G)$ e $\varphi_u \in Aut_U(G)$. Pela Proposição 3.2.2 concluímos que $\varphi_u^2 = \varphi_{u^2} \in Inn(G)$. Seja t a ordem de φ_u, pelo Lema 3.2.2 temos que t é ímpar. Logo, t e 2 são números inteiros relativamente primos. Assim, existem r e s números inteiros tais que $2r + ts = 1$. Daí,

$$\varphi_u = \varphi_u^1 = \varphi_u^{2r+ts} = \varphi_u^{2r} \cdot \varphi_u^{ts} = \varphi_u^{2r} \in Inn(G).$$

■

Graças ao Teorema 3.2.2, para verificar que uma classe de grupos goza da propriedade do normalizador, devemos nos deter aos grupos dessa classe que têm ordem par. Sendo assim, verificar a propriedade do normalizador, reduz-se a análise de um conjunto particular de automorfismos $\varphi_u \in Aut_U(G)$. Com efeito, dado um 2-subgrupo de Sylow S de um grupo G, nós denotamos por I_S o conjunto

$$I_S = \{\varphi \in Aut_U(G) \ : \ \varphi^2 = I, \ \varphi|_S = I\},$$

isto é, o subconjunto de automorfismos de G, determinados por unidades normalizadas, tal que estes automorfismos sejam involuções e a restrição dos mesmos a um 2-subgrupo de Sylow fixado, a identidade. Vale para este conjunto o seguinte resultado.

Teorema 3.2.3 *(Teorema 3.5, [JaM87]) Se $I_S \subseteq Inn(G)$ para um 2-subgrupo de Sylow S de G, então $Aut_U(G) = Inn(G)$.*

Demonstração: Suponhamos que $I_S \subseteq I_{nn}(G)$ e seja $\varphi_u \in Aut_U(G)$ com $u \in N_U(G)$. Como S é um 2-subgrupo de G segue do Teorema 3.2.1, que existe $g_1 \in G$ tal que $\varphi_u(h) = g_1^{-1}hg_1$, para todo $h \in S$. Definindo um automorfismo interno de G, γ, por $\gamma(g) = g_1gg_1^{-1}$, para todo $g \in G$. Para todo $h \in S$ temos que

$$(\gamma \circ \varphi_u)(h) = \gamma(\varphi_u(h)) = \gamma(g_1^{-1}hg_1) = g_1(g_1^{-1}hg_1)g_1^{-1} = h,$$

portanto $\gamma \circ \varphi_u = I$ quando restrito a S. Denotando ug_1^{-1} por v, temos que $v \in N_U(G)$ e para todo $g \in G$ obtemos

$$\begin{aligned}(\gamma \circ \varphi_u)(g) &= \gamma(\varphi_u(g)) = \gamma(u^{-1}gu) = g_1u^{-1}gug_1^{-1} \\ &= (ug_1^{-1})^{-1}g(ug_1^{-1}) = v^{-1}gv = \varphi_v(g).\end{aligned}$$

Logo, $\gamma \circ \varphi_u = \varphi_v \in Aut_U(G)$. Como $v \in N_U(G)$, segue pelo Lema 3.2.1, que $vv^* \in Z(\mathbb{Z}G)$ e na demonstração da Proposição 3.2.2, vemos que existe $f \in G$ tal que $v^* = fv$ e $v^2 = f^{-1}(v^*v)$. Daí,

$$\varphi_v^2(g) = fgf^{-1}. \tag{3.1}$$

Ademais,

$$v = (v^*)^* = (fv)^* = v^*f^* = v^*f^{-1} = fvf^{-1},$$

isto é, f comuta com v. Tomemos $\langle f \rangle$ o grupo cíclico gerado por f. Denotando por $S_2(f)$ o 2-subgrupo de Sylow de $\langle f \rangle$ e por $S_{2'}(f)$ um $2'$-subgrupo de Hall de $\langle f \rangle$, temos

$\langle f\rangle = S_2(f) \times S_{2'}(f)$. Como ambos são cíclicos, existem f_1 e f_2 em $\langle f\rangle$ tais que $S_2(f) = \langle f_1\rangle$ e $S_{2'}(f) = \langle f_2\rangle = \langle f_2^2\rangle$. Daí, concluímos que

$$f = f_1 f_2^2, \tag{3.2}$$

em que f_1 é um 2-elemento e $2 \nmid |f_2|$. Definimos $\delta \in Inn(G)$ como $\delta(g) = f_2^{-1} g f_2$, para todo $g \in G$. Como f comuta com v e $f_2 \in \langle f\rangle$ temos que f_2 comuta com v, e assim, para todo $g \in G$ obtemos

$$\begin{aligned}(\delta \circ \varphi_v)(g) &= \delta(v^{-1}gv) = f_2^{-1}(v^{-1}gv)f_2 \\ &= (vf_2)^{-1}g(vf_2) = (f_2v)^{-1}g(f_2v) \\ &= v^{-1}f_2^{-1}gf_2v = \varphi_v(f_2^{-1}gf_2) \\ &= (\varphi_v \circ \delta)(g).\end{aligned}$$

Portanto, $\delta \circ \varphi_v = \varphi_v \circ \delta$. Agora observe que f pertence ao $C_G(S)$, o centralizador de S em G, pois $\varphi_v = \gamma \circ \varphi_u$, $(\gamma \circ \varphi_u)|_S = I$ e pela equação 3.1, tem-se que, para todo $s \in S$,

$$s = \varphi_v(s) = \varphi_v^2(s) = fsf^{-1}.$$

Consequentemente, o automorfismo $\theta = \delta \circ \varphi_v = \varphi_v \circ \delta$ satisfaz

(i) $\theta(h) = h,\ \forall h \in S$:

Com efeito, como $f \in C_G(S)$ temos que f_1 e f_2 também pertencem a $C_G(S)$. Daí,

$$\begin{aligned}\theta(h) &= (\delta \circ \varphi_v)(h) = (\varphi_v \circ \delta)(h) \\ &= \varphi_v(f_2^{-1}hf_2) = \varphi_v(h) \\ &= h.\end{aligned}$$

(ii) $\theta^2(g) = f_1 g f_1^{-1},\ \forall g \in G$:

Utilizando-se das equações 3.1 e 3.2 obtemos

$$\begin{aligned}
\theta^2(h) &= \theta(\theta(g)) \\
&= \theta((\delta \circ \varphi_v)(g)) \\
&= \theta(\delta(v^{-1}gv)) \\
&= \theta(f_2^{-1}v^{-1}gvf_2) \\
&= (\delta \circ \varphi_v)(f_2^{-1}v^{-1}gvf_2) \\
&= \delta(v^{-1}f_2^{-1}v^{-1}gvf_2v) \\
&= f_2^{-1}v^{-1}f_2^{-1}v^{-1}gvf_2vf_2 \\
&= v^{-2}f_2^{-2}gf_2^2v^2 \\
&= \varphi_v^2(f_2^{-2}gf_2^2) \\
&= ff_2^{-2}gf_2^2f^{-1} \\
&= f_1f_2^2f_2^{-2}gf_2^2f_2^{-2}f_1^{-1} \\
&= f_1gf_1^{-1}.
\end{aligned}$$

Agora, fazendo $\omega = vf_2$ temos, para todo $g \in G$

$$\theta(g) = (\delta \circ \varphi_v)(g) = \delta(v^{-1}gv) = f_2^{-1}v^{-1}gvf_2 = \omega^{-1}g\omega = \varphi_\omega(g)$$

donde $\theta = \varphi_\omega$. Como $f_1 \in C_G(S)$ e $S_2(f) = \langle f_1 \rangle$ denota um 2-subgrupo de Sylow de $\langle f \rangle$, temos que $\langle S, f_1 \rangle$ é um 2-subgrupo de G que contém S, como S é um 2-subgrupo de Sylow de G segue-se que $f_1 \in S$. Em particular, $f_1 \in Z(S)$.

Agora consideremos a ação por conjugação de S sobre G, $\rho : S \times G \ \to \ G$, definida da seguinte forma:

$$(h, g) \mapsto h^{-1}gh, \ \forall h \in S, \ \forall g \in G.$$

Como para todo $h \in S$ temos que $\varphi_\omega(h) = h$, escrevendo

$$\omega = vf_2 = \sum_{g \in G} a_g g,$$

obtemos que

$$\omega = \sum_{g \in G} a_g g = \sum_{g \in G} a_g h^{-1}gh, \ \forall h \in S.$$

Observe que a função $a : G \to \mathbb{Z}, \ g \mapsto a_g$, é constante nas órbitas da ação ρ. Além disso, existe necessariamente um ponto $g_0 \in G$, fixado pela ação no suporte de ω, isto

é, $h^{-1}g_0h = g_0$ e, evidentemente $g_0 \in C_G(S)$. Seja ω_0 a projeção linear de ω no subanel $\mathbb{Z}C_G(S)$. Como g_0 está em $supp(\omega)$, segue que $\omega_0 \neq 0$. Denotamos por $\bar{\omega_0}$ a redução módulo 2 de ω a $\mathbb{Z}_2C_G(S)$.

Como $\bar{\omega_0} \in \mathbb{Z}_2C_G(S)$, concluímos que o cardinal do suporte de $\bar{\omega}$ é igual a $\varepsilon(\bar{\omega})$. Por outro lado, $\varepsilon(\bar{\omega_0}) \equiv \varepsilon(\omega_0)\ (mod\ 2)$. Seja g no suporte de ω. Se $g \in C_G(S)$, então g é um ponto fixo para a ação ρ. Se $g \notin C_G(S)$, então a órbita de g tem comprimento uma potência de 2, isso pois S é um 2-grupo e pelo Teorema da Órbita e do Estabilizador. Como os coeficientes dos elementos em uma mesma órbita são iguais, obtemos que $\varepsilon(\omega_0) \equiv \varepsilon(\omega)\ (mod\ 2)$. Por fim, como $\varepsilon(\omega) = \pm 1$, segue que

$$card(supp(\bar{\omega_0})) = \varepsilon(\bar{\omega_0}) \equiv \varepsilon(\omega_0) \equiv \varepsilon(\omega) \equiv\ 1\ (mod\ 2),$$

ou seja, o suporte de $\bar{\omega_0}$ é constituído por um número ímpar de elementos no centralizador de S em G.

Das igualdades $\omega = vf_2,\ v^* = fv,$ e $f = f_1f_2^2$ e como $fv = vf$ segue que

$$f_1\omega = f_1vf_2 = vf_1f_2 = vff_2^{-1} = fvf_2^{-1} = v^*f_2^{-1} = f_2^{-1}v^* = \omega^*.$$

Vale para a projeção ω_0 de ω: $\omega_0^* = f_1\omega_0$ e, portanto,

$$\bar{\omega_0^*} = f_1\bar{\omega_0}. \tag{3.3}$$

Tomemos um elemento h_1 no suporte de $\bar{\omega_0}$. Pela equação 3.3, temos $f_1h_1 = h_2^{-1}$, para algum h_2 no suporte de $\bar{\omega_0}$. Sendo assim, $f_1h_2 = f_1(h_1^{-1}f_1^{-1}) = h_1^{-1}$. Concluímos que o suporte de $\bar{\omega_0}$ é a união disjunta de conjuntos da forma $\{h_1, h_2\}$, com $f_1h_1 = h_2^{-1}$. Ora, sabemos que o cardinal do suporte de $\bar{\omega_0}$ é ímpar, e portanto para ao menos um destes conjuntos deve valer $f_1h_1 = h_1^{-1}$, ou seja, $f_1 = h_1^{-2}$, porém f_1 é um 2-elemento, o que implica que h_1 também o é, e já que h_1 está em $C_G(S)$, segue que $h_1 \in Z(S)$.

Definimos um automorfismo interno de G, ψ, por $\psi(g) = h_1gh_1^{-1}$ para todo $g \in G$. A composição $\psi \circ \varphi_\omega$ é tal que

(i) para todo $h \in S$:

$$(\psi \circ \varphi_\omega)(h) = \psi(h) = h_1hh_1^{-1} = h.$$

(ii) para todo $g \in G$:

$$\begin{aligned}(\psi \circ \varphi_\omega)^2(g) &= h_1\omega^{-1}h_1\omega^{-1}g\omega h_1^{-1}\omega h_1^{-1} = h_1^2\omega^{-2}g\omega^2 h_1^{-2} \\ &= \psi^2(\varphi^2(g)) = \psi^2(f_1 g f_1^{-1}) = h_1^2 f_1 g f_1^{-1} h_1^{-2} \\ &= g,\end{aligned}$$

pois $\varphi_\omega^2(g) = \theta^2(g) = f_1 g f_1^{-1},\ f_1 = h_1^{-2},\ h_1 \in Z(S)$ e ω comuta com os elementos de S. Logo, a composição $\psi \circ \varphi_\omega$ é um elemento de I_S. Uma vez que I_S está contido em $Inn(G)$, por hipótese, existe $\varphi_g \in Inn(G)$ tal que $\psi \circ \varphi_\omega = \varphi_g$. Portanto, $\varphi_\omega = \psi^{-1} \circ \varphi_g \in Inn(G)$. Como $\varphi_\omega = \theta = \delta \circ \varphi_v$ e $\varphi_v = \gamma \circ \varphi_u$, onde $\delta, \gamma \in Inn(G)$. Vale

$$\varphi_\omega = \delta \circ \varphi_v = \delta \circ \gamma \circ \varphi_u \ \Rightarrow\ \varphi_u = \gamma^{-1} \circ \delta^{-1} \circ \varphi_\omega \in Inn(G).$$

Portanto, $\varphi_u \in Inn(G)$. Como $\varphi_u \in Aut_U(G)$ foi tomado de modo arbitrário temos que $Aut_U(G) \subseteq Inn(G)$, e assim $Aut_U(G) = Inn(G)$.

■

Teorema 3.2.4 *(Teorema 3.6, [JaM87]) A propriedade do normalizador vale para qualquer grupo finito com um 2-subgrupo de Sylow normal.*

Em 2002, Petit Lobão e Polcino Milies, apresentaram o seguinte teorema:

Teorema 3.2.5 *(Teorema 3.1, [PeP02]) Seja G um grupo de Frobenius finito. Então a propriedade do normalizador é válida no anel de grupo integral $\mathbb{Z}G$.*

Eles demostraram que se, G denota um grupo de Frobenius finito, então para todo $u \in N_U(G)$ tal que $\varphi_u \in I_S$ para um 2-subgrupo de Sylow S de G, um dos casos acontecem:

(i) $\varphi_u(g) = g$, para todo $g \in G$; ou

(ii) $\varphi_u(g) = y_0^{-1} g y_0 = \varphi_{y_0}(g)$, para todo $g \in G$, onde $y_0 \in G$ é a única involução no complementar de Frobenius de G.

Isto é, eles mostraram que $I_S \subseteq I_{nn}(G)$ para um 2-subgrupo de Sylow S de G, e assim que a propriedade do normalizador é válida na classe dos grupos de Frobenius finitos. Este é um dos resultados motivadores de nosso trabalho e buscaremos empregar as técnicas usadas pelos autores para obtenção de nossos objetivos no próximo capítulo.

Como vimos na Subseção 2.2.3, os grupos de Camina constituem uma generalização dos grupos de Frobenius e são essencialmente grupos de Frobenius ou p-grupos. Assim,

Pelos Teoremas 3.2.5 e 3.2.1, a propriedade do normalizador é válida trivialmente para a classe dos grupos de Camina finitos.

Seja G um grupo finito e H um subgrupo de G. Se x é um elemento que normaliza H, então a conjugação por x induz um automorfismo de H. Se $H = G$, então este automorfismo preserva classes de conjugação. Em 1988, Walter Feit e Gary Seitz, [FeS88], mostraram que automorfismos de grupos simples finitos que preservam classes de conjugação são automorfismos internos. Assim, em particular, como os automorfismos de um grupo G induzidos por unidades $u \in N_U(G)$ preservam classes de conjugação, temos que, se G é um grupo simples finito, então esses automorfismos são internos, e portanto a propriedade do normalizador é válida para grupos simples finitos. Vejamos o enunciado do teorema de Walter Feit e Gary Seitz.

Teorema 3.2.6 *(Teorema C, [FeS88]) Seja α um automorfismo externo de um grupo simples finito G. Então existe uma classe de conjugação C de G com $\alpha(C) \neq C$.*

Corolário 3.2.3 *Grupos simples finitos satisfazem a propriedade do normalizador.*

A propriedade do normalizador foi investigada em muitos casos particulares e obteve resposta afirmativa em muitas classes de grupos. Para finalizar esta subseção vamos listar algumas classes de grupos que satisfazem a propriedade do normalizador.

Teorema 3.2.7 *Seja G um grupo finito. A propriedade do normalizador tem resposta positiva nos seguintes casos:*

1. *G é um grupo nilpotente (Coleman, [Co64]).*
2. *G é um grupo de ordem ímpar (Jackowski e Marciniak, [JaM87]).*
3. *G tem um 2-subgrupo de Sylow normal (Jackowski e Marciniak, [JaM87]).*
4. *G é um grupo de Frobenius (Petit Lobão e Polcino Milies, [PeP02]).*
5. *G é um grupo simples (Feit e Seitz, [FeS88]).*
6. *G é localmente nilpotente (Jespers, Juriaans, de Miranda e Rogerio, [JeJ02]).*
7. *G possui subgrupo derivado G' um p-subgrupo (Jespers, Juriaans, de Miranda e Rogerio, [JeJ02]).*

3.3 Problema do Isomorfismo

A questão central na teoria de anéis de grupo é o chamado **Problema do Isomorfismo** (Iso). Esta questão busca saber até que ponto o conhecimento da estrutura e propriedades de um dado anel de grupo pode determinar a estrutura do grupo inicial. Assim, o problema do isomorfismo, consiste em verificar quando um grupo é determinado pelo seu anel de grupo, ou seja, dados dois grupos G e H e um anel com unidade R, será que a existência de um isomorfismo $RG \simeq RH$ implica em $G \simeq H$? Desde 1940, esta questão vem sendo discutida a partir dos trabalhos de G. Higman com diversos anéis de coeficientes, entretanto, percebeu-se que podemos obter muitos contraexemplos à questão utilizando-se como anel de coeficientes um corpo. Por exemplo, utilizando-se da teoria de anéis de grupo com anéis de coeficientes corpos, podemos mostrar que se G e H são grupos abelianos de mesma ordem, então as álgebras de grupo $\mathbb{C}G$ e $\mathbb{C}H$ são isomorfas mas, sabemos que existem grupos abelianos de mesma ordem que não são isomorfos, por exemplo, os grupos abelianos de ordem quatro $\mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_4$.

Isto levou a centralizar as atenções sobre os anéis de grupo sobre os inteiros, formulando-se a seguinte conjectura para grupos finitos quaisquer:

Conjectura: *Seja G um grupo finito. Então:*

$$\mathbb{Z}G \simeq \mathbb{Z}H \Longrightarrow G \simeq H.$$

Isto é, os grupos finitos são determinados via isomorfismo pelos seus anéis de grupo integrais.

Um fato importante que também contribuiu para que as atenções fossem voltadas para os anéis de grupo sobre os inteiros, é que, se G e H são grupos tais que $\mathbb{Z}G \simeq \mathbb{Z}H$, então $RG \simeq RH$ para todo anel comutativo R, ver [PoS02] Lema 9.1.1.

Como, em 2001, Hertweck [Her01] construiu um contraexemplo para o Problema do Isomorfismo, a partir de então, esse problema perde o status de conjectura, mas não a relevância, buscando-se conhecer as classes de grupos que são determinados pelos seus anéis de grupo integral.

Definição 3.3.1 *Um isomorfismo $\varphi : RG \to RH$ diz-se um isomorfismo normalizado se*

$$\varepsilon_H \circ \varphi = \varepsilon_G,$$

onde ε_G e ε_H denotam as funções de aumento de RG e RH, respectivamente.

Proposição 3.3.1 *Se existe algum isomorfismo $\varphi : RG \to RH$, então também existe um isomorfismo normalizado entre estes anéis.*

Demonstração: De fato, basta definir uma nova aplicação $\phi : RG \to RH$ da seguinte forma

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G} \frac{a_g}{\varepsilon_H \circ \varphi(g)}\varphi(g).$$

Veja que ϕ está bem definida, pois todo $g \in G$ é uma unidade de $\mathbb{Z}G$, e portanto como φ é um isomorfismo temos $\varphi(g) \in \mathbb{Z}H$ é uma unidade, e assim $\varepsilon_H(\varphi(g))$ é invertível em $\mathbb{Z}$. Para todo $\sum_{g\in G} a_g g,\ \sum_{k\in G} a_k k \in RG$, temos:

$$\begin{aligned}
\phi\big(\sum_{g\in G} a_g g \cdot \sum_{k\in G} a_k k\big) &= \phi\big(\sum_{g,k\in G} (a_g a_k)(gk)\big) = \sum_{g,k\in G} \frac{a_g a_k}{\varepsilon_H \circ \varphi(gk)}\varphi(gk) \\
&= \sum_{g\in G} \frac{a_g}{\varepsilon_H \circ \varphi(g)}\varphi(g) \cdot \sum_{k\in G} \frac{a_k}{\varepsilon_H \circ \varphi(k)}\varphi(k) \\
&= \phi\big(\sum_{g\in G} a_g g\big) \cdot \phi\big(\sum_{k\in G} a_k k\big)
\end{aligned}$$

e

$$\begin{aligned}
\phi\big(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\big) &= \phi\big(\sum_{g\in G} (a_g + b_b) g\big) = \sum_{g\in G} \frac{a_g + b_g}{\varepsilon_H \circ \varphi(g)}\varphi(g) \\
&= \sum_{g\in G} \frac{a_g}{\varepsilon_H \circ \varphi(g)}\varphi(g) + \sum_{g\in G} \frac{b_g}{\varepsilon_H \circ \varphi(g)}\varphi(g) \\
&= \phi\big(\sum_{g\in G} a_g g\big) + \phi\big(\sum_{g\in G} b_g g\big).
\end{aligned}$$

Portanto, ϕ é um homomorfismo de anéis. Agora veja que

$$\begin{aligned}
\phi\big(\sum_{g\in G} a_g g\big) = 0 &\Leftrightarrow \sum_{g\in G} \frac{a_g}{\varepsilon_H \circ \varphi(g)}\varphi(g) = 0 \\
&\Leftrightarrow \sum_{g\in G} \frac{a_g}{\varepsilon_H \circ \varphi(g)} = 0 \\
&\Leftrightarrow \sum_{g\in G} a_g g = 0.
\end{aligned}$$

Assim, ϕ é injetora. Como ε_H é um epimorfismo e φ é um isomorfismo segue que $\varepsilon_H \circ \varphi$ é um epimorfismo, e portanto ϕ é um epimorfismo. Logo, ϕ é um isomorfismo de anéis.

Por fim observe que

$$\begin{aligned}(\varepsilon_H \circ \phi)\big(\sum_{g\in G} a_g g\big) &= \varepsilon_H\big(\sum_{g\in G} \frac{a_g}{\varepsilon_H \circ \varphi(g)}\varphi(g)\big)\\ &= \sum_{g\in G} \frac{a_g}{\varepsilon_H \circ \varphi(g)}\varepsilon_H \circ \varphi(g)\\ &= \sum_{g\in G} a_g = \varepsilon_G\big(\sum_{g\in G} a_g g\big).\end{aligned}$$

Portanto, $\varepsilon_H \circ \phi = \varepsilon_G$, e assim ϕ é um isomorfismo normalizado.

■

Nosso primeiro exemplo de uma classe de grupo que satisfaz o problema do isomorfismo é a classe dos grupos abelianos.

Teorema 3.3.1 *([Hi40]) Seja G um grupo abeliano finito e seja H um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então $G \simeq H$.*

Demonstração: Desde que $\mathbb{Z}G \simeq \mathbb{Z}H$ podemos assumir que existe um isomorfismo normalizado $\varphi : \mathbb{Z}G \to \mathbb{Z}H$. Se G é abeliano, então $\mathbb{Z}G$ é comutativo, e portanto $\mathbb{Z}H$ é comutativo, donde seque que H é abeliano. Como o posto de um módulo livre sobre $\mathbb{Z}$ é invariante, temos que H é finito e que $|G| = |H|$. Para cada $g \in G$ temos que $\varphi(g)$ é uma unidade normalizada em $\mathbb{Z}H$. Como $\mathbb{Z}H$ é comutativo, segue do Corolário 3.1.1 que $\varphi(g) \in \pm H$. Desde que φ é um isomorfismo normalizado, temos que $\varphi(g) \in H$. Assim, provamos que $\varphi(G) \in H$ e como $|G| = |H|$, temos que $\varphi(G) = H$. Em outras palavras, a restrição de φ a G é um isomorfismo de grupo de G em H.

■

Corolário 3.3.1 *Seja G um grupo finito e H um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então $Z(G) \simeq Z(H)$, onde $Z(G)$ e $Z(H)$ denotam os centros de G e H respectivamente.*

Demonstração: Desde que $\mathbb{Z}G \simeq \mathbb{Z}H$ podemos assumir que existe um isomorfismo normalizado $\varphi : \mathbb{Z}G \to \mathbb{Z}H$. Pelo Corolário 3.1.1 as unidades centrais de ordem finita de $\mathbb{Z}G$ são todas triviais, e portanto, $\varphi(Z(G)) = Z(H)$. Isto é, $Z(G) \simeq Z(H)$.

■

Omitimos a demonstração dos próximos três resultados, pois suas demonstrações exigem ferramentas que não abordamos neste trabalho. Recordamos que, para cada $g \in G$, nós denotamos por C_g a classe de conjugação de g em G e escrevemos $\hat{C}_g = \sum_{x\in C_g} x$ a soma de classe. Dados G e H grupos finitos, a próxima proposição mostra que, desde que exista um isomorfismo normalizado entre os anéis de grupo integrais

$\mathbb{Z}G$ e $\mathbb{Z}H$, também existe uma correspondência biunívoca entre as somas de classe de G e H.

Proposição 3.3.2 *Seja $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado e seja $\hat{C}_g$ uma soma de classe em G, então $\varphi(\hat{C}_g)$ é uma soma de classe em H, isto é, existe $h \in H$ tal que $\varphi(\hat{C}_g) = \hat{C}_h$. Temos ainda que:*

(i) $\varphi(\hat{C}_{g^n}) = \hat{C}_{h^n}$, *para todo inteiro n;*

(ii) $o(g) = o(h)$ *e* $|C_g| = |C_h|$;

(iii) Se $\varphi(\hat{C}_g) = \hat{C}_h$ *e* $\varphi(\hat{C}_{g_1}) = \hat{C}_{h_1}$, *então existem* $a, b \in H$ *tais que* $\varphi(\hat{C}_{gg_1}) = \hat{C}_{hh_1^a} = \hat{C}_{h^b h_1}$, *onde* $h_1^a = a^{-1}h_1 a$ *e* $h^b = b^{-1}hb$.

Demonstração: Ver [[Se93], Capítulo 5.].

■

Teorema 3.3.2 *Suponha que $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ é um isomorfismo normalizador. Sejam $N \lhd G$ e $\hat{N} = \sum_{x \in N} x$. Então existe $M \lhd H$ tal que*

(i) $\varphi(\hat{N}) = \hat{M}$

(ii) $|N| = |M|$

(iii) $\mathbb{Z}(\frac{G}{N}) \simeq \mathbb{Z}(\frac{H}{M})$

Demonstração: Ver [[Se93], Teorema 36.10].

■

O teorema anterior mostra que, havendo um isomorfismo normalizado entre dois anéis de grupo integrais, então existe uma correspondência biunívoca entre os subgrupos normais dos grupos em questão. Em particular, essa correspondência preserva inclusões, interseções e produtos.

Proposição 3.3.3 *(Petit Lobão) Seja o isomorfismo $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ se, θ denota a correspondência entre os subgrupos normais de G e H, e C_g é uma classe de conjugação em G à qual corresponde a classe de conjugação C_h em H, então θ associa ao subgrupo normal $\langle C_g \rangle$ em G o subgrupo normal $\langle C_h \rangle$ em H.*

Demonstração: Ver [Pe08].

■

A fim de apresentarmos mais um exemplo de grupo que satisfaz (ISO), destacamos os próximos dois lemas.

Lema 3.3.1 *Sejam G e H grupos finitos e seja $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Seja J um ideal de $\mathbb{Z}G$ tal que $(1 + J) \cap G = \{1\}$. Então também $(1 + \varphi(J)) \cap H = \{1\}$.*

Demonstração: Assuma que $M = (1 + \varphi(J)) \cap H$ não é trivial. Desde que J é um ideal de $\mathbb{Z}G$ temos que $\varphi(J)$ é um ideal de $\mathbb{Z}H$, e portanto para todo $h \in H$ tem-se $n^{-1}\varphi(J)h = \varphi(J)$, e assim M é um subgrupo normal. Agora, veja que

$$M = \{h \in H \ : \ h - 1 \in \varphi(J)\}.$$

Logo, $\Delta_{\mathbb{Z}}(M) \subset \varphi(J)$. Pelo Teorema 3.3.2, existe $N \lhd G$ correspondente a M. Então $|N| = |M|$, donde N não é trivial e $\varphi^{-1}(\Delta_{\mathbb{Z}}(M)) = \Delta_{\mathbb{Z}}(N) \subset J$. Consequentemente, como

$$\Delta_{\mathbb{Z}}(N) = \Big\{ \sum_{n \in N} a_n(n-1) \ : \ n \neq 1, \ a_n \in \mathbb{Z} \Big\}$$

temos que $N \subset (1 + J) \cap G = \{1\}$, uma contradição, pois $|N| = |M|$ e M não é trivial. ■

Lema 3.3.2 *Seja J um ideal de um anel de grupo integral $\mathbb{Z}G$ tal que $(1+J)\cap G = \{1\}$. Então G é isomorfo a um subgrupo do grupo de unidades do anel quociente $\frac{\mathbb{Z}G}{J}$.*

Demonstração: Considere a função $\phi : G \to 1 + \frac{(\Delta_{\mathbb{Z}}(G)+J)}{J}$, definida por

$$x \mapsto 1 + (x - 1) + J.$$

ϕ é homomorfismo de grupo. Com efeito, para cada $x, \ y \in G$ temos

$$\begin{aligned} \phi(x)\phi(y) &= (1 + (x - 1) + J)(1 + (y - 1) + J) \\ &= (1 + (xy - 1) + J) = \phi(xy). \end{aligned}$$

Assim, ϕ é um homomorfismo. ϕ é injetiva, pois se $g \in G$ é tal que $\phi(g) = 1$, então

$$\begin{aligned} 1 = \phi(g) &= 1 + (g - 1) + J \\ &\Rightarrow \ g - 1 \in J \\ &\Rightarrow \ g \in 1 + J \\ &\Rightarrow \ g \in (1 + J) \cap G = 1. \end{aligned}$$

Logo, ϕ é injetiva e G é isomorfo a $\phi(G)$ que é um subgrupo do grupo de unidades do

anel quociente $\frac{\mathbb{Z}G}{J}$.

■

Agora estamos em condições de apresentar um importante exemplo de grupo que satisfaz (Iso), este exemplo é o grupo de unidades de um anel finito.

Teorema 3.3.3 *O grupo de unidades de um anel finito é determinado por seu anel de grupo integral.*

Demonstração: Seja $G = U(R)$ o grupo de unidades de um anel finito R. Identificando R com o subanel gerado por G podemos assumir, sem perda de generalidade, que $R = \langle G \rangle$ como anel. Definimos $\phi : \mathbb{Z}G \to R$ da seguinte forma

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

Como a multiplicação em G é a mesma de R, segue que ϕ é um homomorfismo de anéis e que $\phi(\mathbb{Z}G) = R$. Colocando $J = ker(\phi)$, temos pelo teorema do isomorfismo que

$$R = \phi(\mathbb{Z}G) \simeq \frac{\mathbb{Z}G}{J}.$$

Seja H um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$ e seja $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Então, $\frac{\mathbb{Z}G}{J} \simeq \frac{\mathbb{Z}H}{\varphi(J)}$. Como $(1 + J) \cap G = \{1\}$, pois $G = U(R)$, segue do Lema 3.3.1 que $(1 + \varphi(J)) \cap H = \{1\}$. Segue do Lema 3.3.2 que H é isomorfo a um subgrupo do grupo de unidades de

$$\frac{\mathbb{Z}H}{\varphi(J)} \simeq \frac{\mathbb{Z}G}{J} \simeq R.$$

Como $G = U(R)$, segue que H é isomorfo a um subgrupo de G, como $\mathbb{Z}G \simeq \mathbb{Z}H$ temos que G e H têm mesma ordem, e assim $H \simeq G$.

■

Veja que, em particular, para um grupo finito G qualquer, o grupo de unidades do anel de grupo integral correspondente $U(\mathbb{Z}G)$, satisfaz (Iso).

Corolário 3.3.2 *Seja K um corpo finito. O grupo linear geral $GL(n, K)$ é determinado pelo seu anel de grupo integral.*

Demonstração: Desde que $GL(n, K)$ é o grupo de unidades do anel de matrizes finito $M_n(K)$, o resultado é uma consequência imediatamente do Teorema 3.3.3.

■

Apesar do contraexemplo apresentado por Hertweck em 2001, o Problema do Isomorfismo é estudado em muitos casos particulares e obtém resposta positiva em muitas classes de grupos finitos, das quais, listaremos algumas das mais conhecidas:

Teorema 3.3.4 *Seja G um grupo finito. O problema do isomorfismo tem resposta positiva nos seguintes casos:*

1. *G é abeliano (Higman, [Hi40]).*
2. *G é nilpotente (Roggenkamp e Scott, [RoS87]).*
3. *G é simples (Kimmerle, Lyons, Sandling e Teague, [KiL90]).*
4. *G é metabeliano (Whitecomb, [Wh68]).*
5. *G é um grupo de Frobenius (Petit, [Pe01]).*
6. *$G = A \rtimes B$, onde A é abeliano e B é nilpotente com $(|A|, |B|) = 1$ (Weiss, [[Se93], Capítulo 5]).*
7. *G é um grupo círculo ([[PoS02], p. 303])*
8. *$G = AB$, onde A é abeliano e B é nilpotente (Kimmerle, [Ki92])*
9. *G é um 2-grupo Hamiltoniano ([[PoS02], p. 290]).*

Sejam G e H grupos finitos de mesma ordem e suponhamos que existe $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Se $\varphi(g) \in H$, para todo $g \in G$, então a restrição de φ a G garante um isomorfismo entre G e H. Mas, a questão é que, em geral, não temos maiores informações sobre os elementos $\varphi(g)$ e h com $h \in H$. A informação que temos é que, assim como $h \in H$, o elemento $\varphi(g)$ também é uma unidade no anel de grupo integral $\mathbb{Z}H$, pois se $|G| = n$, então $[\varphi(g)]^n = \varphi(g^n) = \varphi(1) = 1$, uma vez que φ é um isomorfismo. Daí, soa natural que o conhecimento adequado do grupo das unidades de $\mathbb{Z}H$ poderia nos levar a soluções do problema do isomorfismo. Nesta direção, em 1974, H. J. Zassenhaus formulou conjecturas sobre as unidades e os isomorfismos normalizados de um anel de grupo, como seguem:

Conjecturas de Zassenhaus:

(ZC1) Se $u \in U(\mathbb{Z}G)$ tem ordem finita, então existe $\alpha \in \mathbb{Q}G$ tal que $\alpha^{-1}u\alpha \in G$.

(ZC2) Se H é um subgrupo finito de $U_1(\mathbb{Z}G)$ tal que $\mathbb{Z}G = \mathbb{Z}H$ e $\varepsilon_G(H) = 1$, então $\alpha^{-1}H\alpha = G$, para algum $\alpha \in \mathbb{Q}G$.

(ZC3) Se H é um subgrupo finito de $U_1(\mathbb{Z}G)$, então $\alpha^{-1}H\alpha \subseteq G$, para algum $\alpha \in \mathbb{Q}G$.

(Aut) Se $\theta \in Aut(\mathbb{Z}G)$, então existe $\beta \in Aut(G)$ e $\alpha \in U(\mathbb{Q}G)$ tal que $\theta(g) = \alpha^{-1}\beta(g)\alpha$, para todo $g \in G$.

As conjecturas de Zassenhaus despertam muito interesse, sendo estabelecidas em muitas classes de grupos. Além disso, contraexemplos foram apresentados a (ZC2). Em destaque, foram obtidas as seguintes implicações:

1. (ZC3) $\Longrightarrow$ (ZC1) e (ZC2).
2. (ZC2) $\Longrightarrow$ (Iso).
3. (ZC2) $\Longrightarrow$ (Aut).
4. (Aut) + (Iso) $\Longrightarrow$ (ZC2).

Como era esperado, o conhecimento detalhado do grupo das unidades de $\mathbb{Z}G$ leva a soluções ao problema do isomorfismo. Para informações mais detalhadas sobre as conjecturas de Zassenhaus, recomendamos [Se93] Capítulo 5 .

Capítulo 4

Resultados Propostos

Este é o capítulo principal de nosso trabalho e tem como objetivo mostrar que os CIT-grupos e os CN-grupos satisfazem a propriedade do normalizador. Além disso, vamos expor nossas considerações quanto à investigação de (Iso) nestas classes de grupos.

Essas duas classes de grupos foram estudadas por M. Suzuki, W. Feit, M. Hall e J. Thompson, onde ganharam destaque em meados do século passado, no esforço que desenvolveu-se com objetivo de classificar os grupos simples. Por exemplo, M. Suzuki apresentou a conexão entre a classe dos CN-grupos e a classe dos CIT-grupos determinando todos os CN-grupos não solúveis e, ao fazer isso, descobriu uma família infinita de grupos simples que leva seu nome, os chamados *Grupos de Suzuki*; W. Feit, M. Hall e J. Thompson estabeleceram a solubilidade de todos os CN-grupos de ordem ímpar, isso contribui para a prova do *Teorema da Ordem Ímpar: Todo grupo de ordem ímpar é solúvel*. Como observamos nas Seções 2.3 e 2.4, esses grupos são diretamente relacionados com grupos de permutação transitivos, como por exemplo, os grupos de Zassenhaus e os grupos de Frobenius,

Em 2001, Petit Lobão mostrou que os grupos de Frobenius constituem uma solução ao problema do isomorfismo, ver [Pe01]. No ano seguinte, Petit Lobão e Polcino Milies mostraram que esta classe de grupos também é uma solução a propriedade do normalizador, ver [PeP02]. Assim, as duas questões estão fechadas para a classe grupos de Frobenius.

Nas Seções 2.3 e 2.4, vimos que tanto a estrutura dos CN-grupos quanto a estrutura dos CIT-grupos estão diretamente relacionadas com os grupos de Frobenius. Assim, é natural perguntar se essas duas classes de grupos também são uma solução ao isomorfismo e ao normalizador.

4.1 O Normalizador para CIT-grupos e CN-grupos

Nesta sessão, vamos utilizar as técnicas empregadas por Petit Lobão e Polcino Milies em [PeP02], para mostrar que os CIT-grupos são uma solução ao problema do normalizador. Como consequência, teremos que os CN-grupos também são uma solução a (Nor).

Teorema 4.1.1 *Seja G um CIT-grupo. Então a propriedade do normalizador é válida no anel de grupo integral $\mathbb{Z}G$.*

Demonstração: Seja G um CIT-grupo. Se G não é solúvel, então, pelo Teorema 2.4.1, G é um CN-grupo não solúvel. Assim, pelo Teorema 2.3.4, G é um grupo simples ou um grupo de Frobenius. Pelo Corolário 3.2.3 e pelo Teorema 3.2.5, segue que G satisfaz (Nor).

Assuma que G é um CIT-grupo solúvel. Se G contém um subgrupo normal próprio de ordem ímpar, então pelo Teorema 2.4.2, G é um grupo de Frobenius com complementar um 2-subgrupo de Sylow e núcleo abeliano. Novamente, pelo Teorema 3.2.5, o resultado segue.

Assuma que G é um CIT-grupo solúvel, mas que não contém um subgrupo normal próprio de ordem ímpar. Pelo Teorema 2.4.3, G contém uma série de subgrupos normais de ordem par

$$G \rhd L \rhd N \rhd 1,$$

tal que $\frac{G}{L}$ e $\frac{L}{N}$ são cíclicos de ordens relativamente primas, N é um 2-grupo e a extensão de G sobre N é disjunta, digamos $G = N \rtimes K$.

Se $|K| = |\frac{G}{N}|$ é ímpar, então N é um 2-subgrupo de Sylow normal de G. Portanto, pelo Teorema 3.2.4, G satisfaz (Nor).

Se $|K| = |\frac{G}{N}|$ é par, então pela Observação 2.4.1, vê-se que K é um grupo de Frobenius, digamos $K = X \rtimes Y$, com X o núcleo e Y o complementar de Frobenius de K. Logo, podemos escrever $G = N \rtimes (X \rtimes Y)$. Pelo Teorema 2.2.1, temos que X é nilpotente e que $(|X|, |Y|) = 1$. Como estamos assumindo que K tem ordem par, vemos que se $|Y|$ é ímpar, então $|X|$ é par. Nesse caso, X possui um 2-subgrupo de Sylow normal, digamos S_p. Em particular, S_p é o 2-subgrupo de Sylow normal de K. Escrevendo $S = N \rtimes S_p$, obtemos um 2-subgrupo de Sylow normal de G. Novamente pelo Teorema 3.2.4, G satisfaz (Nor).

Agora, se $|Y|$ é par, então $|X|$ é ímpar e pelo Teorema 2.2.1 (iii) e (iv), temos que a ação por conjugação de $Y^* = Y - \{1\}$ sobre X é livre de pontos fixos e Y possui uma única involução z a qual é central em Y e satisfaz $z^{-1}xz = x^{-1}$, para todo $x \in X$.

Sendo assim, $Y \subset C_G(z)$. Como G é um CIT-grupo, segue que $C_G(z)$ é um 2-grupo. Portanto, Y é um 2-grupo.

Assim, estamos com o caso em que, $|X|$ é ímpar e Y é um 2-subgrupo de Sylow de K, em particular, o produto semidireto $S = N \rtimes Y$ é um 2-subgrupo de Sylow de G.

Perceba que a ação por conjugação de $X^* = X - \{1\}$ sobre N é livre de pontos fixos, uma vez que se existisse $x \in X^*$ tal que $x^{-1}nx = n$, para algum $n \in N^*$, teríamos que a ação por x fixaria $\langle n \rangle$ o subgrupo gerado por n. Como $n \in N$ e N é um 2-subgrupo teríamos que $\langle n \rangle$ possuiria uma involução fixada por x. Como estamos em um CIT-grupo x deveria pertencer a um 2-grupo, mas $x \in X$ e X tem ordem ímpar. Portanto, nenhum elemento de X^* comuta com um elemento de N^*, e assim a ação por conjugação de X^* sobre N é livre de pontos fixos. Como Y^* age sobre X sem pontos fixos, segue-se que nenhum elemento de X^* comuta com um elemento de S^*.

Fixemos o seguinte subconjunto dos automorfismos de G:

$$I_S = \{\varphi_u \in Aut_U(G) \ : \ \varphi_u|_S = id \text{ e } \varphi_u^2 = id\},$$

isto é, o subconjunto dos automorfismos de G, determinados por unidades normalizadas, tal que estes automorfismos são involuções e a restrição dos mesmos ao 2-subgrupo de Sylow $S = N \rtimes Y$ fixado, a identidade.

Seja φ_u um elemento de I_S, onde $u \in N_U(G)$. Veja que φ_u fixa os elementos de N e de Y, uma vez que φ_u fixa os elementos de $S = N \rtimes Y$. Vamos estudar a ação de φ_u em X.

Afirmação 1 *Sejam S_p um p-subgrupo de Sylow não trivial de X e $\varphi_u \in I_S$. Então um dos seguintes casos ocorre:*

(i) $u^{-1}xu = x$, *para todo* $x \in S_p$; *ou*

(ii) $u^{-1}xu = y_0^{-1}xy_0 = x^{-1}$, *para todo* $x \in S_p$, *onde* y_0 *é a única involução em* Y; *ou*

(iii) $u^{-1}xu = n_0^{-1}xn_0$, *para todo* $x \in S_p$, *onde* $n_0 \in N$ *é uma involução; ou*

(iv) $u^{-1}xu = y_0^{-1}n_0^{-1}xn_0y_0$, *para todo* $x \in S_p$, *onde* y_0 *é a única involução em* Y *e* $n_0 \in N$ *é uma involução.*

Demonstração: Primeiramente, como $|Y|$ é par, pelo Teorema 2.2.1 (iii), X é nilpotente abeliano de ordem ímpar. Daí segue-se que X é produto de seus p-subgrupos de Sylow. Se S_p denota um p-subgrupo de Sylow de X, então $p \neq 2$ e S_p é um p-subgrupo

de Sylow de G. Pelo Teorema 3.2.1, existe $g_0 = n_0x_0y_0 \in G$, onde $n_0 \in N$, $x_0 \in X$ e $y_0 \in Y$, tal que

$$u^{-1}xu = g_0^{-1}xg_0 = y_0^{-1}x_0^{-1}n_0^{-1}xn_0x_0y_0,$$

para todo $x \in S_p$.

Por um lado, suponhamos que $n_0 = 1$. Então, usando que X é abeliano, vemos para todo $x \in S_p$ que

$$u^{-1}xu = y_0^{-1}x_0^{-1}xx_0y_0 = y_0^{-1}xy_0.$$

Como $\varphi_u \in I_S$, temos que $\varphi_u^2 = id$, logo

$$x = y_0^{-2}xy_0^2,$$

para todo $x \in S_p$. Como a ação de Y^* sobre X é livre de pontos fixos, temos que $y_0^2 = 1$. Assim, $y_0 = 1$ ou $y_0 \in Y$ é a única involução em Y, em particular, y_0 é central em Y. No primeiro caso, $u^{-1}xu = x$, para todo $x \in S_p$, no segundo caso, tem-se que $u^{-1}xu = y_0^{-1}xy_0 = x^{-1}$, para todo $x \in S_p$.

Segue-se que, se $n_0 = 1$, então $u^{-1}xu = x$, para todo $x \in S_p$ ou $u^{-1}xu = y_0^{-1}xy_0 = x^{-1}$, para todo $x \in S_p$, onde $y_0 \in Y$ é a única involução em Y.

Por outro lado, suponhamos que $n_0 \neq 1$. Nesse caso, para todo $x \in S_p$ temos que

$$u^{-1}xu = y_0^{-1}x_0^{-1}n_0^{-1}xn_0x_0y_0.$$

Como $\varphi_u \in I_S$ e X é abeliano, temos que

$$\begin{aligned} x &= y_0^{-2}x_0^{-2}n_0^{-2}xn_0^2x_0^2y_0^2 \\ &\Leftrightarrow\ y_0^2xy_0^{-2} = x_0^{-2}n_0^{-2}xn_0^2x_0^2 \\ &\Leftrightarrow\ x_0^2(y_0^2xy_0^{-2})x_0^{-2} = n_0^{-2}xn_0^2 \\ &\Leftrightarrow\ y_0^2xy_0^{-2} = n_0^{-2}xn_0^2 \\ &\Leftrightarrow\ x = n_0^2y_0^2xy_0^{-2}n_0^{-2}. \end{aligned}$$

Como elementos de X^* não comutam com elementos de S^* e $n_0^2y_0^2 \in S$, temos que $n_0^2y_0^2 = 1$, e portanto $n_0^2 = y_0^2 = 1$. Assim, $y_0 = 1$ ou y_0 é uma involução e, como $n_0 \neq 1$, segue que $n_0 \in N$ é uma involução.

Por um lado, admitimos que $y_0 = 1$. Então usando o fato que φ_u fixa os elementos

de N, obtemos para todo $x \in S_p$ que

$$\begin{aligned} u^{-1}xu &= x_0^{-1}n_0^{-1}xn_0x_0 \\ &\Leftrightarrow u^{-1}n_0^{-1}xn_0u = n_0^{-1}x_0^{-1}(n_0^{-1}xn_0)x_0n_0 \\ &\Leftrightarrow n_0^{-1}xn_0 = n_0^{-2}x_0^{-2}(n_0^{-1}xn_0)x_0^2n_0^2 \\ &\Leftrightarrow n_0^{-1}xn_0 = x_0^{-2}(n_0^{-1}xn_0)x_0^2 \\ &\Leftrightarrow x = n_0x_0^{-2}n_0^{-1}xn_0x_0^2n_0^{-1} \\ &\Leftrightarrow x = n_0x_0^{-2}n_0^{-1}x_0^2x_0^{-2}xx_0^2x_0^{-2}n_0x_0^2n_0^{-1} \\ &\Leftrightarrow x = (n_0x_0^{-2}n_0^{-1}x_0^2)x(x_0^{-2}n_0x_0^2n_0^{-1}). \end{aligned}$$

Da normalidade de N, vemos que $x_0^{-2}n_0x_0^2n_0^{-1} \in N$. Como a ação de X^* sobre N é livre de pontos fixos, temos que $x_0^{-2}n_0x_0^2n_0^{-1} = 1$, e portanto $n_0 = x_0^{-2}n_0x_0^2$. Outra vez, pela ação de X^* sobre N ser livre de pontos fixos, temos que $x_0^2 = 1$. Como $|X|$ é ímpar, segue-se que $x_0 = 1$. Logo, $y_0 = 1$ implica que $x_0 = 1$, e assim $u^{-1}xu = n_0^{-1}xn_0$, para todo $x \in S_p$, onde $n_0 \in N$ é uma involução.

Por outro lado, admitindo que $y_0 \neq 1$, segue que $y_0 \in Y$ é a única involução em Y e é central em Y. Para todo $x \in S_p$ temos

$$\begin{aligned} u^{-1}xu &= y_0^{-1}x_0^{-1}n_0^{-1}xn_0x_0y_0 \\ &\Leftrightarrow u^{-1}n_0^{-1}xn_0u = n_0^{-1}y_0^{-1}x_0^{-1}n_0^{-1}xn_0x_0y_0n_0 \\ &\Leftrightarrow n_0^{-1}xn_0 = n_0^{-2}y_0^{-2}x_0^{-2}(n_0^{-1}xn_0)x_0^2y_0^2n_0^2 \\ &\Leftrightarrow n_0^{-1}xn_0 = x_0^{-2}n_0^{-1}xn_0x_0^2 \\ &\Leftrightarrow x = (n_0x_0^{-2}n_0^{-1}x_0^2)x(x_0^{-2}n_0x_0^2n_0^{-1}). \end{aligned}$$

Como $x_0^{-2}n_0x_0^2n_0^{-1} \in N$ e a ação de X^* sobre N é livre de pontos fixos, vemos que $x_0^{-2}n_0x_0^2n_0^{-1} = 1$. Logo, $n_0 = x_0^{-2}n_0x_0^2$, e assim $x_0^2 = 1$. Como $|X|$ é ímpar, temos que $x_0 = 1$. Segue que, $u^{-1}xu = y_0^{-1}n_0^{-1}xn_0y_0$, para todo $x \in S_p$, onde $y_0 \in Y$ é a única involução em Y e $n_0 \in N$ é uma involução.

Assim, temos os casos:

(i) $u^{-1}xu = x$, para todo $x \in S_p$; ou

(ii) $u^{-1}xu = y_0^{-1}xy_0 = x^{-1}$, para todo $x \in S_p$, onde y_0 é a única involução em Y; ou

(iii) $u^{-1}xu = n_0^{-1}xn_0$, para todo $x \in S_p$, onde $n_0 \in N$ é uma involução; ou

(iv) $u^{-1}xu = y_0^{-1}n_0^{-1}xn_0y_0$, para todo $x \in S_p$, onde y_0 é a única involução em Y e

$n_0 \in N$ é uma involução.

■

Afirmação 2 *Para todo p-subgrupo de Sylow de X, exatamente um dos casos listados na Afirmação 1 ocorre.*

Demonstração: Sejam L_1 o produto de todos os p-subgrupos de Sylow de X que são pontos fixados por φ_u, L_2 o produto de todos os p-subgrupos de Sylow de X tal que (ii) ocorre, $L_3 = S_{p_1} \times \cdots \times S_{p_r}$ o produto de todos os p-subgrupos de Sylow de X tal que (iii) ocorre e $L_4 = S_{q_1} \times \cdots S_{q_s}$ o produto de todos os p-subgrupos de Sylow de X tal que (iv) ocorre.

Assim, $X = L_1 \times L_2 \times L_3 \times L_4$. Veja que, provar a afirmação equivale a provar que $X = L_i$, para algum $1 \leq i \leq 4$.

Pela Afirmação 1, existem $n_1, \ldots, n_r \in N$ involuções tais que

$$u^{-1}xu = n_1^{-1}x_1n_1 \cdots n_r^{-1}x_rn_r,$$

para todo $x = x_1 \cdots x_r \in L_3$, $x_i \in S_{p_i}$. Também, existem $m_1, \ldots, m_s \in N$ involuções tais que

$$u^{-1}wu = y_0^{-1}m_1^{-1}w_1m_1y_0 \cdots y_0^{-1}m_s^{-1}w_sm_sy_0,$$

para todo $w = w_1 \cdots w_s \in L_4$, $w_i \in S_{q_i}$.

Dado $x \in X$, podemos escrever $x = l_1l_2l_3l_4$ com $l_i \in L_i$, $1 \leq i \leq 4$, $l_3 = x_1 \ldots x_r$ e $l_4 = y_1 \ldots y_s$. Daí, temos que

$$u^{-1}xu = l_1y_0^{-1}l_2y_0\big(\prod_{j=1}^{r} n_j^{-1}x_jn_j\big)\big(\prod_{j=1}^{s} y_0^{-1}m_j^{-1}w_jm_jy_0\big).$$

Pela Proposição 3.2.1, temos que x e $\varphi_u(x)$ são conjugados em G, assim existe $g = n'x'y' \in G$, onde $n' \in N$, $x' \in X$ e $y' \in Y$ tal que

$$u^{-1}xu = y'^{-1}x'^{-1}n'^{-1}xn'x'y' = y'^{-1}x'^{-1}n'^{-1}l_1l_2l_3l_4n'x'y'.$$

Logo,

$$l_1y_0^{-1}l_2y_0\big(\prod_{j=1}^{r} n_j^{-1}x_jn_j\big)\big(\prod_{j=1}^{s} y_0^{-1}m_j^{-1}w_jm_jy_0\big) = y'^{-1}x'^{-1}n'^{-1}l_1l_2l_3l_4n'x'y'.$$

Assim obtemos que

- $l_1 = y'^{-1}x'^{-1}n'^{-1}l_1n'x'y'$;
- $y_0^{-1}l_2y_0 = y'^{-1}x'^{-1}n'^{-1}l_2n'x'y'$;
- $\left(\prod_{j=1}^{r} n_j^{-1}x_jn_j\right) = y'^{-1}x'^{-1}n'^{-1}l_3n'x'y'$ e
- $\left(\prod_{j=1}^{s} y_0^{-1}m_j^{-1}w_jm_jy_0\right) = y'^{-1}x'^{-1}n'^{-1}l_4n'x'y'$.

Veja que, $l_1 = y'^{-1}x'^{-1}n'^{-1}l_1n'x'y'$ implica em l_1 comutar com n', x' e y'. Como elementos de X^* não comutam com elementos de N^* e de Y^*, segue que $n' = y' = 1$ ou $l_1 = 1$, para todo $l_1 \in L_1$, isto é, $L_1 = 1$.

Se $n' = y' = 1$, então:

$y_0^{-1}l_2y_0 = y'^{-1}x'^{-1}n'^{-1}l_2n'x'y'$ implica $l_2^{-1} = y_0^{-1}l_2y_0 = x'^{-1}l_2x' = l_2$. Logo, $l_2^2 = 1$. Como $2 \nmid |X|$, segue que $l_2 = 1$ para todo $l_2 \in L_2$. Assim, $L_2 = 1$.

Também, $\left(\prod_{j=1}^{r} n_j^{-1}x_jn_j\right) = y'^{-1}x'^{-1}n'^{-1}l_3n'x'y'$ implica $\left(\prod_{j=1}^{r} n_j^{-1}x_jn_j\right) = x'^{-1}l_3x' = l_3$. Logo, $n_j^{-1}x_jn_j = x_j$, para todo $1 \leq j \leq r$. Como a ação de X^* sobre N é livre de pontos fixos, temos que $x_j = 1$ para todo j. Isto é, $l_3 = 1$ para todo $l_3 \in L_3$. Ademais $L_3 = 1$.

Por fim, a igualdade $\left(\prod_{j=1}^{s} y_0^{-1}m_j^{-1}w_jm_jy_0\right) = y'^{-1}x'^{-1}n'^{-1}l_4n'x'y'$ implica em $\left(\prod_{j=1}^{s} y_0^{-1}m_j^{-1}w_jm_jy_0\right) = x'^{-1}l_4x' = l_4$. Logo, $y_0^{-1}m_j^{-1}w_jm_jy_0 = w_j$, para todo $1 \leq j \leq s$. Daí, $w_j = 1$ para todo j, pois $m_jy_0 \in S^*$ e elementos de X^* não comutam com elementos de S^*. Logo, $l_4 = 1$ para todo $l_4 \in L_4$, e assim $L_4 = 1$.

Concluímos que se $n' = y' = 1$, então $L_2 = L_3 = L_4 = 1$, e portanto $X = L_1$.

Agora se $L_1 = 1$, então admitindo que $L_2 \neq 1$, vemos que:

$y_0^{-1}l_2y_0 = y'^{-1}x'^{-1}n'^{-1}l_2n'x'y'$ implica

$$\begin{aligned} l_2 &= y_0y'^{-1}x'^{-1}n'^{-1}l_2n'x'y'y_0^{-1} \\ &= y_0y'^{-1}x'^{-1}n'^{-1}x'l_2x'^{-1}n'x'y'y_0^{-1} \\ &= (y_0y'^{-1}x'^{-1}n'^{-1}x')l_2(x'^{-1}n'x'y'y_0^{-1}). \end{aligned}$$

Como $x'^{-1}n'x'y'y_0^{-1} \in S$ e elementos de X^* não comutam com elementos de S^*, temos que $x'^{-1}n'x'y'y_0^{-1} = 1$. Daí, $x'^{-1}n'x' = 1$ e $y'y_0^{-1} = 1$, donde $n' = 1$ e $y_0 = y'$.

Substituindo $n' = 1$ e $y_0 = y'$ na igualdade $\left(\prod_{j=1}^{r} n_j^{-1}x_jn_j\right) = y'^{-1}x'^{-1}n'^{-1}l_3n'x'y'$, vemos que $\left(\prod_{j=1}^{r} n_j^{-1}x_jn_j\right) = y_0^{-1}x'^{-1}l_3x'y_0 = y_0^{-1}l_3y_0$. Logo, $n_j^{-1}x_jn_j = y_0^{-1}x_jy_0$, para todo $1 \leq j \leq r$. Portanto, $x_j = y_0^{-1}n_j^{-1}x_jn_jy_0$, para todo $1 \leq j \leq r$. Como elementos de X^* não comutam com elementos de S^*, temos que $x_j = 1$ para todo j. Isto é, $l_3 = 1$ para todo $l_3 \in L_3$. Assim $L_3 = 1$.

Substituindo $n' = 1$ e $y_0 = y'$ em $\left(\prod_{j=1}^{s} y_0^{-1} m_j^{-1} w_j m_j y_0\right) = y'^{-1} x'^{-1} n'^{-1} l_4 n' x' y'$, segue que $\left(\prod_{j=1}^{s} y_0^{-1} m_j^{-1} w_j m_j y_0\right) = y_0^{-1} x'^{-1} l_4 x' y_0 = y_0^{-1} l_4 y_0$. Logo, $y_0^{-1} m_j^{-1} w_j m_j y_0 = y_0^{-1} w_j y_0$, para todo $1 \leq j \leq s$, e portanto $m_j^{-1} w_j m_j = w_j$, para todo $1 \leq j \leq s$. Daí, $w_j = 1$ para todo j, pois a ação de X^* sobre N é livre de ponto fixos. Logo, $l_4 = 1$ para todo $l_4 \in L_4$, e assim $L_4 = 1$.

Segue que se $L_1 = 1$ e $L_2 \neq 1$, então $L_3 = L_4 = 1$ e $X = L_2$.

Agora se $L_1 = 1$, mas admitindo que $L_3 \neq 1$ obtemos:
$\left(\prod_{j=1}^{r} n_j^{-1} x_j n_j\right) = y'^{-1} x'^{-1} n'^{-1} l_3 n' x' y'$ implica em $n_j^{-1} x_j n_j = y'^{-1} x'^{-1} n'^{-1} x_j n' x' y'$, para todo $1 \leq j \leq r$. Logo,

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

Como $x'^{-1} n' x' y' n_j^{-1} \in S$ e elementos de X^* não comutam com elementos de S^*, temos que $x'^{-1} n' x' y' n_j^{-1} = 1$. Assim, $x'^{-1} n' x' = n_j y'^{-1}$, e portanto $n_j = x'^{-1} n' x'$ para todo j e $y' = 1$. Isto é, $n_1 = \ldots = n_r = x'^{-1} n' x'$ e $y' = 1$.

Substituindo $y' = 1$ na igualdade $y_0^{-1} l_2 y_0 = y'^{-1} x'^{-1} n'^{-1} l_2 n' x' y'$, temos que

$$\begin{aligned} l_2 &= y_0 x'^{-1} n'^{-1} l_2 n' x' y_0^{-1} \\ &= y_0 x'^{-1} n'^{-1} x' l_2 x'^{-1} n' x' y_0^{-1} \\ &= (y_0 x'^{-1} n'^{-1} x') l_2 (x'^{-1} n' x' y_0^{-1}). \end{aligned}$$

Como $x'^{-1} n' x' y_0^{-1} \in S^*$ e elementos de X^* não comutam com elementos de S^* temos que $l_2 = 1$, para todo $l_2 \in L_2$. Daí, $L_2 = 1$.

Fazendo $y' = 1$ na expressão $\left(\prod_{j=1}^{s} y_0^{-1} m_j^{-1} w_j m_j y_0\right) = y'^{-1} x'^{-1} n'^{-1} l_4 n' x' y'$, temos que $\left(\prod_{j=1}^{s} y_0^{-1} m_j^{-1} w_j m_j y_0\right) = x'^{-1} n'^{-1} l_4 n' x'$. Logo, $y_0^{-1} m_j^{-1} w_j m_j y_0 = x'^{-1} n'^{-1} w_j n' x'$, para todo $1 \leq j \leq s$, e portanto

$$\begin{aligned} w_j &= m_j y_0 x'^{-1} n'^{-1} w_j n' x' y_0^{-1} m_j^{-1} \\ &= m_j y_0 x'^{-1} n'^{-1} x' w_j x'^{-1} n' x' y_0^{-1} m_j^{-1} \\ &= (m_j y_0 x'^{-1} n'^{-1} x') w_j (x'^{-1} n' x' y_0^{-1} m_j^{-1}), \end{aligned}$$

para todo $1 \leq j \leq s$. Daí, $w_j = 1$ para todo j, pois $x'^{-1} n' x' y_0^{-1} m_j^{-1} \in S^*$ e elementos de X^* não comutam com elementos de S^*. Logo, $l_4 = 1$ para todo $l_4 \in L_4$, e assim $L_4 = 1$.

Segue que se $L_1 = 1$, mas $L_3 \neq 1$, então $L_2 = L_4 = 1$ e $n_1 = \ldots = n_r = n_0$, onde $X = L_3$.

Finalmente no último caso $L_1 = 1$, mas admitindo que $L_4 \neq 1$ obtemos que: $\left(\prod_{j=1}^{s} y_0^{-1} m_j^{-1} w_j m_j y_0\right) = y'^{-1}x'^{-1}n'^{-1}l_4 n'x'y'$ implica que, para todo $1 \leq j \leq s$ tem-se $y_0^{-1}m_j^{-1}w_j m_j y_0 = y'^{-1}x'^{-1}n'^{-1}w_j n'x'y'$, e portanto

$$\begin{aligned} w_j &= m_j y_0 y'^{-1}x'^{-1}n'^{-1}w_j n'x'y'y_0^{-1}m_j^{-1} \\ &= m_j y_0 y'^{-1}x'^{-1}n'^{-1}x'w_j x'^{-1}n'x'y'y_0^{-1}m_j^{-1} \\ &= (m_j y_0 y'^{-1}x'^{-1}n'^{-1}x')w_j(x'^{-1}n'x'y'y_0^{-1}m_j^{-1}), \end{aligned}$$

para todo $1 \leq j \leq s$. Daí, $x'^{-1}n'x'y'y_0^{-1}m_j^{-1} = 1$ para todo j, pois $x'^{-1}n'x'y'y_0^{-1}m_j^{-1} \in S$ e elementos de X^* não comutam com elementos de S^*. Logo, $x'^{-1}n'x'y' = m_j y_0$, e assim $m_j = x'^{-1}n'x'$ e $y_0 = y'$, para todo $1 \leq j \leq s$. Isto é, $m_1 = \ldots = m_s = x'^{-1}n'x'$ e $y_0 = y'$.

Colocando $y_0 = y'$ na igualdade $y_0^{-1}l_2 y_0 = y'^{-1}x'^{-1}n'^{-1}l_2 n'x'y'$, então obtêm-se que $y_0^{-1}l_2 y_0 = y_0^{-1}x'^{-1}n'^{-1}l_2 n'x'y_0$. Logo,

$$\begin{aligned} l_2 &= x'^{-1}n'^{-1}l_2 n'x' \\ &= x'^{-1}n'^{-1}x'l_2 x'^{-1}n'x' \\ &= (x'^{-1}n'^{-1}x')l_2(x'^{-1}n'x'). \end{aligned}$$

Como $x'^{-1}n'x'$ é uma involução, pois $m_1 = \ldots = m_s = x'^{-1}n'x'$, temos que $l_2 = 1$, para todo $l_2 \in L_2$. Daí, $L_2 = 1$.

Fazendo a mesma substituição na igualdade $\left(\prod_{j=1}^{r} n_j^{-1} x_j n_j\right) = y'^{-1}x'^{-1}n'^{-1}l_3 n'x'y'$, então, para todo j, temos $n_j^{-1}x_j n_j = y_0^{-1}x'^{-1}n'^{-1}x_j n'x'y_0$. Logo,

$$\begin{aligned} x_j &= n_j y_0^{-1}x'^{-1}n'^{-1}x_j n'x'y_0 n_j^{-1} \\ &= n_j y_0^{-1}x'^{-1}n'^{-1}x'x_j x'^{-1}n'x'y_0 n_j^{-1} \\ &= (n_j y_0^{-1}x'^{-1}n'^{-1}x')x_j(x'^{-1}n'x'y_0 n_j^{-1}). \end{aligned}$$

Como $x'^{-1}n'x'y_0 n_j^{-1} \in S^*$ e elementos de X^* não comutam com elementos de S^*, temos que $x_j = 1$ para todo j. Assim, $l_3 = 1$, para todo $l_3 \in L_3$, e portanto $L_3 = 1$.

Segue que, se $L_1 = 1$, mas $L_4 \neq 1$, então $L_2 = L_3 = 1$ e $m_1 = \ldots = m_s = m_0$, onde $X = L_4$.

Concluímos que unicamente um dos únicos casos ocorre:

(i) $u^{-1}xu = x$, para todo $x \in X$ $(X = L_1)$; ou

(ii) $u^{-1}xu = y_0^{-1}xy_0$, para todo $x \in X$, onde $y_0 \in Y$ é a única involução em Y ($X = L_2$); ou

(iii) $u^{-1}xu = n_0^{-1}xn_0$, para todo $x \in X$, onde $n_0 \in N$ é uma involução ($X = L_3$); ou

(iv) $u^{-1}xu = y_0^{-1}m_0^{-1}xm_0y_0$, para todo $x \in X$, onde $m_0 \in N$ é uma involução ($X = L_4$).

■

Precisamos analisar a ação em G das involuções $y_0 \in Y$ e $n_0, m_0 \in N$ nos respectivos casos acima. A conclusão da prova do teorema decorrerá das próximas três afirmações.

Afirmação 3 *Se $u^{-1}xu = y_0^{-1}xy_0$, para todo $x \in X$, onde $y_0 \in Y$ é a única involução em Y, em particular, central em Y, então $N \subseteq C_G(y_0)$, isto é, $y_0n = ny_0$, para todo $n \in N$.*

Demonstração: *Procedemos por contradição. Suponhamos que existe $n \in N^*$ tal que $y_0n \neq ny_0$. Assim, fixado $x \in X^*$ temos que $g = nx = xn_2$ para algum $n_2 \in N$, pois a ação por conjugação de X^* sobre N é livre de pontos fixos. Logo, $n_2 = x^{-1}nx$ e temos que $g^{-1} = x^{-1}n^{-1} = n_2^{-1}x^{-1}$. Tomando $\varphi_u \in I_S$ e assumindo que $u^{-1}xu = y_0^{-1}xy_0$, temos que*

$$u^{-1}gu = u^{-1}nxu = ny_0^{-1}xy_0$$

e

$$(u^{-1}gu)^{-1} = u^{-1}g^{-1}u = u^{-1}n_2^{-1}x^{-1}u = n_2^{-1}y_0^{-1}x^{-1}y_0.$$

Logo,

$$\begin{aligned}
(ny_0^{-1}xy_0)(n_2^{-1}y_0^{-1}x^{-1}y_0) &= 1 \\
&\Leftrightarrow\ ny_0^{-1}xy_0 = y_0^{-1}xy_0n_2 \\
&\Leftrightarrow\ nx^{-1} = x^{-1}n_2 \\
&\Leftrightarrow\ nx^{-1} = x^{-1}x^{-1}nx \\
&\Leftrightarrow\ nx^{-1} = x^{-2}nx \\
&\Leftrightarrow\ n = x^{-2}nx^2.
\end{aligned}$$

Como X^* age sobre N sem pontos fixos, temos que $x^2 = 1$. Como $2 \nmid |X|$ segue que $x = 1$, que é um absurdo, pois $x \in X^*$. Logo, a afirmação é verdadeira, isto é, se $u^{-1}xu = y_0^{-1}xy_0$, onde $y_0 \in Y$ denota a única involução em Y, então $y_0n = ny_0$, para todo $n \in N$. ■

Afirmação 4 *Se $u^{-1}xu = n_0^{-1}xn_0$, para todo $x \in X$, onde $n_0 \in N$ é uma involução, então $S \subseteq C_G(n_0)$, isto é, $n_0(ny) = (ny)n_0$, para todo $ny \in S$.*
Demonstração: *Seja $ny \in S$ arbitrário com $n \in N$ e $y \in Y$. Fixemos $x \in X^*$. Como $\varphi_u(nxy)$ e nxy são conjugados em G, existe $g' = n'x'y' \in G$, com $n' \in N$, $x' \in X$ e $y' \in Y$ tal que $u^{-1}nxyu = nu^{-1}xuy = (n'x'y')^{-1}nxy(n'x'y')$. Logo, supondo que $u^{-1}wu = n_0^{-1}wn_0$, para todo $w \in X$ temos que*

$$nn_0^{-1}xn_0y = (n'x'y')^{-1}nxy(n'x'y').$$

Assim, $n = (n'x'y')^{-1}n(n'x'y')$, $y = (n'x'y')^{-1}y(n'x'y')$ e $n_0^{-1}xn_0 = (n'x'y')^{-1}x(n'x'y')$. Segue que n e y comutam com n', x' e y'. Daí, $x' = 1$ ou $n = y = 1$, pois elementos de X^* não comutam com elementos de N^* e de Y^*. Se $n = y = 1$, então claro que $n_0(ny) = (ny)n_0$. Se $x' = 1$, então

$$n_0^{-1}xn_0 = (n'y')^{-1}x(n'y') \Rightarrow x = n_0(n'y')^{-1}x(n'y')n_0^{-1}.$$

Como $(n'y')n_0^{-1} \in S$ e elementos de X^* não comutam com elementos de S^*, vemos que $(n'y')n_0^{-1} = 1$, e assim, $n_0 = n'$ e $y' = 1$. Como ny foi tomado arbitrariamente em S, e n e y comutam com n', segue que $n_0 = n'$ é central em S.

■

Afirmação 5 *Se $u^{-1}xu = y_0^{-1}m_0^{-1}xm_0y_0$, para todo $x \in X$, onde $y_0 \in Y$ é a única involução em Y e $m_0 \in N$ é uma involução, então $S \subseteq C_G(m_0y_0)$, isto é, $m_0y_0(ny) = (ny)m_0y_0$, para todo $ny \in S$.*
Demonstração: *Seja $ny \in S$ arbitrário com $n \in N$ e $y \in Y$. Fixemos $x \in X^*$. Como $\varphi_u(nxy)$ e nxy são conjugados em G, existe $g' = n'x'y' \in G$, com $n' \in N$, $x' \in X$ e $y' \in Y$ tal que $u^{-1}nxyu = nu^{-1}xuy = (n'x'y')^{-1}nxy(n'x'y')$. Logo, supondo que $u^{-1}wu = y_0^{-1}m_0^{-1}wm_0y_0$, para todo $w \in X$ temos que*

$$ny_0^{-1}m_0^{-1}xm_0y_0y = (n'x'y')^{-1}nxy(n'x'y').$$

Daí,
$n = (n'x'y')^{-1}n(n'x'y')$, $y = (n'x'y')^{-1}y(n'x'y')$ e $y_0^{-1}m_0^{-1}xm_0y_0 = (n'x'y')^{-1}x(n'x'y')$. Segue que n e y comutam com n', x' e y'. Daí, $x' = 1$ ou $n = y = 1$, pois elementos de X^* não comutam com elementos de N^* e de Y^*. Se $n = y = 1$, então $m_0y_0(ny) =$

$(ny)m_0y_0$. *Se* $x' = 1$, *então*

$$y_0m_0^{-1}xm_0y_0 = (n'y')^{-1}x(n'y') \Rightarrow x = m_0y_0(n'y')^{-1}x(n'y')y_0^{-1}m_0^{-1}.$$

Como $(n'y')y_0^{-1}m_0^{-1} \in S$ *e elementos de* X^* *não comutam com elementos de* S^*, *vemos que* $(n'y')y_0^{-1}m_0^{-1} = 1$, *e assim,* $m_0 = n'$ *e* $y_0 = y'$. *Como* ny *foi tomado arbitrariamente em* S, *e* n *e* y *comutam com* n' *e* y', *segue que* $m_0y_0 = n'y'$ *é central em* S.

■

De posse dessas afirmações estamos em condições de concluir a prova do teorema. Se $u \in N_U(G)$ é tal que $\varphi_u \in I_S$, então $\varphi_u(nxy) = nxy$, para todo $nxy \in G$; ou $\varphi_u(nxy) = ny_0^{-1}xy_0y = y_0^{-1}nxyy_0$, para todo $nxy \in G$, onde $y_0 \in Y$ é a única involução em Y; ou $\varphi_u(nxy) = nn_0^{-1}xn_0y = n_0^{-1}nxyn_0$, para todo $nxy \in G$, onde $n_0 \in N$ é uma involução; ou $\varphi_u(nxy) = ny_0^{-1}m_0^{-1}xm_0y_0y = y_0^{-1}m_0^{-1}nxym_0y_0$, para todo $nxy \in G$, onde $m_0 \in N$ é uma involução. Em todo caso, $\varphi_u \in Inn(G)$. Logo, $I_S \subseteq Inn(G)$. Consequentemente, pelo Teorema 3.2.3 $Aut_U(G) = Inn(G)$, e assim G satisfaz a propriedade do normalizador.

■

A estrutura de um CIT-grupo G é peculiar, por definição, o centralizador em G de toda involução é um 2-grupo. Esse fato foi fundamental na prova do último teorema, pois influenciou na escolha do 2-subgrupo de Sylow S, e assim em todo desfecho da demonstração. Agora, vamos usar nosso resultado para concluir que CN-grupos também são uma solução ao normalizador.

Lema 4.1.1 *Todo grupo de* 3*-passos de ordem par é um CIT-grupo.*

Demonstração: Seja G é um grupo de 3-passos de ordem par com respeito a um primo p. Então, pela Definição 2.3.1 (i), vemos que $p = 2$. Seja $z \in G$ uma involução. Podemos tomar P um 2-subgrupo de Sylow de G contendo z. Pela Observação 2.3.1, vemos que $G = PA$, onde A é um subgrupo cíclico de ordem ímpar. Além disso, $C_G(x)$ é um 2-grupo, para todo $x \in P$. Em particular, $C_G(z)$ é um 2-grupo. Logo G é um CIT-grupo.

■

Corolário 4.1.1 *Seja* G *um grupo de* 3*-passos. Então a propriedade do normalizador é válida no anel de grupo integral* $\mathbb{Z}G$.

Demonstração: Seja G um grupo de 3-passos com respeito ao primo p. Como vimos no Teorema 3.2.2, a propriedade do normalizador é válida para grupos de ordem ímpar, e portanto podemos assumir que G tem ordem par. Nesse caso, $p = 2$ e pelo Lema 4.1.1, segue que G é um CIT-grupo. Pelo Teorema 4.1.1, obtemos que G satisfaz a propriedade do normalizador.

■

Corolário 4.1.2 *Se G um CN-grupo, então G satisfaz a propriedade do normalizador.*

Demonstração: Se G não é solúvel, então pelo Teorema 2.3.4, segue que G é um grupo simples ou é um grupo de Frobenius. Segue então do Corolário 3.2.3 e do Teorema 3.2.5 que G goza da propriedade do normalizador.

Se G é solúvel, então, o Teorema 2.3.3 diz que G é um grupo nilpotente, ou um grupo de Frobenius ou um grupo de 3-passos. Sabemos do Corolário 3.2.1 e do Teorema 3.2.5 que o resultado é válido para grupos nilpotentes e para grupos de Frobenius respectivamente. Pelo Corolário 4.1.1 os grupos de 3-passos também são uma solução a questão. Portanto, G satisfaz a propriedade do normalizador.

■

Uma aplicação imediata do Corolário 4.1.2 se dá quando G é um CA-grupo, pois é o caso particular em que o centralizador de todo elemento não identidade é abeliano. Como vimos no Teorema 2.3.1, os grupos de Suzuki $Suz(q)$, são grupos de Frobenius ou então CN-grupos simples. Portanto, os grupos de Suzuki também são uma solução ao normalizador.

4.2 O Isomorfismo para CIT-grupos e CN-grupos

Quanto ao isomorfismo, até aqui, não conseguimos concluir que os CIT-grupos e os CN-grupos são ou não determinados pelos seus anéis de grupo integrais, satisfazendo ou não (Iso). Além disso, concluir que os CIT-grupos são uma solução ao isomorfismo não implica que os CN-grupos também o sejam.

Seja G um CIT-grupo. Se G não é solúvel, então sabemos pelo Teorema 2.4.1 que G é um CN-grupo não solúvel, e assim, pelo Teorema 2.3.4, são essencialmente grupos simples ou grupos de Frobenius. Como grupos simples e grupos de Frobenius são determinados pelos seus anéis de grupo integrais, ver Teorema 3.3.4, obtemos que CIT-grupos não solúveis, e portanto CN-grupos não solúveis, satisfazem (Iso).

Assumindo que G é um CIT-grupo solúvel, vimos no Teorema 2.4.2, que se G contém um subgrupo normal próprio de ordem ímpar, então G é um grupo de Frobenius com

complementar um 2-subgrupo de Sylow e núcleo abeliano. Nesse caso, novamente pelo Teorema 3.3.4 5., obtemos resposta positiva para o isomorfismo.

Por outro lado, se G é um CIT-grupo solúvel que não contém um subgrupo normal próprio de ordem ímpar, então como vimos na Observação 2.4.1, G pode ser decomposto em um produto semidireto de um 2-grupo normal por um grupo metacíclico, digamos $G = N \rtimes K$. Assim, estamos com um caso particular, de uma extensão em produto semidireto de um grupo nilpotente por um grupo metacíclico.

Seja H um grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Pela Proposição 3.3.1, podemos supor que esse isomorfismo é normalizado. O Teorema 3.3.2, diz que, existe uma correspondência biunívoca entre os subgrupos normais de G e H que preserva inclusões, interseções e produtos. Logo, existe $M \lhd H$ correspondente a N e vale

$$\mathbb{Z}\left(\frac{G}{N}\right) \simeq \mathbb{Z}\left(\frac{H}{M}\right).$$

Como $K \simeq \frac{G}{N}$ é metacíclico, extraímos do Teorema 3.3.4 4. que $\frac{G}{N} \simeq \frac{H}{M}$. Logo, $K \simeq \frac{H}{M}$, e assim existe $S \leq H$, com $S \simeq K$, tal que $H = M \rtimes S$. Assim, para concluir que os CIT-grupos satisfazem (Iso), resta mostrar que $N \simeq M$.

Até aqui, não conseguimos mostrar que N e M são isomorfos. A dificuldade se apresenta por não termos maiores informações sobre a ação de K sobre N na extensão $G = N \rtimes K$. Mas, continuamos a investigar a questão.

No caso em que G é um CN-grupo solúvel, sabemos do Teorema 2.3.3 que G é nilpotente; ou G é um grupo de Frobenius com complementar cíclico ou produto direto de um cíclico de ordem ímpar por um grupo de quatérnios generalizado; ou G é um grupo de 3-passos. Nos dois primeiros casos G é uma solução ao isomorfismo, ver Teorema 3.3.4 2. e Teorema 3.3.4 5.. Assim, resta investigar o caso em que G é um grupo de três passos.

Até aqui não conseguimos mostrar que os grupos de três passos satisfazem (ISO). Analisando a definição de um grupo de três passos Definição 2.3.1, vemos que esses grupos são internamente relacionados com os grupos de Frobenius, grupos esses que são uma solução ao isomorfismo. Isto leva a intuição que os grupos de três passos também são solução à questão. Assim, continuamos a investigar (ISO) nesses grupos.

No caso particular em que G denota um grupo cujo centralizador de todo elemento não identidade é abeliano, isto é, G é um CA-grupo, segue do Teorema 2.3.2 que G é uma solução trivial a (Iso), pois é um grupo abeliano, um grupo de Frobenius ou um grupos simples isomorfo ao grupo projetivo $PSL(2, 2^m)$, com $m > 3$.

Observe que, se G denota um grupo de Suzuki, temos pelo Teorema 2.3.1 que G é

um CN-grupo do tipo Zassenhaus simples ou G é um grupo de Frobenius de ordem 20 com núcleo isomorfo ao grupo cíclico $\mathbb{Z}_5$ e complementar isomorfo ao grupo cíclico $\mathbb{Z}_4$. Como o isomorfismo é válido para grupos simples e para grupos de Frobenius, temos que os grupos de Suzuki constituem uma solução trivial a questão do isomorfismo.

A investigação de (Iso) para a classe dos CIT-grupos e dos CN-grupos continua, observando que para CIT-grupos estamos em um caso particular de uma extensão em produto semidireto de um grupo nilpotente por um grupo metacíclico, o que remete, em uma perspectiva futura, um direcionamento de estudos de (Iso) nessa direção.

Conclusão

O problema do isomorfismo e a propriedade do normalizador são questões de destaque em teoria de anéis de grupo e nesse trabalho, investigamos estas questões para CIT-grupos e para CN-grupos.

Inicialmente fizemos uma exposição de conceitos e resultados da teoria de grupos com destaque para os CN-grupos e os CIT-grupos. Em seguida, apresentamos os anéis de grupo, sobretudo a propriedade do normalizador e o problema do isomorfismo, analisando alguns resultados desenvolvidos na teoria que estão presentes na literatura.

Mostramos no quarto capítulo, que a questão do normalizador tem resposta positiva em CIT-grupos e consequentemente, se estende a classe dos CN-grupos. Ademais, é imediato que CA-grupos e grupos de Suzuki são soluções a questão. Desta forma, dada a importância dos CN-grupos e dos CIT-grupos, vemos que estas classes de grupos engrandecem a classe dos grupos em que a propriedade do normalizador é válida.

Quanto ao isomorfismo, é imediato que CA-grupos e grupos de Suzuki são soluções à questão. Mas, não conseguimos concluir aqui, que CIT-grupos e CN-grupos são soluções à questão. Continuamos investigando a questão para essas classes de grupos e temos como perspectiva futura direcionar nossos estudos de (Iso) em extensões do tipo produto semidireto de grupos nilpotentes por grupos metacíclicos.

Referências Bibliográficas

[BrSW58] Brauer, R.; Suzuki, M. e Wall, G. E., *A characteriztion of the one-dimensional unimodular projetive groups over finite fields*; Illinois J. Math. v. 2, p. 718-745, 1958.

[Ca78] Camina, A. R. *Some conditions which almost characterize Frobenius groups*; Isr. J. Math. v. 31, p. 153-160, 1978.

[Cay54] Cayley, A. *On the theory of groups as depending on the symbolic equation* $\theta^n = 1$, Phil. Mag., v. 7, p. 40-47, 1854.

[ChH08] Chillag, D. e Herzog, M., *Finite groups with almost distinct character degrees*; J. Alg v. 319, p. 716-729, 2008.

[ChM84] Chillag, D. e Macdonald, I. D., *Generalized Frobenius Groups*; Isr. J. Math. v. 47, p. 111-122, 1984.

[Co64] Coleman, D. B., *On the modular group ring of a p-group*; Proc. Amer. Math. Soc. v. 15, p. 511-514, 1964.

[DaS96] Dark R. e Scoppola C. M., *On Camina Groups of Prime Power Order*; J. Alg. v. 181, p. 787-802, 1996.

[FeS88] Feit, W. e Seitz, G. M., *On finite rational groups e related topics*; Illinois J. Math. v. 33, Spring, 1988.

[FHT60] Feit, W., Hall, M. e Thompson, J. G., *Finite group in which the Centralizer of any non-identity element is nilpotent*; Math. Zeit. v. 74, p.1-17, 1960.

[Go80] Gorenstein, D. *Finite groups*; Chelsea Publishing Company. Second Editon, New York, 1980.

[GrS12] Groen, T. M. e Smit, B., *Suzuki groups and the other Zassenhus groups*; Bachelor thesis. Universiteit Leiden, Nederland, 2012.

[Her01] Hertweck, M., *A counterexample to the isomorphism problem for integral group rings*; Ann. Math. v. 154, p. 1-26, 2001.

[Hi40] Higman, G., *Units of group rings*; Ph.D. Thesis, University of Oxford, Oxford, 1940.

[HuB82] Huppert, B. e Blackbum, N., *Finite Groups III*; Grundlehren Der Mathematischen Wissenschaften, Springer-Verlag, New York 1982.

[JaM87] Jackowski, S. e Marciniak, Z., *Group automorphisms inducing the identity map on cohomology*; j. Pure Appl. algebra, v. 44, p. 241-250, 1987.

[JeJ02] Jespers, E.; Juriaans, S. O.; Miranda, J. M. e Rogerio, J. R., *On the Normalizer Problem*; J. Alg. v. 247, p. 24-36, 2002.

[KiL90] Kimmerle, W., Lyons, R., Sandling, R. e Teague, D., *Composition factors from the group ring and Artin's theorem on orders of simple groups*; Proc. London Math. Soc. v. 60, p. 89-122, 1990.

[Ki92] Kimmerle, W., *Class sums of p-elements*; In DMV Seminar Band v.18, p. 117-124, 1992.

[Ma95] Manzur, M. *On the isomorphism problem for integral group rings of infinite groups*; Exposition; v. 13, p. 433-445, 1995.

[Pe01] Petit Lobão, T., *Frobenius groups and the isomorphism problem*; Mat. Cont. v. 21, p. 147-156, 2001.

[PeP02] Petit Lobão, T. e Polcino Milies, F. C., *The normalizer property for integral group rings of Frobenius group*; J. Alg. v. 256, p. 1-6, 2002.

[PeS03] Petit Lobão, T. e S. K. Sehgal, *The Normalizer Property for Integral Group Rings of Complete Monomial Groups*; Communications in Algebra, v. 31, p. 2971-2983, 2003.

[Pe08] Petit Lobão, T., *The isomorphism problem for some complete monomial groups*; Communications In Algebra V. 36 , p. 4407-4412, 2008.

[PoS02] Polcino Milies, F.C. e S. K. Sehgal, *An introduction to group rings*; Kluwer Academic publishers, Dordrecht, 2002.

[RoS87] Roggenkamp, K. W. e Scott, L. L., *Isomorphisms of p-adic group rings*; Ann. Math. v. 126, p. 593-647, 1987.

[Rot95] Rotman, J. J., *An Introduction to the Theory of Groups*; Springer-Verlag, ed. 4, New York 1995.

[Sc64] Scott, W. R., *Group Theory*, Dover, New York, 1964.

[Se93] Sehgal, S. K. *Units in Integral Group Rings*; Longman, Essex, 1993.

[Su57] suzuki, M., *The nonexistence of a certain type of simple groups of odd order*; Proc. Amer. math. Soc. V. 8, p. 686-695, 1957.

[Su60] Suzuki, M., *A new type of simple groups of finite order*; Proceedings of the National Academy of Sciences of the United States of America, V. 46, p. 868-870, 1960.

[Su61] Suzuki, M., *Finite group with nilpotent centralizer*; Trans. Amer. Math. Soc. V. 99, p. 425-470, 1961.

[Suz61] Suzuki, M., *On a class of doubly transitive groups*; Annals of Math. 2º ed, v. 75, p. 105-145, 1961.

[Su86] Suzuki, M., *group theory II*; Springer-Verlag, Berlim, New York, 1986.

[YFW98] Yu-Fen Wu, *Groups in which commutativity is a transitive relation*; J. Alg. v. 207, p. 165-181, 1998.

[We25] Weisner, L., *Groups in which the normalizer of every element except identity is abelian*; Bulletin Amer. Math. Soc. v. 31, p. 413-416, 1925.

[Wh68] Whitcomb, A., *The Group Ring Problem*; Ph.D. Thesis, University of Chicago, 1968.