Propriedades de Jordan em anéis de grupo

Anderson Geraldo

DISSERTAÇÃO APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO TÍTULO
DE
MESTRE EM CIÊNCIAS

Programa: Matemática
Orientador: Prof. Dr. Rodrigo Lucas Rodrigues

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro do CNPq.
São Paulo, 04 de Julho de 2019.

Propriedades de Jordan em anéis de grupo

Esta é a versão original da dissertação elaborada pelo candidato Anderson Geraldo, tal como submetida à Comissão Julgadora.

Propriedades de Jordan
em anéis de grupo

Esta versão da dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 04/07/2019. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissao Julgadora:

- Prof. Dr. Rodrigo Lucas Rodrigues - Centro de Ciências - UFC.
- Profa. Dra. Rosemary Miguel Pires - Universidade Federal Fluminense - UFF
- Prof. Dr. Thierry Petit Lobão - Universidade Federal da Bahia - UFBA.

Agradecimentos

Agradeço ao meu orientador Rodrigo Lucas Rodrigues pelo voto de confiança que me deu ao acreditar que seria possível a realização deste trabalho.

À minha família e a todos os meus amigos.

A todos os professores da Universidade Presbiteriana Mackenzie, na qual obtive o grau de licenciado em matemática. Agradeço de modo especial aos professores Adilson Morais, Ângela Hum Tchemra, Eriko Matsui Yamamoto, Fausto Hossamu Mizutani, Fernanda Monti Steffens, Renate Gompertz Watanabe, Suzana Abreu de Oliveira Souza e Vera Lúcia Antônio Azevedo.

Ao CNPQ pelo auxílio financeiro.

Resumo

GERALDO, A. **Propriedades de Jordan em anéis de grupo**. 2019. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2019.

Neste trabalho estudamos alguns resultados a respeito do conjunto dos elementos que são simétricos sobre uma involução, orientada ou não, de um anel de grupo. Dado um anel de grupo RG, onde R é comutativo e com elemento identidade 1, e uma involução orientada $\alpha \to \alpha^{\#}$; apresentamos as condições necessárias e suficientes sobre R e G para que o subconjunto $(RG)^+ = \{\alpha \in RG : \alpha^{\#} = \alpha\}$ seja anticomutativo, ou equivalentemente, o produto de Jordan seja trivial em $(RG)^+$.

Além disso, estudamos um caso de nilpotência de Jordan no anel de grupo RG e no seu subconjunto $(RG)^+$, para o caso onde a involução não possui orientação.

Palavras-chave: anéis de grupo, involução orientada, elementos simétricos, nilpotência de Jordan.

Abstract

GERALDO, A. **Properties of Jordan in group rings**. 2019. Dissertação (Mestrado) - Instituto de Matemática e Estatísitca - Universidade de São Paulo, São Paulo, 2019.

In this work we study some results regarding the set of elements that are symmetrical about an involution, oriented or not, in a group ring. Given a group ring RG, where R is commutative and with identity element 1, and an oriented involution $\alpha \to \alpha^{\#}$ we present the necessary and sufficient conditions on R and G so that the set $(RG)^{+} = \{\alpha \in RG : \alpha^{\#} = \alpha\}$ is anticomutative, or equivalently, the Jordan product is trivial in $(RG)^{+}$.

In addition we study a case of Jordan's nilpotency in the group RG and its subset $(RG)^{+}$, for the case where involution has no orientation.

Keywords: group rings, oriented involution, symmetrical elements, Jordan nilpotency.

Sumário

Lista de símbolos e abreviaturas **ix**

Introdução **xi**

1 Conceitos Preliminares **1**
1.1 Anéis de Grupo 1
1.2 Involuções de Grupos e de Anéis 3

2 Grupos SLC **7**
2.1 Comutadores 7
2.1.1 Subgrupo Comutador 9
2.2 Grupos C, LC e SLC 9
2.2.1 Classificação dos Grupos SLC 14
2.2.2 Caracterização dos grupos SLC através de uma involução 15

3 Involuções de RG e anticomutatividade em $(RG)^+$ **19**
3.1 O produto de Jordan trivial em RG 19
3.2 O produto de Jordan trivial em $(RG)^+$ 19

4 Involuções orientadas e produto de Jordan trivial em $(RG)^+$. **25**
4.1 Orientação para um Grupo G 25
4.2 Involução orientada de RG 26
4.3 O conjunto $(RG)^+$ 27
4.4 Produto de Jordan trivial em $\mathcal{G}$ 28

5 Nilpotência para o produto de Jordan em RG e $(RG)^+$ **39**
5.1 Jordan 3-nilpotência em RG 39
5.2 Jordan 3 - nilpotência em $(RG)^+$ 40

6 Considerações Finais **57**

Referências Bibliográficas **59**

Lista de símbolos e abreviaturas

C_n	grupo cíclico de ordem n
(g,h)	comutador dos elementos g e h pertencentes a ao grupo G
$\langle X \rangle$	subgrupo gerado por um subconjunto X de G
G'	$\langle (g,h) : g,h \in G \rangle$ subgrupo comutador de G
$H \leq G$	H é um subgrupo de G
$H \trianglelefteq G$	H é um subgrupo normal de G
$Z(G)$	centro do grupo G
$G \times H$	produto direto dos grupos G e H
$G \cong H$	o grupo G é isomorfo ao grupo H
$[G : H]$	o índice do subgrupo H de G
$[x,y]$	$xy - yx$, o colchete de Lie de x e y
$x \circ y$	$xy + yx$, o produto de Jordan de x e y
$\mathrm{car}(R)$	característica do anel R
$\mathrm{supp}(\alpha)$	suporte do elemento $\alpha \in RG$

Introdução

Nos últimos anos, muitos pesquisadores têm se dedicado ao estudo de anéis de grupo com involução, e este crescente interesse tem resultado na publicação de diversos artigos.

Escolhemos nos aprofundar nas demonstrações de dois resultados bastante recentes. Um deles diz respeito à trivialidade do produto de Jordan entre os elementos de um anel de grupo RG que são fixos sobre uma involução orientada de RG. O outro, diz respeito à nilpotência de índice 3, também no conjunto dos elementos que são fixos sobre uma involução de RG. No segundo caso, trata-se de uma involução sem orientação; em outras palavras, uma involução de RG cuja a orientação é trivial. Antes de, nesta introdução, falarmos a respeito de tais problemas, comentaremos sobre alguns resultados que foram obtidos anteriormente.

Veremos no Capítulo 1, onde apresentamos os conceitos preliminares, que se RG é um anel de grupo, onde R é comutativo e possui elemento identidade 1, então uma involução $g \mapsto g^*$ de G pode, de modo bastante natural, ser estendida linearmente à uma involução $\alpha \mapsto \alpha^*$ de RG da seguinte maneira: $\left(\sum_{g\in G} \alpha_g g\right)^* = \sum_{g\in G} \alpha_g g^*$.

Considerando um anel de grupo RG com uma involução $*$ que descrevemos no parágrafo anterior, temos dois subconjuntos que chamaram a atenção de alguns pesquisadores. O primeiro é o subconjunto dos *elementos simétricos* de RG, isto é, dos elementos que são fixos a respeito da involução $*$ e que representamos por $(RG)^+$, isto é, $(RG)^+ = \{\alpha \in RG : \alpha^* = \alpha\}$. O segundo subconjunto é o dos elementos antissimétricos, que representamos por $(RG)^-$, isto é, $(RG)^- = \{\alpha \in RG : \alpha^* = -\alpha\}$.

É natural indagar quando que estes dois subconjuntos são subanéis de RG.

É fácil ver que $(RG)^+$ é subanel de RG se, e somente se, dados $\alpha, \beta \in (RG)^+$, se verifica $\alpha\beta = (\alpha\beta)^* = \beta^*\alpha^* = \beta\alpha$, isto é, se, e somente se, $(RG)^+$ é comutativo. De modo similar, $(RG)^-$ é subanel se, e somente se, para quaisquer $\alpha, \beta \in (RG)^-$, tivermos $\alpha\beta = -\beta\alpha$, isto é, se, e somente se, $(RG)^-$ é anticomutativo. Assim, surgem os questionamentos a respeito de quando $(RG)^+$ é comutativo e quando que $(RG)^-$ é anticomutativo.

Quando fazemos tais questionamentos, é porque estamos interessados em saber quais são as condições necessárias e suficientes sobre R e G tais que $(RG)^+$ e $(RG)^-$ sejam, respectivamente, comutativo e anticomutativo. Ou, escrevendo de outro modo, queremos a caracterização dos grupos G para que tais coisas ocorram.

Em [2], O. B. Cristo respondeu ao primeiro questionamento para o caso da involução natural $g \mapsto g^{-1}$ de G, isto é, no seu artigo, caracteriza-se os grupos G para os quais os elementos simétricos de RG comutam entre si. Já em [7], E. G. Goodaire e C. Polcino Milies conseguiram responder ao segundo questionamento para uma involução $g \mapsto g^*$.

Prosseguindo, vamos olhar para outras duas perguntas que foram feitas a respeito de $(RG)^-$ e $(RG)^+$.

Quando $(RG)^-$ é comutativo? Quando $(RG)^+$ é anticomutativo?

A respeito da primeira pergunta, é bem fácil ver que o conjunto $(RG)^-$ é fechado para o colchete de Lie $[\alpha, \beta] = \alpha\beta - \beta\alpha$ e que $(RG)^-$ é comutativo se, e somente se, $\alpha\beta - \beta\alpha = 0$ para quaisquer α, $\beta \in (RG)^-$; isto é, se, e somente se, o colchete de Lie é *trivial* em $(RG)^-$. Mais uma vez, O. B. Cristo, juntamente com C. P. Milies [3], determinaram, para o caso da involução natural de G, as condições necessárias e suficientes para que o colchete de Lie seja trivial em $(RG)^-$.

Foi a partir da última pergunta que nos motivamos a escrever este trabalho. Seja RG um anel de grupo, onde R é comutativo e com elemento identidade 1, e seja o produto de Jordan $\circ$ em RG, que é definido como $\alpha \circ \beta = \alpha\beta + \beta\alpha$. É fácil ver, de modo similar ao caso do colchete de Lie, que $(RG)^+$ é fechado para o produto de Jordan $\circ$ e que tal produto é trivial em $(RG)^+$, isto é, $\alpha \circ \beta = 0$ para quaisquer $\alpha, \beta \in RG$ se, e somente se, $(RG)^+$ é anticomutativo.

No artigo [7], que nos serviu como referência para escrever o Capítulo 3, os professores E. G. Godaire e C. Polcino Milies, responderam quando é que $(RG)^+$ é anticomutativo. Já adiantamos que todos os capítulos foram escritos utilizando como referência artigos escritos em conjunto por estes dois autores.

No Capítulo 4, dado um grupo G com uma involução $g \mapsto g^*$ e um homomorfismo de grupos $\sigma : G \to \{1, -1\}$, tal que $\sigma(g) = \sigma(g^*)$ para todo $g \in G$, mostraremos que a aplicação $\alpha = \sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \sigma(g)\alpha_g g^* = \alpha^\#$ é uma involução de RG e estudaremos a anticomutatividade no conjunto $(RG)^+ = \{\alpha \in RG : \alpha^\# = \alpha\}$. É fácil ver que os resultados obtidos no Capítulo 3 são válidos no subgrupo $N = \ker(\sigma)$ de G.

No Capítulo 5, para o caso de uma involução sem orientação $\alpha \mapsto \alpha^*$ de RG estudamos a caracterização da nilpotência de Jordan de índice 3 em RG e em $(RG)^+$, isto é, as condições necessárias e suficientes para que dados α, β, γ em RG ou no seu subconjunto $(RG)^+$ vefirique-se $(\alpha \circ \beta) \circ \gamma = 0$. Além disso faremos uma conexão com o que foi visto no Capítulo 3.

Capítulo 1

Conceitos Preliminares

Apresentamos neste capítulo, de modo sucinto, alguns dos conceitos elementares a respeito da estrutura algébrica na qual se concentra esta dissertação: o anel de grupo. Estes conceitos são suficientes para a compreensão de todo o trabalho. Ao leitor que estiver interessado em aprofundar seus estudos a respeito desta estrutura, recomendamos a referência [15].

Também relembramos as definições de involução de um grupo e de um anel, mostramos algumas de suas propriedades, bem como construímos uma involução de um anel de grupo.

1.1 Anéis de Grupo

Sejam G um grupo multiplicativo (não necessariamente finito) e R um anel associativo com elemento identidade 1. Denotamos por RG o conjunto das combinações lineares formais com elementos de G que sejam da forma $\sum_{g\in G} \alpha_g g$, onde os coeficientes α_g são pertencentes a R e são tais que $\alpha_g = 0$ exceto para um número finito de coeficientes. Definimos o *suporte* de um elemento $\alpha = \sum_{g\in G} \alpha_g g$, que denotamos por $\mathrm{supp}(\alpha)$, como sendo o conjunto dos elementos de G que efetivamente aparecem na expressão de α, isto é, $\mathrm{supp}(\alpha) = \{g \in G : \alpha_g \neq 0\}$. Para quaisquer elementos $\alpha = \sum_{g\in G} \alpha_g g$ e $\beta = \sum_{g\in G} \beta_g g$ pertencentes a RG, $\alpha = \beta$ se, e somente se, $\alpha_g = \beta_g$ para qualquer $g \in G$.

A soma de dois elementos $\alpha = \sum_{g\in G} \alpha_g g$ e $\beta = \sum_{g\in G} \beta_g g$ pertencentes a RG é definida como $\alpha + \beta = \sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$. Esta operação possui elemento neutro, que representamos por 0_{RG} ou simplesmente por 0, e que é a combinação linear $\sum_{g\in G} \alpha_g g$ tal que $\alpha_g = 0$ para qualquer $g \in G$. A multiplicação entre α e β é definida como $\alpha\beta = \left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{g\in G} \beta_g g\right) = \sum_{g,h\in G} \alpha_g \beta_h gh$. Reordenando os termos na última expressão, escrevemos este produto como $\alpha\beta = \sum_{u\in G} c_u u$, onde $c_u = \sum_{gh=u} \alpha_g \beta_h$.

É fácil verificar que, munido das operações de soma e multiplicação que definimos, o conjunto RG é um anel associativo e com elemento identidade, que representamos por 1_{RG} ou simplesmente por 1, e que é a combinação $\sum_{g\in G} \alpha_g g$ tal que $\alpha_g = 1$ se g é o elemento neutro 1_G de G e $\alpha_g = 0$ em caso contrário. Dizemos que este conjunto é o *anel de grupo* RG.

Definimos a multiplicação de um elemento $\sum_{g\in G} \alpha_g g \in RG$ por $\lambda \in R$ como $\lambda\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} (\lambda\alpha_g)g$. Com respeito à esta multiplicação, o anel de grupo RG é um R-módulo e, se R for um anel comutativo, RG é uma R-álgebra.

Observação 1.1.1 O monomorfismo de anéis $\zeta: R \to RG$ definido por $\zeta(r) = r1_G$ pode ser visto como uma inclusão de R em RG, o que nos permite considerar R como um subanel de RG. Iremos sempre representar o elemento $r1_G \in RG$ simplesmente por r.

Exemplo 1.1.2 [4, Exemplo 1.24] Sejam o grupo $C_2 = \langle g : g^2 = 1_{C_2}\rangle$ e o corpo $\mathbb{Z}_3 = \{0,1,2\}$. Podemos construir o anel de grupo $\mathbb{Z}_3C_2 = \{a.1_{C_2} + b.g : a,b \in \mathbb{Z}_3\} = \{0,1,2,g,2g,1+g,1+2g,2+g,2+2g\}$. Exibimos abaixo as suas tábuas de operações.

+	0	1	2	g	2g	1 + g	1 + 2g	2 + g	2 + 2g
0	0	1	2	g	2g	1 + g	1 + 2g	2 + g	2 + 2g
1	1	2	0	1 + g	1 + 2g	2 + g	2 + 2g	g	2g
2	2	0	1	2 + g	2 + 2g	g	2g	1 + g	1 + 2g
g	g	1 + g	2 + g	2g	0	1 + 2g	1	2 + 2g	2
2g	2g	1 + 2g	2 + 2g	0	g	1	1 + g	2	2 + g
1 + g	1 + g	2 + g	g	1 + 2g	1	2 + 2g	2	2g	0
1 + 2g	1 + 2g	2 + 2g	2g	1	1 + g	2	2 + g	0	g
2 + g	2 + g	g	1 + g	2 + 2g	2	2g	0	1 + 2g	1
2 + 2g	2 + 2g	2g	1 + 2g	2	2 + g	0	g	1	1 + g

Tabela 1.1: Tábua da adição do anel de grupo $\mathbb{Z}_3C_2$.

·	0	1	2	g	2g	1 + g	1 + 2g	2 + g	2 + 2g
0	0	0	0	0	0	0	0	0	0
1	0	1	2	g	2g	1 + g	1 + 2g	2 + g	2 + 2g
2	0	2	1	2g	g	2 + 2g	2 + g	1 + 2g	1 + g
g	0	g	2g	1	2	1 + g	2 + g	1 + 2g	2 + 2g
2g	0	2g	g	2	1	2 + 2g	1 + 2g	2 + g	1 + g
1 + g	0	1 + g	2 + g	1 + g	2 + 2g	2 + 2g	0	0	1 + g
1 + 2g	0	1 + 2g	2 + g	2 + g	1 + 2g	0	2 + g	1 + 2g	0
2 + g	0	2 + g	1 + 2g	1 + 2g	2 + g	0	1 + 2g	2 + g	0
2 + 2g	0	2 + 2g	1+g	2 + 2g	1+g	1+g	0	0	2 + 2g

Tabela 1.2: Tábua da multiplicação do anel de grupo $\mathbb{Z}_3C_2$.

1.2 Involuções de Grupos e de Anéis

Definição 1.2.1 Dizemos que uma aplicação ϕ de um grupo G é uma *involução de* G se para quaisquer $g, h \in G$ verificam-se:

- $\phi(gh) = \phi(h)\phi(g)$;
- $\phi(\phi(g)) = g$.

Proposição 1.2.2 Se ϕ é uma involução de um grupo G, então

(i) $\phi(1_G) = 1_G$;

(ii) $\phi(g^{-1}) = \phi(g)^{-1}$ para qualquer $g \in G$.

Demonstração: Primeiramente, note que $1_G = \phi(\phi(1_G)) = \phi(1_G\phi(1_G)) = \phi(\phi(1_G))\phi(1_G) = 1_G\phi(1_G) = \phi(1_G)$, o que já prova (i). Para provar (ii) basta ver que para qualquer $g \in G$ verifica-se $\phi(g^{-1})\phi(g) = \phi(gg^{-1}) = \phi(1_G) = 1_G$, e isto implica que $\phi(g^{-1}) = \phi(g)^{-1}$. ■

Definição 1.2.3 Dizemos que uma aplicação ψ de um anel R é uma *involução de* R se para quaisquer $r, s \in R$ verificam-se:

- $\psi(r+s) = \psi(r) + \psi(s)$;
- $\psi(rs) = \psi(s)\psi(r)$;
- $\psi(\psi(r)) = r$.

Proposição 1.2.4 Se ψ é uma involução de um anel R com identidade 1, então

(i) $\psi(1) = 1$;

(ii) $\psi(0) = 0$;

(iii) $\psi(-r) = -\psi(r)$, para todo $r \in R$.

Demonstração: O item (i) já provamos na Proposição 1.2.2. Para verificar a validade do item (ii) note que $0 + \psi(0) = \psi(0) = \psi(0+0) = \psi(0) + \psi(0)$, o que implica que $\psi(0) = 0$. Para provar (iii) observe que $0 = \psi(0) = \psi(r + (-r)) = \psi(r) + \psi(-r)$, o que implica que $\psi(-r) = -\psi(r)$. ■

Em [7] uma involução de um grupo G é chamada de *antiautomorfismo* de ordem 2. Comentamos no próximo parágrafo um pouco à respeito deste termo.

Sejam G e H grupos multiplicativos. Sabemos que é possível definir o grupo H^{op}, munido da operação $\cdot$, definida por $a \cdot b = ba$ para quaisquer $a, b \in H$. Desta maneira, se $f: G \to H^{op}$ é um homomorfismo de grupos, então se verifica $f(gh) = f(h)f(g)$ para quaisquer g, h pertencentes a G. Note que, devido ao fato de H^{op} e H serem iguais como conjuntos, então f é uma aplicação de G em H, e que chamamos de anti-homomorfismo. É evidente que se $f: G \to H$ é um anti-homomorfismo então $f(1_G) = 1_H$ e $f(g^{-1}) = (f(g))^{-1}$ para qualquer $g \in G$. Desta forma, um anti-isomorfismo é um anti-homomorfismo bijetor e um antiautomorfismo é um anti-isomorfismo $f: G \to G$. Da mesma maneira que se define para automorfismos de grupos, dizemos que um antiautomorfismo ϕ possui ordem 2 se ϕ^2 é igual a aplicação identidade em G, o que particularmente ocorre se, e somente se, $\phi = \phi^{-1}$. Concluímos que qualquer involução de um grupo G é, por definição, um antiautomorfismo de ordem 2.

Observação 1.2.5 É bem fácil notar que a inversão $g \mapsto g^{-1}$ é uma involução de G, que chamamos de *involução natural* ou *canônica*. Um elemento $g \in G$ ($r \in R$) é *simétrico* (ou fixo) à respeito de uma involução ϕ de G (ψ de R), se $\phi(g) = g$ ($\psi(r) = r$). Também afirmamos que existe uma involução que fixa todo elemento de G (de R) se, e somente se, G é um grupo abeliano (R é um anel comutativo). Com efeito, seja ϕ (ψ) uma involução de G (de R) tal que para qualquer $g \in G$ ($r \in R$) se verifica que $\phi(g) = g$ ($\psi(r) = r$). Então, para quaisquer $g, h \in G$ ($r, s \in R$) vale que $gh = \phi(gh) = \phi(h)\phi(g) = hg$ ($rs = \phi(rs) = \phi(s)\phi(r) = sr$), o que implica que G é abeliano (R é comutativo). Reciprocamente, suponhamos que G é abeliano (R é comutativo), então a aplicação identidade de G (de R) é uma involução e, dessa forma, o grupo G (o anel R) possui uma involução que fixa todos os seus elementos.

Exemplo 1.2.6 (involução de um anel de grupo) Sejam RG um anel de grupo, ϕ uma involução de G e ξ uma involução de R. Definimos uma aplicação ψ em RG, como $\psi\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \xi(\alpha_g)\phi(g)$. Afirmamos que ψ é uma involução de RG. Com efeito,

(i)

$$\begin{aligned}
\psi\left(\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g\right) &= \psi\left(\sum_{g\in G} (\alpha_g + \beta_g) g\right) = \sum_{g\in G} \xi(\alpha_g + \beta_g)\phi(g) \\
&= \sum_{g\in G} (\xi(\alpha_g) + \xi(\beta_g))\phi(g) = \sum_{g\in G} \xi(\alpha_g)\phi(g) + \sum_{g\in G} \xi(\beta_g)\phi(g) \\
&= \psi\left(\sum_{g\in G} \alpha_g g\right) + \psi\left(\sum_{g\in G} \beta_g g\right);
\end{aligned}$$

(ii)

$$\begin{aligned}
\psi\left(\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right)\right) &= \psi\left(\sum_{g,h\in G} (\alpha_g\beta_h)(gh)\right) = \sum_{g,h\in G} \xi(\alpha_g\beta_h)\phi(gh) \\
&= \sum_{g,h\in G} \xi(\beta_h)\xi(\alpha_g)\phi(h)\phi(g) = \sum_{h\in G} \xi(\beta_h)\phi(h) \sum_{g\in G} \xi(\alpha_g)\phi(g) \\
&= \psi\left(\sum_{h\in G} \beta_h h\right)\psi\left(\sum_{g\in G} \alpha_g g\right);
\end{aligned}$$

(iii)

$$\psi\left(\psi\left(\sum_{g\in G} \alpha_g g\right)\right) = \psi\left(\sum_{g\in G} \xi(\alpha_g)\phi(g)\right) = \sum_{g\in G} \xi(\xi(\alpha_g))\phi(\phi(g)) = \sum_{g\in G} \alpha_g g.$$

Se R é um anel comutativo, então de acordo com a Observação 1.2.5 a aplicação identidade é uma involução de R. Sendo assim, conforme o Exemplo 1.2.6, dada uma involução ϕ de G obtemos uma involução ψ de RG definindo:

$$\psi\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g \phi(g). \tag{1.1}$$

Dizemos que a involução ψ definida pela equação (1.1) é a involução induzida de RG pela involução ϕ de G ou também que é a involução obtida da extensão linear da involução ϕ de G.

Daqui em diante, acompanhando a notação dos artigos que estudamos, representamos uma involução de G por $g \mapsto g^*$ ou simplesmente por $*$. Em todos estes artigos o anel R de coeficientes é associativo, possui elemento identidade 1 e é comutativo, e uma involução de RG, que será representada por $\alpha \mapsto \alpha^*$ ou também por $*$, é uma extensão linear da involução de G, isto é, $\alpha^* = \left(\sum_{g \in G} \alpha_g g\right)^* = \sum_{g \in G} \alpha_g g^*$.

Capítulo 2

Grupos SLC

Nos artigos que estudamos para escrever esta dissertação, seus autores realizaram as caracterizações dos grupos G para os quais se verifica nos anéis de grupo RG a anticomutatividade ou a Jordan nilpotência de índice 3 nos seus subconjuntos cujos elementos são fixos sobre uma involução de RG. Veremos no Capítulo 3, que um SLC satisfaz, no caso de a característica de R ser igual a 4, a anticomutatividade em $(RG)^+$.

Dedicamos a primeira seção deste capítulo a relembrar a definição de comutador de um grupo G, provar as principais propriedades dos comutadores, bem como comentar a respeito de alguns resultados pertinentes ao subgrupo comutador de G. Na segunda seção definimos os grupos que estudamos para escrever esta dissertação, provamos várias das suas propriedades e estudamos a classificação destes grupos.

2.1 Comutadores

Definição 2.1.1 Dados dois elementos g e h pertencentes a um grupo G, dizemos que o *comutador* de g e h é o elemento $(g,h) = g^{-1}h^{-1}gh$.

Sejam x e y elementos de um grupo G. Denotando o elemento $y^{-1}xy$ como x^y, seguem no próximo lema algumas propriedades importantes que são satisfeitas por comutadores.

Lema 2.1.2 [15, Lema 1.5.2] Sejam x, y, z e t elementos de um grupo G e $(x,y,z) = ((x,y),z)$. Então

(i) $(x,y) = 1_G$ se, e somente se, $xy = yx$;

(ii) $(x,y)^{-1} = (y,x)$;

(iii) $(xy,z) = (x,z)^y(y,z) = (x,z)((x,z),y)(y,z)$;

(iv) $(x,yz) = (x,z)(x,y)^z = (x,z)(x,y)((x,y),z)$;

(v) $(x,y)z = z(x^z,y^z)$;

(vi) $(x^y,z) = (x,z)^{(x,y)}(x,y,z)$;

(vii) $(x^{yz},t) = (x^y,t)^{(x^y,z)}(x^y,z,t)$.

Demonstração: Para quaisquer x, y, z, t pertencentes a G, temos:

(i) $(x,y) = x^{-1}y^{-1}xy = 1_G$ se, e somente se, $yx(x^{-1}y^{-1}xy) = yx$ se, e somente se, $xy = yx$.

(ii) $(x,y)^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = (y,x)$.

(iii)

$$\begin{aligned}(x,z)^y(y,z) &= y^{-1}(x,z)yy^{-1}z^{-1}yz = y^{-1}(x,z)z^{-1}yz = y^{-1}x^{-1}z^{-1}xzz^{-1}yz\\ &= y^{-1}x^{-1}z^{-1}(xy)z = (xy)^{-1}z^{-1}(xy)z\\ &= (xy,z).\end{aligned}$$

$$\begin{aligned}(x,z)((x,z),y)(y,z) &= x^{-1}z^{-1}xz((z,x)y^{-1}(x,z)y)y^{-1}z^{-1}yz\\ &= x^{-1}z^{-1}xzz^{-1}x^{-1}zxy^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz\\ &= y^{-1}x^{-1}z^{-1}xyz = (xy)^{-1}z^{-1}xyz\\ &= (xy,z).\end{aligned}$$

(iv)

$$\begin{aligned}(x,z)(x,y)^z &= x^{-1}z^{-1}xzz^{-1}x^{-1}y^{-1}xyz = x^{-1}z^{-1}y^{-1}xyz\\ &= x^{-1}(yz)^{-1}x(yz)\\ &= (x,yz).\end{aligned}$$

$$\begin{aligned}(x,z)(x,y)((x,y),z) &= x^{-1}z^{-1}xzx^{-1}y^{-1}xy(y,x)z^{-1}(x,y)z\\ &= x^{-1}z^{-1}xzx^{-1}y^{-1}xyy^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz = x^{-1}z^{-1}y^{-1}xyz\\ &= (x,yz).\end{aligned}$$

(v)

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

(vi)

$$\begin{aligned}(x,z)^{(x,y)}(x,y,z) &= (y,x)(x,z)(x,y)((x,y),z)\\ &= y^{-1}x^{-1}yxx^{-1}z^{-1}xzx^{-1}y^{-1}xy(y,x)z^{-1}(x,y)z\\ &= y^{-1}x^{-1}yxx^{-1}z^{-1}xzx^{-1}y^{-1}xyy^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz\\ &= y^{-1}x^{-1}yz^{-1}y^{-1}xyz = (x^y)^{-1}z^{-1}x^yz\\ &= (x^y,z).\end{aligned}$$

(vii)

$$\begin{aligned}
(x^y,t)^{(x^y,z)}(x^y,z,t) &= (x^y,z)^{-1}(x^y,t)(x^y,z)((x^y,z),t)\\
&= (y^{-1}xy,z)^{-1}(y^{-1}xy,t)(y^{-1}xy,z)((y^{-1}xy,z),t)\\
&= z^{-1}y^{-1}x^{-1}yzt^{-1}z^{-1}y^{-1}xyzt\\
&= (yz)^{-1}x^{-1}(yz)t^{-1}(yz)^{-1}x(yz)t = (x^{(yz)})^{-1}t^{-1}x^{yz}t\\
&= (x^{yz},t).
\end{aligned}$$

■

2.1.1 Subgrupo Comutador

Relembremos que se X é um subconjunto de um grupo G, então o *subgrupo gerado* por X, que denotamos por $\langle X\rangle$, é o menor subgrupo de G que contém X ou, equivalentemente, a interseção de todos os subgrupos de G que contém X. De acordo com [16, Teorema 2.7], se $X = \varnothing$, então $\langle X\rangle = \{1_G\}$, caso contrário, o subgrupo $\langle X\rangle$ é formado por todos os elementos de G que são produtos finitos $x_1^{\xi_1}\cdots x_k^{\xi_k}$, onde $x_i \in X$ e $\xi_i = \pm 1$ para qualquer $1 \le i \le k$.

O *subgrupo comutador* ou *subgrupo derivado* de G, que denotamos por G', é o subgrupo gerado pelo conjunto de todos os comutadores de G. Conforme [16, Teorema 2.23], G' é um subgrupo normal de G, e se $H \trianglelefteq G$, então G/H é abeliano se, e somente se, $G' \le H$. Então, em particular, G/G' é abeliano. Além disso, é fácil ver que, como consequência do item (i) do Lema 2.1.2, G é abeliano se, e somente se, $G' = \{1_G\}$.

2.2 Grupos C, LC e SLC

Começamos esta seção com dois exemplos. Em cada um deles, apresentamos um grupo bastante conhecido e a sua respectiva tábua de multiplicação.

Exemplo 2.2.1 [4, Exemplo 2.5] Grupo dos quatérnios de ordem 8, $Q_8 = \langle i,j : i^4 = 1, i^2 = j^2, ij = ji^{-1}\rangle$.

$\cdot$	1	i	i^2	i^3	j	ij	i^2j	i^3j
1	1	i	i^2	i^3	j	ij	i^2j	i^3j
i	i	i^2	i^3	1	ij	i^2j	i^3j	j
i^2	i^2	i^3	1	i	i^2j	i^3j	j	ij
i^3	i^3	1	i	i^2	i^3j	j	ij	i^2j
j	j	i^3j	i^2j	ij	i^2	i	1	i^3
ij	ij	j	i^3j	i^2j	i^3	i^2	i	1
i^2j	i^2j	ij	j	i^3j	1	i^3	i^2	i
i^3j	i^3j	i^2j	ij	j	i	1	i^3	i^2

Tabela 2.1: Tábua de multiplicação do grupo dos quatérnios Q_8.

Exemplo 2.2.2 [4, Exemplo 2.6] Grupo diedral de ordem 8, $D_4 = \langle \theta, r : \theta^4 = r^2 = 1, r^{-1}\theta r = \theta^{-1} \rangle$.

$\cdot$	1	θ	θ^2	θ^3	r	$r\theta$	$r\theta^2$	$r\theta^3$
1	1	θ	θ^2	θ^3	r	$r\theta$	$r\theta^2$	$r\theta^3$
θ	θ	θ^2	θ^3	1	$r\theta^3$	r	$r\theta$	$r\theta^2$
θ^2	θ^2	θ^3	1	θ	$r\theta^2$	$r\theta^3$	r	$r\theta$
θ^3	θ^3	1	θ	θ^2	$r\theta$	$r\theta^2$	$r\theta^3$	r
r	r	$r\theta$	$r\theta^2$	$r\theta^3$	1	θ	θ^2	θ^3
$r\theta$	$r\theta$	$r\theta^2$	$r\theta^3$	r	θ^3	1	θ	θ^2
$r\theta^2$	$r\theta^2$	$r\theta^3$	r	$r\theta$	θ^2	θ^3	1	θ
$r\theta^3$	$r\theta^3$	r	$r\theta$	$r\theta^2$	θ	θ^2	θ^3	1

Tabela 2.2: Tábua de multiplicação do grupo diedral D_4.

Estamos interessados em conhecer os comutadores destes dois grupos. De acordo com as suas tábuas de multiplicação, é possível ver que, além de seus elementos neutros, os demais comutadores dos grupos Q_8 e D_4 são, respectivamente, os elementos i^2 e θ^2, apenas. Sendo assim, denotando como *não trivial* qualquer elemento de um grupo G que é diferente do seu elemento neutro, estamos motivados a dar a próxima definição.

Definição 2.2.3 Dizemos que um grupo não abeliano G possui um único comutador não trivial s, se para quaisquer $g, h \in G$ tais que $gh \neq hg$, se verifica que $(g, h) = s$.

Se G é um grupo que possui um único comutador não trivial s, então conforme o item (ii) do Lema 2.1.2, temos que $s = s^{-1}$ e, equivalentemente, $s^2 = 1_G$. Desta maneira, de acordo com a definição de subgrupo comutador, temos que $G' = \{1_G, s\}$. Sendo assim, $Q_8' = \{1, i^2\}$ e $D_4' = \{1, \theta^2\}$.

As tabelas 2.1 e 2.2 também nos mostram que $Z(Q_8) = \{1, i^2\}$ e $Z(D_4) = \{1, \theta^2\}$, isto é, em Q_8 e D_4 os seus subgrupos comutadores coincidem com os seus centros o que, em particular, nos diz que seus (únicos) comutadores não triviais pertencem ao centro de G, isto é, são elementos *centrais*. Sabendo que o centro $Z(G)$ é um subgrupo normal de G, então, de acordo com o que comentamos na Subseção 2.1.1, os grupos $Q_8/Z(Q_8)$ e $D_4/Z(D_4)$ são abelianos. Este fato é generalizado na próxima proposição.

Proposição 2.2.4 Suponhamos que G seja um grupo que contém um único comutador não trivial s. Então s é um elemento central de G. Em particular $G/Z(G)$ é um grupo abeliano.
Demonstração: Suponhamos que exista $g \in G$ tal que $gs \neq sg$, então $s = (s, g) = s^{-1}g^{-1}sg$ o que, de acordo com o item (ii) do Lema 2.1.2, implica que $sg = g$ o que é absurdo se $s \neq 1_G$.

Consequentemente, $G' \leq Z(G)$ e, portanto, $G/Z(G)$ é um grupo abeliano. ■

Mais adiante veremos que se G é um grupo que contém um único comutador não trivial, então possui outras propriedades que também implicam em $G/Z(G)$ ser abeliano.

Queremos prosseguir dando mais uma definição, entretanto, faremos antes uma observação que é motivada por uma propriedade satisfeita pelos quadrados dos elementos de Q_8 e D_4.

Observação 2.2.5 As tábuas de multiplicação dos grupos Q_8 e D_4 nos mostram que seus quadrados são centrais. Afirmamos que se G é um grupo não abeliano cujo os quadrados são centrais, então os comutadores são centrais e possuem ordem 2. Com efeito, $(g,h) = g^{-1}h^{-1}gh = g^{-2}(gh^{-1})^2h^2$ para quaisquer g, h pertencentes a G e, desta forma, se os quadrados são centrais, então os comutadores são centrais. Agora, seja $s = (g,h) \neq 1_G$. Então $h^2g = gh^2 = (gh)h = (hgs)h = s((hg)h) = s(h(gh)) = s(h(hgs)) = s^2h^2g$, o que nos permite concluir que $s^2 = 1_G$.

Definição 2.2.6 Dizemos que um grupo não abeliano G possui a propriedade C, ou é um *grupo* C, se para quaisquer g, h, k pertencentes a G tais que $(g,h) \neq 1_G$ e $(g,k) \neq 1_G$, valer que $(g,h) = (g,k)$.

É imediato que um grupo que possui um único comutador não trivial satisfaz a propriedade C e, sendo assim, os Exemplos 2.2.1 e 2.2.2 garantem a existência de grupos com tal propriedade. A próxima proposição mostrará que, reciprocamente, se G é um grupo C, então G possui um único comutador não trivial. Antes de enunciar esta proposição iremos mostrar um lema.

Lema 2.2.7 Se G é um grupo C, então quadrados são centrais e comutadores não triviais são centrais e possuem ordem 2.
Demonstração: Suponhamos que G seja um grupo C e sejam g e h elementos arbitrários de G. Se $gh = hg$, então $g^2h = ggh = ghg = hg^2$, isto é, $(h,g^2) = 1_G$. Assim, se $(h,g^2) \neq 1_G$, então $(h,g) \neq 1_G$, o que implica que $(h,g^2) = (h,g)$, isto é, $h^{-1}g^{-2}hg^2 = h^{-1}g^{-1}hg$, ou, equivalentemente $hg = gh$, o que é uma contradição. Portanto, quadrados são centrais e, conforme a Observação 2.2.5, comutadores são centrais e possuem ordem 2. ■

Proposição 2.2.8 Um grupo G tem a propriedade C se, e somente se, possui um único comutador não trivial.
Demonstração: Suponhamos que G seja um grupo C e consideremos g, h, x, y pertencentes a G tais que os comutadores (g,h) e (x,y) sejam ambos não triviais. Vamos mostrar que $(g,h) = (x,y)$, e faremos isso analisando cada uma das seguintes possibilidades:

(a) $(g,x) \neq 1_G$ (b) $(g,y) \neq 1_G$ (c) $(h,x) \neq 1_G$ (d) $(h,y) \neq 1_G$ (e) g e h comutam com x e y

(a) Se (g,x) e (g,h) são ambos não triviais, então $(g,x) = (g,h)$. Além disso, sabemos do lema anterior que comutadores não triviais possuem ordem 2, então $(g,x) = (x,g)$. Deste modo, sendo $(x,y) \neq 1_G$ e $(x,g) \neq 1_G$, temos $(x,g) = (x,y)$. Portanto, $(g,h) = (g,x) = (x,g) = (x,y)$.

(b) A princípio já sabemos que $(g,h) = (g,y)$ e que como consequência do lema anterior $(g,y) = (y,g)$ e $(x,y) = (y,x)$. Sendo assim $(y,g) = (y,x)$ e, portanto, $(g,h) = (g,y) = (y,g)^{-1} = (y,x)^{-1} = (x,y)$.

(c) Sabemos que $(g,h) = (h,g)$ e, sendo assim$(g,h) = (h,x)$. Além disso, $(h,x) = (x,h) = (x,y)$. Então $(g,h) = (h,x) = (x,h) = (x,y)$.

(d) Novamente, sabendo que $(g,h) = (h,g)$, temos $(g,h) = (h,y)$. Também $(h,y) = (y,h) = (y,x) = (x,y)$. Então, $(g,h) = (x,y)$.

(e) Por último, suponhamos que g e h comutam com x e y. Então, afirmamos que $(g,hx) \neq 1_G$ e $(hx,y) \neq 1_G$. Com efeito, se $gh \neq hg$, então $(xg)h \neq (xh)g$ e, como g e h comutam com x, temos

$g(hx) \neq (hx)g$ e, portanto, $(g, hx) \neq 1$. Sabemos também que $xy \neq yx$, então $(hx)y \neq (hy)x$ e, como x e y comutam com h, segue que $(hx)y \neq y(hx)$ e, portanto, $(hx, y) \neq 1_G$.

Então $(g, h) = (g, hx) = (hx, g) = (hx, y) = (y, hx) = (y, x) = (x, y)$.

Concluímos que G possui um único comutador não trivial. ■

Observação 2.2.9 Vamos voltar rapidamente à Proposição 2.2.4. Nesta proposição, mostramos que se G é um grupo que possui um único comutador não trivial então $G/Z(G)$ é abeliano. Agora, olhando novamente para a Proposição 2.2.8 e para o Lema 2.2.7, podemos concluir que se G possui um único comutador não trivial, os quadrados são centrais. Veja que qualquer grupo G cujos quadrados são centrais possui a propriedade de $G/Z(G)$ ser abeliano. Por um lado, isto ocorre devido ao fato de seus comutadores serem centrais, isto é, $G' \leq Z(G)$ e, por outro lado, ocorre porque qualquer elemento pertencente a $G/Z(G)$ possui ordem 2.

Vamos prosseguir falando de mais um fato que pode ser percebido fazendo a análise das tábuas de Q_8 e D_4. Examinando-as, notamos que nestes dois grupos, para quaisquer elementos g e h tais que $gh = hg$, se verifica que g ou h ou gh é um elemento central. Este fato nos motiva a dar mais uma definição.

Definição 2.2.10 Dizemos que um grupo não abeliano G tem a propriedade da comutatividade limitada, ou é um grupo LC (do inglês "lack of commutativity"), se para quaisquer g, h pertencentes a G tais que $gh = hg$, valer que $g \in Z(G)$ ou $h \in Z(G)$ ou $gh \in Z(G)$.

Se G é um grupo LC, então por definição os quadrados são centrais e, conforme vimos na Observação 2.2.9, o quociente $G/Z(G)$ é um grupo abeliano.

Antes de darmos a próxima (e principal) definição desta seção, é pertinente que estejamos seguros de que as propriedades C e LC não são equivalentes. Vamos começar com o seguinte exemplo:

Exemplo 2.2.11 [5, Ex. 3.2, p.94] Seja o grupo $G = \langle x_1, x_2, x_3 : x_i^4 = (x_i^2, x_j) = ((x_i, x_j), x_k) = 1$, com i, j, k distintos$\rangle$. De acordo com a nossa referência, G é um grupo LC, entretanto possui três comutadores não triviais (x_1, x_2), (x_1, x_3) e (x_2, x_3).

O Exemplo 2.2.11 nos mostra que a propriedade LC não implica na propriedade C. Entretanto, ainda podemos nos perguntar: se um grupo possui um único comutador não trivial, então será necessariamente um grupo LC? O próximo exemplo mostra que não.

Exemplo 2.2.12 [18, TYPE 32/43 $\Gamma_5 a_2$] Seja o grupo $G = \langle 2, 3, 9, 17 : 2^2 = 3^4 = 9^2 = 1, 17^2 = 3^2, 2.9 = 9.3^2.2, 3.9 = 9.3^{-1}, 2.17 = 17.3^2.2\rangle$. Analisando a tábua de multiplicação deste grupo (Tabela 2.4), que se encontra na página 18, podemos ver que 5 é o seu único comutador não trivial e que $Z(G) = \{1, 5\}$. Entretanto nota-se que $32.27 = 27.32 = 2$, o que nos mostra que G não é um grupo LC.

Os grupos Q_8 e D_4 que nos motivaram a dar as definições de grupo C e LC, finalmente nos motivam a enunciar a próxima, e mais importante, definição desta seção.

Definição 2.2.13 (Grupo SLC) Dizemos que um grupo não abeliano G possui a propriedade SLC, ou é um grupo SLC se é, simultaneamente, um grupo C e LC.

Em outras palavras, podemos dizer que um grupo SLC é um grupo que possui a propriedade LC e um único comutador não trivial.

A próxima etapa será estudar a classificação dos grupos SLC. Antes disso, vamos fazer uma observação a respeito dos grupos C. Vejamos que os grupos que foram mostrados nos Exemplos 2.2.1, 2.2.2 e 2.2.12, que possuem um único comutador não trivial, são tais que $G' = Z(G)$. Entretanto, isto não se verifica sempre. O próximo exemplo mostra um grupo que possui um único comutador não trivial, mas que $G' \subsetneq Z(G)$.

Exemplo 2.2.14 [18, TYPE 16/9 $\Gamma_2 c_1$] Consideremos o grupo $G = \langle a, b, c : a^4 = b^2 = c^2 = 1,\ ab = ba,\ ac = ca^3b,\ bc = cb\rangle$, com a sua tábua de multiplicação mostrada logo abaixo.

$\cdot$	1	a	a^2	a^3	b	ab	a^2b	a^3b	c	ac	a^2c	a^3c	bc	abc	a^2bc	a^3bc
1	1	a	a^2	a^3	b	ab	a^2b	a^3b	c	ac	a^2c	a^3c	bc	abc	a^2bc	a^3bc
a	a	a^2	a^3	1	ab	a^2b	a^3b	b	ac	a^2c	a^3c	c	abc	a^2bc	a^3bc	bc
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab	a^2c	a^3c	c	ac	a^2bc	a^3bc	bc	abc
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b	a^3c	c	ac	a^2c	a^3bc	bc	abc	a^2bc
b	b	ab	a^2b	a^3b	1	a	a^2	a^3	bc	abc	a^2bc	a^3bc	c	ac	a^2c	a^3c
ab	ab	a^2b	a^3b	b	a	a^2	a^3	1	ac	a^2c	a^3c	c	abc	a^2bc	a^3bc	bc
a^2b	a^2b	a^3b	b	ab	a^2	a^3	1	a	a^2bc	a^3bc	bc	abc	a^2c	a^3c	c	ac
a^3b	a^3b	b	ab	a^2b	a^3	1	a	a^2	a^3bc	bc	abc	a^2bc	a^3c	c	ac	a^2c
c	c	a^2bc	a^2c	abc	bc	a^3c	a^2bc	ac	1	a^3b	a^2	ab	b	a^3	a^2b	a
ac	ac	bc	a^3c	a^2bc	abc	c	a^3bc	a^2c	a	b	a^3	a^2b	ab	1	a^3b	a^2
a^2c	a^2c	abc	c	a^3bc	a^2bc	ac	bc	a^3c	a^2	ab	1	a^3b	a^2b	a	b	a^3
a^3c	a^3c	a^2bc	ac	bc	a^3bc	a^2c	abc	c	a^3	a^2b	a	b	a^3b	a^2	ab	1
bc	bc	a^3c	a^2bc	ac	c	a^3bc	a^2c	abc	b	a^3	a^2b	a	1	a^3b	a^2	ab
abc	abc	c	a^3bc	a^2c	ac	bc	a^3c	a^2bc	ab	1	a^3b	a^2	a	b	a^3	a^2b
a^2bc	a^2bc	ac	bc	a^3c	a^2c	abc	c	a^3bc	a^2b	a	b	a^3	a^2	ab	1	a^3b
a^3bc	a^3bc	a^2c	abc	c	a^3c	a^2bc	ac	bc	a^3b	a^2	ab	1	a^3	a^2b	a	b

Tabela 2.3: Tábua de multiplicação de $G = \langle a, b, c : a^4 = b^2 = c^2 = 1,\ ab = ba,\ ac = ca^3b,\ bc = cb\rangle$..

É possível constatar que $(x, a) = (x, a^3) = (x, ab) = (x, a^3b) = a^2b$ onde $x \in \{c,\ ac,\ a^2c,\ a^3c,\ bc,\ abc, a^2bc,\ a^3bc\}$, e os demais comutadores são triviais; portanto, a^2b é o único comutador não trivial de G. Além disso é fácil observar que $Z(G) = \{1, a^2, b, a^2b\}$, isto é $G' \subsetneq Z(G)$.

Podemos verificar também que G é um grupo LC. De fato, sejam a, a^3, ab, a^3b, c, ac, a^2c, a^3c, bc, abc, a^2bc, $a^3bc \in G\backslash Z(G)$; de acordo com a Tabela 2.3, temos que $a(ab) = (ab)a = a^2b$, $a(a^3b) = (a^3b)a = b$, $a^3(ab) = (ab)a^3 = b$, $a^3(a^3b) = (a^3b)a^3 = a^2b$, $ab(a^3b) = (a^3b)ab = 1$, $c(a^2c) = (a^2c)c = a^2$, $c(bc) = (bc)c = b$, $c(a^2bc) = (a^2bc)c = a^2b$, $(ac)(a^3c) = (a^3c)(ac) = a^2b$, $(ac)(abc) = (abc)(ac) = 1$, $(ac)(a^3bc) = (a^3bc)(ac) = a^2$, $(a^2c)(bc) = (bc)(a^2c) = a^2b$, $a^2c(a^2bc) = (a^2bc)(a^2c) = b$, $(a^3c)(abc) = (abc)(a^3c) = a^2$, $(a^3c)(a^3bc) = (a^3bc)(a^3c) = 1$, $(bc)(a^2bc) = (a^2bc)(bc) = a^2$, $(abc)(a^3bc) = (a^3bc)(abc) = a^2b$. Estas multiplicações nos mostram que dados dois elementos g e h não centrais de G, se $gh = hg$, então gh é central. Portanto G é um grupo SLC.

2.2.1 Classificação dos Grupos SLC

É sempre pertinente conhecer, claro, quando isto é possível, a classificação dos grupos com os quais estamos trabalhando. Em todos os exemplos que foram dados em que os grupos possuem a propriedade SLC, notamos imediatamente que $|G/Z(G)| = 4$. Também é possível provar que $Q_8/Z(Q_8) = \{\overline{1}, \overline{i}, \overline{j}, \overline{ij}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ e $D_4/Z(D_4) = \{\overline{e}, \overline{\theta}, \overline{r}, \overline{r\theta}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Este fato nos induz a fazer algumas perguntas.

Será que todo grupo G que possui a propriedade SLC satisfaz $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$? Por outro lado, será que se G satisfaz $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ então é um grupo SLC?

A resposta é positiva para as duas perguntas e o próximo teorema prova isto, ou seja, faz a classificação dos grupos SLC.

Vamos antes relembrar uma definição.

Definição 2.2.15 Seja p um número primo. Dizemos que um grupo G é um *p-grupo abeliano elementar* se G é abeliano e qualquer $g \in G$ possui ordem p.

Desse modo, se G é um grupo C ou LC, então de acordo com a Observação 2.2.9, $G/Z(G)$ é um 2-grupo abeliano elementar.

Teorema 2.2.16 [5, Proposição 3.6, p. 98] Um grupo não abeliano G possui a propriedade SLC se, e somente se, $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Demonstração: Suponhamos que G seja um grupo SLC. Desse modo, como já comentamos, $G/Z(G)$ é um 2 - grupo abeliano elementar. Assim, pelo Teorema Fundamental dos Grupos Abelianos Finitos/Finitamente Gerados, $G/Z(G) \cong \langle\overline{g_1}\rangle \times \langle\overline{g_2}\rangle \times ... \times \langle\overline{g_n}\rangle \times ...$, em que cada $\langle\overline{g_i}\rangle$ é uma cópia de $\mathbb{Z}_2$ e $\overline{g_i} \neq \overline{g_j}$ sempre que $i \neq j$. Queremos mostrar que $n = 2$. Para isso, vamos supor que $G/Z(G)$ contenha $\langle\overline{g_1}\rangle \times \langle\overline{g_2}\rangle \times \langle\overline{g_3}\rangle$, onde $\overline{g_1}, \overline{g_2}, \overline{g_3}$ são distintos e $g_1, g_2, g_3 \notin Z(G)$.

Afirmamos que os elementos g_1, g_2, g_3 não podem, dois a dois, comutarem. Com efeito, sem perda de generalidade, se $g_1g_2 = g_2g_1$, uma vez que $g_1 \notin Z(G)$, $g_2 \notin Z(G)$ e G é um grupo LC, podemos concluir que $g_1g_2 \in Z(G)$, isto é, $\overline{g_1g_2} = \overline{1_G} = \overline{g_1}^2$ e consequentemente, $\overline{g_1} = \overline{g_2}$ o que é uma contradição.

Além disso, de acordo com o item (iii) do Lema 2.1.2, temos que $(g_1g_2, g_3) = (g_1, g_3)^{g_2}(g_2, g_3) = (g_1, g_3)(g_2, g_3) = s^2 = 1_G$, pois sabemos que os comutadores são centrais.

Consequentemente, $g_1g_2 \in Z(G)$ ou $g_3 \in Z(G)$ ou $g_1g_2g_3 \in Z(G)$. Entretanto isto não ocorre. Já sabemos que $g_3 \notin Z(G)$. Se $g_1g_2 \in Z(G)$, então $g_1g_2g_1 = g_1g_1g_2$, o que implicaria que g_1 comutaria com g_2, o que não ocorre. Finalmente, se $g_1g_2g_3 \in Z(G)$, então $\overline{g_1g_2g_3} = \overline{1_G}$. Assim, $\overline{g_1g_2g_3^2} = \overline{g_3}$, o que é uma contradição. Portanto, podemos concluir que G contém no máximo duas cópias de $\mathbb{Z}_2$, isto é, $G/Z(G) \cong \mathbb{Z}_2$ ou $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Se $G/Z(G)$ é isomorfo a Z_2, então $G/Z(G)$ é cíclico, o que implica que G seria abeliano. Logo, $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Reciprocamente, suponhamos que $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \langle\overline{g_1}\rangle \times \langle\overline{g_2}\rangle$, onde $g_1, g_2 \in G$ são tais que $g_1g_2 \neq g_2g_1$. Inicialmente, vamos provar que G é um grupo LC. Afirmamos que se $x, y \notin Z(G)$, então $xy = yx$ se, e somente se, $\overline{x} = \overline{y}$. Com efeito, se $\overline{x} = \overline{y}$, então $xy^{-1} \in Z(G)$ e, consequentemente, $(xy) = (xy^{-1})yy = y(xy^{-1})y = yx$. Por outro lado, suponhamos por absurdo que $x, y \in G$ são tais que $xy = yx$ mas $\overline{x} \neq \overline{y}$.

É suficiente analisar os seguintes casos:

$$\text{(I)} \quad \overline{x} = \overline{g_1} \text{ e } \overline{y} = \overline{g_2} \qquad \text{(II)} \ \overline{x} = \overline{g_1} \text{ e } \overline{y} = \overline{g_1g_2}$$

Se valer (I), então $xg_1^{-1} = z_1$ e $yg_2^{-1} = z_2$ para alguns $z_1, z_2 \in Z(G)$. Desse modo, $z_1g_1z_2g_2 = xy = yx = z_2g_2z_1g_1$, o que implica que $g_1g_2 = g_2g_1$, pois z_1 e z_2 são elementos centrais, o que é um absurdo.

Já se ocorrer (II), tem-se que $xg_1^{-1} = z_1$ e $yg_2^{-1}g_1^1 = z_2$, para alguns $z_1, z_2 \in Z(G)$. Neste caso, $z_1g_1z_2g_1g_2 = xy = yx = z_2g_1g_2z_1g_1$, de onde decorre que $g_1g_2 = g_2g_1$ devido a centralidade dos elementos z_1 e z_2; e novamente chegamos a uma contradição.

Assim, como $G/Z(G) = \langle\overline{g_1}\rangle \times \langle\overline{g_2}\rangle$, se $xy = yx$, $x \notin Z(G)$ e $y \notin Z(G)$, então $\overline{x} = \overline{y} = \overline{g_1}$ ou $\overline{x} = \overline{y} = \overline{g_2}$, o que implica que $\overline{xy} = \overline{1_G}$, pois $\overline{g_1}^2 = \overline{g_2}^2 = \overline{1_G}$.

Logo, $xy \in Z(G)$ e podemos concluir que G é um grupo LC.

A seguir, vamos verificar que G também é um grupo C. Para isso, seja $(g_1, g_2) = s \neq 1_G$. Mostremos que para quaisquer $x, y \in G$ tais que $xy \neq yx$, tem-se $(x, y) = s$.

Note que se x e y não comutam, então x e y não podem pertencer concomitantemente a $\overline{g_1}$, $\overline{g_2}$, $\overline{g_1g_2}$. Desse modo, é suficiente analisar os seguintes casos:

(a) $x = z_1g_1$ e $y = z_2g_2$

(b) $x = z_1g_1$ e $y = z_3g_1g_2$, onde $z_1, z_2, z_3 \in Z(G)$.

Se $x = z_1g_1$ e $y = z_2g_2$, então pelos itens (iii) e (iv) do Lema 2.1.2 temos $(x, y) = (z_1g_1, z_2g_2) = (z_1, z_2g_2)^{g_1}(g_1, z_2g_2) = (g_1, z_2g_2) = (g_1, g_2)(g_1, z_2)^{g_2} = (g_1, g_2) = s$.

Se ocorrer (b), então $(x, y) = (z_1g_1, z_3g_1g_2) = (z_1, z_3g_1g_2)^{g_1}(g_1, z_3g_1g_2) = (g_1, g_2)(g_1, z_3g_1)^{g_2} = (g_1, g_2)g_2^{-1}(g_1, g_1)(g_1z_3)g_2 = (g_1, g_2) = s$.

Logo, G possui um único comutador não trivial e, portanto, é um grupo SLC. ■

Agora que conhecemos esta classificação, podemos, por exemplo, constatar que o grupo do Exemplo 2.2.12 é C mas não é LC, sabendo apenas que $|G'| = |Z(G)| = 2$.

2.2.2 Caracterização dos grupos SLC através de uma involução

Queremos apresentar uma caracterização dos grupos SLC por meio de uma involução. Vamos começar chamando a atenção para certos fatos que se verificam em alguns dos grupos que apresentamos em exemplos anteriores.

Consideremos novamente o grupo dos quaternios $Q_8 = \{1, i, i^2, i^3, j, ij, i^2j, i^3j\}$, e seja a sua involução canônica $g \mapsto g^{-1}$. De acordo com a sua tábua de multiplicação (Tabela 2.1), temos que $(i^2)^{-1} = i^2$ e $(i^r)^{-1} = i^2i^r$, onde $r \in \{1, 3\}$, e também que $(i^rj)^{-1} = i^2(i^rj)$, onde $r \in \{0, 1, 2, 3\}$. Sabendo que $Z(Q_8) = Q_8' = \{1, i^2\}$, vemos que $g^{-1} = g$ se $g \in Z(Q_8)$ e que $g^{-1} = sg$ se $g \notin Z(Q_8)$, onde s é igual a i^2, que é o único comutador não trivial de Q_8. Este fato a respeito de Q_8 nos motiva a ter uma ideia. Seja G um grupo não abeliano e que possui um único comutador não trivial s; definimos sobre G uma aplicação φ da seguinte maneira:

$$\varphi(g) = g \text{ se } g \in Z(G) \text{ e } \varphi(g) = sg, \text{ se } g \notin Z(G), \tag{2.1}$$

onde s é o único comutador não trivial de G.

A respeito da aplicação φ de G definida por (2.1), decorre do fato de s ser, de acordo com o Lema 2.2.7, um elemento central e de ordem 2, que $\varphi^2(g) = g$ para todo $g \in G$. Sendo assim, um questionamento que surge naturalmente é se φ é uma involução de G. Para verificar se isto é verdade, isto é, se vale que $\varphi(gh) = \varphi(h)\varphi(g)$ para quaisquer $g, h \in G$, vamos analisar certas possibilidades para a multiplicação entre elementos pertencentes a G. Antes de fazer isso, notemos que para todo $g \in G$, de acordo com o Lema 2.2.7, vale que $g^2 \in Z(G)$ e, desta forma, $\varphi(g^2) = g^2 = \varphi^2(g)$.

Primeiro, suponhamos que g e h não comutam, então temos que $gh \notin Z(G)$, pois, do contrário, teríamos $(gh)g = g(gh)$ o que implica que $gh = hg$ o que contradiz a hipótese a respeito de g e h. Desta forma, $\varphi(gh) = s(gh) = s(hgs) = shsg = \varphi(h)\varphi(g)$.

Agora, suponhamos que g e h comutam. Verifiquemos os seguintes casos:

(a) Se $g \in Z(G)$ e $h \in Z(G)$, então $gh \in Z(G)$. Assim $\varphi(gh) = gh = hg = \varphi(h)\varphi(g)$;

(b) $g \notin Z(G)$ e $h \in Z(G)$, então $gh \notin Z(G)$ e temos que $\varphi(gh) = sgh = hsg = \varphi(h)\varphi(g)$;

(c) $g \in Z(G)$ e $h \notin Z(G)$, segue que $gh \notin Z(G)$ e vale que $\varphi(gh) = sgh = shg = \varphi(h)\varphi(g)$.

Falta ver o caso em que g e h comutam e ambos não pertencem ao centro de G. Para estudarmos esta situação, vamos considerar o grupo $G = \langle 2,3,9,17 : 2^2 = 3^4 = 9^2 = 1, 17^2 = 3^2, 2.9 = 9.3^2.2, 3.9 = 9.3^{-1}, 2.17 = 17.3^2.2\rangle$ [18, TYPE 32/43 $\Gamma_5 a_2$] que já citamos no Exemplo 2.2.12 e cuja tábua de multiplicação é a Tabela 2.4. A respeito deste grupo, já sabemos que $Z(G) = G' = \{1,5\}$. Consideremos os elementos não centrais 3 e 4, que comutam. Temos que $\varphi(3.4) = \varphi(6) = 5.6 = 2$ e que $\varphi(4)\varphi(3) = (5.4)(5.3) = 8.7 = 6$, isto é, $\varphi(3.4) \neq \varphi(4)\varphi(3)$. Desta maneira, concluímos que para um grupo não comutativo G, possuir um único comutador não trivial s não implica que a aplicação definida em (2.1) seja uma involução de G.

Vamos inserir nesta discussão o grupo diedral $D_4 = \{1, \theta, \theta^2, \theta^3, r, r\theta, r\theta^2, r\theta^3\}$, para o qual já sabemos que $Z(D_4) = D_4' = \{1, \theta^2\}$. De acordo com a sua tábua que multiplicação (Tabela 2.2), temos que $r^{-1} = r$, o que nos mostra que no grupo dieldral de ordem 8, a involução canônica não satisfaz as condições descritas em (2.1). Entretanto, afirmamos que a aplicação definida por (2.1) é uma involução de D_4. Com efeito, seja $G \backslash Z(D_4) = \{\theta, \theta^3, r, r\theta, r\theta^2, r\theta^3\}$. De acordo com a tábua de multiplicação de D_4 (Tabela 2.2), temos que $\varphi(\theta) = \theta^3$, $\varphi(\theta^3) = \theta$, $\varphi(r) = r\theta^2$, $\varphi(r\theta) = r\theta^3$, $\varphi(r\theta^2) = r$ e $\varphi(r\theta^3) = r\theta$. Conforme mostramos acima, nos itens (a), (g) e (c), é suficiente aplicarmos φ em produtos do tipo gh onde $g \notin Z(G)$, $h \notin Z(G)$, e que satisfaçam $gh = hg$. Sendo assim, como $\varphi((r\theta^3)(r\theta)) = \varphi(\theta^2) = \theta^2 = (r\theta^3)(r\theta) = \varphi(r\theta)\varphi(r\theta^3)$ e $\varphi((r\theta^2)(r\theta)) = \varphi(\theta^2) = \theta^2 = (r\theta^2)(r\theta) = \varphi(r\theta)\varphi(r\theta^2)$, concluímos que a aplicação φ definida por (2.1) é uma involução de D_4.

Vimos que nos grupos SLC, Q_8 e D_4, a aplicação definida por (2.1) são involuções. Afirmamos que em todo grupo SLC, esta aplicação é uma involução. Com efeito, tomemos $g \notin Z(G)$ e $h \notin Z(G)$, então temos que $gh \in Z(G)$, pois G é um grupo LC. Desse modo, $\varphi(gh) = gh = s^2gh = s^2hg = (sh)(sg) = \varphi(h)\varphi(g)$.

Por último, mostremos que a involução de um grupo SLC definida por (2.1) satisfaz $h^{-1}gh \in \{g, \varphi(g)\}$ para quaisquer $g, h \in G$. Com efeito, se $g \in Z(G)$, então para qualquer $h \in G$ se verifica $h^{-1}gh = g$; se $g \notin Z(G)$, então para qualquer $h \in G$ que satisfaça $gh \neq hg$ temos que $h^{-1}gh = h^{-1}ghg^{-1}g = (h, g^{-1})g = sg = \varphi(g)$. Portanto $h^{-1}gh \in \{g, \varphi(g)\}$ para quaisquer $g, h \in G$.

Teorema 2.2.17 [5, Teorema 3.3, p. 95] Um grupo não abeliano G possui uma involução $g \mapsto g^*$ tal que $h^{-1}gh \in \{g, g^*\}$ para quaisquer $g, h \in G$ se, e somente se, G é um grupo SLC. Para tal grupo, esta involução é definida por:

$$g^* = \begin{cases} g, & \text{se} \quad g \in Z(G) \\ sg, & \text{se} \quad g \notin Z(G), \end{cases} \tag{2.2}$$

onde s é o único comutador não trivial de G.

Demonstração: Consideremos uma involução $g \mapsto g^*$ de G, tal que se verifique $h^{-1}gh \in \{g, g^*\}$ para quaisquer g, $h \in G$. Afirmamos que se g é fixo sobre a involução $*$, então g é central. Com efeito, se $g^* = g$, então, por suposição $h^{-1}gh = g$ para todo $h \in G$ e, portanto, g é central.

Prosseguindo, vamos mostrar que se g e h são dois elementos de G que não comutam, então se verifica que $g^{-1}g^* = h^{-1}h^*$. Primeiro, notemos que $(gg^*)^* = gg^*$, então de acordo com a afirmação que provamos no parágrafo anterior, temos que $gg^* \in Z(G)$ para qualquer $g \in G$ e, deste modo, $g(gg^*) = (gg^*)g$, isto é, para todo $g \in G$, g e g^* comutam.

Agora,sejam $g, h \in G$ tais que $gh \neq hg$, isto é, $g^{-1}hg \neq h$. Por suposição $g^{-1}hg = h^*$ e, portanto, $gh^* = hg$ (i). Notemos que o fato de g e h não comutarem implica que $h^{-1}g^*h = g$, pois, do contrário (isto é, se $h^{-1}g^*h = g^*$), teremos $g^*h = hg^*$ e, consequentemente, $ghg^* = gg^*h = hgg^*$ e, portanto, $gh = hg$, o que contradiz a hipótese sobre g e h. Concluímos que $hg = g^*h$ (ii). Comparando as igualdades (i) e (ii) obtemos $gh^* = g^*h$ e, multiplicando esta última igualdade por h^{-1} à direita e por g^{-1} à esquerda mostramos que $g^{-1}g^* = h^{-1}h^*$ sempre que g e h não comutam.

Afirmamos que $s = g^{-1}g^*$ é independente do elemento $g \notin Z(G)$. Com efeito, seja x um elemento não central de G. Se $xg \neq gx$ ou $xh \neq hx$ então $x^{-1}x^* = g^{-1}g^* = h^{-1}h^* = h^*h^{-1}$. Por outro lado, supondo que $xg = gx$ e $xh = hx$, temos em particular que $h^{-1}(gx)h = gx$ ou $h^{-1}(gx)h = (gx)^* = x^*g^* = g^*x^*$. Como também $h^{-1}(gx)h = (h^{-1}gh)(h^{-1}xh) = g^*x$, então $g = g^*$ ou $x = x^*$ o que contradiz a suposição de os elementos g e x não serem centrais.

Deste modo, se $gh \neq hg$, então $s = h^{-1}h^* = h^{-1}g^{-1}hg$ o que mostra que s é o único comutador não trivial de G. Além disso, $g^* = sg$

Sejam $g \in Z(G)$ e $h \notin Z(G)$, então $gh \notin Z(G)$. Desta maneira, $(sh)g^* = h^*g^* = (gh)^* = sgh = shg$, o que implica que $g^* = g$. Então, a involução $*$ é definida por (2.2)

Por último, para mostrar que G possui também a propriedade LC recordemos que s é um elemento central e de ordem 2 e daí supondo $g, h \notin Z(G)$ tais que $gh = hg$, então $(gh)^* = h^*g^* = shsg = hg = gh$, donde concluímos que gh é central.

Portanto o grupo G possui a propriedade SLC. ■

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15	18	17	20	19	22	21	24	23	26	25	28	27	30	29	32	31
3	3	4	5	6	7	8	1	2	11	12	13	14	15	16	9	10	19	20	21	22	23	24	17	18	27	28	29	30	31	32	25	26
4	4	3	6	5	8	7	2	1	12	11	14	13	16	15	10	9	20	19	22	21	24	23	18	17	28	27	30	29	32	31	26	25
5	5	6	7	8	1	2	3	4	13	14	15	16	9	10	11	12	21	22	23	24	17	18	19	20	29	30	31	32	25	26	27	28
6	6	5	8	7	2	1	4	3	14	13	16	15	10	9	12	11	22	21	22	24	23	18	17	20	19	30	29	32	31	26	28	27
7	7	8	1	2	3	4	5	6	15	16	9	10	11	12	13	14	23	24	17	18	19	20	21	22	31	32	25	26	27	28	29	30
8	8	7	2	1	4	3	6	5	16	15	10	9	12	11	14	13	24	23	18	17	20	19	22	21	32	31	26	25	28	27	30	29
9	9	14	15	12	13	10	11	16	1	6	7	4	5	2	3	8	25	30	31	28	29	26	27	32	17	22	23	20	21	18	19	24
10	10	13	16	11	14	9	12	15	2	5	8	6	6	1	4	7	26	29	32	27	30	25	28	31	18	21	24	19	22	17	20	23
11	11	16	9	14	15	12	13	10	3	8	1	6	7	4	5	2	27	32	25	30	31	28	29	26	18	24	17	22	23	20	21	18
12	12	15	10	13	16	11	14	9	4	7	2	5	8	3	6	1	28	31	26	29	32	27	30	25	20	23	18	21	24	19	22	17
13	13	10	11	16	9	14	15	12	5	2	3	8	1	6	7	4	29	26	27	32	25	30	31	28	21	18	19	24	17	22	23	20
14	14	9	12	15	10	13	16	11	6	1	4	7	2	5	8	3	30	25	28	31	26	29	32	27	22	17	20	23	18	21	24	19
15	15	12	13	10	11	16	9	14	7	4	5	2	3	8	1	6	31	28	29	26	27	32	25	30	23	20	21	18	19	24	17	22
16	16	11	14	9	12	15	10	13	8	3	6	1	4	7	2	5	32	27	30	25	28	31	26	29	24	19	22	17	20	23	18	21
17	17	22	19	24	21	18	23	20	25	30	27	32	29	26	31	28	5	2	7	4	1	6	3	8	13	10	15	12	9	14	11	16
18	18	21	20	23	22	17	24	19	26	29	28	31	30	25	32	27	6	1	8	3	2	5	4	7	14	9	16	11	10	13	12	15
19	19	24	21	18	23	20	17	22	27	32	29	26	31	28	25	20	7	4	1	6	3	8	5	2	15	12	9	14	11	16	13	10
20	20	23	22	17	24	19	18	21	28	31	30	25	32	27	26	29	8	3	2	5	4	7	6	1	16	11	10	17	12	15	14	9
21	21	18	23	20	17	22	19	24	29	26	31	28	25	30	27	32	1	6	3	8	5	2	7	4	9	14	11	16	13	10	15	12
22	22	17	24	19	18	21	20	23	30	25	32	27	26	29	28	31	2	5	4	7	6	1	8	3	10	13	12	15	14	9	16	11
23	23	20	17	22	19	24	21	18	31	28	25	30	27	32	29	26	3	8	5	2	7	4	1	6	11	16	13	10	15	12	9	14
24	24	19	18	21	20	23	22	17	32	27	26	29	28	31	30	25	4	7	6	1	8	3	2	5	12	15	14	9	16	11	10	13
25	25	26	31	32	29	30	27	28	17	18	23	24	21	22	19	20	13	14	11	12	9	10	15	16	5	6	3	4	1	2	7	8
26	26	25	32	31	30	29	28	27	18	17	24	23	22	21	20	19	14	13	12	11	10	9	16	15	6	5	4	3	2	1	8	7
27	27	28	25	26	31	32	29	30	19	20	17	18	23	24	21	22	15	16	13	14	11	12	9	10	7	8	5	6	3	4	1	2
28	28	27	26	25	32	31	30	29	20	19	18	17	24	23	22	21	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
29	29	30	27	28	25	26	31	32	21	22	19	20	17	18	23	24	9	10	15	16	13	14	11	12	1	2	7	8	5	6	3	4
30	30	29	28	27	26	25	32	31	22	21	20	19	18	17	24	23	10	9	16	15	14	13	12	11	2	1	8	7	6	5	4	3
31	31	32	29	30	27	28	25	26	23	24	21	22	19	20	17	18	11	12	9	10	15	16	13	14	3	4	1	2	7	8	5	6
32	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	12	11	10	9	16	15	14	13	4	3	2	1	8	7	6	5

Tabela 2.4: Tábua de multiplicação do grupo $G = \langle 2,3,9,17 : 2^2 = 3^4 = 9^2 = 1, 17^2 = 3^2, 2.9 = 9.3^2.2, 3.9 = 9.3^{-1}, 2.17 = 17.3^2.2\rangle$ [18, TYPE 32/43 $\Gamma_5 a_2$]

Capítulo 3

Involuções de RG e anticomutatividade em $(RG)^+$

Estudamos para escrever este capítulo, o artigo "Involutions and anticommutativity in group rings" [7] de autoria de E.G. Goodaire e C. P. Milies. Lembrando que o produto de Jordan $\circ$ em um anel de grupo RG é definido como $\alpha \circ \beta = \alpha\beta + \beta\alpha$, estudamos as condições necessárias e suficientes para que o produto de Jordan seja trivial em $(RG)^+$, isto é, para que se verifique $\alpha \circ \beta = \alpha\beta + \beta\alpha = 0$ para quaisquer $\alpha, \beta \in (RG)^+$.

3.1 O produto de Jordan trivial em RG

Proposição 3.1.1 O produto de Jordan é trivial em um anel de grupo RG se, e somente se, a característica de R é igual a 2 e G é abeliano.
Demonstração: Suponhamos que o produto de Jordan seja trivial em RG. Neste caso, em particular, $0 = 1 \circ 1 = 2$ e, portanto, a característica de R é igual a 2. Além disso, dados g e h elementos arbitrários de G, temos que $0 = g \circ h = gh + hg$ o que implica que $gh = -hg = hg$; consequentemente G é abeliano. Reciprocamente, se a característica de R é igual a 2, então quaisquer $g, h \in G$ e, consequentemente, $\alpha \circ \beta = 0$ para quaisquer $\alpha, \beta \in RG$. ■

3.2 O produto de Jordan trivial em $(RG)^+$

Daqui em diante vamos indicar a característica de um anel de coeficientes R por $\mathrm{car}(R)$. Desta forma, supondo que RG seja um anel de grupo tal que $\mathrm{car}(R) \neq 2$, teremos como consequência da Proposição 3.1.1 que existem $\alpha, \beta \in RG$ tais que $\alpha \circ \beta \neq 0$.

Vamos considerar uma involução de um anel de grupo RG como a que é dada pela Equação (1.1), e que foi construída no Exemplo 1.2.6. Isto já nos diz que devemos considerar o anel R como sendo comutativo e com elemento identidade 1. Estamos interessados em estudar o produto de Jordan trivial em $(RG)^+$. Geralmente, quando se estuda as propriedades de um certo subconjunto de um anel de grupo, é suficiente trabalhar com o seu conjunto gerador. Sendo assim, queremos encontrar o conjunto que gera $(RG)^+$.

É bem fácil notar que qualquer elemento $\alpha = \sum_{g \in G} \alpha_g (g + g^*)$ pertence a $(RG)^+$, isto é, o conjunto de RG que é gerado por $S = \{g + g^* : g \in G\}$ está contido em $(RG)^+$. Afirmamos que vale

a inclusão contrária. Com efeito, seja $\alpha = \sum_{g\in G} \alpha_g g$ um elemento fixo para a involução $*$ e seja $k \in \operatorname{supp}(\alpha)$. Se $k^* = k$, o coeficiente α_k de k em $\alpha^* = \sum_{g\in G} \alpha_g g^*$ é o mesmo que em $\alpha = \sum_{g\in G} \alpha_g g$. Por outro lado, se $k^* \neq k$, então existe $g \in \operatorname{supp}(\alpha)$ tal que $\alpha_k k = \alpha_g g^*$, o que implica que $g^* = k$ onde $k \neq g$ e $\alpha_k = \alpha_g$. Assim $\alpha_k k + \alpha_g g = \alpha_g g^* + \alpha_g g = \alpha_g(g^* + g)$.

Concluímos que $(RG)^+$ é gerado pelo conjunto $S = \{g + g^* : g \in G\}$ e podemos fazer a partição $S = S_1 \bigcup S_2$, onde $S_1 = \{g + g^* : g^* = g\}$ e $S_2 = \{g + g^* : g^* \neq g\}$.

Lema 3.2.1 Seja G um grupo com uma involução $g \mapsto g^*$ tal que os elementos da forma $g + g^*$, onde $g \in G$, anticomutam em um anel de grupo RG, cuja $\operatorname{car}(R) \neq 2$. Então, uma das seguintes condições se verifica:

(i) $\operatorname{car}(R) = 4$, $gg^* = g^*g$ e $g^2 = (g^*)^2$, para qualquer $g \in G$;

(ii) $\operatorname{car}(R) = 8$, G é abeliano e $g^* = g$, para qualquer $g \in G$.

Demonstração: Sabemos, através do item (i) da Proposição 1.2.2 , que vale a igualdade $1_G^* = 1_G$ e, sendo assim, $4 = (1_G + 1_G)(1_G + 1_G) = -(1_G + 1_G)(1_G + 1_G) = -4$ e, portanto, a característica de R é igual a 4 ou 8.

Se os elementos $g + g^*$ anticomutam em RG, então vale a igualdade

$$2g^2 + 2gg^* + 2g^*g + 2(g^*)^2 = 0 \tag{3.1}$$

para todo $g \in G$. Sendo assim, supondo que $\operatorname{car}(R) = 4$, então para qualquer $g \in G$ deve, necessariamente, se verificar uma das três possibilidades:

$$g^2 = gg^* \text{ e } (g^*)^2 = g^*g \qquad g^2 = g^*g \text{ e } (g^*)^2 = gg^* \qquad g^2 = (g^*)^2 \text{ e } g^*g = gg^*.$$

Como os dois primeiros casos implicam que $g^* = g$, concluímos que se $\operatorname{car}(R) = 4$, então $gg^* = g^*g$ e $g^2 = (g^*)^2$ para qualquer $g \in G$, e está provado o item (i).

Se $\operatorname{car}(R) = 8$, então de acordo com a equação (3.1) temos $2g^2 = 2gg^* = 2g^*g = 2(g^*)^2$. Neste caso, $g = g^*$ para qualquer $g \in G$, isto é, a involução $*$ fixa os elementos de G e, portanto, conforme a Observação 1.2.5, G é abeliano. Mostramos o item (ii). ■

Observação 3.2.2 (Recíproca do item (ii) do Lema 3.2.1) Sejam R um anel de característica 8 e G um grupo abeliano com uma involução $g \mapsto g^*$ que fixa todo elemento de G. Afirmamos que os elementos da forma $g + g^*$, onde $g \in G$, anticomutam em RG. Com efeito, se $\operatorname{car}(R) = 8$, G é abeliano e qualquer elemento de G é fixo sobre involução $*$, então $gh + g^*h + gh^* + g^*h^* + hg + h^*g + hg^* + h^*g^* = 8gh = 0$, para quaisquer g, h pertencentes a G.

Como

$$gh + g^*h + gh^* + g^*h^* + hg + h^*g + hg^* + h^*g^* = 0 \tag{3.2}$$

se, e somente se, $(g + g^*)(h + h^*) = -(h + h^*)(g + g^*)$, provamos a afirmação.

Podemos resumir a condição (ii) do Lema 3.2.1 e a Observação 3.2.2 na próxima proposição.

Proposição 3.2.3 Sejam R um anel de característica 8 e um grupo G com uma involução $g \mapsto g^*$. Então, os elementos da forma $g + g^*, g \in G$, anticomutam em RG se, e somente se, G é abeliano e $g^* = g$ para todo $g \in G$. ■

Agora, suponhamos que G é um grupo com uma involução $g \mapsto g^*$ e R é um anel de característica 4. Então, de acordo com o Proposição 3.1.1, o produto de Jordan não é trivial em RG. O próximo teorema caracteriza, para o caso em que $\mathrm{car}(R) = 4$, os grupos G tais que $(RG)^+$ seja anticomutativo.

Teorema 3.2.4 Seja G um grupo com uma involução $*$ e seja R um anel comutativo, com elemento identidade 1 e característica igual a 4. Então os elementos da forma $g + g^*$, onde $g \in G$, anticomutam em RG se, e somente se, verifica-se uma das seguintes condições:

(i) G é abeliano, existe $s \in G$ tal que $s^2 = 1_G$ e para qualquer $g \in G$, $g^* = g$ ou $g^* = sg$;

(ii) G é não abeliano com um único comutador não trivial s e para qualquer $g \in G$, $g^* = g$ ou $g^* = sg$.

Demonstração: Primeiramente mostraremos que os elementos da forma $g + g^*$, onde $g \in G$, anticomutam em RG se é válida alguma das condições (i) e (ii). Nos dois casos é suficiente mostrar a validade da equação (3.2).

Suponhamos que vale (i), então o primeiro membro da equação (3.2) pode ser reescrito como $2gh + 2g^*h + 2gh^* + 2g^*h^*$. Se g e h são fixados pela involução $*$, o resultado já está provado.

Vejamos as demais possibilidades:

- se $g^* = g$ e $h^* = sh$ ou, se $g^* = sg$ e $h^* = h$, então $2gh + 2g^*h + 2gh^* + 2g^*h^* = 2gh + 2gh + 2sgh + 2sgh = 4gh + 4sgh = 0$;
- se $g^* = sg$ e $h^* = sh$, então $2gh + 2g^*h + 2gh^* + 2g^*h^* = 2gh + 2sgh + 2sgh + 2gh = 4gh + 4sgh = 0$.

Assumindo que (ii) é satisfeita, de acordo com a Proposição 2.2.8, G é um grupo C e, portanto, pelo Lema 2.2.7, seu único comutador não trivial s é um elemento central e de ordem 2. Então, como fizemos no caso anterior, vamos sempre tomar o primeiro membro da equação (3.2) e analisar cada possibilidade para a involução $*$ sobre g e h.

- se $g^* = g$ e $h^* = h$, então $gh + g^*h + gh^* + g^*h^* + hg + h^*g + hg^* + h^*g^* = 4gh + 4hg = 0$;
- se $g^* = sg$ e $h^* = h$ ou, se $g^* = g$ e $h^* = sg$, então $gh + g^*h + gh^* + g^*h^* + hg + h^*g + hg^* + h^*g^* = 2gh + 2sgh + 2hg + 2shg$. Se $gh = hg$ então $2gh + 2sgh + 2hg + 2shg = 4gh + 4sgh = 0$. Por outro lado, se $gh \neq hg$ sabemos que $hg = sgh$, o que implica que $2gh + 2sgh + 2hg + 2shg = 4gh + 4sgh = 0$;
- se $g^* = sg$ e $h^* = sh$ então $gh + g^*h + gh^* + g^*h^* + hg + h^*g + hg^* + h^*g^* = gh + sgh + sgh + gh + hg + shg + shg + hg = 2gh + 2hg + 2sgh + 2shg = 4gh + 4sgh = 0$.

Mostramos que em ambas as condições, os elementos da forma $g + g^*$, onde $g \in G$, anticomutam em RG.

Reciprocamente, suponhamos que os elementos da forma $g + g^*$, onde $g \in G$, anticomutam em RG. Vamos assumir primeiro que G é um grupo abeliano. Então a equação (3.2) pode ser reescrita como $2gh + 2g^*h + 2gh^* + 2g^*h^* = 0$. Sendo assim, se $g^* \neq g$ e $h^* \neq h$, temos $gh \neq g^*h$ e $gh \neq gh^*$, o que implica que $gh = g^*h^*$ e $g^*h = gh^*$. Multiplicando a última igualdade por $g^{-1}h^{-1}$, podemos concluir que para quaisquer g e h tais que $g^* \neq g$ e $h^* \neq h$, é válida a igualdade

$g^*g^{-1} = h^*h^{-1}$, isto é, existe um único elemento não trivial s, tal que $s = g^*g^{-1}$ para qualquer $g \in G$ que satisfaça $g^* \neq g$. Como vimos no item (i) do Lema 3.2.1 $(g^*)^2 = g^2$, o que implica que $s^2 = 1_G$.

Mostramos que se G é abeliano, então existe $s \in G$ satisfazendo $s^2 = 1_G$, tal que para qualquer $g \in G$ tal que $g^* \neq g$ vale $g^* = sg$, isto é, $g^* = g$ ou $g^* = sg$ para qualquer $g \in G$.

Daqui em diante suponhamos que G é não abeliano e tomemos $g, h \in G$ tais que $gh \neq hg$. Vamos mostrar que se $g^* \neq g$ então que $g^* = h^{-1}gh$.

Se $h^* \neq h$, então afirmamos que $gh = g^*h^*$. Com efeito, vamos supor por absurdo que $gh \neq g^*h^*$, então, de acordo com a validade da equação (3.2), devemos ter $gh = hg^* = h^*g = h^*g^*$, o que é impossível pois $h^*g \neq h^*g^*$. Então $gh = g^*h^*$ e, equivalentemente, $hg = h^*g^*$ e, deste modo, a equação (3.2) pode ser reescrita como $2gh + 2hg + g^*h + gh^* + hg^* + h^*g = 0$, o que implica que $gh = hg^* = h^*g$ e, consequentemente, $g^* = h^{-1}gh$.

Se $h^* = h$, temos duas situações para analisar. A primeira é aquela em que $(gh)^* = gh$ e, neste caso, é imediato que $g^* = h^{-1}gh$. Se $(gh)^* \neq gh$, então, como $g(gh) \neq (gh)g$, repetindo para g e gh o que fizemos no parágrafo anterior para g e h, concluímos que $g^* = (gh)^{-1}g(gh) = h^{-1}gh$.

Mostramos que se G é não abeliano, então para qualquer $g \in G$, vale que $g^* = g$ ou $h^{-1}gh \in \{g, g^*\}$ para todo $h \in G$.

Prosseguindo, vamos considerar o conjunto $T = \{g \in G : g^* \neq g\}$ que, de acordo com a Observação 1.2.5, é não vazio. Concluiremos a demonstração estudando o caso em que T é não comutativo e o caso em que T é comutativo.

• T não comutativo. Tomemos $t_1, t_2 \in T$ que não comutam, então $t_1t_2t_1^{-1} \neq t_2$ e $t_2^{-1}t_1t_2 \neq t_1$ e, portanto, são válidas as igualdades $t_1t_2t_1^{-1} = t_2^*$ e $t_2^{-1}t_1t_2 = t_1^*$ que implicam que $t_2^*t_1 = t_2t_1^*$. Multiplicando esta última igualdade por t_2^{-1} à esquerda e por t_1^{-1} à direita e usando o item (i) do Lema 3.2.1, segue que $t_1^{-1}t_1^* = t_2^{-1}t_2^*$ e, portanto, $t_1^{-1}t_2^{-1}t_1t_2 = t_2^{-1}t_1^{-1}t_2t_1$. Deste modo, mostramos que se $t_1, t_2 \in T$ são tais que $t_1t_2 \neq t_2t_1$, então $(t_1, t_2) = (t_2, t_1)$. Então, fixando tais elementos e escrevendo $(t_1, t_2) = s$, obtemos $s^2 = 1_G$.

Seja $t \in T$ tal que $tt_1 \neq t_1t$. Conforme mostramos no parágrafo anterior, $t^{-1}t^* = t_1^{-1}t_1^* = t_2^{-1}t_1^{-1}t_2t_1 = (t_2, t_1) = s$, o que implica que se t é um elemento de T tal que $t^{-1}t^* \neq s$, então t comuta com t_1 e com t_2. Deste modo, vamos supor que t é um elemento que comuta com t_1 e com t_2, então afirmamos que $(tt_1)^* = tt_1$. Com efeito, vamos supor por contradição que $(tt_1)^* \neq tt_1$, então, como nós sabemos, $t_2^{-1}(tt_1)t_2 = tt_1$ ou $t_2^{-1}(tt_1)t_2 = (tt_1)^* = t_1^*t^* = t^*t_1^*$; entretanto se $t_2^{-1}(tt_1)t_2 = tt_1$, então $t_1t_2 = t_2t_1$ (para ver isto, basta multiplicar $t_2^{-1}(tt_1)t_2 = tt_1$ por t_2 à esquerda e ver que t e t_2 comutam), o que contradiz a hipótese sobre t_1 e t_2. Sendo assim, devemos ter $t_2^{-1}(tt_1)t_2 = t^*t_1^*$, no entanto, observe que $t_2^{-1}(tt_1)t_2 = (t_2^{-1}tt_2)(t_2^{-1}t_1t_2) = tt_1^*$. Então, se $(tt_1)^* \neq tt_1$, vale $t^*t_1^* = tt_1^*$, que implica $t^* = t$ o que contradiz a hipótese sobre t. Desta maneira, concluímos que $(tt_1)^* = tt_1$.

Então, se t comuta com t_1 e t_2, temos $t_1t^* = t_1t$ e, portanto, $t^*t^{-1} = (t_1^*)t_1 = (t_1^{-1}t_1^*)^{-1} = s^{-1} = s$. Isto mostra que s é independente de $t \in T$, isto é, para qualquer $t \in T$, $t^{-1}t^* = s$, isto é, para qualquer $g \in G$ tal que $g^* \neq g$ se verifica $g^* = sg$. É evidente que s é o único comutador não trivial para os elementos pertencentes a T. Vamos provar no próximo parágrafo que s é o único comutador não trivial de G.

Sejam $t \in T$ e $g \in G$ tais que $gt \neq tg$, então $(t, g) = t^{-1}g^{-1}tg = t^{-1}t^* = s$. Por último, tomemos $g, h \in G\backslash T$ e suponhamos que $gh \neq hg$. Então $gh \in T$, pois em caso, isto é, se $(gh)^* = gh$ teremos $gh = h^*g^* = hg$ o que contradiz a hipótese sobre g e h. Sendo assim, como também $g(gh) \neq (gh)g$, então, de acordo o o item (iii) do Lema 2.1.2 $s = (gh, g) = (h, g)$, então $(g, h) = (h, g) = s^{-1} = s$.

Concluímos que s é o único comutador não trivial de G.

• T comutativo. Vamos começar este caso considerando o subgrupo A gerado por T. Afirmamos que $[G : A] = 2$ e que todo elemento $a \in A$ que é simétrico a respeito da involução $*$ é central. Com efeito, tomemos $g, h \in G\backslash A$ e $t \in T$; como, em particular, $tg \notin T$, então $tg = (tg)^* = g^*t^* = gt^*$ e, portanto, $t^* = g^{-1}tg$. Como T é, evidentemente, fechado a respeito da involução $*$, então $t = g^{-1}t^*g$ e, deste modo, $(gh)^{-1}t(gh) = h^{-1}g^{-1}tgh = h^{-1}t^*h = t$. Vamos supor que $gh \notin A$, então $t^* = (gh)^{-1}t(gh) = t$, o que contradiz a hipótese sobre t. Concluímos que $gh \in A$, o que mostra que $[G : A]$ é igual a no máximo 2, mas como G é não abeliano, $[G : A] = 2$. Além disso, tomemos $a \in A$ e $g \in G\backslash A$, então $ga = (ga)^* = a^*g^* = ag$, isto é, a comuta com qualquer elemento de G.

Como T é fechado para a involução $*$, então A também é. Então, de acordo com o que provamos para o caso em que G é abeliano, sabemos que existe $s \in A$, tal que $s^2 = 1_G$ e $a^* = a$ ou $a^* = sa$ para todo $a \in A$. Observemos que $g^* = g$ para qualquer $g \notin A$. Deste modo temos $g^* = g$ ou $g^* = sg$ para qualquer g pertencente a G. Como G é não abeliano, então a involução $*$ não fixa todos os seus elementos e, portanto, $s \neq 1_G$. Além disso, s é fixo sobre a involução $*$, pois do contrário $s^* = ss = 1_G$, o que é uma contradição. Então s é um elemento central.

Vamos mostrar que s é o único comutador não trivial de G, e para isto vamos fixar $c \in G\backslash A$; como $[G : A] = 2$, podemos escrever $G = A \bigcup Ac$. Deste modo, para finalizar a demonstração é suficiente analisar as possibilidades para comutadores de G:

(a) (a, c); $a \in A$ (b) (ac, c); $a \in A$ (c) (a_1, a_2c); $a_1, a_2 \in A$ (d) (a_1c, a_2c); $a_1, a_2 \in A$

(a) Se $a \in A$ é simétrico sobre a involução $*$, então $(a, c) = 1_G$. Por outro lado, sabemos que para algum $a \in A$, tal que $a^* \neq a$ se verifica $ac \neq ca$, pois do contrário G seria um grupo abeliano. Seja a tal elemento, sabemos que $a^* = c^{-1}ac$ e $a^* = sa$, então $s = c^{-1}aca^{-1} = (c, a^{-1})$. Como $(a^{-1})^* \neq a^{-1}$ e $a^{-1}c \neq ca^{-1}$, entao $(a^{-1})^* = c^{-1}a^{-1}c$ e $(a^{-1})^* = c^{-1}a^{-1}c$ e, portanto, $s = c^{-1}a^{-1}ca = (c, a)$, e como $s^2 = 1_G$, então $s = (a, c)$. Concluímos que $(a, c) = 1$ ou $(a, c) = s$ para qualquer $a \in A$.

(b) Vendo que $c^2 \in A$, de acordo com o item (a)

$$(ac, c) = c^{-1}a^{-1}c^{-1}ac^2 = c^{-1}a^{-1}c^{-1}c^2a = (c, a) = (a, c) = 1_G \text{ ou } s. \tag{3.3}$$

(c) Usando o item (iv) do Lema 2.1.2,

$$(a_1, a_2c) = (a_1, c)(a_1, a_2)^c = (a_1, c) = 1_G \text{ ou } s. \tag{3.4}$$

(d) Usando o item (iii) do Lema 2.1.2 e as equações (3.3) e (3.4) temos $(a_1c, a_2c) = (a_1, a_2c)^c(c, a_2c) = (a_1, a_2c)^c(a_2c, c) = 1_G$ ou s.

■

Suponhamos que RG seja um anel de grupo, onde $\mathrm{car}(R) = 4$ e G é um grupo SLC. Então G possui uma involução definida por (2.2) que, em particular, satisfaz as condições descritas no (ii) do Teorema 3.2.4. Sendo assim, se $\mathrm{car}(R) = 4$ e G é um grupo SLC, então o produto de Jordan é trivial em $(RG)^+$.

Capítulo 4

Involuções orientadas e produto de Jordan trivial em $(RG)^+$.

Para escrever este capítulo, estudamos artigo "Oriented group involutions and anticommutativity in group rings" [10], também de autoria de E.G. Goodaire e C. P. Milies, em que novamente é feita a caracterização da trivialidade do produto de Jordan no subconjunto de RG dos elementos que são simétricos, mas desta vez, sobre uma nova involução, chamada de involução orientada, e que iremos em seguida definir.

Veremos que os resultados obtidos no artigo que serviu como referência para escrevermos o Capítulo 3 tiveram extrema importância para obtenção destes novos resultados.

4.1 Orientação para um Grupo G

Definição 4.1.1 Sejam um grupo G e um anel associativo R com elemento identidade 1. Consideremos o subgrupo $\{1, -1\}$, ou simplesmente $\{\pm 1\}$, do grupo de unidades de R. Dizemos que um homomorfismo $\sigma : G \to \{\pm 1\}$ é uma *orientação* para o grupo G.

Observação 4.1.2 Uma orientação $\sigma : G \to \{\pm 1\}$ é não trivial se existir $g \in G$ tal que $\sigma(g) \neq 1$. Deste modo, se uma orientação $\sigma : G \mapsto \{\pm 1\}$ é não trivial, então a característica de R é diferente de 2, pois, do contrário, $\sigma(g) = 1$ para qualquer $g \in G$.

Definição 4.1.3 Dizemos também que a orientação σ é compatível com uma involução $g \mapsto g^*$ de G se, para todo $g \in G$ se verifica $\sigma(g) = \sigma(g^*)$.

Observação 4.1.4 É claro que a uma orientação trivial é compatível com qualquer involução de G.

Exemplo 4.1.5 Consideremos o grupo $GL(n, \mathbb{R})$ das matrizes invertíveis de ordem n sobre $\mathbb{R}$ e a involução $A \mapsto A^T$. Definindo $\sigma(A) = \frac{\det A}{|\det A|}$, é bastante simples ver que $\sigma : GL(n, \mathbb{R}) \to \{\pm 1\}$ é uma orientação e que $\sigma(A) = \sigma(A^T)$ para qualquer $A \in GL(n, \mathbb{R})$.

Exemplo 4.1.6 (um caso de não compatibilidade) Considere o grupo diedral $D_4 = \langle \theta, r : \theta^4 = r^2 = 1, r\theta r^{-1} = \theta^{-1} \rangle$, com a involução $\theta^* = \theta^{-1}$ e $r^* = \theta r$. Seja a orientação dada por $\sigma(\theta) = -1$ e $\sigma(r) = 1$. Se $\mathrm{car}(R) \neq 2$, esta orientação não é compatível com $*$, pois $\sigma(\theta r) = -1$, enquanto $\sigma((\theta r)^*) = \sigma(r^* \theta^*) = \sigma(\theta r \theta^{-1}) = \sigma(\theta^2 r) = 1$.

Observação 4.1.7 Qualquer orientação não trivial σ é compatível com a involução natural $g \mapsto g^{-1}$. De fato, supondo por absurdo que exista uma orientação não trivial $\sigma : G \to \{\pm 1\}$ tal que para um determinado $g \in G$, tenhamos $\sigma(g) \neq \sigma(g^{-1})$. Isto implica $\sigma(g) \neq \sigma(g)^{-1}$, o que é impossível no grupo $\{\pm 1\}$.

Os Exemplos 4.1.5 e 4.1.6 e a Observação 4.1.7 encontram-se em [6, p.2]. Ao leitor interessado, os autores fazem, nesta mesma referência, mais alguns comentários a respeito de orientações para grupos.

Observação 4.1.8 Afirmamos que uma orientação $\sigma : G \mapsto \{\pm 1\}$ é não trivial se, e somente se, o subgrupo $N = \ker(\sigma)$ possui índice 2 em G. Com efeito, se $[G : N] = 2$, então $N \subsetneq G$ e, portanto, existe $g \in G$ tal que $\sigma(g) \neq 1$. Reciprocamente, suponhamos que σ é não trivial e tomemos $g, h \notin N$. Então $\sigma(gh) = \sigma(g)\sigma(h) = 1$ e, consequentemente, $gh \in N$. Portanto $[G : N] = 2$.

Um outro fato bastante simples de perceber é que, se uma orientação não trivial σ é compatível com uma involução $g \mapsto g^*$, então esta involução é antiautomorfismo em N e em seu complemento, isto é, se $g \in N$ então $g^* \in N$; e se $g \in G \backslash N$, então $g^* \in G \backslash N$.

4.2 Involução orientada de RG

Sejam G um grupo com uma involução $g \mapsto g^*$ e R um anel comutativo com elemento identidade 1. Consideremos o anel de grupo RG e uma orientação $\sigma : G \to \{\pm 1\}$ que é compatível com a involução supracitada de G. Definimos uma aplicação $\alpha = \sum_{g \in G} \alpha_g g \mapsto \alpha^\# = \sum_{g \in G} \sigma(g)\alpha_g g^*$. Esta aplicação é uma involução de RG.

De fato, sejam $\alpha = \sum_{g \in G} \alpha_g g$ e $\beta = \sum_{g \in G} \beta_g g$, então

$$\begin{aligned}
(\alpha\beta)^\# &= \left(\sum_{g,h \in G} \alpha_g \beta_h gh\right)^\# = \sum_{g,h \in G} \sigma(gh)\alpha_g\beta_h(gh)^* \\
&= \sum_{g,h \in G} \sigma(g)\sigma(h)\alpha_g\beta_h h^* g^* = \sum_{g,h \in G} \sigma(h)\beta_h\sigma(g)\alpha_g h^* g^* \\
&= \left(\sum_{h \in G} \sigma(h)\beta_h h^*\right)\left(\sum_{g \in G} \sigma(g)\alpha_g g^*\right) \\
&= \beta^\# \alpha^\#
\end{aligned}$$

$$\begin{aligned}
(\alpha + \beta)^\# &= \left(\sum_{g \in G} (\alpha_g + \beta_g) g\right)^\# = \sum_{g \in G} \sigma(g)(\alpha_g + \beta_g) g^* \\
&= \sum_{g \in G} \sigma(g)\alpha_g g^* + \sum_{g \in G} \sigma(g)\beta_g g^* \\
&= \alpha^\# + \beta^\#
\end{aligned}$$

$$\begin{aligned}
(\alpha^\#)^\# &= \left(\sum_{g \in G} \sigma(g)\alpha_g g^*\right)^\# = \sum_{g \in G} \sigma(g^*)\sigma(g)\alpha_g (g^*)^* \\
&= \sum_{g \in G} \alpha_g g = \alpha,
\end{aligned}$$

pois σ é compatível com a involução $*$.

Mostramos que $\alpha \to \alpha^\#$ é uma involução e que chamamos de *involução orientada* no anel de grupo RG. Diremos que tal involução possui orientação não trivial, ou é orientada não trivialmente, se σ é não trivial.

4.3 O conjunto $(RG)^+$

Vamos considerar um anel de grupo RG com uma involução orientada não trivial # que foi definida na seção anterior. Iremos, também neste capítulo, representar por $(RG)^+$ o subconjunto de RG cujos elementos são fixos para a involução #. Assim como fizemos no Capítulo 3, vamos determinar qual é o conjunto gerador para $(RG)^+$.

Sejam $g \mapsto g^*$ uma involução de G, σ uma orientação não trivial compatível com $*$ e $N = \ker(\sigma)$. Podemos fazer a partição de $G = S_1 \bigcup S_2 \bigcup S_3 \bigcup S_4$, onde

$$S_1 = \{n \in N : n^* = n\}, \quad S_2 = \{n \in N : n^* \neq n\}, \quad S_3 = \{x \notin N : x^* = x\}, \quad S_4 = \{x \notin N : x^* \neq x\}.$$

Sendo assim, qualquer $\alpha \in RG$ pode ser escrito como

$$\alpha = \sum_{g \in G} \alpha_g g = \sum_{g \in S_1} \alpha_g g + \sum_{g \in S_2} \alpha_g g + \sum_{g \in S_3} \alpha_g g + \sum_{g \in S_4} \alpha_g g,$$

o que implica que

$$\alpha^\# = \sum_{g \in S_1} \alpha_g g + \sum_{g \in S_2} \alpha_g g^* - \sum_{g \in S_3} \alpha_g g - \sum_{g \in S_4} \alpha_g g^*$$

e, portanto,

$$\alpha^\# = \alpha \quad \text{se, e somente se,} \quad \begin{cases} \alpha_g = \alpha_{g^*}, & \text{se} \quad g \in S_2; \\ \alpha_g = -\alpha_g, & \text{se} \quad g \in S_3; \\ \alpha_g = -\alpha_{g^*} & \text{se} \quad g \in S_4. \end{cases}$$

Concluímos que $(RG)^+$ é gerado, sobre R, por elementos pertencentes aos conjuntos $\mathcal{G}_1 = \{n \in N : n^* = n\}$, $\mathcal{G}_2 = \{n + n^* : n \in N,\ n^* \neq n\}$, $\mathcal{G}_3 = \{\alpha_x x : x^* = x \notin N,\ 2\alpha_x = 0\}$ e $\mathcal{G}_4 = \{x - x^* : x \notin N,\ x^* \neq x\}$.

Como já comentamos, estamos interessados na anticomutatividade dos elementos do conjunto $(RG)^+$. Note que os elementos de $(RG)^+$ anticomutam se, e somente se, quaisquer elementos no conjunto $\bigcup_{i=1}^{4} \mathcal{G}_i$ anticomutam. Entretanto, se os elementos de $\mathcal{G}_1$ são anticomutativos, então $2n^2 = 0$ para qualquer $n \in \mathcal{G}_1$, e isto implica que $\mathrm{car}(R) = 2$. Por estarmos assumindo que σ é não trivial, devemos ter, de acordo com a Observação 4.1.2, que a característica de R é diferente de 2 e, desta maneira, o que iremos fazer adiante é estudar a anticomutatividade no maior conjunto de

$(RG)^+$, que contém $\mathcal{G}_2 \bigcup \mathcal{G}_3 \bigcup \mathcal{G}_4$, mas não contém elementos de $\mathcal{G}_1$, isto é, o conjunto que é gerado por

$$\mathcal{G} = \{n + n^*,\ n \in N\} \bigcup \{\alpha_x x : x^* = x \notin N,\ 2\alpha_x = 0\} \bigcup \{x - x^* : x \notin N\}, \tag{4.1}$$

e que iremos denotar por $\langle \mathcal{G} \rangle$. Sabemos, claramente, que é suficiente estudar a anticomutatividade nos elementos de $\mathcal{G}$.

4.4 Produto de Jordan trivial em $\mathcal{G}$

Nesta seção, estudaremos o principal resultado deste capítulo que é o Teorema 4.4.2, onde se caracteriza a anticomutatividade dos elementos de $\mathcal{G}$. Antes de enunciarmos este teorema é pertinente que façamos duas observações.

A primeira delas é que, considerando um anel de grupo RG, onde o grupo G é munido de uma involução $g \mapsto g^*$ e que tenhamos uma orientação $\sigma : G \to \{\pm 1\}$ que seja compatível com a involução $*$, podemos considerar o anel RN, onde $N = \ker(\sigma)$ e cujos elementos são da forma $\alpha = \sum_{n \in N} \alpha_n n$. É bem fácil notar que a involução orientada # de RG, quando restrita a RN nada mais é do que a involução definida no Exemplo 1.2.6.

A segunda, é que se supusermos que $\mathcal{G}$ é um conjunto anticomutativo, então, em particular, os elementos da forma $n + n^*$, com $n \in N$, anticomutam e consequentemente, de acordo com o Teorema 3.2.4 o produto de Jordan $\circ$ é trivial em $(RN)^+$.

Deste modo, se # é uma involução orientada não trivial de RG, então sintetizando a Proposição 3.2.3 e o Teorema 3.2.4, podemos concluir que para o anel de grupo RN é válido o seguinte resultado:

Teorema 4.4.1 Seja G um grupo com uma involução $g \mapsto g^*$, que se estende linearmente à uma involução de um anel de grupo RG, onde car(R) $\neq 2$. Então os elementos da forma $g + g^*$, onde $g \in G$, anticomutam em RG se, e somente se, uma das seguintes condições se verifica:

(a) $\mathrm{car}(R) = 4$ ou 8, G é abeliano e $*$ é a identidade em G;

(b) $\mathrm{car}(R) = 4$ e existe $s \in G$ tal que $s \neq 1_G$ e $s^2 = 1_G$, $g^* = g$ ou $g^* = sg$ para todo $g \in G$ e, ou G é abeliano ou G é não abeliano com $G' = \{1_G, s\}$.

■

Enunciamos a seguir o principal resultado deste capítulo.

Teorema 4.4.2 Sejam $g \mapsto g^*$ uma involução de um grupo G , R um anel comutativo com elemento identidade 1 e de característica diferente de 2, e $\sigma : G \to \{\pm 1\}$ uma orientação não trivial de G, tal que $\sigma(g) = \sigma(g^*)$ para todo $g \in G$. Sejam também o subconjunto $R_2 = \{r \in R :\ 2r = 0\}$ e a involução orientada $\alpha^\# = \sum_{g \in G} \sigma(g)\alpha_g g^*$ de RG. Então, se os elementos de

$$\mathcal{G} = \{n + n^*,\ n \in N\} \bigcup \{\alpha_x x : x^* = x \notin N,\ 2\alpha_x = 0\} \bigcup \{x - x^* : x \notin N\}$$

anticomutam em RG , uma das seguintes condições se verifica:

(1) $\mathrm{car}(R) = 4$ ou 8, G é abeliano e $*$ é a identidade em G;

(2) $\mathrm{car}(R) = 4$, G é abeliano e $*$ é a identidade no núcleo N de σ;

(3) $\mathrm{car}(R) = 4$ e

(i) $G' = \{1_G, s\}$, para algum $s \neq 1_G$;

(ii) para qualquer $g \in G$, $g^* = g$ ou $g = sg$;

(iii) os elementos de G que são simétricos sobre a involução $*$ e que não pertencem a N comutam, ou $R_2^2 = \{0\}$.

Reciprocamente, suponhamos que G é um grupo com um subgrupo N de índice 2 que é núcleo da orientação σ, então os elementos de $\mathcal{G}$ anticomutam em qualquer das condições (1), (2) e (3).

Demonstração: Vamos primeiramente mostrar a validade da recíproca, onde é suficiente analisar em cada uma das condições (1), (2) e (3) todas as possibilidades para produtos entre os elementos de $\mathcal{G}$.

(1) Se $\mathrm{car}(R) = 4$ ou 8, G é abeliano e $*$ é a aplicação identidade em G, então podemos escrever $\mathcal{G} = \{2n,\ n \in N\} \cup \{\alpha_x x : x \notin N,\ 2\alpha_x = 0\}$. Assim, as possibilidades para quaisquer elementos g_1 e g_2 de $\mathcal{G}$ são:

(a) $g_1 = 2n$, $n \in N$; e $g_2 = 2m$, $m \in N$.

Neste caso, se $\mathrm{car}(R) = 4$, então $4 = 0$, e se $\mathrm{car}(R) = 8$, então $4 = -4$. Em ambos os casos se verifica $g_1 g_2 = 2n2m = 4nm = -4mn = -2m2n = -g_2 g_1$, pois G é abeliano.

(b) $g_1 = \alpha_x x$, $x \notin N$, $2\alpha_x = 0$; e $g_2 = \alpha_y y$, $y \notin N$, $2\alpha_y = 0$.

Aqui, em particular, temos que $\alpha_x = -\alpha_x$, o que implica que $g_1 g_2 = \alpha_x x \alpha_y y = -\alpha_y y \alpha_x x = -g_2 g_1$, pois G é abeliano e R é comutativo.

(c) $g_1 = 2n$, $n \in N$; e $g_2 = \alpha_x x$, $x \notin N$ e $2\alpha_x = 0$.

É uma consequência imediata que $2n\alpha_x x = -\alpha_x x 2n = 0$, pois $2\alpha_x = 0$.

(2) Se $\mathrm{car}(R) = 4$, G é abeliano e $*$ é a identidade em N, então

$$\mathcal{G} = \{2n,\ n \in N\} \cup \{\alpha_x x : x^* = x \notin N,\ 2\alpha_x = 0\} \cup \{x - x^* : x \notin N\}.$$

O estudo de quaisquer produtos envolvendo apenas os elementos dos dois primeiros subconjuntos de $\mathcal{G}$ é análogo ao dos itens (a), (b) e (c). Desse modo, vamos analisar produtos que englobam elementos g_1 e g_2 do terceiro subconjunto de $\mathcal{G}$.

(d) $g_1 = x - x^*$, $x \notin N$; e $g_2 = y - y^*$, $y \notin N$.

De acordo com a Observação 4.1.8, se $x \notin N$ então $x^* \notin N$ e, sendo assim, como $[G : N] = 2$, já sabemos que xy e xy^* pertencem a N. Desse modo $xy = (xy)^* = y^* x^* = x^* y^*$ e $xy^* = (xy^*)^* = yx^* = x^* y$ o que implica que $(x - x^*)(y - y^*) = xy - xy^* - x^* y + x^* y^* = 2xy - 2xy^*$. Consequentemente, segue que $2(x - x^*)(y - y^*) = 4xy - 4xy^* = 0$. Portanto, $(x - x^*)(y - y^*) = -(x - x^*)(y - y^*) = -(y - y^*)(x - x^*)$, isto é, $g_1 = x - x^*$ e $g_2 = y - y^*$ anticomutam.

(e) $g_1 = 2n$, $n \in N$; e $g_2 = x - x^*$, $x \notin N$.

Sabemos que $4n(x - x^*) = 0$ e, sendo assim, $2n(x - x^*) = -2n(x - x^*) = -(x - x^*)2n$, o que quer dizer que $g_1 = 2n$ e $g_2 = x - x^*$ anticomutam.

(f) $g_1 = \alpha_x x$, $x^* = x \notin N$, $2\alpha_x = 0$; e $g_2 = y - y^*$, $y \notin N$.

Neste caso, vale que $2\alpha_x x(y - y^*) = 0$, ou seja, $\alpha_x x(y - y^*) = -\alpha_x(y - y^*)x$ e, portanto, $g_1 = \alpha_x x$ e $g_2 = y - y^*$ anticomutam.

(3) Suponhamos que $\mathrm{car}(R) = 4$, $G' = \{1_G, s\}$, para algum $s \neq 1_G$, $g^* = g$ ou $g^* = sg$, para qualquer $g \in G$, ou elementos os elementos de G que são simétricos sobre a involução $*$ e que não pertencem a N comutam, ou $R_2^2 = \{0\}$.

É imediato que s possui ordem 2. Além disso, de acordo com o Lema 2.2.7 e a Proposição 2.2.8, s é um elemento central.

Novamente, seguindo os mesmos procedimentos dos casos (1) e (2) as possibilidades quaisquer dois elementos g_1 e g_2 de $\mathcal{G}$ são:

(a) $g_1 = n + n^*$ $n \in N$; $g_2 = m + m^*$, $m \in N$.

Aqui, temos as seguintes situações a considerar:

(i) se $n^* = n$ e $m^* = m$ então $g_1g_2 = 2n2m = 4nm = 0 = -4mn = -2m2n = -g_2g_1$.

(ii) se $n^* = n$ e $m^* = sm$; ou se $n^* = sn$ e $m^* = m$, então

$$(n + n^*)(m + m^*) = 2(1_G + s)nm \quad = \begin{cases} 2(1_G + s)mn, & \text{se} \quad nm = mn \\ 2(1_G + s)smn, & \text{se} \quad nm \neq mn \end{cases}$$

Agora, como $2(1_G + s)smn = 2s + 2mn = 2(1_G + s)mn$; e 2 = -2, podemos concluir que $(n + n^*)(m + m^*) = -2(1_G + s)mn = -(m + m^*)(n + n^*)$, isto é, $g_1 = n + n^*$ e $g_2 = m + m^*$ anticomutam.

(iii) se $n + n^* = (1_G + s)n$ e $m + m^* = (1_G + s)m$, então como $(1_G + s)^2 = 1_G + 2s + s^2 = 2 + 2s$, segue que $(n + n^*)(m + m^*) = 2(1_G + s)nm$. Desta maneira, o resultado é obtido de modo análogo ao do item (ii).

(b) $g_1 = \alpha_x x$, $x^* = x \notin N$, $2\alpha_x = 0$; $g_2 = \alpha_y y$, $y^* = y \notin N$, $2\alpha_y = 0$.

Se $xy = yx$, então $g_1g_2 = \alpha_x x\alpha_y y = \alpha_x\alpha_y xy = -\alpha_x\alpha_y yx = -\alpha_y\alpha_x yx = -\alpha_y y\alpha_x x = -g_2g_1$.

Por outro lado, se $xy \neq yx$, de acordo com a hipótese, $R_2^2 = \{0\}$, então segue que $g_1g_2 = \alpha_x x\alpha_y y = \alpha_x\alpha_y xy = 0 = -\alpha_y\alpha_x yx = -\alpha_y y\alpha_x x = 0$.

Portanto, em ambos os casos, g_1 e g_2 anticomutam.

(c) $g_1 = x - x^*$, $x^* \neq x \notin N$; $g_2 = y - y^*$ $y^* \neq y \notin N$.

Neste caso, temos que

$$\begin{aligned}
g_1g_2 &= (x-x^*)(y-y^*) = [(1_G-s)x][(1_G-s)y] \\
&= (1_G-s)^2xy = 2(1_G-s)xy \\
&= \begin{cases} 2(1-s)yx = -2(1+s)yx, & \text{se} \quad xy = yx \\ 2(1_G-s)syx = -2(1-s)yx & \text{se} \quad yx \neq xy \end{cases} \\
&= -(2-2s)yx = -(1_G-s)^2yx = -[(1_G-s)y][(1_G-s)x] \\
&= -g_1g_2
\end{aligned}$$

Logo, g_1 e g_2 anticomutam.

(d) $g_1 = n + n^*$, $n \in N$; $g_2 = \alpha_x x$, $x^* = x \notin N$ e $2\alpha_x = 0$.

Se $n^* = n$, então $g_1g_2 = 2\alpha_x nx = 0 = -g_2g_1$.

Por outro lado, se $n^* \neq n$, temos que

$$\begin{aligned}
g_1g_2 = (n+n^*)\alpha_x x &= \alpha_x(1_G+s)nx \\
&= \begin{cases} \alpha_x(1_G+s)xn = -\alpha_x x(n+n^*) = -g_2g_1, & \text{se} \quad nx = xn \\ \alpha_x(1_G+s)sxn = \alpha_x(1_G+s)xn = -\alpha_x x(n+n^*) = -g_2g_1, & \text{se} \quad nx \neq xn \end{cases}
\end{aligned}$$

(e) $g_1 = n + n^*$, $n \in N$; $g_2 = x - x^*$, $x \neq x^*$ e $x \notin N$.

Se $n = n^*$, então

$$g_1g_2 = 2(1_G-s)nx = \begin{cases} -2(1_G-s)xn = -(1_G-s)x(n+n^*) = -g_2g_1, & \text{se} \quad xn = nx \\ 2(1_G-s)sxn = -2(1_G-s)xn = -(1_G-s)x(n+n^*) = -g_2g_1 & \text{se} \quad xn \neq nx \end{cases}$$

Caso contrário, $g_1g_2 = (n+n^*)(1_G-s)x = (1_G+s)n(1_G-s)x = (1_G-s^2)nx = 0 = -g_2g_1$.

(f) $g_1 = \alpha_x x$, $x^* = x \notin N$, $2\alpha_x = 0$; e $g_2 = y - y^*$, $y \neq y^*$ $y \notin N$.

Neste caso

$$\begin{aligned}
g_1g_2 = [\alpha_x x][(1_G-s)y] &= \alpha_x(1_G-s)xy \\
&= \begin{cases} -\alpha_x(1_G-s)yx, & \text{se} \quad xy = yx \\ \alpha_x(1_G-s)syx = -\alpha_x(1_G-s)yx = -g_1g_2, & \text{se} \quad xy \neq yx \end{cases}
\end{aligned}$$

Reciprocamente, suponhamos que os elementos de $\mathcal{G}$ anticomutam em RG e vamos mostrar que uma das condições (1), (2) e (3) se verifica.

Se os elementos de $\mathcal{G}$ anticomutam, então em particular os elementos da forma $n+n^*$, $n \in N$, são anticomutativos; desta maneira, de acordo com o Teorema 4.4.1, é válida uma das seguintes condições:

(A) $\mathrm{car}(R) = 4$ ou 8, N é um grupo abeliano e a involução $*$ é a aplicação identidade em N;

(B) $\mathrm{car}(R) = 4$, existe $s \in N$ tal que $s \neq 1_G$ e $s^2 = 1_G$, $n^* = n$ ou $n^* = sn$ para todo $n \in N$ e, ou N é abeliano ou N não é abeliano com $N' = \{1_G, s\}$.

Primeiramente, vamos assumir que seja válida a condição (A).

Se $*$ é a aplicação identidade em G, pela Observação 1.2.5, o grupo G é abeliano e se verifica a condição (1) do teorema.

Caso contrário, existe $a \in G \backslash N$ tal que $a^* \neq a$; e, por hipótese, $(a-a^*)(a-a^*) = -(a-a^*)(a-a^*)$, o que significa que

$$2a^2 - 2aa^* - 2a^*a + 2(a^*)^2 = 0. \tag{4.2}$$

Além disso, $a^2 \in N$, pois $[G:N] = 2$, o que implica que $(a^*)^2 = a^2$. Desse modo, a equação (4.2) pode ser reescrita como

$$4a^2 - 2aa^* - 2a^*a = 0,$$

ou, equivalentemente

$$-4a^2 + 2aa^* + 2a^*a = 0. \tag{4.3}$$

Se $\mathrm{car}(R) = 8$, então

$$4a^2 + 2aa^* + 2a^*a = 0, \tag{4.4}$$

o que implica $aa^* = a^*a = a^2$ e, consequentemente, $a = a^*$, contradizendo a hipótese sobre a.

Sendo assim, se a involução $*$ é a aplicação identidade em N mas não é em G, então $\mathrm{car}(R) = 4$. Se G é abeliano, o item (2) do Teorema é satisfeito. Suponhamos que G é um grupo que não é abeliano. Vamos mostrar que se $a \in G \backslash N$ é tal que $a^* \neq a$, então para qualquer $n \in N$,tem-se que ou $an = na$ ou $a^{-1}a^* = (a,n)$.

Inicialmente, observe que como $\mathrm{car}(R) = 4$, pela Equação (4.3), decorre que $aa^* = a^*a$. Se $(an)^* = an$, então $an \neq na$. De fato, $an = na$ implica que $na = an = (an)^* = na^*$, o que é uma contradição, pois $a^* \neq a$. Por outro lado, supondo que $(an)^* \neq an$, como elementos do conjunto $\{x - x^* : x \notin N\}$ anticomutam, em particular, $(a-a^*)(an-(an)^*) = -(an-(an)^*)(a-a^*)$, isto é,

$$\begin{aligned} 0 &= (a-a^*)(an-na^*) + (an-na^*)(a-a^*) \\ &= a^2n - ana^* - a^*an + a^*na^* + ana - ana^* - na^*a + n(a^*)^2, \end{aligned}$$

isto é,

$$2a^2n - 2ana^* - 2aa^*n + ana + a^*na^* = 0, \tag{4.5}$$

pois $a^2 \in N$, $aa^* \in N$ e N é abeliano.

Neste caso, como $\mathrm{car}(R) = 4$, segue que $ana = a^*na^* = aan$ ou $ana = a^*na^* = aa^*n$, de onde resulta que $na = an$ (ou equivalentemente $a^{-1}n^{-1}na^* = a^{-1}n^{-1}an$, isto é, $a^{-1}a^* = (a,n)$).

Em vista de que N é um subgrupo de índice 2 em G, podemos escrever $G = N \bigcup Na$. Desse modo, se $an = na$, para todo $n \in N$, como N é um grupo abeliano, teríamos que G seria abeliano, contradizendo nossa hipótese. Portanto, existe um elemento $s = (a,n) = a^{-1}a^* \neq 1_G$. Observe que $s \in N$ pois $a^{-1} \notin N$ e $a^* \notin N$; $a^* = as$ e $(a^*, a^{-1}) = (a^*)^{-1}aa^*a^{-1} = (a^*)^{-1}a^*aa^* = 1_G$ implica que $s^2 = a^{-1}a^*a^{-1}a^* = a^{-1}a^{-1}a^*a^* = (a^{-1})^2(a^*)^2 = (a^2)^1a^2 = 1_G$. Além disso, uma vez que $s \in N$, sabemos que $as = sa$ ou $(a,s) = a^{-1}a^* = s$. Entretanto, se $(a,s) = s$, então $a^{-1}s^{-1}as = s$, o que implica que $s^{-1}a = a$, o que é uma contradição, pois $s \neq 1_G$. Logo, podemos concluir que s é um elemento central de $G = N \bigcup Na$.

Prosseguindo, vamos mostrar que s é o único comutador não trivial de G. Para isso analisaremos as seguintes possibilidades entre produtos de elementos de G.

- Se $n \in N$ e $x \notin N$, então existe $m \in N$ tal que $x = ma$ e, assim,

$$xn = man = \begin{cases} mna = nma = nx, & \text{se} \quad an = na \\ msna = smna = snma = snx & \text{se} \quad an \neq na \end{cases}$$

  Portanto, $(x,n) = 1$ ou $(x,n) = s$.

- Se $x \notin N$ e $y \notin N$, então $x = na$ e $y = ma$, para alguns $n, m \in N$. Similarmente, temos que

$$xy = nama = \begin{cases} nma^2 & \text{se} \quad am = ma \\ snma^2 & \text{se} \quad am \neq ma \end{cases}$$

  e

$$yx = mana = \begin{cases} nma^2, & \text{se} \quad an = na \\ snma^2, & \text{se} \quad an \neq na \end{cases}$$

  O que nos permite concluir que $(x,y) = 1_G$ ou s, para quaisquer $x, y \in G \backslash N$. Logo s é o único comutador não trivial de G e $G' = \{1_G, s\}$ pois $s^2 = 1_G$.

  Agora, se $x = na \notin N$, então

$$x^* = a^*n = san = \begin{cases} sna = sx, & \text{se} \quad na = an \\ s(sna) = na = x, & \text{se} \quad na \neq an \end{cases}$$

Além disso, como sabemos que $*$ é a identidade sobre o subgrupo N, segue que $g^* = g$ ou $g^* = sg$ para qualquer $g \in G$.

Finalmente, vamos mostrar que os elementos de G que são simétricos sobre a involução $*$ e que não pertencem a N comutam ou $R_2^2 = \{0\}$. Para isso, tome $x, y \in G\backslash N$ tais que $x^* = x$, $y^* = y$ e $xy \neq yx$. Sejam $\alpha_x, \alpha_y \in R_2$. De acordo com a hipótese $\alpha_x\alpha_y xy = -\alpha_x\alpha_y yx$, ou seja, $\alpha_x\alpha_y(xy + yx) = 0$. Assim, como x e y não comutam, temos que $\alpha_x\alpha_y = 0$. Portanto, $R_2^2 = \{0\}$ e o item (3) do Teorema é válido

Vamos assumir agora que é satisfeita a possibilidade (B).

Se a involução $*$ é a identidade sobre G, então pela Observação 1.2.5, sabemos que G é abeliano e, sendo assim, verifica-se a condição (1) do Teorema.

Suponhamos agora que G não é abeliano e, assim, $*$ não é identidade sobre G. Desse modo, similarmente ao que fizemos no final da demonstração do caso (A), podemos concluir que existem $x \in G\backslash N$ e $y \in G\backslash N$ tais que $x^* = x$, $y^* = y$ e $xy \neq yx$, então $R_2^2 = \{0\}$.

Prosseguindo.vamos provar que o Teorema é válido por intermédio de 5 etapas.

Passo 1. Inicialmente, vamos reduzir a demonstração ao caso em que $x^* \neq x$ para algum $x \in G\backslash N$. Para isto, iremos provar que o Teorema é valido se $x^* = x$ para todo $x \in G\backslash N$.

Será suficiente analisar todas as possibilidades para o produto de elementos de G quando N é abeliano, e quando N não é abeliano e possui subgrupo comutador $N' = \{1_G, s\}$.

Suponhamos que N é abeliano.

Sejm $n \in N$ e $x \in G\backslash N$. Se $n^* = n$ então $nx = (nx)^* = xn$ e como $G = N \bigcup Nx$ e N é abeliano, segue que n é um elemento central. Por outro lado, se $n^* \neq n$, então $nx = (nx)^* = x^*n^* = xn^*$, isto é, $n^* = x^{-1}nx$. Desse modo, como $n^* = ns$, segue que $x^{-1}nx = ns$, isto é, $s = n^{-1}x^{-1}nx = (n, x) = n^{-1}n^*$ é independente de x e então podemos escrever $s = (n, x^{-1})$.

Agora, consideremos $x \in G\backslash N$ e $y \in G\backslash N$. Em vista de que o índice de N em G é igual a 2, temos que $y = mx^{-1}$ para algum $m \in N$. Observe que se $(m, x^{-1}) = 1_G$, então $xy = xmx^{-1} = xx^{-1}m = m = mxx^{-1} = yx$, isto é, $(x, y) = 1_G$. Assim, se x e y não comutam, então m e x^{-1} não comutam. Consequentemente, $(x, y) = x^{-1}y^{-1}xy = x^{-1}(mx^{-1})^{-1}xmx^{-1} = x^{-1}xm^{-1}xmx^{-1} = (m, x^{-1}) = s$.

Suponhamos que N não é abeliano e $N' = \{1, s\}$.

Sejam $n \in N$ e $x \in G\backslash N$. Então $nx \notin N$. Se $n^* = n$, então $nx = (nx)^* = x^*n^* = xn$, o que implica que n comuta com todo elemento que não está em N. Além disso, dado $m \in N$, temos que $nmx = mxn = mnx$, de onde decorre que $nm = mn$. Assim, n também comuta com todo elemento de N. Portanto n é central. Por outro lado, se $n^* \neq n$; então $s = n^{-1}x^{-1}nx = (n, x) = n^{-1}n^*$ é independente de x e $(n, x^{-1}) = s$, como no caso abeliano.

Se $x, y \in G\backslash N$, novamente, de modo análogo ao caso em que N é abeliano, é possível mostrar que se $(x, y) \neq 1_G$, então $(x, y) = (m, x^{-1}) = s$, onde $m = yx$.

Em ambos os casos analisados, mostramos que s é o único comutador não trivial de G e como $g^* = g$ ou $g^* = sg$, para qualquer $g \in G$, é válida a afirmação (3) do Teorema, o que completa o Passo 1.

Daqui em diante, vamos assumir a existência de $x \in G\backslash N$ tal que $x^* \neq x$.

Passo 2. Vamos provar que s é um elemento central de G.

No Passo 1, já mostramos que s é central em N se $N' = \{1_G, s\}$, o que também é verdadeiro se N é abeliano. Desse modo, s é central em N em qualquer caso. Sendo assim, resta provar que s comuta com todo elemento de $G\backslash N$. Agora, como $G = N \bigcup Nx$ para todo $x \in G\backslash N$, é suficiente mostrar que existe um elemento pertencente a $G\backslash N$ que comute com s. Suponhamos o contrário, isto é, que $sx \neq xs$ para qualquer $x \in G\backslash N$.

Escolha um elemento $\in G\backslash N$ tal que $x^* \neq x$. Em particular, $(x - x^*)^2 = -(x - x^*)^2$, isto é, vale a equação

$$2x^2 + 2xx^* + 2x^*x + 2(x^*)^2 = 0, \tag{4.6}$$

pois $\mathrm{car}(R) = 4$. Além disso, como $x^* \neq xx^*$ e $x^2 \neq x^*x$, decorre que $x^2 = (x^*)^2 = (x^2)^*$ e $xx^* = x^*x$.

Da mesma forma, os elementos $x - x^*$ e $s + s = 2s$ anticomutam, o que dá origem à equação $2sn + 2sx^* + 2xs + 2x^*s = 0$. Em vista da suposição $sx \neq xs$ e do elemento x satisfazer $x^* \neq x$, devemos ter $sx = x^*s$, isto é

$$x^* = sxs.$$

Agora, tome $y \in G\backslash N$ tal que $y \neq y^*$. Desse modo, $y^* = sys$. Também sabemos que $xy \in N$ e, sendo assim, $(xy)^* = xy$ ou $(xy)^* = sxy$. Por outro lado, note que $(xy)^* = y^*x^*) = (sys)(sxs) = syxs = s^2yx = yx$, pois $yx \in N$ e comuta com s. Consequentemente

$$yx = xy \quad \text{ou} \quad yx = sxy.$$

Pela anticomutatividade dos elementos $x - x^*$ e $y - y^*$ segue que $xy - xy^* - x^*y + x^*y^* + yx - yx^* - y^*x + y^*x^* = 0$, isto é,

$$xy + yx + x^*y^* + y^*x^* = xy^* + x^*y + yx^* + y^*x.$$

Suponhamos que $xy \neq yx$, então como $x^* \neq x$ e $y^* \neq y$, existem duas possibilidades, $xy = yx^*$ ou $xy = y^*x$. Entretanto, $xy = yx^*$ implica $syx = ysxs$ ou, equivalentemente, $yxs = ysxs$, pois $yx \in N$ comuta com s, de onde decorre que $y = ys$, o que é uma contradição, visto que $s \neq 1_G$. Por outro lado, $xy = y^*x$ implica $syx = syxy$ o que novamente, resultado em $y = ys$, um absurdo. Concluímos que $xy = yx$, para quaisquer $x, y \in G\backslash N$ que satisfazem $x^* \neq x$ e $y^* \neq y$.

Afirmamos que se $x \in G\backslash N$ é tal que $x^* \neq x$, então sx é fixado pela involução $*$. Com efeito, se valesse $(sx)^* \neq sx$, no parágrafo anterior teríamos que sx e x comutariam e, consequentemente, $sx = xs$, o que seria uma contradição. Desta maneira, tomando $n \in N$ tal que $n^* \neq n$, sabemos que $(sx)^* + sx = 2sx$ e $n + n^*$ anticomutam o que significa que

$$2sxn + 2sxn^* + 2nsx + 2n^*sx = 0. \tag{4.7}$$

Em vista de que $sxn = sxn^*$, decorre da equação (4.7) que $sxn = nsx$ ou $sxn = n^*sx$.

Se $sxn = nsx$, então pela centralidade do elemento s em N, segue que $xn = nx$. Além disso, neste caso, como também é valida a igualdade $sxn^* = n^*sx$ e $n^* = sn$, obtemos que $sxsn = snsx$, o que implica que $xsn = nsx = sxn$ e, cancelando n, resulta em $xs = sx$, uma contradição.

A outra possibilidade é $sxn = n^*sx$ e $sxn^* = nsx$. Neste caso, $xn = n^*x = nsx = sxn^*$. Multiplicando à esquerda, ambos os membros da equação $xn = sxn^*$, obtemos $sxn = xn^* = xns$ e,

portanto, $xs = sn$, um absurdo.

Passo 3: Vamos mostrar que para qualquer $a \in G\backslash N$ se verifica $a^* = sa$ ou senão $(a,n) \in \{1, a^{-1}a^*\}$.

Seja $n \in N$ tal que $n^* = n$. Sabemos que $n^{-1} + (n^{-1})^* = 2n^{-1}$ e $a - a^*$ anticomutam, o que nos fornece a equação $2n^{-1}a - 2n^{-1}a^* + 2an^{-1} - 2a^*n^{-1} = 0$, isto é

$$2n^{-1}a + 2an^{-1} = 2n^{-1}a^* + 2a^*n^{-1}.$$

Em vista de que $n^{-1}a \neq n^{-1}a^*$, existem duas possibilidades, $an^{-1} = n^{-1}a$ (e, consequentemente, a e n comutam) ou então $n^{-1}a = a^*n^{-1}$, ou seja, $a^* = n^{-1}an$, o que implica $a^{-1}a^* = a^{-1}n^{-1}an = (a,n)$.

Agora, tome $n \in N$ tal que $n \neq n^* \in N$. Pela anticomutatividade dos elemento $n + n^*$ e $a - a^*$ segue que $na - na^* + n^*a - n^*a^* + an + an^* - a^*n - a^*n^* = 0$, isto é

$$na + n^*a + an + an^* = na^* + n^*a^* + a^*n + a^*n^*. \tag{4.8}$$

Uma vez que $na \neq n^*a$, o elemento na efetivamente aparece no primeiro membro desta equação e, assim, também em seu segundo membro. Como $na \neq na^*$, há três casos para serem analisados.

(a) $na = n^*a^*$ (b) $na = a^*n$ (c) $na = a^*n^*$.

(a) Neste caso, como $n^* = sn$, segue que $na = sna^*$, o que implica que $a^* = sa$, pois s é um elemento central que possui ordem 2.

(b) Se $na = a^*n$ (ou, equivalentemente, $a^* = nan^{-1}$), aplicando a involução $*$ em ambos os membros segue que $a^*n^* = n^*a$ e, sendo assim, a equação (4.8) pode ser reescrita como

$$an + an^* = na^* + n^*a^* \tag{4.9}$$

o que origina dois subcasos:

(b_1) $an = na^*$ (b_2) $an = n^*a^*$.

(b_1) Se $an = na^*$, então $a^* = n^{-1}an$ e, portanto, $a^{-1}a^* = a^{-1}n^{-1}an = (a,n)$.

(b_2) Se $an = n^*a^*$, então pela equação (4.9) também temos que $an^* = na^*$ ou, equivalentemente $san = an^* = na^* = n(nan^{-1}) = n^2an^{-1}$, isto é, $san^2 = n^2a$. Logo a e n^2 não comutam. Afirmamos que $n^2 \in N$ é invariante sobre $*$. Com efeito, $(n^2)^* = (n^*)^2 = (sn)^2 = n^2$. Agora, como $a \notin N$, $a^* \neq a$, $n^2 \in N$ e $n^* = n$, pelo que provamos no inicio da Etapa 3, sabemos que $an^2 = n^2a$ ou, $(a,n^2) = a^{-1}a^*$. Em vista de que a e n^2 não comutam, podemos concluir que $a^{-1}(n^2)^{-1}an^2 = a^{-1}a^*$, isto é, $a^* = n^{-2}an^2$ ou, equivalentemente, $n^2a^* = an^2$. Portanto, $sn^2a = an^2 = n^2a^*$ e, concluímos que $a^* = sa$.

(c) Finalmente, se $na = a^*n^*$, então a equação (4.8) se torna

$$n^*a + an + an^* = na^* + n^*a^* + a^*n, \tag{4.10}$$

e como $n^*a \neq n^*a^*$, novamente existem dois subcasos:

$$(c_1)\quad n^*a = na^* \qquad \text{ou} \qquad (c_2)\quad n^*a = a^*n.$$

(c_1) Neste caso, temos que $nsa = snan^*a = na^*$ e, portanto, $a^* = sa$.

(c_2) Se $n^*a = a^*n$, então de acordo com a equação (4.10) segue que $an + an^* = na^* + n^*a^*$. Agora, devido à característica de R ser diferente de 2, nenhum dos membros desta equação é nulo, de onde decorre que $an = na^*$ ou $an = n^*a^*$. Se $an = na^*$, então $(a,n) = a^{-1}n^{-1}an = a^{-1}n^{-1}na^* = a^{-1}a^*$. Por outro lado, se valerem as igualdades $an = n^*a^* = (an)^*$, decorre que $2an \in \mathcal{G}_3 \subseteq \mathcal{G}$ anticomuta com $a - a^*$, o que fornece a equação $2ana - 2ana^* + 2a^2n - 2a^*an = 0$, equivalente a

$$2ana + 2a^2n = 2ana^* + 2a^*an. \tag{4.11}$$

Se $ana = a^2n$, então $an = na$; senão, cada membro da equação (4.11), tem dois elementos diferentes do grupo com coeficientes não nulos e, sendo assim, devemos ter $a^2n = a^*an$ ou $a^2n = ana^*$. Se $a^2n = a^*an$, então $a = a^*$, o que contradiz a hipótese sobre a. Desta forma, temos que $a^2n = ana^*$, o que implica que $an = na^*$, ou, equivalentemente, $(a,n) = a^{-1}n^{-1}na^* = a^{-1}a^*$.

Passo 4: Mostraremos que $a^* = sa$ para algum $a \in G\backslash N$. Para isto, vamos supor por contradição que $x^* \neq sx$, para qualquer $x \notin N$.

Por suposição, existe um elemento $a \in G\backslash N$ tal que $a^* \neq a$; originando o elemento não trivial $t = a^{-1}a^* \in N$.Além disso, como também por pressuposto, $a^* \neq sa$, nós temos, pelo Passo 3, a pertinência $(a,t) \in \{1_G, t\}$.

Afirmamos que a e t comutam e que t possui ordem 2. Supondo que a e t não comutassem, teríamos que $t = (a,t) = a^{-1}t^{-1}at$, o que implicaria que $t = 1_G$, um absurdo. Além disso, de acordo com a igualdade $(a - a^*)^2 = -(a - a^*)^2$, de acordo com a igualdade (4.6), nós temos que $aa^* = a^*a$ e $(a^2)^* = a^2$. Desta maneira, $t^2 = a^{-1}a^*a^{-1}a^* = a^{-2}(a^2)^* = a^{-2}a^2 = 1_G$.

Agora, iremos dividir a demonstração em dois casos e para o primeiro deles vamos usar o elemento t e suas propriedades.

Caso 1: N é abeliano.

Vamos motrar primeiramente que t é o único comutador não trivial de G e, consequentemente que $G' = \{1, t\}$.

Recorde que podemos escrever $G = N \cup Na$ e, sendo assim, qualquer comutador de G possui alguma das seguintes formas: (n,m), (n,ma), (na,m), (na,ma) onde n e m são elementos arbitrários de N. Entretanto, como N é abeliano, já sabemos que $(n,m) = 1_G$ e pelas fórmulas (iii) e (iv) do Lema 2.1.2 também decorre que $(n,ma) = (n,a)$, $(na,m) = (a,m)$ e $(na.ma) = (n,a)(a,m)$. Deste modo, em vista de que $(a,n) \in \{1_G, t\}$ para qualquer $n \in N$ e $t^2 = 1_G$, podemos concluir que $G' = \{1_G, t\}$. Uma consequência útil deste fato é que t é independente de $x \notin N$ tal que $x^* \neq x$.

Prosseguindo, tome $n \in N$ satisfazendo $n^* = sn$. Assim, pela validade da igualdade $a^* = ta$, observe que

$$(na)^* = a^*n^* = tasn = stan = \begin{cases} stna, & \text{se} \quad an = na \\ sna & ,\text{se} \quad an \neq na. \end{cases} \tag{4.12}$$

Se $(na)^* \neq na$, então $t = (na)^{-1}(na)^*$, ou seja, $(na)^* = tna$. Neste caso $na = an$, então de acordo com (4.12) $stna = tna$ o que é impossível pois $s \neq 1_G$. Desta forma, devemos ter $na \neq an$. Novamente, por (4.12), decorre que $tna = sna$ e, consequentemente $t = s$.

Por outro lado, vamos supor que $(na)^* = na$. Se $na \neq an$, então $sna = na$ e mais uma vez obtemos uma contradição pois $s \neq 1_G$. Finalmente, se $na = an$ então $stna = na$, o que resulta em $s = t$.

Em ambos os casos, $s = t$, mas então $a^* = ta = sa$, o que é uma contradição.

Caso 2: $N' = \{1, s\}$.

Vamos primeiramente mostrar que $an \neq na$ para algum $n \in N$. Suponhamos o contrário, que $an = na$ para todo $n \in N$. Neste caso $n^*a^* = a^*n^*$ para qualquer $n \in N$, e como $n^* = n$ ou $n^* = sn$, onde s é um elemento central de G, segue que $a^*n = na^*$ para todo $n \in N$.

Seja $n \in N$ tal que $n^* = sn$. Observe que $(na)^* = a^*n^* = n^*a^* = sna^* \neq na$ pois $a^* \neq sa$. Consequentemente, $a - a^*$ e $na - (na)^* = na - sna^*$ anticomutam, o que dá origem à seguinte equação:

$$ana - sana^* - a^*na + sa^*na^* + na^2 - naa^* - sna^*a + sn(a^*)^2 = 0. \tag{4.13}$$

Agora, em vista das igualdades $an = na$, $a^*n = na^*$, $(a^*)^2 = a^2$, e $aa^* = a^*a$, a equação (4.13) pode ser reescrita como:

$$2na^2 + 2sna^2 = 2naa^* + 2snaa^*. \tag{4.14}$$

Assim, na^2 efetivamente aparece no primeiro membro desta equação, também deve aparecer no segundo membro. Entretanto isto não é possível, pois $a \neq a^*$ e $a^* = sa$. Desse modo podemos concluir que existe $n \in N$ tal que $na = an$. Assim, $(a, n) = t$.

Além disso, como an e n não comutam e a hipótese de que $(an)^* \neq san$ implica, pelo Passo 3 que $(an, n) = (an)^{-1}(an)^*$. Contudo, $an = nat$ implica que $a^{-1}n = na^{-1}t$ e também que $a^* = ta$. Portanto

$$(an)^{-1}(an)^* = n^{-1}a^{-1}n^*a^* = sn^{-1}a^{-1}na^* = sn^{-1}na^{-1}tta = s.$$

Logo $(an)^* = s(an)$ o que é contradiz a nossa hipótese e conclui a prova desse passo.

Assim completamos a Etapa 4.

Etapa 5: Conclusão dos argumentos.

De acordo com o Passo 4, podemos tomar um elemento $a \in G \backslash N$ tal que $a^* = sa$. Tanto no caso em que N é abeliano quanto se não o é e possui subgrupo $N' = \{1_G, s\}$, foi possível mostrar que $G' = \{1_G, s\}$ e, consequentemente $x^* = sx$ para qualquer $x \in G \backslash N$ tal que $x^* \neq x$. Desta forma, de acordo com o Teorema 4.4.1, podemos concluir que $g^* = g$ ou $g^* = sg$ para todo $g \in G$. ■

Capítulo 5

Nilpotência para o produto de Jordan em RG e $(RG)^+$

Para escrever este último capítulo, estudamos o artigo "Jordan nilpotency in group rings" [9]. Assim como nos Capítulos 3 e 4, iremos considerar o anel de grupo RG onde R é um anel comutativo e com elemento identidade 1. Um anel A é *Jordan nilpotente de índice n* ou *Jordan n-nilpotente*, onde $n \geq 2$, se $(\ldots((x_1 \circ x_2) \circ x_3)\ldots) \circ x_n = 0$, para quaisquer $x_1, x_2, \ldots, x_n \in A$. Iremos estudar as condições necessárias e suficientes sobre R e G para que se verifique $(\alpha \circ \beta) \circ \gamma = 0$, tanto no anel de grupo RG quanto no subconjunto $(RG)^+$, isto é, para que sejam Jordan 3-nilpotentes.

5.1 Jordan 3-nilpotência em RG

A princípio, assim como fizemos na Proposição 3.1.1, a seguir vamos caracterizar a Jordan 3-nilpotência em um anel de grupo RG.

Proposição 5.1.1 Um anel de grupo RG é Jordan 3-nilpotente se, e somente se, uma das seguintes condições se verifica:

(1) $\mathrm{car}(R) = 4$ e G é abeliano,

(2) $\mathrm{car}(R) = 2$ e G é abeliano ou G possui um único comutador não trivial s.

Demonstração: Suponhamos que vale (1), então RG é um anel comutativo. Consequentemente, $(\alpha \circ \beta) \circ \gamma = (2\alpha\beta) \circ \gamma = 4\alpha\beta\gamma = 0$ e, portanto, RG é Jordan 3-nilpotente.

Vamos supor que $\mathrm{car}(R) = 2$. Se G é abeliano, então de acordo com a Proposição 3.1.1, $\alpha \circ \beta = 0$ para quaisquer $\alpha, \beta \in RG$ e, em particular, RG é Jordan 3-nilpotente. Suponhamos que G possua um único comutador não trivial s. Sabemos que $s^2 = 1_G$ e, de acordo com a Proposição 2.2.4, s é um elemento central. Para comprovar a Jordan nilpotência de índice 3 de RG, é suficiente estabelecê-la em G. Sendo assim, tomemos $g, h, k \in G$ e analisemos inicialmente o que ocorre no caso em que g e h comutam, e na situação contrária.

Se $gh = hg$, então $(g \circ h) \circ k = (gh + hg) \circ k = 2gh \circ k = 0$. Se $gh \neq hg$, então $hg = ghs$ e, deste modo, $g \circ h = gh + ghs = gh + sgh = (1_G + s)gh$. Agora, basta analisar o comutador dos elementos gh e k.

Se $(gh, k) = 1_G$, então $(g \circ h) \circ k = (1_G + s)ghk + k(1_G + s)gh = (1_G + s)ghk + (1_G + s)ghk = 2(1_G + s)ghk = 0$. Do contrário, temos $k(gh) = (gh)ks = s(gh)k$, então $(g \circ h) \circ k = (1_G + s)gh \circ k =$

$(gh+sgh)\circ k = (gh+sgh)k+k(gh+sgh) = (gh)k+s(gh)k+k(gh)+sk(gh) = (gh)k+s(gh)k+s(gh)k+s^2(gh)k = (1_G+2s+s^2)(gh)k = (1_G+2s+1_G)(gh)k = 2(1_G+s)(gh)k = 0$.

Reciprocamente, suponhamos que RG é Jordan 3-nilpotente. Em particular, como $0 = (1\circ 1)\circ 1 = 4$, devemos ter $\mathrm{car}(R) = 2$ ou 4.

Se $\mathrm{car}(R) = 4$, então para quaisquer $g, h \in G$, vale que $(g\circ h)\circ 1_G = (gh+hg)\circ 1_G = (gh+hg)1_G + 1_G(gh+hg) = gh+hg+gh+hg = 2gh+2hg = 0$, isto é, $2hg = 2gh$, o que implica que $gh = hg$ e, portanto, G é abeliano.

Se $\mathrm{car}(R) = 2$ e G é abeliano, já está provada a proposição.

Suponhamos que G não é abeliano e sejam g, h elementos arbitrários de G. Note que $0 = (g\circ h)\circ g = (gh+hg)\circ g = (gh+hg)g + g(gh+hg) = ghg+hg^2+g^2h+ghg = 2ghg+hg^2+g^2h = hg^2+g^2h$, que implica que $hg^2 = g^2h$, para quaisquer $g, h \in G$, isto é, que quadrados são centrais em G. Desta maneira, segue da demonstração do Lema 2.2.7 que qualquer comutador não trivial de G é central e possui ordem 2.

Afirmamos que para quaisquer $a, b, c \in G$ satisfazendo $ab \neq ba$ vale que $(ab)c = c(ab)$ ou $(ab)c = c(ba)$. Com efeito, por hipótese $0 = (a\circ b)\circ c = abc+bac+cab+cba$. Se $ab \neq ba$, então $(ab)c \neq (ba)c$ e $c(ab) \neq c(ba)$ e, consequentemente, $(ab)c = c(ab)$ ou $(ab)c = c(ba)$.

Tomemos g, h e $k \in G$ pertencentes a G, tais que $gh \neq hg$ e $gk \neq kg$, e escrevemos $gh = hgs_1$ e $gk = kgs_2$, onde $s_1 = (g,h) \neq 1_G$ e $s_2 = (g,k) \neq 1_G$. Por hipótese, $0 = (gh\circ h)\circ k = (gh)hk + h(gh)k + k(gh)h + kh(gh)$, e como gh e h não comutam, de acordo com a afirmação que provamos, segue que $(gh)hk = k(gh)h$ ou $(gh)hk = kh(gh)$. Deste modo, em vista de que quadrados são centrais em G, vale que $gkh^2 = kgh^2$ ou $gkh^2 = khgh$.

Se $gkh^2 = kgh^2$, então $gk = kg$, o que contradiz a hipótese sobre g e k. Portanto $khgh = gkh^2$ o que implica que $khg = gkh = kgs_2h = kghs_2 = khgs_1s_2$. Logo, $s_1s_2 = 1_G$ e, consequentemente, $s_1 = s_2$, pois $s_2^2 = 1_G$. Assim, para quaisquer $g, h, k \in G$ tais que $(g,h) \neq 1_G$ e $(g,k) \neq 1_G$ verificamos que $(g,h) = (g,k)$ e, portanto, G é um grupo C. Decorre da Proposição 2.2.8 que G possui um único comutador não trivial s. ■

5.2 Jordan 3 - nilpotência em $(RG)^+$

Sejam R um anel de característica diferente de 2, G um grupo que possui uma involução $g \mapsto g^*$ e considere o anel de grupo RG. De acordo com a Proposição 5.1.1, a menos que $\mathrm{car}(R) = 4$ e G seja abeliano, existem $\alpha, \beta, \gamma \in RG$ tais que $(\alpha\circ\beta)\circ\gamma \neq 0_{RG}$. Assim como no Exemplo 1.2.6, a involução $*$ pode ser estendida linearmente para RG. Estamos interessados em estudar a Jordan 3-nilpotência em $(RG)^+$ que, conforme já mostramos na Seção 3.2, é gerado, sobre R, pelo conjunto $S = S_1 \cup S_2$, onde $S_1 = \{g+g^* : g \in G, g^* = g\}$ e $S_2 = \{g+g^* : g \in G, g^* \neq g\}$. É evidente que podemos fazer $S_1 = \{g \in G : g^* = g\}$.

Primeiramente, vamos provar resultados auxiliares. Supondo que $(RG)^+$ é Jordan 3-nilpotente, veremos que a característica de R deve ser 4 e que o conjunto dos elementos de G que são fixos sobre a involução $*$ possuem propriedades interessantes. Com tais resultados será possível determinar condições que são satisfeitas por dois elementos g e h de G que não comutam.

Lema 5.2.1 Seja RG um anel de grupo tal que a característica de R é diferente de 2. Se $(RG)^+$ é Jordan 3-nilpotente, então a característica de R é igual a 4, o conjunto $S_1 = \{g \in G : g^* = g\}$ é um subgrupo central de G e, além disso, $gg^* = g^*g$ e $g^{-1}g^* = g^*g^{-1}$, para qualquer $g \in G$.

Demonstração: Em vista de que $1_G \in S_1$, em particular, temos que $(1_G \circ 1_G) \circ 1_G = 4.1_G = 0$. Consequentemente, tomando $g, h \in S_1$, as igualdades $0 = (g \circ h) \circ 1_G = 2gh + 2hg$, implicam que $gh = hg$ e, portanto, S_1 é um subconjunto comutativo de G. Deste modo, se g e h pertencem a S_1, então $(gh)^* = h^*g^* = hg = gh$, isto é, $gh \in S_1$, o que prova que S_1 é um subgrupo de G.

Afirmamos que os elementos de S_1 são centrais. Com efeito, dados $g \in S_1$ e $h \in G\backslash S_1$, em particular, $h^* \neq h$, implica que $h + h^* \in S_2$. Então $0 = [g \circ (h + h^*)] \circ 1_G = 2gh + 2gh^* + 2hg + 2h^*g$ e, como $gh \neq gh^*$, segue que $gh = hg$ ou $gh = h^*g$. Supondo que $gh = h^*g$, teremos $gh = h^*g^* = h^*g = (gh)^*$ significando que $gh \in S_1$,o que é impossível pois $h \in G\backslash S_1$. Portanto, $gh = hg$, para todo $h \in G\backslash S_1$, e concluímos que $S_1 \subseteq Z(G)$.

Finalmente, dado $g \in G$, observe que, como $gg^* \in S_1$, $gg^* = gg^*g^{-1}g = g^{-1}gg^*g = g^*g$ e também, $g^*g^{-1} = g^*g^{-1}gg^{-1} = g^*gg^{-1}g^{-1} = g^{-1}g^*gg^{-1} = g^{-1}g^*$. ■

Lema 5.2.2 Seja RG um anel de grupo, onde $\text{car}(R) \neq 2$ e $(RG)^+$ é Jordan 3-nilpotente. Então, para quaisquer $g, h \in G$ que não comutam, uma das seguintes possibilidades se verifica:

(1a) $gh = g^*h^*$, $h^*g^* = hg$, $gh^* = g^*h$, $hg^* = h^*g$, $g^{-1}g^* = h^{-1}h^*$ é um elemento central de ordem 2 e g^2, h^2 pertencem a S_1;

(2a) $gh = hg^*$, $h^*g^* = gh^*$, $g^*h = hg$, $h^*g = g^*h^*$, $g^{-1}g^* = (g, h)$ e h^2 comuta com g;

(3a) $gh = h^*g$, $h^*g^* = g^*h$, $gh^* = hg$, $hg^* = g^*h^*$, $h^{-1}h^* = (h, g)$ e g^2 comuta com h.

Demonstração: Se g e h não comutam, então de acordo com o Lema 5.2.1 $g^* \neq g$ e $h^* \neq h$ e, portanto, os elementos $g + g^*$ e $h + h^*$ pertencem ao conjunto S_2. Sendo assim, $[(g + g^*) \circ (h + h^*)] \circ 1_G = 0$, isto é, vale a equação

$$2gh + 2gh^* + 2g^*h + 2g^*h^* + 2hg + 2hg^* + 2h^*g + 2h^*g^* = 0. \tag{5.1}$$

Dado que $gh \neq hg$, $gh \neq gh^*$ e $gh \neq g^*h$ e $\text{car}(R) = 4$, a equação (5.1) implica na validade de alguma das seguintes igualdades:

(1) $gh = g^*h^*$ (2) $gh = hg^*$ (3) $gh = h^*g$ (4) $gh = h^*g^*$.

Vamos analisar cada uma delas.

(1) Se $gh = g^*h^*$ a equação (5.1) pode ser reescrita como

$$2gh^* + 2g^*h + 2hg^* + 2h^*g = 0, \tag{5.2}$$

o que nos conduz a examinar os seguintes subcasos:

(1a) $gh^* = g^*h$ (1b) $gh^* = hg^*$ (1c) $gh^* = h^*g$.

(1a) Suponhamos que $g^*h = gh^*$. Multiplicando esta igualdade por g^{-1} à esquerda e por h^{-1} à direita, obtemos $g^{-1}g^* = h^*h^{-1}$. Mostramos no Lema 5.2.1, conhece-se que $g^*g^{-1} = g^{-1}g^*$,

para qualquer $g \in G$ e, sendo assim, $g^{-1}g^* = h^{-1}h^*$. Afirmamos que este elemento possui ordem 2 e é central. Com efeito, multiplicando-o por g^* à esquerda resulta em $g^*(g^{-1}g^*) = g^*(h^{-1}h^*) = g^*(h^*h^{-1}) = (g^*h^*)h^{-1} = (gh)h^{-1} = g$, então $(g^{-1}g^*)^2 = (g^{-1}g^*)(g^{-1}g^*) = g^{-1}(g^*g^{-1}g^*) = g^{-1}g = 1_G$. Para mostrar que $g^{-1}g^* = h^{-1}h^*$ é um elemento central, multiplicamos os dois membros dessa igualdade por g à esquerda e por g^* à direita, e decorre que $(g^2)^* = (g^*)^2 = gg^{-1}gg^* = gh^{-1}h^*g = gh^{-1}hg = g^2$ e, portanto, $g^2 \in S_1$. De modo similar $h^2 \in S_1$. Para concluir, suponhamos que $g^{-1}g^* \notin S_1$, isto é, $g(g^*)^1 = (g^{-1}g^*)^* \neq g^{-1}g^*$. Neste caso, $g(g(g^*)^{-1})g^* \neq g(g^{-1}g^*)g^*$ e, portanto, $(g^*)^2 \neq g^2$, o que é uma contradição. Portanto, $g^{-1}g^* = h^{-1}h^* \in S_1 \subseteq Z(G)$.

(1b) Se $gh^* = (gh^*)^*$, então $gh^* \in S_1$, e assim, gh^* é um elemento central. Em particular $ghh^* = gh^*h = hgh^*$, o que implica que g e h comutam, uma contradição.

(1c) Assumimos que $gh^* = h^*g$. Neste caso, $ghh^* = gh^*h = h^*gh = h^*g^*g^* = hgh^*$, de onde concluímos que $gh = hg$, um absurdo.

(2) Suponhamos que $gh = hg^*$. Multiplicando esta igualdade por $g^{-1}h^{-1}$ à esquerda, obtemos $g^{-1}g^* = g^{-1}h^{-1}gh = (g,h)$. Agora, aplicando a involução $*$ em ambos os membros da igualdade $gh = hg^*$, obtemos a igualdade $gh^* = h^*g^*$ e podemos reescrever a equação (5.1) como

$$2g^*h + 2g^*h^* + 2hg + 2h^*g = 0. \tag{5.3}$$

Assim, como $g^*h \neq g^*h^*$, temos dois subcasos para analisar:

(2a) $g^*h = hg$ (2b) $g^*h = h^*g$

(2a) Assumimos que $g^*h = hg$. Desse modo, $g^* = hgh^{-1}$, o que implica que $hg^* = h^2gh^{-1}$ ou, equivalentemente, $gh = h^2gh^{-1}$, por hipótese. Portanto, $gh^2 = h^2g$.

(2b) Suponha que $g^*h = h^*g$. Então $(g^*h)^* = h^*g = g^*h$, isto é, $g^*h \in S_1$ e, portanto, é central. Consequentemente, $(g^*h)h^* = h^*(g^*h)$ e, como $hh^* = h^*h$, segue que $g^*h^*h = h^*g^*h$, então $g^*h^* = h^*g^*$ e aplicando novamente a involução $*$ concluímos que $gh = hg$, o que é uma contradição. Portanto, este subcaso não ocorre.

(3) Supondo que $gh = h^*g$, podemos reescrever a equação (5.1) como

$$2gh^* + 2g^*h^* + hg + hg^* = 0. \tag{5.4}$$

Sabendo que $gh^* \neq g^*h^*$, novamente existem duas possibilidades a serem consideradas.

(3a) $gh^* = hg$ (3b) $gh^* = hg^*$

(3a) Suponhamos que $gh^* = hg$ e multiplicamos esta igualdade por $h^{-1}g^{-1}$ à esquerda, então $h^{-1}h^* = h^{-1}g^{-1}hg = (h,g)$. Agora multiplicando $gh^* = hg$ por g^{-1} à esquerda e $gh = h^*g$ por g^{-1} à direita segue que $h^* = g^{-1}hg = ghg^{-1}$ e concluímos que $hg^2 = g^2h$, ou seja, g^2 comuta com h.

(3b) Por hipótese $gh^* = hg^* = (gh^*)^*$, isto é, $gh^* \in S_1$ e, portanto, $(gh^*)g^* = g^*(gh^*)$. Assim, como $g^*g = gg^*$, temos que $gh^*g^* = gg^*h^*$, o que implica que $h^*g^* = g^*h^*$ e, portanto, $gh = hg$, o que é uma contradição.

(4) Finalmente, neste caso, $gh = h^*g^* = (gh)^*$ implica que $(gh) \in Z(G)$, pois $gh \in S_1$. ■

A caracterização da Jordan 3-nilpotência em $(RG)^+$ é feita para dois casos distintos, em dois teoremas. No primeiro, iremos supor que $(g^2)^* \neq g^2$ para algum $g \in G$, isto é, nem todos os quadrados são fixos sobre a involução $*$. No segundo, iremos supor que $(g^2)^* = g^2$, para qualquer $g \in G$, isto é, que quadrados são fixos pela involução $*$.

Teorema 5.2.3 Sejam R um anel comutativo com elemento identidade e característica diferente de 2, G um grupo e $\alpha \mapsto \alpha^*$ a involução do anel de grupo RG que é a extensão linear de uma involução $g \mapsto g^*$ de G tal que $(g^2)^* \neq g^2$, para algum $g \in G$. Então $(RG)^+$ é Jordan 3-nilpotente se, e somente se, $\mathrm{car}(R) = 4$, e G é abeliano ou, G não é abeliano e satisfaz as seguintes propriedades:

(a) qualquer $g \in G$ tal que $g^* = g$ é central;

(b) G contém um subgrupo abeliano A de índice 2;

(c) existe $c \notin A$ tal que $c^* \neq c$ e $(c^2)^* = c^2$;

(d) $a^* = c^{-1}ac$, para todo $a \in A$.

Demonstração: Vamos começar provando a recíproca do teorema. Assuma que $\mathrm{car}(R) = 4$. Se G é abeliano, então de acordo com a Proposição 5.1.1 RG é Jordan 3-nilpotente e assim, $(RG)^+$ também o é. Agora, suponhamos que G não seja abeliano e que possua uma involução $g \mapsto g^*$ que não fixa todos os quadrados e que, além disso, satisfaça as propriedades (a), (b), (c) e (d). É suficiente mostrar que para quaisquer $\alpha, \beta, \gamma \in S = S_1 \bigcup S_2$, se verifica $(\alpha \circ \beta) \circ \gamma = 0$.

Seja A um subgrupo abeliano de índice 2 de G e seja $c \in G \backslash A$ tal que $c^* \neq c$ e $(c^2)^* = c^2$. Então para qualquer $a \in A$, podemos escrever $G = A \bigcup A(ac)$. O elemento ac não é central, pois caso contrário G seria abeliano. Desta forma, de acordo com o item (a), temos que $(ac)^* \neq ac$. Assim, qualquer elemento de S_2 é da forma $a + a^*$ tal que $a \in A$ e $a^* \neq a$ ou pode ser escrito como $ac + (ac)^*$ tal que $a \in A$.

Afirmamos que $(a + a^*)(c + c^*) = (c + c^*)(a + a^*)$ e que $ac + (ac)^* = a(c + c^*)$ para qualquer $a \in A$ e, além disso, que $(c + c^*)^2 = 2c(c^* + c)$. Com efeito, de acordo com o item (d),vale que $a^* = c^{-1}ac$ (se, e somente se, $ca^* = ac$ se, e somente se, $ac^* = c^*a^*$), para qualquer $a \in A$. Por outro lado, decorre dos itens (a) e (c) que c^2 é um elemento central e, sendo assim, $a^* = c^{-1}ac$ se, e somente se, $a^*c = c^{-1}ac^2$, para todo $a \in A$, o que implica $a^*c = ca$, e portanto, $c^*a = a^*c^*$.

Desse modo, obtivemos as igualdades $ca^* = ac$, $ac^* = c^*a^*$, $a^*c = ca$ e $c^*a = a^*c^*$ e, consequentemente, podemos concluir que $(a + a^*)(c + c^*) = ac + ac^* + a^*c + a^*c^* = ca + ca^* + c^*a + c^*a^* = (c + c^*)(a + a^*)$, $(ac) + (ac)^* = ac + c^*a^* = ac + ac^* = a(c + c^*)$ e $(c + c^*)^2 = c^2 + cc^* + c^*c + (c^*)^2 = c^2 + 2cc^* + c^2 = 2cc^* + 2c^2 = 2c(c^* + c)$.

Para mostrar que $(RG)^+$ é Jordan 3-nilpotente de índice 3 é suficiente mostrar que $(\alpha \circ \beta) \circ \gamma = 0$ para quaisquer α, β, γ, cada um sendo de alguma das seguintes formas:

- z é um elemento central de A;
- $a + a^*$, tal que $a \in A$;
- $a(c + c^*)$, tal que $a \in A$ e c satisfaz (c).

Se dois dentre os elementos α, β e γ são centrais, segue diretamente que $(\alpha \circ \beta) \circ \gamma = 4\alpha\beta\gamma = 0$. Então vamos supor que um, dentre α, β, γ é central, e sem perda de generalidade seja $\alpha = z$ um elemento central de A. Assim teremos as seguintes possibilidades para β e γ:

(i) $\beta = a_1 + a_1^*$ e $\gamma = a_2 + a_2^*$.

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= [z \circ (a_1 + a_1^*)] \circ (a_2 + a_2^*)] \\
&= z(a_1 + a_1^*) + (a_1 + a_1^*)z \circ (a_2 + a_2^*) \\
&= 2z(a_1 + a_1^*) \circ (a_2 + a_2^*) \\
&= 4z(a_1 + a_1^*)(a_2 + a_2^*) \\
&= 0,
\end{aligned}$$

pois $z(a_1 + a_1^*)$ e $a_2 + a_2^*$ comutam.

(ii) $\beta = a_1 + a_1^*$ e $\gamma = a_2(c + c^*)$.

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= [z \circ (a_1 + a_1^*)] \circ a_2(c + c^*) \\
&= [z(a_1 + a_1^*) + (a_1 + a_1^*)z] \circ a_2(c + c^*) \\
&= 2z(a_1 + a_1^*) \circ a_2(c + c^*) \\
&= 2z(a_1 + a_1^*)a_2(c + c^*) + a_2(c + c^*)2z(a_1 + a_1^*) \\
&= 4z(a_1 + a_1^*)a_2(c + c^*) \\
&= 0,
\end{aligned}$$

pois $a_1 + a_1^*$ comuta com a_2 e com $c + c^*$.

(iii) $\beta = a_1(c + c^*)$ e $\gamma = a_2 + a_2^*$.

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= [z \circ a_1(c + c^*)] \circ (a_2 + a_2^*) \\
&= [za_1(c + c^*) + a_1(c + c^*)z] \circ (a_2 + a_2^*) \\
&= 2za_1(c + c^*) \circ (a_2 + a_2^*) \\
&= 2za_1(c + c^*)(a_2 + a_2^*) + 2za_1(a_2 + a_2^*)(c + c^*) \\
&= 4za_1(a_2 + a_2^*)(c + c^*) \\
&= 0.
\end{aligned}$$

(iv) $\beta = a_1(c+c^*)$, $\gamma = a_2(c+c^*)$

$$\begin{aligned}
(\alpha\circ\beta)\circ\gamma &= [z\circ a_1(c+c^*)]\circ a_2(c+c^*)\\
&= [za_1(c+c^*)+a_1(c+c^*)z]\circ a_2(c+c^*)\\
&= 2za_1(c+c^*)\circ a_2(c+c^*)\\
&= 2za_1(c+c^*)a_2(c+c^*)+2za_2(c+c^*)a_1(c+c^*)\\
&= 2za_1(ca_2+c^*a_2)(c+c^*)+2za_2(ca_1+c^*a_1)(c+c^*)\\
&= 2za_1(a_2^*c+a_2^*c^*)(c+c^*)+2za_2(a_1^*c+a_1^*c^*)(c+c^*)\\
&= 2za_1a_2^*(c+c^*)^2+2za_2a_1^*(c+c^*)^2\\
&= 4za_1a_2^*c(c^*+c)+4za_2a_1^*c(c^*+c)\\
&= 0
\end{aligned}$$

Agora, vejamos os casos em que nenhum dos elementos α, β, γ são centrais, isto é, são da forma $a+a^*$ ou $a(c+c^*)$, onde $a\in A$.

(1) $\alpha = a_1+a_1^*$, $\beta = a_2+a_2^*$ e $\gamma = a_3+a_3^*$.

$$\begin{aligned}
(\alpha\circ\beta)\circ\gamma &= [(a_1+a_1^*)\circ(a_2+a_2^*)]\circ(a_3+a_3^*)\\
&= [(a_1+a_1^*)(a_2+a_2^*)+(a_2+a_2^*)(a_1+a_1^*)]\circ(a_3+a_3^*)\\
&= 2[a_1a_2+a_1a_2^*+a_1^*a_2+a_1^*a_2^*]\circ(a_3+a_3^*)\\
&= 2(a_1a_2a_3+a_1a_2a_3^*+a_1a_2^*a_3+a_1a_2^*a_3^*+a_1^*a_2a_3+a_1^*a_2a_3^*+a_1^*a_2^*a_3+a_1^*a_2^*a_3^*\\
&+ a_3a_1a_2+a_3a_1a_2^*+a_3a_1^*a_2+a_3a_1^*a_2^*+a_3^*a_1a_2+a_3^*a_1a_2^*+a_3^*a_1^*a_2+a_3^*a_1^*a_2^*)\\
&= 4(a_1a_2a_3+a_1^*a_2a_3+a_1a_2^*a_3+a_1a_2a_3^*+a_1^*a_2^*a_3+a_1^*a_2a_3^*+a_1a_2^*a_3^*+a_1^*a_2^*a_3^*\\
&= 0.
\end{aligned}$$

(2) $\alpha = a_1+a_1^*$, $\beta = a_2+a_2^*$ e $\gamma = a_3(c+c^*)$.

$$\begin{aligned}
(\alpha\circ\beta)\circ\gamma &= [(a_1+a_1^*)\circ(a_2+a_2^*)]\circ a_3(c+c^*)\\
&= 2(a_1+a_1^*)(a_2+a_2^*)\circ a_3(c+c^*)\\
&= 2(a_1+a_1^*)(a_2+a_2^*)a_3(c+c^*)+2a_3(c+c^*)(a_1+a_1^*)(a_2+a_2^*)\\
&= 4a_3(a_1+a_1^*)(a_2+a_2^*)(c+c^*)\\
&= 0.
\end{aligned}$$

(3) $\alpha = a_1 + a_1^*$, $\beta = a_2(c + c^*)$ e $\gamma = a_3 + a_3^*$.

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= 2a_2(a_1 + a_1^*)(c + c^*) \circ (a_3 + a_3^*) \\
&= 2a_2(a_1 + a_1^*)(c + c^*)(a_3 + a_3^*) + 2(a_3 + a_3^*)a_2(a_1 + a_1^*)(c + c^*) \\
&= 2[2a_2(a_1 + a_1^*)(a_3 + a_3^*)(c + c^*)] \\
&= 4a_2(a_1 + a_1^*)(a_3 + a_3^*)(c + c^*) \\
&= 0
\end{aligned}$$

(4) $\alpha = a_1 + a_1^*$, $\beta = a_2(c + c^*)$ e $\gamma = a_3(c + c^*)$.

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= [(a_1 + a_1^*) \circ a_2(c + c^*)] \circ a_3(c + c^*) \\
&= [(a_1 + a_1^*)a_2(c + c^*) + a_2(c + c^*)(a_1 + a_1^*)] \circ a_3(c + c^*) \\
&= 2a_2(a_1 + a_1^*)(c + c^*) \circ a_3(c + c^*) \\
&= 2a_2(a_1 + a_1^*)(c + c^*)a_3(c + c^*) + 2a_3(c + c^*)a_2(a_1 + a_1^*)(c + c^*) \\
&= 2a_2(a_1 + a_1^*)(ca_3 + c^*a_3)(c + c^*) + 2a_3(ca_2 + c^*a_2)(c + c^*)(a_1 + a_1^*) \\
&= 2a_2a_3^*(a_1 + a_1^*)(c + c^*)^2 + 2a_3a_2^*(c + c^*)^2(a_1 + a_1^*) \\
&= 4a_2a_3^*(a_1 + a_1^*)c(c^* + c) + 4a_3a_2^*c(c^* + c)(a_1 + a_1^*) \\
&= 0.
\end{aligned}$$

(5) $\alpha = a_1(c + c^*)$, $\beta = a_2 + a_2^*$ e $\gamma = a_3 + a_3^*$.

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= [a_1(c + c^*) \circ (a_2 + a_2^*)] \circ (a_3 + a_3^*) \\
&= 2a_1(a_2 + a_2^*)(c + c^*) \circ (a_3 + a_3^*) \\
&= 4a_1(a_2 + a_2^*)(a_3 + a_3^*)(c + c^*) \\
&= 0.
\end{aligned}$$

(6) $\alpha = a_1(c + c^*)$, $\beta = a_2 + a_2^*$ e $\gamma = a_3(c + c^*)$.

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= 2a_1(a_2 + a_2^*)(c + c^*) \circ a_3(c + c^*) \\
&= 2a_1(a_2 + a_2^*)(c + c^*)a_3(c + c^*) + 2a_3(c + c^*)a_1(a_2 + a_2^*)(c + c^*) \\
&= 2a_1a_3^*(a_2 + a_2^*)(c + c^*)^2 + 2a_3a_1^*(c + c^*)^2(a_2 + a_2^*) \\
&= 4a_2a_3^*(a_2 + a_2^*)c(c^* + c) + 4a_3a_1^*c(c^* + c)(a_2 + a_2^*) \\
&= 0.
\end{aligned}$$

(7) $\alpha = a_1(c+c^*)$, $\beta = a_2(c+c^*)$ e $\gamma = a_3 + a_3^*$.

$$\begin{aligned}
\alpha \circ \beta &= a_1(c+c^*) \circ a_2(c+c^*) \\
&= a_1(c+c^*)a_2(c+c^*) + a_2(c+c^*)a_1(c+c^*) \\
&= a_1a_2^*(c+c^*)^2 + a_2a_1^*(c+c^*)^2 \\
&= 2(a+a^*)c(c+c^*), \text{ onde } a = a_1a_2^*
\end{aligned}$$

e, então

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= 2(a+a^*)c(c+c^*) \circ (a_3 + a_3^*) \\
&= 2(a+a^*)c(c+c^*)(a_3+a_3^*) + 2(a_3+a_3^*)(a+a^*)c(c+c^*) \\
&= 4(a+a^*)(a_3+a_3^*)c(c+c^*) \\
&= 0.
\end{aligned}$$

(8) $\alpha = a_1(c+c^*)$, $\beta = a_2(c+c^*)$, $\gamma = a_3(c+c^*)$.

Como em (7) temos que $\alpha \circ \beta = 2(a+a^*)c(c+c^*)$ onde $a = a_1a_2^*$,

então,

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= 2(a+a^*)c(c+c^*) \circ a_3(c+c^*) \\
&= 2(a+a^*)c(c+c^*)a_3(c+c^*) + 2a_3(c+c^*)(a+a^*)c(c+c^*) \\
&= 2(a+a^*)ca_3^*(c+c^*)^2 + 2a_3(a+a^*)c(c+c^*)^2 \\
&= 4(a+a^*)ca_3^*c(c^*+c) + 4a_3(a+a^*)c^2(c^*+c) \\
&= 0.
\end{aligned}$$

Mostramos que se RG é um anel de grupo, onde $\text{car}(R) = 4$ e G é um grupo abeliano ou, não abeliano satisfazendo as propriedade s (a) à (d), então para quaisquer α, β, $\gamma \in S = S_1 \bigcup S_2$ verifica-se $(\alpha \circ \beta) \circ \gamma = 0$ e, consequentemente $(RG)^+$ é Jordan-nilpotente.

Reciprocamente, vamos assumir que $(RG)^+$ é Jordan 3-nilpotente. Então, de acordo com o Lema 5.2.1, sabemos que $\text{car}(R) = 4$ e, sendo assim, se G é um grupo abeliano, o resultado já está provado. Suponhamos que G é não abeliano. Então, também pelo Lema 5.2.1, todo elemento $g \in G$ tal que $g^* = g$ é central e, desta forma, mostramos a validade de (a).

Vamos provar que a propriedade (b) é válida. Considere o conjunto $T = \{g \in G : (g^2)^* \neq g^2\}$ que é, por hipótese, não vazio. Afirmamos que T é um subconjunto comutativo de G. Com efeito, vamos supor, por contradição, que T não é comutativo, e sejam g, $h \in T$ tais que $gh \neq hg$. Assim, g e h satisfazem as condições descritas em algum dos itens (1.a), (2.a) e (3.a) do Lema 5.2.2. Entretanto, como $(g^2)^* \neq g^2$ e $(h^2)^* \neq h^2$ já sabemos que g e h não podem satisfazer as condições do item (1.a).

Admitamos que ocorra o caso (2.a). Em particular o par g, h satisfaz as duas igualdades:

$$gh = hg^* \tag{5.5}$$

$$h^*g = g^*h^*. \tag{5.6}$$

Por suposição gh e h também não comutam. Sendo assim, o par gh, h satisfaz as condições descritas de algum dos itens (1.a), (2.a) e (3.a) do Lema 5.2.2 e, novamente, temos a imediata exclusão do item (1.a) devido o pressuposto de que $(h^2)^* \neq h^2$.

Se gh e h satisfazem as condições do item (2.a) do Lema 5.22, de acordo com a igualdade (5.5), segue que $(gh)h = h(gh)^* = hh^*g^*$. Lembrando que, de acordo com o Lema 5.2.1 vale que $hh^* = h^*h$ e que $hh^* \in S_1 \subseteq Z(G)$, então $(gh)h = (g^*h^*)h$, isto é, se verifica

$$gh = g^*h^*. \tag{5.7}$$

Deste modo, usando as equações (5.6), (5.7) e o fato de que $g^*g = g^*g$ é um elemento central, decorre que $h^*g^2 = (h^*g)g = (g^*h^*)g = g^*(h^*g) = g^*(g^*h^*) = g^*(gh) = (g^*g)h = h(g^*g) = h(gg^*) = (hg)g^* = (h^*g^*)g^* = h^*(g^*)^2$, o que implica que $(g^*)^2 = g^2$, o que é uma contradição.

Supondo que gh e h satisfaçam (3.a), então, em particular $(gh)h = h^*(gh)$. Desse modo, de acordo com a equação (5.7), temos que $(gh)h = (g^*h^*)h$, isto é, $gh = g^*h^*$. Então, usando novamente a equação (5.6) e o fato de $g^*g = gg^*$ ser central para todo $g \in G$, note que $h^*g^2 = (h^*g)g = (g^*h^*)g = g^*(h^*g) = g^*(g^*h^*) = g^*(gh) = (g^*g)h = h(g^*g) = h(gg^*) = (hg)g^* = (h^*g^*)g^* = h^*(g^*)^2$, o que implica em $(g^*)^2 = g^2$ e temos novamente uma contradição.

Vamos supor, finalmente, que para g e h verifica-se o item (3.a) do Lema 5.2.2. Em particular, são válidas as duas igualdades:

$$gh = h^*g \tag{5.8}$$

$$gh^* = hg. \tag{5.9}$$

Os elementos hg e g não comutam, entretanto por suposição $g^2 \neq (g^2)^*$, então, sendo assim, podem valer para hg e g apenas os itens (2.a) ou (3.a) do Lema 5.2.2.

Se hg e g satisfazem (2.a), então pela igualdade (5.9) temos que $(hg)g = g(hg)^* = g(g^*h^*) = (gg^*)h^* = h^*(gg^*) = h^*(g^*g)$, isto é, $hg = h^*g^*$ e, equivalentemente $gh = g^*h^*$. Agora, usando a equação (5.8), observe que $h^*g^2 = (h^*g)g = (gh)g = (g^*h^*)g = g^*(h^*g) = g^*(gh) = (g^*g)h = h(g^*g) = h(gg^*) = (hg)g^* = (h^*g^*)g^* = h^*(g^*)^2$ e, portanto, $g^2 = (g^*)^2$, o que é um absurdo.

Por outro lado, se hg e g satisfazem (3.a) então de acordo com as equações (5.8) e (5.9), repare que $(hg)g = g^*(hg) = g^*(gh^*) = (g^*g)h^* = h^*(g^*g) = (h^*g^*)g$ e, portanto $hg = h^*g^*$ e, equivalentemente, $gh = g^*h^*$. Usando novamente a equação (5.8),note que $h^*g^2 = (h^*g)g = (gh)g = (g^*h^*)g = g^*(h^*g) = g^*(gh) = (g^*g)h = h(g^*g) = h(gg^*) = (hg)g^* = (h^*g^*)g^* = h^*(g^*)^2$. Portanto, $g^2 = (g^*)^2$, o que é uma contradição.

Concluímos que T é um subconjunto comutativo de G, e o término da prova do teorema seguirá do seguinte lema:

Lema 5.2.4 Seja $A = \langle T \rangle$ o subgrupo abeliano gerado por $T = \{g \in G : (g^2)^* \neq g^2\}$. Então quaisquer elementos $t \in T$ e $g \in G \backslash A$ não comutam e satisfazem as igualdades do item (3.a) do Lema 5.2.2. Além disso, $[G : A] = 2$.

Demonstração: Sejam $t \in T$ e $g \in G \backslash A$. Então $gt \notin A$ e, desta forma, $((gt)^*)^2 = (gt)^2$, isto é,

$$t^* g^* t^* g^* = gtgt \tag{5.10}$$

Vamos supor por contradição que $gt = tg$. Então $g^* t^* = t^* g^*$ e, consequentemente a equação (5.10) pode ser reescrita como $g^2 t^2 = (t^2)^*(g^2)^*$. Em vista de que g^2 é fixo sobre a involução $*$, segue que g^* é um elemento central, então $t^2 g^2 = (t^2)^*(g^*)^2$ e isto implica que $t^2 = (t^2)^*$, o que é uma contradição. Isto nos permite concluir que g e t não comutam.

Os elementos g e t devem satisfazer todas as condições de algum dos itens (1a), (2a) ou (3a) do Lema 5.2.2. Entretanto, como $(t^2)^* \neq t^2$, g e t não satisfazem (1a). Afirmamos que g e t satisfazem (3a). Com efeito, suponhamos por contradição que verificassem (2.a). Neste caso, em particular, seriam válidas as seguintes igualdades:

$$g^* t^* = t^* g \tag{5.11}$$

$$tg = g^* t \tag{5.12}$$

Então, vamos analisar o primeiro membro da igualdade (5.10), isto é, o elemento $t^* g^* t^* g^*$. De acordo com a equação (5.11), usando o fato que $gg^* = g^* g$ é central, para qualquer $g \in G$, podemos escrever $t^*(g^* t^*) g^* = gg^*(t^*)^2$. Prosseguindo, tomando o segundo membro da equação (5.10), isto é, o elemento $gtgt$, e aplicando a equação (5.12), temos que $g(tg)t = gg^* t^2$. Comparando $gg^*(t^*)^2$ e $gg^* t^2$, chegamos a $(t^2)^* = t^2$, o que é uma contradição.

Até aqui mostramos que quaisquer elementos $t \in T$ e $g \in G \backslash A$ não comutam e satisfazem as igualdades do item (3.a) do Lema 5.2.2.

Prosseguindo, provemos que o índice de A em G é igual a 2. Para isto, tomemos g e h pertencentes a $G \backslash A$ e $t \in T$. Acabamos de mostrar que g e h não comutam com t e, que além disso, para cada um dos pares g, t e h, t valem as igualdades do item (3a) do Lema 5.2.2 Em particular,

$$ht = t^* h \tag{5.13}$$

$$gt^* = tg \tag{5.14}$$

Sendo assim, de acordo com as equações (5.13) e (5.14), note que $(gh)t = (gt^*)h = t(gh)$; e como $t^* \neq t$, temos que $(gh)t \neq t^*(gh)$, isto é, gh e t não satisfazem a equação (5.13) e, portanto, não satisfazem o item (3a) do Lema 5.2.2. Concluímos que $gh \in A$. Agora, tomemos $c \notin A$. De acordo com o que acabamos de mostrar, para quaisquer $g \notin A$ verifica-se que $gc^{-1} \in A$ e, portanto, $g \in Ac$, o que implica que $G = A \bigcup Ac$, isto é, $[G : A] = 2$. □

O elemento c não é fixado pela involução $*$, pois do contrário, de acordo com o Lema 5.2.1, este seria um elemento central, o que implicaria que G seria um grupo abeliano, o que não é o nosso caso. Além disso como $c \notin T$, então $(c^2)^* = c^2$ e com isso, mostramos o item (c).

Finalmente, para $c \neq A$ e $t \in T$, estes elementos não comutam e satisfazem as condições do caso (3.a) do Lema 5.2.2 e, em particular, pela terceira equação segue que $ct^* = tc$ e, então $t^* = c^{-1}tc$. Assim, como T gera A segue que $a^* = c^{-1}ac$ para todo $a \in A$, e o item (d) está provado. ■

Conforme comentamos, iremos no próximo teorema caracterizar a Jordan 3-nilpotência em $(RG)^+$ para o caso em que quadrados são fixos pela involução $*$. Note que, de acordo com o Lema 5.2.1,

sabemos que $(g^2)^* = g^2$,para qualquer $g \in G$, o que implica que quadrados são centrais em G, o que nos motiva a enunciar o teorema da seguinte maneira:

Teorema 5.2.5 Seja RG um anel de grupo, onde R é um anel comutativo, com elemento identidade e característica diferente de 2. Seja $g \mapsto g^*$ uma involução de G que se estende linearmente à uma involução $*$ de RG. Então $(RG)^+$ é Jordan 3-nilpotente se, e somente se, $\mathrm{car}(R) = 4$ e G é abeliano ou não é abeliano com os quadrados centrais e a involução $g \mapsto g^*$ satisfazendo as seguintes propriedades:

(a) Qualquer $g \in G$ tal que $g^* = g$ é central;

(b) Para cada $g \in G$, existe um elemento central s_g, tal que $g^* = s_g g$ e $s_g^2 = 1_G$;

(c) Se $g, h \in G$ não comutam, então $s_g = s_h$ ou $s_g = (g,h)$ ou $s_h = (g,h)$;

(d) Para quaisquer $g, h, k \in G$ tais que $g^* \neq g$, $h^* \neq h$ e $k^* \neq k$, alguma das seguintes condições se verifica:

  (i) três entre os elementos s_g, s_h, s_k, (g,h), (gh,k) são iguais;

  (ii) $(g,h) \in \mathcal{A} = \{1, s_g, s_h, s_k, s_g s_h, s_g s_k, s_h s_k, s_g s_h s_k\}$ e $s_g \in \mathcal{B} = \{s_h, s_k, s_h s_k, s_g s_h s_k\}$;

  (iii) $(gh,k) \in \mathcal{A}$ e $s_g \in \mathcal{B}$;

  (iv) $(g,h) \in \mathcal{A}$ e $(gh,k) \in \mathcal{A}$;

  (v) $(g,h) = (gh,k)x$, para algum $x \in \mathcal{A}$ e $s_g \in \mathcal{B}$;

  (vi) $(g,h) = (gh,k)x$, para algum $x \in \mathcal{A}$ e $s_g = (gh,k)y$, para algum $y \in \mathcal{A}$.

Demonstração: Suponhamos que $(RG)^+$ seja Jordan 3-nilpotente. Então, de acordo com o Lema 5.2.1 temos que $\mathrm{car}(R) = 4$. Se G é abeliano, então segue o resultado. Se G não é abeliano, então novamente pelo Lema 5.2.1, todo elemento de G que é fixo sobre a involução $*$ é central e, com isso, o item (a) é válido.

Para comprovar o item (b), multiplicamos a igualdade $(g^*)^2 = g^2$ por g^{-1} do lado esquerdo e por $(g^*)^{-1}$ do lado direito, concluindo que $g^{-1}g^* = g(g^*)^{-1}$, para qualquer $g \in G$. Escrevendo $g^{-1}g^* = s_g$, temos que $s_g^* = (g^{-1}g^*)^* = g(g^{-1})^* = g(g^*)^{-1} = g^{-1}g^* = s_g$, isto é, s_g é um elemento central e, desta forma, $g^* = gs_g = s_g g$, para qualquer $g \in G$. Agora, usando o fato que g^*g também é central, note que $s_g^2 = s_g s_g = s_g s_g^* = (g^{-1}g^*)(g(g^*)^{-1}) = g^{-1}(g^*g)(g^*)^{-1} = g^{-1}((g^*)^{-1}g^*)g = g^{-1}g = 1_G$, para qualquer $g \in G$.

Mostremos (c). Sejam $g, h \in G$ tais que $gh \neq hg$. Então g e h satisfazem as igualdades que estão descritas em um dos itens (1a), (2a) e (3a) do Lema 5.2.2. Desta forma, temos respectivamente que

- $g^{-1}g^* = h^{-1}g^*$ e, portanto, $s_g = s_h$;
- $g^{-1}g^* = (g,h)$, isto é, $s_g = (g,h)$;
- $h^{-1}h^* = (h,g)$, isto é, $s_h = (h,g)$.

Agora, somente falta verificar a validade de (d). Para isto, inicialmente tomemos os elementos $\alpha = g + g^*$, $\beta = h + h^*$ e $\gamma = k + k^*$ pertencentes a S_2. Mostramos no item (a) que os elementos

$s_g = g^{-1}g^*$, $s_h = h^{-1}h^*$ e $s_k = k^{-1}k^*$ são centrais, e de acordo com o Lema 2.2.7, todos os comutadores também são centrais e possuem ordem 2. Desta maneira, temos que

$$\begin{aligned}
0 &= (\alpha \circ \beta) \circ \gamma = [(g+g^*) \circ (h+h^*)] \circ (k+k^*) \\
&= (g+g^*)(h+h^*)(k+k^*) + (h+h^*)(g+g^*)(k+k^*) \\
&+ (k+k^*)(g+g^*)(h+h^*) + (k+k^*)(h+h^*)(g+g^*) \\
&= ghk + ghk^* + gh^*k + gh^*k^* + g^*hk + g^*hk^* + g^*h^*k + g^*h^*k^* \\
&+ hgk + hgk^* + hg^*k + hg^*k^* + h^*gk + h^*gk^* + h^*g^*k + h^*g^*k^* \\
&+ kgh + kgh^* + kg^*h + kg^*h^* + k^*gh + k^*gh^* + k^*g^*h + k^*g^*h^* \\
&+ khg + khg^* + kh^*g + kh^*g^* + k^*hg + k^*hg^* + k^*h^*g + k^*h^*g^* \\
&= (1_G + s_g + s_h + s_k + s_gs_h + s_gs_k + s_hs_k + s_gs_hs_k)(ghk + hgk + kgh + khg) \\
&= kgh(1_G + s_g)(1_G + s_h)(1_G + s_k)(1_G + (g,h))(1_G + (gh,k)).
\end{aligned}$$

Denotando $(g,h) = c_1$ e $(gh,k) = c_2$, obtemos a equação

$$(1_G + s_g)(1_G + s_h)(1_G + s_k)(1_G + c_1)(1_G + c_2) = 0. \tag{5.15}$$

O lado esquerdo da equação (5.15) é formado por 32 parcelas, onde cada uma delas é um elemento de G. Desta forma, devido a característica de R ser igual a 4, podemos concluir que o conjunto destas 32 parcelas é formado pela união de 8 subconjuntos, onde cada um deles contêm exatamente 4 elementos iguais. Tomando $1_G + s_g + s_h + s_k + s_gs_h + s_gs_k + s_hs_k + s_gs_hs_k = A$, a equação (5.15) pode ser reescrita como

$$A + c_1A + c_2A + c_1c_2A = 0 \tag{5.16}$$

ou, equivalentemente,

$$(1_G + c_2)(A + c_1A) = 0. \tag{5.17}$$

Note que o conjunto $\mathcal{A}$, descrito em no item (ii) do teorema é o suporte de A e é também um subgrupo de G. Iremos tomar $s_g \in \mathcal{A}$ e analisar, por exaustão, os seguintes casos:

(I) Quatro elementos de $\mathcal{A}$ são iguais a s_g;

Já sabemos que $s_g \neq 1_G$, $s_g \neq s_gs_h$ e que $s_g \neq s_gs_k$ e, desta forma $s_g = s_gs_hs_k$, o que implica que $s_h = s_k$ e, portanto, mostramos (i).

(II) $s_g = c_1x$ para algum $x \in \mathcal{A}$;

Neste caso, $c_1 = s_gx \in \mathcal{A}$, então $c_1 \in \mathcal{A}$. Isto implica que $c_1A = A$, então a equação (5.17) pode ser reescrita como $2(1+c_2)A = 0$. Como $\mathrm{car}(R) \neq 2$, obtemos que

$$A + c_2A = 0. \tag{5.18}$$

Agora, a equação (5.18), nos fornece dois subcasos a considerar:

(II') $s_g = y$, para algum $y \in \mathrm{supp(A)}$ e (II'') $s_g = c_2y$, para algum $y \in \mathrm{supp(A)}$

(II′) Neste caso, $s_g \in \mathcal{B} = \{s_h, s_k, s_h s_k, s_g s_h s_k\}$ e segue o caso (ii).

(II″) Se $s_g = c_2 y$, $y \in \mathcal{A}$, então como tivemos anteriormente $c_2 = s_g y \in \mathcal{A}$, isto é, $(gh, k) \in \mathcal{A}$, de onde segue o caso (iv).

(III) $s_g = c_2 x$ para algum $x \in \mathcal{A}$.

Usando os mesmos argumentos do caso (II), temos $c_2 \in \mathcal{A}$, $c_2 A = A$ e a equação

$$A + c_1 A = 0 \tag{5.19}$$

Similarmente, a equação (5.19) nos diz que $s_g = y \in \mathcal{A}$, o que implica que $s_g \in \mathcal{B}$ seguindo-se o caso (iii); ou $s_g = c_1 y$, o que implica que $c_1 = s_g y \in \mathcal{A}$, seguindo-se o caso (iv).

(IV) $s_g = c_1 c_2 x$ para algum $x \in \mathcal{A}$.

Primeiramente $c_1 c_2 = s_g x \in \mathcal{A}$. Em vista de que comutadores são centrais e possuem ordem 2, temos que $c_1 = c_2 s_g x$, e como $s_g x \in \mathcal{A}$, então $c_1 A = c_2 s_g x A = c_2 A$. Deste modo, $A + c_1 A + c_2 A + c_1 c_2 A = A + c_2 A + c_2 A + A = 2(A + c_2 A) = 0$, isto é, $A + c_2 A = 0$ de onde segue que $s_g \in \mathcal{B}$, o que mostra (v); ou $s_g = c_2 y = (gh, k) y$, $y \in \mathcal{A}$, que é o caso (vi).

Reciprocamente, mostraremos que se $\mathrm{car}(R) = 4$ e G é um grupo que não é abeliano satisfazendo as propriedades (a)-(d) do teorema, então $(RG)^+$ é Jordan 3-nilpotente. Para isto, é suficiente mostrar que

$$(\alpha \circ \beta) \circ \gamma = 0 \tag{5.20}$$

para quaisquer $\alpha, \beta, \gamma \in S = S_1 \cup S_2$.

Dividimos a prova nas 3 partes seguintes:

(I) Pelo menos dois dentre α, β e γ pertencem a S_1.

(II) Apenas um dentre α, β, γ pertence a S_1.

(III) α, β e γ pertencem a S_2.

(I) Se pelo menos dois dentre α, β e γ pertencem a S_1, isto é, são centrais, é imediato que $(\alpha \circ \beta) \circ \gamma = 2\alpha\beta \circ \gamma = 4\alpha\beta\gamma = 0$.

(II) Suponhamos, sem perda de generalidade, que $\alpha \in S_1$ e vamos escrever $\alpha = z$. Sabemos de acordo com (b) que que $\beta = g + s_g g$ e $\gamma = h + s_h h$ onde $s_g, s_h \in Z(G)$ e $s_g^2 = s_h^2 = 1_G$. Desta forma, $\alpha \circ \beta = 2(1_G + s_g) zg$ e, portanto, podemos reescrever o lado esquerdo da equação (5.20) da seguinte maneira:

$$\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= 2(1_G + s_g) zg \circ (1_G + s_h) h \\
&= 2z(1_G + s_g)(1_G + s_h) gh + 2z(1_G + s_g)(1_G + s_h) hg \\
&= 2z(1_G + s_g)(1_G + sh)(gh + hg).
\end{aligned}$$

Se $gh = hg$, então $(\alpha \circ \beta) \circ \gamma = 4z(1 + s_g)(1 + s_h) hg = 0$.

Suponhamos que $gh \neq hg$. Por hipótese, sabemos que quadrados são centrais. Então, relembrando que, de acordo com a demonstração do Lema 2.2.7, comutadores são centrais e possuem ordem 2, podemos escrever $hg = (g,h)gh$ e, desta forma, $(\alpha \circ \beta) \circ \gamma = 2z(1+s_g)(1+s_h)(1+(g,h))gh$.

Pelo item (c), temos que $s_g = s_h$ ou $s_g = (g,h)$ ou $s_h = (g,h)$ e em qualquer um destes casos teremos $(\alpha \circ \beta) \circ \gamma = 0$.

(III) Sejam $\alpha = g + g^*$, $\beta = h + h^*$ e $\gamma = k + k^* \in S_2$. Utilizando (b) e o fato de que comutadores são centrais e possuem ordem 2, da mesma maneira que construímos a equação (5.15), decorre que

$$(\alpha \circ \beta) \circ \gamma = (1+s_g)(1+s_h)(1+s_k)(1+c_1)(1+c_2) \tag{5.21}$$

onde $c_1 = (g,h)$ e $c_2 = (gh,k)$.

Então, vamos aplicar ao lado direito da equação (5.21) cada uma das condições (i), (ii), (iii) e (iv) do item (d).

(i) Três dentre s_g, s_h, s_k, c_1, c_2 são iguais a um mesmo elemento s. Neste caso ocorre $(1_G + s)^3 = 4(1_G + s) = 0$.

(ii) $c_1 \in \mathcal{A} = \{1_G, s_g, s_h, s_k, s_g s_h, s_g s_k, s_h s_k, s_g s_h s_k\}$ e $s_g \in \mathcal{B} = \{s_h, s_k, s_h s_k, s_g s_h s_k\}$.
Vamos novamente fazer $1_G + s_g + s_h + s_k + s_g s_h + s_g s_k + s_h s_k + s_g s_h s_k = A$. Então, de maneira similar à construção da equação (5.17), reescrevemos a equação (5.21) como

$$(\alpha \circ \beta) \circ \gamma = (1_G + c_2)(A + c_1 A) \tag{5.22}$$

Sabendo que c_1 pertence a $\mathcal{A}$, o que é um grupo, o lado direito da equação (5.22) pode ser reescrito como $2(1_G + c_2)A$. Agora, como $s_g \in \mathcal{B} = \{s_h, s_k, s_h s_k, s_g s_h s_k\}$, temos os seguintes casos para analisar:

- $s_g = s_h$.
  Neste caso,

$$\begin{aligned} A &= 1_G + s_g + s_g + s_k + s_g s_g + s_g s_k + s_g s_k + s_g s_g s_k \\ &= 2 + 2s_g + 2s_k + 2s_h s_k = 2(1_G + s_g + s_k + s_g s_k) \\ &= 2B_1, \text{ onde } \mathrm{B_1 = 1_G + s_g + s_k + s_g s_k}. \end{aligned}$$

  Então $(\alpha \circ \beta) \circ \gamma = 4(1_G + c_2)B_1 = 0$.

- $s_g = s_k$.
  Neste caso,

$$\begin{aligned} A &= 1_G + s_g + s_h + s_g + s_g s_h + s_g s_g + s_h s_g + s_h \\ &= 2(1_G + s_g + s_h + s_g s_h) \\ &= 2B_2, \text{ onde } \mathrm{B_2 = 1_G + s_g + s_h + s_g s_h}. \end{aligned}$$

  Então $(\alpha \circ \beta) \circ \gamma = 4(1_G + c_2)B_2 = 0$.

- $s_g = s_h s_k$.
  Neste caso,

$$\begin{aligned} A &= 1_G + s_h s_k + s_h + s_k + s_h s_k s_h + s_h s_k s_k + s_h s_k + s_h s_k s_h s_k \\ &= 2(1_G + s_h s_k + s_k + s_h) \\ &= 2B_3, \text{ onde } \mathrm{B_3 = 1_G + s_k + s_h + s_h s_k}. \end{aligned}$$

  Então $(\alpha \circ \beta) \circ \gamma = 4(1_G + c_2)B_3 = 0$.
- $s_g = s_g s_h s_k$, isto é, $s_h = s_k$. Neste caso,

$$\begin{aligned} A &= 1_G + s_g + s_h + s_h + s_g s_h + s_g s_h + 1 + s_g \\ &= 2(1_G + s_g + s_h + s_g s_h) \\ &= 2B_4, \text{ onde } \mathrm{B_4 = 1_G + s_g + s_h + s_g s_h}. \end{aligned}$$

  Então $(\alpha \circ \beta) \circ \gamma = 4(1_G + c_2)B_4 = 0$.

(iii) Por suposição, tem-se que $c_2 \in \mathcal{A}$. Então utilizando o mesmo argumento que em (ii), podemos reescrever o lado direito da equação (5.22) como $2(1_G + c_1)A$. Também sabemos que $s_g \in \mathcal{B}$ e mostramos em (ii) que se $s_g \in \mathcal{B}$, então $A = 2B$ e, desta maneira,

$$(\alpha \circ \beta) \circ \gamma = 4(1_G + c_1)2B = 0.$$

(iv) Se c_1 e c_2 pertencem a $\mathcal{A}$, então da equação (5.22):

$$(\alpha \circ \beta) \circ \gamma = A + c_1 A + c_2 A + c_1 c_2 A = A + A + A + A = 4A = 0.$$

(v) Se $c_1 = c_2 x$, para algum $x \in \mathcal{A}$, então $c_1 A = c_2 x A = c_2 A$. Além disso, $c_1 c_2 = x \in \mathcal{A}$ e, portanto, $c_1 c_2 A = A$. Desta forma, o lado direito da equação (5.22) pode ser escrito como $2A + 2c_2 A$. Assim, como também $s_g \in \mathcal{B}$, então do mesmo modo que em (iii):

$$(\alpha \circ \beta) \circ \gamma = 4B + 4c_2 B = 0.$$

(vi) Da mesma maneira que em (v), temos que $(\alpha \circ \beta) \circ \gamma = 2A + 2c_2 A$. Se $s_g = c_2 y$, para algum $y \in \mathcal{A}$, então $c_2 = s_g y^{-1} \in \mathcal{A}$ e, desta maneira, $c_2 A = A$. Então,

$$(\alpha \circ \beta) \circ \gamma = 2A + 2A = 4A = 0.$$

■

Concluímos este capítulo com um exemplo que comprova que a Jordan nilpotência de índice 3 de $(RG)^+$ não implica a Jordan nilpotência de índice 3 de RG. Com efeito, o exemplo é um grupo G satisfazendo as condições (a) - (d) do Teorema 5.2.5 (o que implica em característica 4, $(RG)^+$ é Jordan nilpotente de índice 3), mas G não é abeliano (então, R não é Jordan nilpotente de índice 3 em característica 4) nem existe um único comutador não trivial.

Exemplo 5.2.6 Seja $G = G_1 \times G_2$ o produto direto dos grupos SLC G_1 e G_2, onde $G_1' = \{1, s_1\}$ e $G_2' = \{1, s_2\}$, e seja a involução $*$ de G definida por $(a, b)^* = (a^*, b^*)$, onde as involuções de G_1 e G_2 são as canônicas. Afirmamos que G satisfaz as condições do Teorema 5.2.5. Com efeito,

(a) Seja $g = (a,b) \in G$, tal que $g^* = g$. Então $a^* = a$ e $b^* = b$. De acordo com o Teorema 2.2.17, $a \in Z(G_1)$ e $b \in Z(G_2)$ e, portanto, $g = (a,b)$ é um elemento central.

(b) Se $a \in G_1$, então $a^* = a$ ou $a = s_1 a$ e, da mesma forma, se $b \in G_2$, então $b^* = b$ ou $b^* = s_2 b$. Desta maneira, para qualquer $g \in G$ existe um elemento s_g central e de ordem 2, tal que $g^* = s_g g$ e s_g deve, necessariamente, ser algum dos seguintes elementos $(1,1)$, $(s_1,1)$, $(1,s_2)$, (s_1,s_2). Cada um deles é central de ordem 2.

(c) Sejam $g = (a,b)$ e $h = (x,y)$ pertencentes a G e que não comutam. Então verifica-se alguma das seguintes condições:

(i) $ax \neq xa$ e $by = yb$ (ii) $by \neq yb$ e $ax = xa$ (iii) $ax \neq xa$ e $by \neq yb$

(i) Se $ax \neq xa$, então $ax = s_1 xa$. Desta forma, $gh = (a,b)(x,y) = (ax,by) = (s_1 xa, yb) = (s_1,1)(x,y)(a,b) = (s_1,1)hg = hg(s_1,1) = hgs_g$. Portanto $s_g = (g,h)$.

(ii) Se $by \neq yb$, então $by = s_2 yb$. Desse modo, $gh = (a,b)(x,y) = (ax,by) = (xa, s_2 yb) = (1,s_2)(x,y)(a,b) = (1,s_2)hg = hg(1,s_2) = hgs_g$. Logo, $s_g = (g,h)$.

(iii) Se $ax \neq xa$ e $by \neq yb$, então $ax = s_1 xa$ e $by = s_2 yb$. Assim, $gh = (a,b)(x,y) = (ax,by) = (s_1 xa, s_2 yb) = (s_1,s_2)(x,y)(a,b) = (s_1,s_2)hg = hg(s_1,s_2) = hgs_g$. Consequentemente, $s_g = (g,h)$.

(d) Se $g, h, k \in G$ são tais que $g^* \neq g$, $h^* \neq h$ e $k^* \neq k$, então $s_g \neq 1$, $s_h \neq 1$ e $s_k \neq 1$. Se $s_g = s_h = s_k$, então verifica-se o item (i). Caso contrário, o subgrupo central $\mathcal{A}$ possui ordem 4. Desta forma, $\mathcal{A} = Z(G)$ e segue o item (iv).

Capítulo 6

Considerações Finais

Nesta dissertação, nosso principal objetivo era estudar a nilpotência de Jordan em um anel de grupo RG e de um subconjunto particular bastante conhecido $(RG)^+$. Apesar de não seguirmos a abordagem que vamos citar, os casos em que (RG) e $(RG)^+$ são Jordan nilpotentes de índice 2, ou equivalentemente, RG e $(RG)^+$ são anticomutativos foram detalhadamente apresentados no Capítulo 3, onde consideramos $(RG)^+$ com uma involução arbitrária.

Uma generalização natural de uma involução arbitrária e obviamente da involução clássica, e que tem sido bastante estudada nos últimos anos, é a involução orientada. Expomos no Capítulo 4, as condições necessárias e suficientes para que $(RG)^+$ seja anticomutativo com tal involução.

Finalmente, no último capítulo, apresentamos as demonstrações de quando RG e $(RG)^+$ são Jordan nilpotentes de índice 3, do artigo [9], que foi publicado, recentemente, em 2014.

Apresentamos nas tabelas a seguir um histórico do andamento da pesquisa neste assunto.

$(RG)^+$	Involução Clássica	Involução Arbitrária	Involução Orientada
Comutativo	[2]	[12]	[8]
Anticomutativo	-	Capítulo 3 [7]	Capítulo 4 [10]

Tabela 6.1: Pesquisas sobre comutatividade e anticomutatividade em $(RG)^+$

$(RG)^-$	Involução Clássica	Involução Arbitrária	Involução Orientada
Comutativo	[3]	[11] e [14]	[13]
Anticomutativo	-	[7]	[8]

Tabela 6.2: Pesquisas sobre comutatividade e anticomutatividade em $(RG)^-$

Nilpotência de Jordan	RG	$(RG)^+$ involução arbitrária	$(RG)^-$ involução arbitrária
Índice 2	Capítulo 3 [7] [2]	Capítulo 3 [7]	[7]
Índice 3	Capítulo 5 [9]	Capítulo 5 [9]	Problema em aberto
Índices maiores	Problema em aberto	Problema em aberto	Problema em aberto

Tabela 6.3: Pesquisas sobre nilpotência de Jordan em RG, $(RG)^+$ e $(RG)^-$

Por uma questão de espaço, decidimos não abordar o também famoso subconjunto de RG, $(RG)^-$. Entretanto, é importante salientar que sequer se conhece ainda as condições necessárias e suficientes para que este seja Jordan nilpotente de índice 3, assim como permanecem como problemas em aberto estudar tal questão para índices maiores de RG, $(RG)^+$ e $(RG)^-$.

Durante a dissertação, apareceram propriedades interessantes que são satisfeitas por grupos SLC. Tais propriedades também possuem conexão com a teoria de loops, o que motiva o estudo da classificação dos grupos C que não são LC e vice-versa, assim como a abordagem dos problemas mencionados para o caso não associativo.

Referências Bibliográficas

[1] O. B. Cristo. *A comutatividade dos elementos simétricos e antissimétricos em Anéis de Grupo - Tese de doutorado*. Instituto de Matemática e Estatística da Universidade de São Paulo, IME - USP, 2003.

[2] O. B. Cristo. Commutativity of symmetric elements in group rings. *J. Group Theory*, 9:673–683, 2006.

[3] O. B. Cristo and C. Polcino Milies. Commutativity of skew symmetric elements in group rings. *Proceedings of the Edinburgh Mathematical Society*, 50:37–47, 2007.

[4] R. B. dos Santos. *Elementos Simétricos sob Involuções Orientadas em Anéis de Grupos - Dissertação de Mestrado*. Instituto de Ciências Exatas - UFMG, Departamento de Matemática, 2012.

[5] E. Goodaire, E. Jespers and C. Polcino Milies. *Alternative Loop Rings*. North-Holand Math. Stud., Elsevier Amsterdam, 1996.

[6] E. G. Goodaire and C. Polcino Milies. Oriented involutions, symmetric and skew- symmetric elements in group rings. *J. Group Theory*, 17:1–17, 2011.

[7] E. G. Goodaire and C. Polcino Milies. Involutions and anticommutativity in group rings. *Canad. Math. Bull*, 56(2):344 – 353, 2013.

[8] E. G. Goodaire and C. Polcino Milies. Oriented involutions and skew symmetric elements in group rings. *J. Algebra Appl*, 12(1):125 –131, 2013.

[9] E. G. Goodaire and C. Polcino Milies. Jordan nilpotency in group rings. *J. Group Theory*, 17:541–557, 2014.

[10] E. G. Goodaire and C. Polcino Milies. Oriented group involutions and anticommutativity in group rings. *Communications in Algebra*, 42:1657–1667, 2014.

[11] E. Jespers and M. R. Marin. Antissymetric elements in group rings. *J. Algebra Appl*, 4(4):341 – 351, 2005.

[12] E. Jespers and M. R. Marin. On symmetric elements and symmetric units in group rings. *Comm. Algebra*, 34:727 – 736, 2006.

[13] E. J. O. B. Cristo and M. R. Marin. Antissymetric elements in group rings with an orientation morphism. *Forum Math*, 21(3):427 – 454, 2009.

[14] E. J. O. B. Cristo and C. P. Milies. Antissymetric elements in group rings ii. *J. Algebra Appl*, 8(1):115 – 127, 2009.

[15] C. Polcino Milies and S. K. Sehgal. *An Introdution to Group Rings*. Kluwer Academic, Dordrecht, 2002.

[16] J. J. Rotman. *An introduction to Theory of Groups, 4th Edition*. Graduate Texts in Mathematics. Springer-Verlag, New York, 1995.

[17] W. R. Scott. *Group Theory*. Dover Publications, New York, 1987.

[18] A. D. Thomas and G. V. Wood. *Group Tables*. Shiva Publishing Limited, 1980.