UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Dissertação de Mestrado

Elementos Simétricos sob Involuções Orientadas em Anéis de Grupos

Rafael Bezerra dos Santos

Belo Horizonte

2012

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Rafael Bezerra dos Santos

Elementos Simétricos sob Involuções Orientadas em Anéis de Grupos

Dissertação apresentada ao corpo docente de Pós-Graduação em Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, como parte dos requisitos para a obtenção do título de Mestre em Matemática.

Orientadora: Paula Murgel Veloso

Belo Horizonte
13 de fevereiro de 2012

Aos meus pais,
Aurino e Célia.

"Sempre me pareceu estranho que todos aqueles que estudam seriamente esta ciência acabam tomados de uma espécie de paixão pela mesma. Em verdade, o que proporciona o máximo de prazer não é o conhecimento e sim a aprendizagem, não é a posse mas sim a aquisição, não é a presença mas o ato de atingir a meta."

Carl Friedrich Gauss

ATA DA CENTÉSIMA NONAGÉSIMA TERCEIRA DEFESA DE DISSERTAÇÃO DO ALUNO RAFAEL BEZERRA DOS SANTOS, REGULARMENTE MATRICULADO NO PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE MINAS GERAIS, REALIZADA NO DIA 13 DE FEVEREIRO DE 2012.

Aos treze dias do mês de fevereiro de 2012, às 15:00 horas, na Sala 3060, reuniram-se os professores abaixo relacionados, formando a Comissão Examinadora homologada pelo Colegiado do Programa de Pós-Graduação em Matemática, para julgar a defesa de dissertação do aluno **Rafael Bezerra dos Santos**, intitulada: *"Elementos Simétricos sob Involuções Orientadas em Anéis de Grupos"*, requisito final para obtenção do Grau de mestre em Matemática. Abrindo a sessão, a Senhora Presidente da Comissão, Profª. Paula Murgel Veloso, após dar conhecimento aos presentes o teor das normas regulamentares do trabalho final, passou a palavra ao aluno para apresentação de seu trabalho. Seguiu-se a arguição pelos examinadores com a respectiva defesa do aluno. Após a defesa, os membros da banca examinadora reuniram-se sem a presença do aluno e do público, para julgamento e expedição do resultado final. Foi atribuída a seguinte indicação: o aluno foi considerado aprovado, por unanimidade. O resultado final foi comunicado publicamente ao aluno pela Senhora Presidente da Comissão. Nada mais havendo a tratar, a Presidente encerrou a reunião e lavrou a presente Ata, que será assinada por todos os membros participantes da banca examinadora. Belo Horizonte, 13 de fevereiro de 2012.

Paula Murgel Veloso

PROFª. PAULA MURGEL VELOSO
Orientadora (UFMG)

Carmen Rosa Giraldo V

PROFª. CARMEN ROSA GIRALDO VERGARA
Examinador (UFMG)

PROF. FRANCISCO CÉSAR POLCINO MILIES
Examinador - (USP)

Sumário

Agradecimentos

Aos meus pais, Aurino e Célia, por sempre acreditarem que o conhecimento é a maior herança que pode ser deixada.

À minha orientadora Paula Murgel Veloso, pela presença, apoio, compreensão e motivação.

Aos professores que participaram da banca examinadora, Francisco César Polcino Milies, Carmen Rosa Giraldo Vergara e Ana Cristina Vieira, que contribuíram com correções e valiosas sugestões.

Aos professores do Departamento de Matemática da UFMG que contribuíram para a minha formação.

Às professoras Maria Elisa Esteves Lopes Galvão e Marly Mandia que, durante a minha graduação no Centro Universitário FIEO, sempre acreditaram na minha capacidade e me incentivaram à pesquisa.

Aos amigos e colegas da Pós-Graduação em Matemática da UFMG, em especial ao Celso, Danilo e Juliano pelas proveitosas discussões e pela agradável companhia durante as pausas para o café.

Às meninas da Secretaria de Pós-Graduação em Matemática, Andréa e Kelli, pela constante ajuda.

À toda minha família, pelo apoio incondicional, em especial às minhas avós Maria e Dalva pelas orações.

À CAPES pelo auxílio financeiro.

Resumo

Sejam R um anel comutativo com identidade, G um grupo e RG o anel de grupo de G sobre R. Dados σ uma orientação de G e φ uma involução em G, considere $\sigma\varphi$ uma involução orientada em RG. O objetivo deste trabalho é obter condições necessárias e suficientes sobre o anel R e o grupo G para que $(RG)_{\sigma\varphi}$, o conjunto dos elementos simétricos de RG sob a involução orientada $\sigma\varphi$, seja comutativo. Este trabalho é baseado na referência [8].

Palavras chave: Anel de grupo, involução orientada, elementos simétricos.

Abstract

Let R be a commutative ring with identity, G be a group and RG be the group ring of G over R. Given σ an orientation of G and φ an involution in G, consider $\sigma\varphi$ an oriented involution in RG. The main goal of this work is to obtain necessary and sufficient conditions on the ring R and the group G for $(RG)_{\sigma\varphi}$, the set of symmetric elements of RG under the oriented involution $\sigma\varphi$, to be commutative. This work is based on the reference [8].

Keywords: Group ring, oriented involution, symmetric elements.

Lista de Símbolos

$o(g)$	ordem do elemento g
$G \times H$	produto direto de G e H
(g, h)	$g^{-1}h^{-1}gh$, comutador de g e h
G'	$\langle (g, h) : g, h \in G \rangle$, subgrupo derivado de G
$H \lhd G$	H é um subgrupo normal de G
$[G : H]$	índice do subgrupo H em G
C_n	$\langle g : g^n = 1 \rangle$, grupo cíclico de ordem n
$\varphi\|_H$	restrição da aplicação φ ao subconjunto H
$A \cong B$	A é isomorfo a B
$[x, y]$	$xy - yx$, colchete de Lie de x e y
$[x_1, x_2, \ldots, x_n]$	$[[x_1, x_2, \ldots, x_{n-1}], x_n]$, colchete de Lie de peso n de $x_1, x_2, \ldots x_n$
$\mathcal{Z}(A)$	centro de A
A_φ	$\{a \in A : \varphi(a) = a\}$, conjunto dos elementos φ-simétricos em A
$\mathrm{car}(R)$	característica do anel R
$\mathrm{supp}(\alpha)$	suporte do elemento α

Introdução

Sejam R um anel comutativo com identidade, A uma R-álgebra e φ uma involução em A. Dizemos que um elemento $a \in A$ é *φ-simétrico* se $\varphi(a) = a$. Denotamos por $A_\varphi = \{a \in A : \varphi(a) = a\}$ o conjunto dos elementos φ-simétricos de A. Vários autores estudaram as propriedades algébricas do conjunto A_φ. Por exemplo, o conjunto A_φ é um subanel de A se, e somente se, é um conjunto comutativo. Um problema clássico é determinar quais propriedades de A_φ podem ser levantadas para toda a álgebra A.

Sejam $X = \{x_1, x_2, \ldots\}$ um conjunto enumerável de variáveis não comutantes, $R\langle X\rangle$ a álgebra livre unitária gerada por X e $S \subset A$. Dizemos que S satisfaz uma *identidade polinomial* se existe um polinômio não-nulo $f(x_1, \ldots, x_n) \in R\langle X\rangle$ tal que $f(a_1, \ldots, a_n) = 0$, para toda n-upla de elementos $a_1, a_2, \ldots, a_n \in S$. Se a álgebra A satisfaz uma identidade polinomial, dizemos que A é uma *PI-álgebra*. Amitsur [10] mostrou que se A_φ satisfaz uma identidade polinomial, então a álgebra A satisfaz uma (não necessariamente a mesma) identidade polinomial. Problemas deste tipo podem ser considerados em álgebras de grupo.

Sejam R um anel comutativo com identidade, G um grupo e RG o anel de grupo de G sobre R. Se φ é uma involução definida em G, podemos estendê-la R-linearmente para RG por $\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \varphi(g)$ e, assim, podemos considerar $(RG)_\varphi = \{\alpha \in RG : \varphi(\alpha) = \alpha\}$ o conjunto dos elementos φ-

simétricos de RG. Se o anel R é um corpo de característica p, então o Teorema de Amitsur é válido em RG e é equivalente a dizer que G possui um subgrupo p-abeliano de índice finito [11, 12]. Lembramos que um grupo é *p-abeliano* se o subgrupo derivado é um p-grupo finito.

Dizemos que um subconjunto S de uma R-álgebra A é *comutativo* se $[x, y] = 0$, para todos $x, y \in S$. Dizemos que S é *Lie nilpotente* se, para algum inteiro $n \geq 2$, $[x_1, x_2, \ldots, x_n] = 0$, para todo $x_i \in S$. Dizemos que S é *Lie n-Engel* se $[x, \underbrace{y, y, \ldots, y}_{n \text{ vezes}}] = 0$, para todos $x, y \in S$. Observe que se S é Lie nilpotente de índice n, então S é Lie n-Engel. Uma identidade polinomial é uma *identidade de Lie* se é a identidade de comutatividade, Lie nilpotência ou Lie n-Engel. Giambruno, Sehgal e Milies [13] mostraram que se G é um grupo sem 2-elementos e K é um corpo de $\mathrm{car}(K) \neq 2$, então KG é Lie nilpotente (Lie n-Engel) se, e somente se, $(KG)_\varphi$ é Lie nilpotente (Lie m-Engel).

Um outro problema que pode ser considerado é o seguinte: se RG não satisfaz uma determinada identidade de Lie, então é possível que $(RG)_\varphi$ satisfaça esta mesma identidade de Lie? Se sim, quais condições sobre o anel R e o grupo G devem ser impostas para que $(RG)_\varphi$ satisfaça tal identidade de Lie? Por exemplo, se R é um anel comutativo e G é um grupo não-abeliano, então RG não é comutativo. Então, quais condições devemos impor sobre o anel R e o grupo G para que $(RG)_\varphi$ seja comutativo?

Um homomorfismo $\sigma : G \to \{\pm 1\}$ é dito uma *orientação* de G. Dadas uma orientação não-trivial σ de G e uma involução φ de G tal que $\varphi(\ker(\sigma)) = \ker(\sigma)$, uma *involução orientada* $\sigma\varphi$ em RG, onde R é um anel comutativo com identidade, é definida por

$$\sigma\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \sigma(g)\varphi(g).$$

Tais involuções foram introduzidas por Novikov em [9] no contexto da K-teoria, onde φ era a involução clássica de G.

Nesta dissertação, iremos obter condições necessárias e suficientes para que o conjunto $(RG)_{\sigma\varphi}$ seja comutativo.

No Capítulo 1, introduziremos a noção de módulos, álgebras e anéis de grupos e o conceito de involução em anéis e em grupos.

No Capítulo 2, estudaremos os LC-grupos, grupos que desempenham um papel central no desenvolvimento da teoria.

No Capítulo 3, determinaremos condições necessárias e suficientes para que o conjunto $(RG)_{\varphi}$ seja comutativo e, com isso, determinaremos condições necessárias e suficientes para que o conjunto $(RG)_{\sigma\varphi}$ seja comutativo.

Capítulo 1

Preliminares

Neste capítulo faremos uma exposição sucinta dos conceitos de módulos, álgebras e anéis de grupos e introduziremos a noção de involução em anéis e em grupos. O leitor interessado pode consultar, por exemplo, [1, 2]. No que segue, todos os anéis possuem identidade.

1.1 Módulos e Álgebras

Definição 1.1. *Seja R um anel. Um grupo abeliano $(M, +)$ é chamado de um* R-módulo *(à esquerda) se para cada $r \in R$ e cada $m \in M$ corresponde um elemento $rm \in M$ tal que:*

(i) $(r + s)m = rm + sm$;

(ii) $r(m + n) = rm + rn$;

(iii) $(rs)m = r(sm)$;

(iv) $1m = m$,

para todos $r, s \in R$, $m, n \in M$.

De maneira análoga, podemos definir um R-módulo à direita. Utilizaremos a expressão R-módulo para nos referirmos a um R-módulo à esquerda.

Exemplo 1.2. Todo espaço vetorial sobre um corpo K é um K-módulo.

Exemplo 1.3. Sejam $(G,+)$ um grupo abeliano e $n \in \mathbb{Z}$. Dado $g \in G$, defina:

$$ng = \begin{cases} g+g+\cdots+g \ (n \text{ vezes}) & , \text{se } n > 0 \\ (-g)+(-g)+\cdots+(-g) \ (|n| \text{ vezes}) & , \text{se } n < 0 \\ 0 & , \text{se } n = 0 \end{cases} .$$

Com a multiplicação assim definida, G é um $\mathbb{Z}$-módulo.

Exemplo 1.4. Sejam R um anel e I um ideal à esquerda (à direita) de R. Então I pode ser considerado um R-módulo à esquerda (à direita). Em, particular R pode ser visto como um módulo sobre si próprio. Para explicitar quando estaremos observando R como R-módulo à esquerda (à direita) utilizaremos a notação ${}_RR$ (R_R).

Exemplo 1.5. Seja $(G,+)$ um grupo abeliano e indique por $End(G)$ o conjunto dos endomorfismos de G. Podemos dar uma estrutura de anel a $End(G)$ colocando $(f_1+f_2)(g) = f_1(g)+f_2(g)$ e $(f_1f_2)(g) = f_1(f_2(g)), \forall f_1, f_2 \in End(G), \forall g \in G$. Então G pode ser visto como um $End(G)$-módulo associando a cada $f \in End(G)$ e $g \in G$ o elemento $fg = f(g) \in G$.

Definição 1.6. *Seja M um R-módulo. Um subconjunto N de M é dito um* R-submódulo *(ou simplesmente um* submódulo*) de M se:*

(i) $(N,+)$ é um subgrupo de $(M,+)$;

(ii) Para todo $r \in R$ e todo $n \in N$, tem-se que $rn \in N$.

Exemplo 1.7. Seja V um K-espaço vetorial. Os K-submódulos de V são seus subespaços.

Exemplo 1.8. Seja R um anel. Os R-submódulos de ${}_RR$ são os seus ideais à esquerda.

Definição 1.9. *Sejam M e N dois R-módulos. Uma aplicação $f : M \to N$ é chamada de um* R-homomorfismo *se, para quaisquer $m, n \in M$ e $r \in R$, tem-se:*

(i) $f(m+n) = f(m) + f(n)$;

(ii) $f(rm) = rf(m)$.

Definição 1.10. *Um R-homomorfismo $f : M \to N$ é chamado de um* R-isomorfismo *se é injetor e sobrejetor. Quando existir um R-isomorfismo entre M e N, diremos que M e N são* isomorfos *e escreveremos $M \cong N$.*

Dado um R-homomorfismo $f : M \to N$, chamam-se *imagem* de f e *núcleo* (ou *kernel*) de f, respectivamente, os conjuntos:

$\mathrm{Im}(f) = \{n \in N : (\exists m \in M) f(m) = n\}$;

$\ker(f) = \{m \in M : f(m) = 0\}$.

É fácil mostrar que $\mathrm{Im}(f)$ é um submódulo de N e $\ker(f)$ é um submódulo de M. Também, temos que f é injetor se, e somente se, $\ker(f) = \{0\}$.

Assim como em anéis, temos o teorema do homomorfismo para módulos.

Teorema 1.11. *[2, Teorema II.1.1] Sejam M e N R-módulos e $f : M \to N$ um R-homomorfismo. Então* $\dfrac{M}{\ker(f)} \cong \mathrm{Im}(f)$.

Definição 1.12. *Sejam R um anel e I um conjunto de índices. Dizemos que uma sequência $(\lambda_i)_{i \in I}$ de elementos de R é* quase-nula *se apenas uma quantidade finita de elementos da sequência é não-nula.*

Definição 1.13. *Seja M um R-módulo. Um conjunto $\{x_i\}_{i \in I}$ de elementos de M é dito um* conjunto gerador *de M (ou dizemos que $\{x_i\}_{i \in I}$* gera *M) se, para todo $m \in M$, existe uma sequência quase-nula $(\lambda_i)_{i \in I}$ de elementos de R tal que $m = \sum_{i \in I} \lambda_i x_i$. Se o conjunto $\{x_i\}_{i \in I}$ é finito, dizemos que M é* finitamente gerado.

Definição 1.14. *Seja M um R-módulo. Um conjunto $\{x_i\}_{i\in I}$ de elementos de M diz-se* linearmente independente *(ou* livre*) se para toda sequência quase-nula $(\lambda_i)_{i\in I}$ de elementos de R tem-se que $\sum_{i\in I}\lambda_i x_i = 0$ implica que $\lambda_i = 0$ para todo $i \in I$.*

Definição 1.15. *Seja M um R-módulo. Um conjunto $\{x_i\}_{i\in I}$ de elementos de M diz-se uma R-*base *de M se $\{x_i\}_{i\in I}$ é um conjunto linearmente independente e gera M.*

Definição 1.16. *Um R-módulo M é chamado de* livre *se possui uma R-base.*

Diferentemente de espaços vetoriais, nem sempre duas R-bases de um R-módulo livre possuem o mesmo número de elementos (veja, por exemplo, [14]). No entanto, utilizando o Lema de Zorn, pode-se demonstrar o seguinte resultado:

Teorema 1.17. *[1, Teorema 2.4.4] Sejam R um anel comutativo e M um R-módulo livre finitamente gerado. Então quaisquer duas R-bases de M possuem o mesmo número de elementos.*

Definição 1.18. *Seja M um R-módulo. Se M é livre e todas as R-bases de M possuem o mesmo número de elementos, a cardinalidade de uma R-base é chamada de* posto *de M e é denotada por $posto(M)$.*

Definição 1.19. *Seja R um anel comutativo. Um R-módulo A é chamado de uma R-*álgebra *(associativa) se existe uma multiplicação definida em A de tal maneira que com a adição em A e esta multiplicação, A é um anel e para todos $r \in R$, $a, b \in A$ é válida a seguinte condição: $r(ab) = (ra)b = a(rb)$.*

Conceitos como R-subálgebra, homomorfismo de R-álgebras, isomorfismo de R-álgebras, bem como núcleo e imagem de um homomorfismo de

R-álgebras são definidos de maneira análoga ao que foi feito com módulos. Ressaltamos também que o Teorema 1.11 é válido para R-álgebras.

Dizemos que uma R-álgebra A é *comutativa* se o anel A é comutativo.

Exemplo 1.20. Seja R um anel comutativo. O conjunto $M_n(R)$ das matrizes de ordem n com coeficientes em R com as operações de adição e multiplicação usuais é uma R-álgebra não-comutativa. O conjunto $UT_n(R)$ das matrizes triangulares superiores é uma subálgebra de $M_n(R)$.

Exemplo 1.21. Qualquer anel comutativo é uma álgebra comutativa sobre si próprio.

Exemplo 1.22. Sejam K um corpo e $X = \{x_1, x_2, \ldots\}$ um conjunto infinito enumerável de variáveis não-comutantes. Denote por $K\langle X\rangle$ o K-espaço vetorial gerado pelas sequências $x_{i_1}x_{i_2}\cdots x_{i_n}$, $n \geq 0$, onde a sequência com $n = 0$ denota a identidade de K. Defina a multiplicação de $K\langle X\rangle$ por justaposição e de modo que os elementos de X comutem com os elementos de K. $K\langle X\rangle$ é uma K-álgebra não-comutativa. $K\langle X\rangle$ é o conjunto dos polinômios com coeficientes em K nas variáveis não-comutantes $\{x_i\}$.

1.2 Anéis de Grupos

Agora vamos construir a estrutura central de todo este trabalho, a estrutura de anel de grupo.

Definição 1.23. *Sejam G um grupo e R um anel. O* anel de grupo de G sobre R, *denotado por RG, é o R-módulo livre com os elementos de G como R-base com a multiplicação definida distributivamente estendendo-se R-linearmente a multiplicação em G.*

Desta forma, RG consiste de todas as combinações lineares formais finitas $\alpha = \sum_{g\in G} a_g g$, com $a_g \in R$. Se $\beta = \sum_{g\in G} b_g g \in RG$ e $r \in R$, então a adição, multiplicação e a multiplicação por elementos de R em RG são definidas por:

$$\begin{aligned} \alpha+\beta &= \sum_{g\in G} a_g g + \sum_{g\in G} b_g g &&= \sum_{g\in G}(a_g+b_g)g \\ \alpha\beta &= \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) &&= \sum_{g,h\in G}(a_g b_h)(gh) \\ r\alpha &= r\left(\sum_{g\in G} a_g g\right) &&= \sum_{g\in G}(ra_g)g \end{aligned}.$$

Observe que RG é um anel com identidade $1_{RG} = 1_R 1_G$, que de agora em diante denotaremos por 1.

Se R é comutativo e G é finito temos, pelo Teorema 1.17, que o posto de RG sobre R está bem definido e $posto(RG) = |G|$. Também, utilizando o monomorfismo de anéis $\zeta : R \to RG$ definido por $\zeta(r) = r1_G$, podemos considerar R como um subanel de RG.

Sendo RG um anel, podemos considerar

$$\mathcal{U}(RG) = \{\alpha \in RG : (\exists\, \beta \in RG)\, \alpha\beta = \beta\alpha = 1\},$$

o *grupo das unidades de* RG. Em geral, determinar $\mathcal{U}(RG)$ não é um problema fácil.

Dado $\alpha = \sum_{g\in G} a_g g \in RG$, o conjunto $\text{supp}(\alpha) = \{g \in G : a_g \neq 0\}$ é chamado de *suporte de* α. Em outras palavras, $\text{supp}(\alpha)$ é conjunto dos elementos de G que efetivamente aparecem na representação de α.

Exemplo 1.24. Vamos construir o anel de grupo de C_2 sobre $\mathbb{Z}_3$, onde $C_2 = \langle g : g^2 = 1_{C_2}\rangle$ denota o grupo cíclico de ordem 2 e $\mathbb{Z}_3$ denota o corpo dos inteiros módulo 3. $\mathbb{Z}_3C_2 = \{a \cdot 1_{C_2} + b \cdot g : a, b \in \mathbb{Z}_3\} = \{0, 1, 2, g, 2g, 1 + g, 1 + 2g, 2 + g, 2 + 2g\}$. Temos as seguintes 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	$1+g$

$\cdot$	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	$2+g$	$1+2g$	$2+g$
$2+g$	0	$2+g$	$1+2g$	$1+2g$	$2+g$	0	$1+2g$	$2+g$	0
$2+2g$	0	$2+2g$	$1+g$	$2+2g$	$1+g$	$1+g$	$2+g$	0	$2+2g$

Observe que $\mathbb{Z}_3C_2$ é comutativo e que $\mathcal{U}(\mathbb{Z}_3C_2) = \{1, 2, g, 2g\} = \pm C_2$.

Podemos, alternativamente, definir o anel de grupo RG via uma "propriedade universal".

Definição 1.25. *Sejam G um grupo e R um anel. Um anel X que contém R munido de uma aplicação $\phi : G \to X$ tal que $\phi(gh) = \phi(g)\phi(h)$, para todos $g, h \in G$, é chamado de* anel de grupo de G sobre R *(e é denotado por RG) se para todos os anéis A que contém R e todas as aplicações $f : G \to A$ que satisfazem $f(gh) = f(g)f(h)$, para todos $g, h \in G$, existe um único homomorfismo de anéis R-linear $f^* : X \to A$ tal que $f = f^* \circ \phi$.*

Vamos, agora, estudar o centro de um anel de grupo.

Sejam G um grupo e $g \in G$. Definimos a *classe de conjugação de* g como sendo o conjunto $C(g) = \{x^{-1}gx : x \in G\}$. Observe que, para todo $h \in G$, $h^{-1}C(g)h = C(g)$.

Definição 1.26. *Sejam G um grupo, R um anel comutativo, RG o anel de grupo de G sobre R e $\{C_i\}_{i\in I}$ o conjunto das classes de conjugação de G que possuem apenas um número finito de elementos. Para cada $i \in I$, escreva $c_i = \sum_{x\in C_i} x \in RG$. Esses elementos são chamados de* somas de classes *de G sobre R.*

Teorema 1.27. *[1, Teorema 3.6.2] Sejam G um grupo e R um anel comutativo. Então o conjunto $\{c_i\}_{i\in I}$ de todas as somas de classes de G sobre R é uma R-base de $\mathcal{Z}(RG)$.*

Demonstração. Seja $g \in G$. Então $g^{-1}c_ig = \sum_{x\in C_i} g^{-1}xg = \sum_{y\in C_i} y = c_i$, já que $g^{-1}C_ig = C_i, \forall\, i \in I, g \in G$. Logo, $gc_i = c_ig, \forall\, i \in I, g \in G$. Como R é comutativo, $c_i \in \mathcal{Z}(RG), \forall\, i \in I$. Portanto, cada c_i é central em RG. Para mostrar que $\{c_i\}_{i\in I}$ gera $\mathcal{Z}(RG)$ como R-módulo, seja $\alpha = \sum_{g\in G} a_g g \in \mathcal{Z}(RG)$. Vejamos que se $k \in \text{supp}(\alpha)$ e $h \in C(k)$ então $h \in \text{supp}(\alpha)$. De fato, $h = y^{-1}ky$, para algum $y \in G$. Como $\alpha \in \mathcal{Z}(RG)$, temos que $\alpha = y^{-1}\alpha y$, i.e., $\sum_{g\in G} a_g g = \sum_{g\in G} a_g y^{-1}gy$. Assim, $a_k = a_h$, $h \in \text{supp}(\alpha)$. Logo, podemos colocar em evidência os coeficientes dos elementos em cada classe de conjugação e escrever $\alpha = \sum_{i\in I} a_ic_i$. Portanto, $\{c_i\}_{i\in I}$ gera $\mathcal{Z}(RG)$ como R-módulo. Agora, sejam $r_i \in R$ tais que $\sum_{i\in I} r_ic_i = 0$, i.e., $\sum_{i\in I} r_i \sum_{x\in C_i} x = 0$. Como a conjugação em G é uma relação de equivalência, somas de classes distintas possuem suportes disjuntos. Logo, como G é livre sobre R, devemos ter $r_i = 0, \forall\, i \in I$. Assim, $\{c_i\}_{i\in I}$ é linearmente independente sobre R e, portanto, $\{c_i\}_{i\in I}$ é uma

R-base de $\mathcal{Z}(RG)$. □

1.3 Involuções

Nesta seção iremos explorar o conceito de involução em grupos e em anéis e introduziremos o conceito de involuções orientadas em anéis de grupos.

1.3.1 Involuções em grupos

Definição 1.28. *Seja G um grupo. Uma aplicação $\varphi : G \to G$ é dita uma* involução *se, para todos $g, h \in G$,*

(i) $\varphi(gh) = \varphi(h)\varphi(g)$;

(ii) $\varphi(\varphi(g)) = g$.

Observe que *(ii)* nos diz que φ é uma bijeção ($\varphi^{-1} = \varphi$).

Lema 1.29. *Sejam G um grupo e φ uma involução em G. Então:*

1. $\varphi(1_G) = 1_G$;
2. $\varphi(g^{-1}) = \varphi(g)^{-1}, \forall\, g \in G$.

Demonstração. (1) Temos que $1_G = \varphi(\varphi(1_G)) = \varphi(1_G\varphi(1_G)) = 1_G\varphi(1_G) = \varphi(1_G)$.

(2) Temos que $1_G = \varphi(1_G) = \varphi(gg^{-1}) = \varphi(g^{-1})\varphi(g)$. Logo, $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

Exemplo 1.30. Seja G um grupo. A aplicação $* : G \to G$ definida por $g^* = g^{-1}$ é uma involução em G, chamada de *inversão* em G.

Exemplo 1.31. Seja $S_3 = \{1_{S_3}, (12), (13), (32), (123), (321)\}$ o grupo de permutações de 3 elementos e considere a aplicação $\varphi : S_3 \to S_3$ definida por $\varphi(g) = (12)g^{-1}(12)$. A aplicação φ é uma involução em S_3. De fato,

(i) $\varphi(gh) = (12)h^{-1}g^{-1}(12) = [(12)h^{-1}(12)][(12)g^{-1}(12)] = \varphi(h)\varphi(g)$
(ii) $\varphi(\varphi(g)) = (12)(12)(g^{-1})^{-1}(12)(12) = g$.

Observe que no exemplo acima $\varphi = \psi \circ *$, onde ψ é o automorfismo de ordem 2 definido por $\psi(g) = (12)g(12)$ (conjugação por um elemento de ordem 2) e $*$ é a inversão. Este exemplo retrata um caso geral, dado pela seguinte proposição:

Proposição 1.32. *[6, Lema 1.1] Seja G um grupo. Uma aplicação $\varphi : G \to G$ é uma involução se, e somente se, $\varphi = \psi \circ *$, onde $*$ denota a inversão de G e ψ é um automorfismo de G de ordem 1 ou 2.*

Demonstração. Suponha que φ seja uma involução de G e seja $\psi = \varphi \circ *$.

1º) ψ é um homomorfismo.

$\psi(gh) = (\varphi \circ *)(gh) = \varphi(h^{-1}g^{-1}) = \varphi(g^{-1})\varphi(h^{-1}) = \psi(g)\psi(h)$.

2º) ψ é injetor.

Suponha que $\psi(g) = \psi(h)$. Então $\varphi(g^{-1}) = \varphi(h^{-1})$ e como φ é bijeção, devemos ter $g = h$.

3º) ψ é sobrejetor.

Seja $g \in G$. Então $\psi(\psi(g)) = \psi(\varphi(g^{-1})) = \varphi(\varphi(g^{-1})^{-1}) = \varphi(\varphi(g)) = g$.

Com isso, como $\psi(\psi(g)) = g, \forall\, g \in G$, temos que ψ é um automorfismo de G de ordem 1 ou 2 e $\varphi = \psi \circ *$.

Reciprocamente, sejam ψ um automorfismo de G de ordem 1 ou 2, $*$ a inversão e $\varphi = \psi \circ *$. Vejamos que a aplicação φ é uma involução. De fato, se ψ é um automorfismo de G de ordem 1, então $\psi = \mathrm{id}$ e $\varphi = *$. Caso contrário, temos

(i) $\varphi(gh) = \psi(h^{-1}g^{-1}) = \psi(h^{-1})\psi(g^{-1}) = \varphi(h)\varphi(g)$.
(ii) $\varphi(\varphi(g)) = \varphi(\psi(g^{-1})) = \psi(\psi(g^{-1})^{-1}) = \psi(\psi(g)) = g$. □

1.3.2 Involuções em anéis

Definição 1.33. *Seja R um anel. Uma aplicação $\varphi : R \to R$ é dita uma* involução *se, para todos $r, s \in R$,*

(i) $\varphi(r+s) = \varphi(r) + \varphi(s)$;

(ii) $\varphi(rs) = \varphi(s)\varphi(r)$;

(iii) $\varphi(\varphi(r)) = r$.

Observe que *(iii)* nos diz que φ é uma bijeção ($\varphi^{-1} = \varphi$).

Lema 1.34. *Sejam R um anel e φ um involução em R. Então:*

1. $\varphi(1) = 1$;
2. $\varphi(0) = 0$;
3. $\varphi(-r) = -\varphi(r), \forall\, r \in R$.

Demonstração. Análoga à demonstração do Lema 1.29. □

Exemplo 1.35. Seja R um anel comutativo. A aplicação identidade é uma involução em R.

Exemplo 1.36. Seja R um anel e considere $M_n(R)$, o anel das matrizes de ordem n com coeficientes em R. A transposição de matrizes é uma involução em $M_n(R)$.

Exemplo 1.37. Seja R um anel comutativo e considere a aplicação $\varphi : M_2(R) \to M_2(R)$ definida por

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

A aplicação φ é uma involução, chamada de *involução simplética*.

Exemplo 1.38. Seja $\mathbb{C}$ o corpo dos números complexos. A conjugação complexa é uma involução em $\mathbb{C}$.

Exemplo 1.39. Seja $\mathbb{H} = \{a_1 + a_2 i + a_3 j + a_4 k : a_i \in \mathbb{R}, i = 1, \ldots, 4\}$ o anel dos quatérnios reais. As aplicações $\varphi_1, \varphi_2 : \mathbb{H} \to \mathbb{H}$ definidas por $\varphi_1(a_1 + a_2 i + a_3 j + a_4 k) = a_1 - a_2 i - a_3 j - a_4 k, \varphi_2(a_1 + a_2 i + a_3 j + a_4 k) = a_1 + a_3 i + a_2 j + a_4 k$, respectivamente, são involuções em $\mathbb{H}$.

Exemplo 1.40. Sejam R um anel comutativo, G um grupo, RG o anel de grupo de G sobre R, ψ uma involução em G e considere a aplicação $\varphi : RG \to RG$ definida por $\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \psi(g)$. A aplicação φ é uma involução em RG. De fato,

$$
\begin{aligned}
(i)\ \varphi\left(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\right) &= \varphi\left(\sum_{g\in G}(a_g + b_g) g\right) \\
&= \sum_{g\in G}(a_g + b_g)\psi(g) \\
&= \sum_{g\in G} a_g\psi(g) + \sum_{g\in G} b_g\psi(g) \\
&= \varphi\left(\sum_{g\in G} a_g g\right) + \varphi\left(\sum_{g\in G} b_g g\right) \\
(ii)\ \varphi\left(\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right)\right) &= \varphi\left(\sum_{g,h\in G}(a_g b_h)(gh)\right) \\
&= \sum_{g,h\in G}(a_g b_h)\psi(gh) \\
&= \sum_{g,h\in G}(a_g b_h)\psi(h)\psi(g) \\
&= \sum_{g,h\in G}(b_h a_g)\psi(h)\psi(g) \\
&= \varphi\left(\sum_{h\in G} b_h h\right)\varphi\left(\sum_{g\in G} a_g g\right)
\end{aligned}
$$

$$(iii)\ \ \varphi\left(\varphi\left(\sum_{g\in G} a_g g\right)\right) = \varphi\left(\sum_{g\in G} a_g\psi(g)\right) = \sum_{g\in G} a_g\psi(\psi(g)) = \sum_{g\in G} a_g g.$$

Chamaremos φ de *involução de RG induzida por ψ* e denotaremos φ por ψ. Em particular, quando $\psi = *$, a inversão de G, chamamos φ de *involução*

canônica de RG. Na próxima seção, daremos um exemplo de uma involução em RG que não é induzida por uma involução de grupo.

Exemplo 1.41. Sejam R um anel, G um grupo, RG o anel de grupo de G sobre R, ψ uma involução em G, ξ uma involução em R e considere a aplicação $\varphi : RG \to RG$ definida por $\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} \xi(a_g)\psi(g)$. De maneira análoga à feita no exemplo anterior, mostra-se que φ é uma involução em RG. Observe que esta é uma generalização do exemplo anterior, tomando R um anel comutativo e ξ igual à identidade.

Definição 1.42. *Sejam R um anel e φ uma involução em R. Um elemento $r \in R$ é chamado de* φ-simétrico *(ou simplesmente* simétrico*, quando a involução φ for clara no contexto) se $\varphi(r) = r$. O conjunto dos elementos φ-simétricos será denotado por $R_\varphi = \{r \in R : \varphi(r) = r\}$.*

Lema 1.43. *Sejam R um anel e φ uma involução em R. O conjunto R_φ é um subanel de R se, e somente se, R_φ é comutativo.*

Demonstração. Sejam $a, b \in R_\varphi$. Então $\varphi(a - b) = \varphi(a) - \varphi(b) = a - b$. Logo, $a - b \in R_\varphi$. Agora, $\varphi(ab) = \varphi(b)\varphi(a) = ba$. Assim, $ab \in R_\varphi$ se, e somente se, $ab = ba$, i.e., se, e somente se, R_φ é comutativo. □

Resultados semelhantes à Proposição 1.32 podem ser encontrados em [7].

1.3.3 Involuções orientadas em anéis de grupos

Definição 1.44. *Seja G um grupo. Um homomorfismo $\sigma : G \to \{\pm 1\}$ é chamado de uma* orientação *de G.*

Seja $N = \ker(\sigma)$. Se σ é uma orientação não-trivial de um grupo G, então $N \neq G$ e $[G : N] = 2$. Logo, se um grupo finito G admite uma orientação não-trivial, a ordem de G é um número par.

Exemplo 1.45. Seja S_n o grupo de permutações de n elementos e considere o homomorfismo $\sigma : S_n \to \{\pm 1\}$ que associa cada permutação a sua assinatura. Então σ é uma orientação de S_n com núcleo $N = A_n$, o grupo das permutações pares.

Seja R um anel comutativo. Dados $\sigma : G \to \{\pm 1\}$ uma orientação de G e $\varphi : G \to G$ uma involução em G, podemos definir uma aplicação $\sigma\varphi : RG \to RG$ dada por

$$\sigma\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \sigma(g)\varphi(g).$$

A aplicação $\sigma\varphi$ é uma involução em RG se, e somente se, $N = \ker(\sigma)$ e $\varphi(N) = N$. De fato,

$$\begin{aligned}
(i)\ \sigma\varphi\left(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\right) &= \sigma\varphi\left(\sum_{g\in G}(a_g + b_g)g\right) \\
&= \sum_{g\in G}(a_g + b_g)\sigma(g)\varphi(g) \\
&= \sum_{g\in G} a_g\sigma(g)\varphi(g) + \sum_{g\in G} b_g\sigma(g)\varphi(g) \\
&= \sigma\varphi\left(\sum_{g\in G} a_g g\right) + \sigma\varphi\left(\sum_{g\in G} b_g g\right) \\
(ii)\ \sigma\varphi\left(\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right)\right) &= \sigma\varphi\left(\sum_{g,h\in G}(a_g b_h)(gh)\right) \\
&= \sum_{g,h\in G}(a_g b_h)\sigma(gh)\varphi(gh) \\
&= \sum_{g,h\in G}(a_g b_h)\sigma(g)\sigma(h)\varphi(h)\varphi(g) \\
&= \sum_{g,h\in G}(b_h\sigma(h))(a_g\sigma(g))\varphi(h)\varphi(g) \\
&= \sigma\varphi\left(\sum_{h\in G} b_h h\right)\sigma\varphi\left(\sum_{g\in G} a_g g\right)
\end{aligned}$$

$$
\begin{aligned}
(iii)\ \sigma\varphi\left(\sigma\varphi\left(\sum_{g\in G} a_g g\right)\right) &= \sigma\varphi\left(\sum_{g\in G} a_g\sigma(g)\varphi(g)\right)\\
&= \sum_{g\in G} a_g\sigma(g)\sigma(\varphi(g))g\\
&= \sum_{g\in G} a_g g
\end{aligned}
$$

já que $\varphi(N) = N$ e $[G : N] = 2$.

Definição 1.46. *A aplicação $\sigma\varphi : RG \to RG$ definida acima é chamada de* involução orientada *em RG.*

Note que, se σ é não-trivial, então esta involução não é induzida por uma involução de G, como no Exemplo 1.18. Se σ é trivial, então uma involução orientada coincide com uma involução induzida por uma involução de G.

Em [9], Novikov introduziu a noção de involução orientada em anéis de grupos no contexto da K-teoria. Nesse trabalho, Novikov trabalhava com involuções orientadas onde φ era a inversão de G.

Em todo o texto, σ é uma orientação de um grupo G, $N = \ker(\sigma)$ e sempre que dissermos que $\sigma\varphi$ é uma involução orientada estaremos supondo que $\varphi(N) = N$.

Se $\sigma\varphi$ é uma involução orientada em RG e σ é não-trivial, então devemos ter $\mathrm{car}(R) \neq 2$. Observe também que se $\sigma\varphi$ é uma involução orientada em RG, então $\sigma\varphi|_{RN} = \varphi$, onde RN é o anel de grupo de N sobre R.

Sendo $\sigma\varphi$ uma involução em RG, podemos considerar $(RG)_{\sigma\varphi}$, o conjunto dos elementos $\sigma\varphi$-simétricos em RG. Os próximos capítulos deste trabalho serão dedicados ao estudo de condições necessárias e suficientes para que $(RG)_{\sigma\varphi}$ seja um subanel de RG, i.e., condições para que $(RG)_{\sigma\varphi}$ seja comutativo.

Capítulo 2

LC-Grupos

Neste capítulo iremos estudar uma classe de grupos que desempenha um papel central neste texto.

Definição 2.1. *Seja G um grupo não-abeliano. Dizemos que um elemento $s \in G$ é o* único comutador não-trivial *de G se $s \neq 1$ e para todos $x, y \in G$, $(x, y) \in \{1, s\}$.*

Lema 2.2. *Seja G um grupo não-abeliano. Se G possui um único comutador não-trivial s, então s é um elemento central de ordem 2.*

Demonstração. Como s^{-1} é também um comutador, então $s = s^{-1}$ e assim $s^2 = 1$. Agora, suponha que exista $g \in G$ tal que $gs \neq sg$. Então $(s, g) = s$. Assim, $s = s^{-1}g^{-1}sg$. Logo, $1 = s^2 = g^{-1}sg$ e com isso $gs = g$. Assim, $s = 1$, absurdo. □

Corolário 2.3. *Seja G um grupo não-abeliano. Se G possui um único comutador não-trivial s, então $G' = \{1, s\} \subseteq \mathcal{Z}(G)$. Em particular, $G/\mathcal{Z}(G)$ é abeliano.*

Definição 2.4. *Um grupo não-abeliano G possui a propriedade de* comutatividade limitada *se, dados $g, h \in G$ tais que $gh = hg$, então $g \in \mathcal{Z}(G)$, ou*

$h \in \mathcal{Z}(G)$, *ou* $gh \in \mathcal{Z}(G)$. *Neste caso, dizemos que* G *é um* LC-grupo.

Com esta definição, quadrados são elementos centrais em LC-grupos. Assim, comutadores também são centrais, já que $(g,h) = g^{-2}(gh^{-1})^2h^2$.

Exemplo 2.5. Seja $K_8 = \langle x, y : x^4 = 1, x^2 = y^2, x^y = x^{-1} \rangle$ o grupo dos quatérnios de ordem 8. Temos que $K_8 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$. Abaixo, temos a tábua de multiplicação de K_8.

$\cdot$	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x	x	x^2	x^3	1	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x^3	x^3	1	x	x^2	x^3y	y	xy	x^2y
y	y	x^3y	x^2y	xy	x^2	x	1	x^3
xy	xy	y	x^3y	x^2y	x^3	x^2	x	1
x^2y	x^2y	xy	y	x^3y	1	x^3	x^2	x
x^3y	x^3y	x^2y	xy	y	x	1	x^3	x^2

É fácil verificar que $\mathcal{Z}(K_8) = \{1, x^2\}$. Observando a tábua de multiplicação de K_8, temos que K_8 é um LC-grupo.

Exemplo 2.6. Seja $D_4 = \langle x, y : x^4 = y^2 = 1, x^y = x^{-1} \rangle$ o grupo diedral de ordem 8. Temos que $D_4 = \{1, x, x^2, x^3, y, yx, yx^2, yx^3\}$. Abaixo, temos a tábua de multiplicação de D_4.

$\cdot$	1	x	x^2	x^3	y	yx	yx^2	yx^3
1	1	x	x^2	x^3	y	yx	yx^2	yx^3
x	x	x^2	x^3	1	yx^3	y	yx	yx^2
x^2	x^2	x^3	1	x	yx^2	yx^3	y	yx
x^3	x^3	1	x	x^2	yx	yx^2	yx^3	y
y	y	yx	yx^2	yx^3	1	x	x^2	x^3
yx	yx	yx^2	yx^3	y	x^3	1	x	x^2
yx^2	yx^2	yx^3	y	yx	x^2	x^3	1	x
yx^3	yx^3	y	yx	yx^2	x	x^2	x^3	1

É fácil verificar que $\mathcal{Z}(D_4) = \{1, x^2\}$. Observando a tábua de multiplicação de D_4, temos que D_4 é um LC-grupo.

Observe que K_8 e D_4 são LC-grupos de ordem 8 não-isomorfos.

A importância do estudo neste trabalho de LC-grupos que possuem um único comutador não-trivial se deve ao fato que certas involuções em tais grupos podem ser escritas de uma maneira muito simples, como mostra o seguinte teorema.

Teorema 2.7. *[4, Teorema 3.3] Seja G um grupo não-abeliano. Então G possui uma involução φ com a propriedade $h^{-1}gh \in \{g, \varphi(g)\}$, para todos $g, h \in G$, se, e somente se, G é um LC-grupo com um único comutador não-trivial s. Neste caso, a involução φ é dada por*

$$\varphi(g) = \begin{cases} g & , \text{ se } g \in \mathcal{Z}(G) \\ sg & , \text{ se } g \notin \mathcal{Z}(G) \end{cases}.$$

Demonstração. Suponha que G é um LC-grupo com um único comutador não-trivial s e defina a aplicação φ como no enunciado. Vamos mostrar que a aplicação φ é uma involução em G com a propriedade $h^{-1}gh \in \{g, \varphi(g)\}$, para todos $g, h \in G$.

(i) $\varphi(\varphi(g)) = g, \forall\, g \in G$.

Se $g \in \mathcal{Z}(G)$, então $\varphi(\varphi(g)) = \varphi(g) = g$. Se $g \notin \mathcal{Z}(G)$, então $\varphi(\varphi(g)) = \varphi(sg) = s^2g = g$, já que, pelo Lema 2.1, s é um elemento central de ordem 2.

(ii) $\varphi(gh) = \varphi(h)\varphi(g), \forall\, g, h \in G$.

Temos dois casos a considerar:

a) $gh \neq hg$.

Então $gh = shg$ e $g, h, gh \notin \mathcal{Z}(G)$ (é claro que $g, h \notin \mathcal{Z}(G)$; se $gh \in \mathcal{Z}(G)$, teríamos que gh comutaria com g, e isto nos daria $gh = hg$). Assim, $\varphi(h)\varphi(g) = (sh)(sg) = s^2hg = hg = sgh = \varphi(gh)$.

b) $gh = hg$.

Como G é um LC-grupo, então $g \in \mathcal{Z}(G)$ ou $h \in \mathcal{Z}(G)$ ou $gh \in \mathcal{Z}(G)$.

Se $g, h \in \mathcal{Z}(G)$, então $gh \in \mathcal{Z}(G)$. Logo, $\varphi(h)\varphi(g) = hg = gh = \varphi(gh)$.

Se $g \in \mathcal{Z}(G)$ e $h \notin \mathcal{Z}(G)$, então $gh \notin \mathcal{Z}(G)$. Logo, $\varphi(h)\varphi(g) = shg = sgh = \varphi(gh)$.

Se $g \notin \mathcal{Z}(G)$ e $h \in \mathcal{Z}(G)$, análogo ao anterior.

Se $g, h \notin \mathcal{Z}(G)$, então $gh \in \mathcal{Z}(G)$. Logo, $\varphi(h)\varphi(g) = (sh)(sg) = s^2hg = hg = gh = \varphi(gh)$.

Portanto, φ é uma involução em G. Agora, se $g \in \mathcal{Z}(G)$, então $h^{-1}gh = g = \varphi(g)$; se $g \notin \mathcal{Z}(G)$, então $h^{-1}gh = h^{-1}ghg^{-1}g = (h, g^{-1})g = sg = \varphi(g)$. Assim, a involução φ possui a propriedade $h^{-1}gh \in \{g, \varphi(g)\}$.

Reciprocamente, suponha que G é um grupo não-abeliano com uma involução φ tal que $h^{-1}gh \in \{g, \varphi(g)\}, \forall\, g, h \in G$. Se $\varphi(g) = g$, então $g \in \mathcal{Z}(G)$. Em particular, $g\varphi(g) \in \mathcal{Z}(G), \forall\, g \in G$, já que $\varphi(g\varphi(g)) = g\varphi(g)$. Também, como $g\varphi(g)$ é central, $g^2\varphi(g) = g\varphi(g)g$ e $g^{-1}g\varphi(g) = g\varphi(g)g^{-1}$. Logo, $g\varphi(g) = \varphi(g)g$ e $g^{-1}\varphi(g) = \varphi(g)g^{-1}$. Assim, $\varphi(g)$ comuta com g e $g^{-1}, \forall\, g \in G$.

Sejam $g, h \in G$ com $gh \neq hg$. Então $g^{-1}hg = \varphi(h)$, i.e., $hg = g\varphi(h)$. Observe que $h^{-1}\varphi(g)h = g$, pois $(h^{-1})^{-1}gh^{-1} \in \{g, \varphi(g)\}$ e $hgh^{-1} \neq g$. Com isso, temos que $hg = g\varphi(h) = \varphi(g)h$. Logo, $g^{-1}\varphi(g) = \varphi(h)h^{-1} = h^{-1}\varphi(h)$, já que $\varphi(h)$ comuta com h^{-1}. Assim, $g^{-1}\varphi(g) = h^{-1}\varphi(h)$.

Afirmação: Se $g \notin \mathcal{Z}(G)$, então o elemento $s = g^{-1}\varphi(g)$ não depende de g.

De fato, fixe $g, h \in G$ com $gh \neq hg$ e seja $x \notin \mathcal{Z}(G)$. Se $xg \neq gx$ e $hx \neq xh$ então, como acima, $x^{-1}\varphi(x) = g^{-1}\varphi(g) = h^{-1}\varphi(h)$. Se $xg \neq gx$ e $xh = hx$ (ou vice-versa), então $x^{-1}\varphi(x) = g^{-1}\varphi(g)$. Se $xg = gx$ e $xh = hx$, então $h^{-1}(gx)h = gx$ ou $h^{-1}(gx)h = \varphi(gx) = \varphi(xg) = \varphi(x)\varphi(g) = \varphi(g)\varphi(x)$. Mas $h^{-1}(gx)h = (h^{-1}gh)(h^{-1}xh) = \varphi(g)x$. Então $gx = \varphi(g)x$ ou $\varphi(g)\varphi(x) = \varphi(g)x$, ambos nos produzindo uma contradição, já que $g, x \notin \mathcal{Z}(G)$. Isto demonstra a afirmação.

Agora, sejam $g, h \in G$ com $gh \neq hg$. Então $(g, h) = g^{-1}h^{-1}gh = g^{-1}\varphi(g) = s$. Logo, s é o único comutador não-trivial de G e $\varphi(g) = h^{-1}gh = sg$. Se $g \in \mathcal{Z}(G)$ e $h \notin \mathcal{Z}(G)$, então $gh \notin \mathcal{Z}(G)$. Logo, $(sh)\varphi(g) = \varphi(h)\varphi(g) = \varphi(gh) = sgh = shg$. Então $\varphi(g) = g$ e assim, φ é definida como no enunciado.

Falta mostrar que G é um LC-grupo. Sejam $g, h \in G$ com $gh = hg$ mas $g, h \notin \mathcal{Z}(G)$. Então $\varphi(g) = sg, \varphi(h) = sh$ e $\varphi(gh) = \varphi(h)\varphi(g) = (sh)(sg) = s^2hg = hg = gh$. Logo, $\varphi(gh) = gh$ e assim $gh \in \mathcal{Z}(G)$. Portanto, G é um LC-grupo. □

Definição 2.8. *Seja G um grupo não-abeliano junto com uma involução φ. Dizemos que G é um LC-*grupo especial (*ou um SLC-*grupo) *com respeito à involução φ se G é um LC-grupo com um único comutador não-trivial s e a involução φ é dada por*

$$\varphi(g) = \begin{cases} g & , \text{ se } g \in \mathcal{Z}(G) \\ sg & , \text{ se } g \notin \mathcal{Z}(G) \end{cases}.$$

Agora, vamos classificar os LC-grupos que possuem um único comutador não-trivial.

Teorema 2.9. *[4, Proposição 3.6] Seja G um grupo não-abeliano. Então G é um LC-grupo com um único comutador não-trival se, e somente se, $G/\mathcal{Z}(G) \cong C_2 \times C_2$.*

Demonstração. Suponha que G é um LC-grupo com um único comutador não-trivial s. Pelo Corolário 2.3, $G/\mathcal{Z}(G)$ é abeliano. Como quadrados são centrais em LC-grupos, temos que $G/\mathcal{Z}(G)$ é um 2-grupo abeliano elementar. Assim, se $g \notin \mathcal{Z}(G)$, $\langle \overline{g} \rangle$ é um grupo cíclico de ordem 2. Suponha que $G/\mathcal{Z}(G)$ contém o produto $\langle \overline{a} \rangle \times \langle \overline{b} \rangle \times \langle \overline{c} \rangle$, com $\overline{a}, \overline{b}$ e $\overline{c}$ distintos e $a, b, c \notin \mathcal{Z}(G)$. Como G é um LC-grupo, a, b, c não podem, dois a dois, comutar. De fato, por exemplo, se $ab = ba$, então $a \in \mathcal{Z}(G)$ ou $b \in \mathcal{Z}(G)$ ou $ab \in \mathcal{Z}(G)$. Se $ab \in \mathcal{Z}(G)$, então $\overline{ab} = \overline{1}$. Assim, como $G/\mathcal{Z}(G)$ é um 2-grupo abeliano elementar, $\overline{a} = \overline{b}$, absurdo. Os outros dois casos são análogos.

Agora, em todo grupo é válida a relação $(xy, z) = (x, z)((x, z), y)(y, z)$. Como G é um LC-grupo, os comutadores são centrais. Assim, $(xy, z) = (x, z)(y, z), \forall\, x, y, z \in G$. Com isso, $(ab, c) = (a, c)(b, c) = s^2 = 1$. Logo, ou $ab \in \mathcal{Z}(G)$ ou $c \in \mathcal{Z}(G)$ ou $abc \in \mathcal{Z}(G)$, o que não ocorre. De fato, $c \notin \mathcal{Z}(G)$. Se $ab \in \mathcal{Z}(G)$, ab comutaria com a, e com isso, $ab = ba$. Se $abc \in \mathcal{Z}(G)$, então $\overline{abc} = \overline{1}$. Como $\overline{c}^2 = \overline{1}$, temos que $\overline{ab} = \overline{c}$, absurdo. Logo, $G/\mathcal{Z}(G)$ possui

no máximo o produto direto de duas cópias de C_2. Como G é não-abeliano, $G/\mathcal{Z}(G)$ possui exatamente duas. Portanto, $G/\mathcal{Z}(G) \cong C_2 \times C_2$.

Reciprocamente, suponha que G é um grupo tal que $G/\mathcal{Z}(G) \cong \langle\overline{a}\rangle \times \langle\overline{b}\rangle$ com $\langle\overline{a}\rangle \cong C_2 \cong \langle\overline{b}\rangle$. Como G é não-abeliano, temos que $ab \neq ba$. Sejam $x, y \notin \mathcal{Z}(G)$. Como a e b não comutam, temos que $xy = yx$ se, e somente se, $\overline{x} = \overline{y}$. De fato, suponha, por exemplo, que $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$. Então existem $z_1, z_2 \in \mathcal{Z}(G)$ tais que $x = az_1$ e $y = bz_2$. Então, se $xy = yx$, temos que $az_1bz_2 = bz_2az_1$. Logo, $abz_1z_2 = baz_1z_2$ implicaria que $ab = ba$. Os outros casos são análogos. Como $\langle\overline{a}\rangle \cong C_2 \cong \langle\overline{b}\rangle$, $(\overline{a})^2 = (\overline{b})^2 = \overline{1}$ e como $\overline{x} = \overline{y}$, temos que $xy \in \mathcal{Z}(G)$. Logo, G é um LC-grupo. Como $G/\mathcal{Z}(G)$ é abeliano, $G' \subseteq \mathcal{Z}(G)$. Assim, todo comutador é central e é válida a relação $(xy, z) = (x, z)(y, z), \forall\, x, y, z \in G$. Sejam $s = (a, b)$ e $x, y \in G$ tais que $xy \neq yx$. Então x e y não pertencem simultaneamente a uma das classes $\overline{a}$, $\overline{b}$, $\overline{ab}$. Da relação $(xy, z) = (x, z)(y, z)$, vem que $(x, y) = (a, b) = s$ e assim, s é o único comutador não-trivial de G. □

Exemplo 2.10. Seja K_8 como no Exemplo 2.5. É fácil verificar que $|\mathcal{Z}(K_8)| = |K_8'| = 2$ e que $K_8/\mathcal{Z}(K_8) = \{\overline{1}, \overline{x}, \overline{y}, \overline{xy}\} \cong C_2 \times C_2$. Logo, pelo Teorema 2.9, K_8 é um LC-grupo que possui um único comutador não-trivial $s = x^2$. Afirmamos que K_8 é um SLC-grupo com respeito à inversão. De fato, $(x^2)^{-1} = x^2$, $(x^i)^{-1} = x^2x^i = sx^i$, $i = 1, 3$ e $(x^iy)^{-1} = y^{-1}x^{-i} = x^2(yx^{-i}) = x^2(x^iy) = s(x^iy)$, $i = 0, 1, 2, 3$. Assim, temos que $g^* = g$, se $g \in \mathcal{Z}(K_8)$ e $g^* = sg$, se $g \notin \mathcal{Z}(K_8)$.

Exemplo 2.11. Seja D_4 como no Exemplo 2.6. É fácil verificar que $|\mathcal{Z}(D_4)| = |D_4'| = 2$ e que $D_4/\mathcal{Z}(D_4) = \{\overline{1}, \overline{x}, \overline{y}, \overline{yx}\} \cong C_2 \times C_2$. Logo, pelo Teorema 2.9, D_4 é um LC-grupo que possui um único comutador não-trivial $s = x^2$.

Observe que, se G é um LC-grupo finito com um único comutador não-trivial, então a ordem de G é necessariamente um número par.

Sejam R um anel comutativo e G um grupo não-abeliano. Queremos informações sobre o centro de RG, quando G é um LC-grupo que possui um único comutador não-trivial s. O corolário abaixo é consequência imediata do Teorema 1.27.

Corolário 2.12. *Sejam R um anel comutativo e G um LC-grupo com um único comutador não-trivial s. Então o conjunto*

$$\mathcal{Z}(G) \cup \{g + sg : g \in G \backslash \mathcal{Z}(G)\}$$

é uma R-base de $\mathcal{Z}(RG)$.

Demonstração. Seja $g \in G$. Se $g \in \mathcal{Z}(G)$ então $C(g) = \{g\}$. Agora, $\forall\, x, y \in G$ tais que $xy \neq yx$, temos que $s = (x, y) = x^{-1}y^{-1}xy$. Logo, $y^{-1}xy = sx$. Assim, se $g \notin \mathcal{Z}(G)$, $C(g) = \{g, sg\}$. Pelo Teorema 1.27, segue o resultado. □

Capítulo 3

Comutatividade de $(RG)_{\sigma\varphi}$

Neste capítulo, determinaremos condições necessárias e suficientes para que o conjunto $(RG)_\varphi$ (Definição 1.42) seja comutativo no caso de $\mathrm{car}(R) \neq 2$ e, com isso, determinaremos condições necessárias e suficientes para que o conjunto $(RG)_{\sigma\varphi}$ (Definição 1.42) seja comutativo. Este capítulo é baseado nos artigos [3, 8].

3.1 Comutatividade de $(RG)_\varphi$

Sejam R um anel comutativo com identidade, G um grupo e φ uma involução em G. Vimos no Exemplo 1.40 que a aplicação $\varphi : RG \to RG$ definida por

$$\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \varphi(g)$$

é uma involução em RG.

Denotaremos por $G_\varphi = \{g \in G : \varphi(g) = g\}$ o conjunto dos elementos φ-simétricos em G. Observe que, para todo $g \in G$, $g\varphi(g) \in G_\varphi$ e $g + \varphi(g) \in (RG)_\varphi$.

Seja $\alpha = \sum_{g\in G} a_g g \in (RG)_\varphi$. Então $\varphi(\alpha) = \alpha$ implica $\sum_{g\in G} a_g g = \sum_{g\in G} a_g \varphi(g)$. Logo, $a_g = a_{\varphi(g)}, \forall\, g \in \text{supp}(\alpha)$. Assim, como R-módulo, $(RG)_\varphi$ é gerado pelo conjunto

$$\mathcal{R} = G_\varphi \cup \{g + \varphi(g) : g \in G \backslash G_\varphi\}.$$

Portanto, o conjunto $(RG)_\varphi$ é comutativo (logo, pelo Lema 1.43, um anel) se, e somente se, o conjunto $\mathcal{R}$ é comutativo.

Exemplo 3.1. Sejam R um anel comutativo com identidade, K_8 o grupo dos quatérnios de ordem 8 e $*$ a inversão. Temos que $(K_8)_* = \{g \in K_8 : g^2 = 1\} = \mathcal{Z}(K_8)$. Também, pelo Exemplo 2.10, K_8 é um SLC-grupo com respeito à inversão. Logo, $(RK_8)_*$ é gerado como R-módulo pelo conjunto $\mathcal{Z}(K_8) \cup \{g + sg : g \in K_8 \setminus \mathcal{Z}(K_8)\}$ que, pelo Corolário 2.12, é uma R-base de $\mathcal{Z}(RK_8)$. Portanto, $(RK_8)_*$ é comutativo.

No que segue, R é um anel comutativo com identidade de $\text{car}(R) \neq 2$.

Iniciaremos a demonstração de algums lemas técnicos.

Lema 3.2. *Se $(RG)_\varphi$ é comutativo, então $G_\varphi \subseteq \mathcal{Z}(G)$. Em particular, $g\varphi(g) = \varphi(g)g \in \mathcal{Z}(G)$, para todo $g \in G$.*

Demonstração. Sejam $g \in G_\varphi$ e $h \in G$. Vamos mostrar que $gh = hg$. Se $h \in G_\varphi$, como $(RG)_\varphi$ é comutativo, temos que $gh = hg$. Suponha que $h \notin G_\varphi$. Então

$$0 = [g, h + \varphi(h)] = gh + g\varphi(h) - hg - \varphi(h)g.$$

Assim, $gh + g\varphi(h) = hg + \varphi(h)g$. Temos que $gh \neq g\varphi(h)$ e $hg \neq \varphi(h)g$, já que $h \notin G_\varphi$. Então $gh = hg$ ou $gh = \varphi(h)g$. Se $gh = \varphi(h)g$, então $gh = \varphi(h)g = \varphi(h)\varphi(g) = \varphi(gh)$. Logo, $gh \in G_\varphi$ e assim gh e g comutam.

Com isso, $g^2h = ghg$ e assim $gh = hg$. Logo, $gh = hg = \varphi(h)g$ e assim, $h \in G_\varphi$, absurdo. Portanto, $gh = hg$.

Em particular, $\forall\, g \in G$, $g\varphi(g) \in G_\varphi \subseteq \mathcal{Z}(G)$. Logo, $g^2\varphi(g) = g\varphi(g)g$ e assim $g\varphi(g) = \varphi(g)g$. □

Lema 3.3. *Se $(RG)_\varphi$ é comutativo e $g, h \in G$ são tais que $gh \neq hg$, então $gh = h\varphi(g)$ ou $gh = \varphi(h)g$.*

Demonstração. Pelo Lema 3.2 temos que $g, h \notin G_\varphi$. Logo

$$\begin{aligned} 0 &= [g + \varphi(g), h + \varphi(h)] \\ &= gh + g\varphi(h) + \varphi(g)h + \varphi(g)\varphi(h) - hg - h\varphi(g) - \varphi(h)g - \varphi(h)\varphi(g). \end{aligned}$$

Temos que $gh \neq g\varphi(h), \varphi(g)h \neq \varphi(g)\varphi(h), hg \neq h\varphi(g)$ e $\varphi(h)g \neq \varphi(h)\varphi(g)$, já que $g, h \notin G_\varphi$. Como $\mathrm{car}(R) \neq 2$, temos que $gh \neq \varphi(g)\varphi(h)$. De fato, se $gh = \varphi(g)\varphi(h)$, então $hg = \varphi(h)\varphi(g)$. Logo, teríamos

$$2gh + g\varphi(h) + \varphi(g)h = 2hg + h\varphi(g) + \varphi(h)g.$$

Como, por hipótese, $gh \neq hg$ e $\mathrm{car}(R) \neq 2$, $2(gh - hg) \neq 0$. Assim, deveríamos ter $2gh = h\varphi(g)$ ou $2gh = \varphi(h)g$, contrariando a igualdade dos elementos. Então $gh = \varphi(h)g$ ou $gh = h\varphi(g)$ ou $gh = \varphi(h)\varphi(g)$. Neste último caso, $gh = \varphi(h)\varphi(g) = \varphi(gh)$. Assim, $gh \in G_\varphi$ e pelo Lema 3.2, gh e g comutam. Logo, $gh = hg$, absurdo. Portanto, $gh = h\varphi(g)$ ou $gh = \varphi(h)g$. □

Lema 3.4. *Sejam $g, h \in G$ tais que $gh \neq hg$ e $\varphi(g) = h^{-1}gh$. Se $(RG)_\varphi$ é comutativo, então $gh = \varphi(h)g$ e $g^2, h^2 \in G_\varphi$.*

Demonstração. Aplicando o Lema 3.3 em gh e h, temos que $gh^2 = h\varphi(h)\varphi(g)$ ou $gh^2 = \varphi(h)gh$.

Se $gh^2 = h\varphi(h)\varphi(g)$, então $gh^2 = h\varphi(h)\varphi(g) = \varphi(g)\varphi(h)h$, já que, pelo Lema 3.2, $h\varphi(h) = \varphi(h)h \in \mathcal{Z}(G)$. Logo, $gh = \varphi(g)\varphi(h)$.

Se $gh^2 = \varphi(h)gh$, então $h\varphi(g) = gh = \varphi(h)g$ (por hipótese). Assim, $gh^2 = \varphi(h)gh = \varphi(h)h\varphi(g) = \varphi(g)\varphi(h)h$, já que, pelo Lema 3.2, $h\varphi(h) = \varphi(h)h \in \mathcal{Z}(G)$. Logo, $gh = \varphi(g)\varphi(h)$.

Em todo caso, $gh = \varphi(g)\varphi(h)$ e $hg = \varphi(h)\varphi(g)$. Então $gh = \varphi(g)\varphi(h) = h^{-1}gh\varphi(h) = h^{-1}h\varphi(h)g = \varphi(h)g$. Por hipótese, temos que $gh = h\varphi(g)$. Logo, $\varphi(h)g = h\varphi(g)$. Assim, $\varphi(h)g^2 = h\varphi(g)g = hg\varphi(g) = \varphi(h)\varphi(g)\varphi(g) = \varphi(h)\varphi(g^2)$. Logo, $\varphi(g^2) = g^2$ e, portanto, $g^2 \in G_\varphi$.

Analogamente, aplicando o Lema 3.3 em g e gh, temos que $gh = \varphi(h)g$ e $h^2 \in G_\varphi$. □

Lema 3.5. *Se $(RG)_\varphi$ é comutativo e $g, h \in G$ são tais que $gh \neq hg$, então $gh = h\varphi(g) = \varphi(h)g$.*

Demonstração. Pelo Lema 3.3, temos que $gh = h\varphi(g)$ ou $gh = \varphi(h)g$.

Se $gh = h\varphi(g)$, então $\varphi(g) = h^{-1}gh$. Neste caso utilizamos o Lema 3.4 e obtemos $gh = h\varphi(g) = \varphi(h)g$.

Se $gh = \varphi(h)g$, então $\varphi(h)\varphi(g) = \varphi(g)h \neq \varphi(g)\varphi(h)$ e, como $\varphi(h) = ghg^{-1}$, $h = \varphi(\varphi(h)) = \varphi(g)^{-1}\varphi(h)\varphi(g)$. Logo, pelo Lema 3.4, $\varphi(h)\varphi(g) = \varphi(\varphi(g))\varphi(h) = g\varphi(h)$. Portanto, $gh = \varphi(h)g = h\varphi(g)$. □

Lema 3.6. *Se $(RG)_\varphi$ é comutativo e $g, h \notin \mathcal{Z}(G)$ então $g^{-1}\varphi(g) = h^{-1}\varphi(h)$.*

Demonstração. Se $gh \neq hg$, pelo Lema 3.5, $g^{-1}\varphi(g) = \varphi(h)h^{-1}$. Pelo Lema 3.2, $h\varphi(h) \in \mathcal{Z}(G)$. Logo, $h^{-1}h\varphi(h) = h\varphi(h)h^{-1}$. Assim, $h^{-1}\varphi(h) = \varphi(h)h^{-1}$. Portanto, $g^{-1}\varphi(g) = h^{-1}\varphi(h)$.

Se $gh = hg$, tome $x \in G$ tal que $gx \neq xg$. Se $hx \neq xh$, pelo Lema 3.5 e pelo visto acima, $g^{-1}\varphi(g) = x^{-1}\varphi(x) = h^{-1}\varphi(h)$. Se $hx = xh$, então $g(xh) \neq (xh)g$. De fato, suponha que $g(xh) = (xh)g = (hx)g$. Então $g(xh) = ghx = hgx$, que por sua vez é igual a hxg, o que implicaria $gx = xg$. Logo, pelo Lema 3.5, $g(xh) = xh\varphi(g) = \varphi(h)\varphi(x)g$ e $gx = \varphi(x)g$. Assim,

$g(xh) = g(hx) = hgx = h\varphi(x)g$, que por sua vez é igual a $\varphi(h)\varphi(x)g$. Logo, $h = \varphi(h)$ e pelo Lema 3.2, $h \in \mathcal{Z}(G)$, contradição. □

Antes de iniciar a demonstração do teorema principal desta seção, recordaremos a seguinte definição.

Definição 3.7. *Um grupo não-abeliano cujos subgrupos são todos normais é chamado de* grupo Hamiltoniano.

Temos, abaixo, a classificação dos grupos Hamiltonianos.

Teorema 3.8. *[1, Teorema 1.8.5] Um grupo não-abeliano G é Hamiltoniano se, e somente se, $G \cong K_8 \times E \times A$, onde K_8 denota o grupo dos quatérnios de ordem 8, E é um 2-grupo abeliano elementar e A é um grupo abeliano no qual todos os elementos possuem ordem ímpar.*

Observe que o grupo E do enunciado do Teorema 3.8 é central em G.

Temos o seguinte resultado.

Proposição 3.9. *Seja G um SLC-grupo com respeito à inversão. Então G é um 2-grupo Hamiltoniano.*

Demonstração. Seja s o único comutador-não trivial de G.

Se $g \in \mathcal{Z}(G)$, então $g^2 = 1$.

Se $g \notin \mathcal{Z}(G)$, então $g^{-1} = sg$. Logo, $g^2 = s$.

Assim, G é um 2-grupo com expoente menor ou igual a 4. Para mostrar que G é Hamiltoniano, basta mostrar que todo subgrupo cíclico é normal. Sejam $g, h \in G$ tais que $gh \neq hg$. Então $g, h, gh \notin \mathcal{Z}(G)$, $g^2 = h^2 = (gh)^2 = s$, $o(g) = o(h) = o(gh) = 4$ e $gh = shg$. Logo, $hgh = hshg = h^2sg = s^2g = g$ e $h^{-1}gh = h^{-1}(hgh)h = gh^2 = sg = g^{-1}$. Portanto, G é um 2-grupo Hamiltoniano. □

Agora, vamos ao teorema principal da seção.

Teorema 3.10. *Sejam G um grupo não-abeliano, φ uma involução em G e R um anel comutativo com* $\mathrm{car}(R) \neq 2$. *Então $(RG)_\varphi$ é comutativo se, e somente se, G é um SLC-grupo. Neste caso, $(RG)_\varphi = \mathcal{Z}(RG)$. Se $\varphi = *$, a inversão de G, então $(RG)_*$ é comutativo se, e somente se, G é um 2-grupo Hamiltoniano.*

Demonstração. Suponha que $(RG)_\varphi$ é comutativo. Sejam $g, h \in G$ tais que $gh \neq hg$. Pelo Lema 3.5, $1 \neq g^{-1}h^{-1}gh = g^{-1}\varphi(g)$. Pelo Lema 3.6, $s = g^{-1}\varphi(g)$ é o único comutador não-trivial de G. Logo, $\varphi(s) = \varphi(g^{-1}\varphi(g)) = g\varphi(g)^{-1} = s$ e $\varphi(g) = sg, \forall\, g \in G\backslash\mathcal{Z}(G)$.

Agora, se $g \in \mathcal{Z}(G)$ e $h \notin \mathcal{Z}(G)$, então $gh \notin \mathcal{Z}(G)$. Assim, $sh\varphi(g) = \varphi(h)\varphi(g) = \varphi(gh) = sgh = shg$. Logo, $\varphi(g) = g$.

Falta mostrar que G é um LC-grupo. Sejam $g, h \in G, g, h \notin \mathcal{Z}(G)$ mas $gh = hg$. Então $\varphi(gh) = \varphi(h)\varphi(g) = shsg = hg = gh$. Logo, $gh \in G_\varphi$ e pelo Lema 3.2, $gh \in \mathcal{Z}(G)$. Portanto, G é um SLC-grupo.

Reciprocamente, suponha que G é um SLC-grupo. Pelo Corolário 2.12, $\mathcal{Z}(RG)$ é gerado como R-módulo por $\mathcal{Z}(G) \cup \{g + sg : g \in G\backslash\mathcal{Z}(G)\}$. Seja $\alpha \in RG$ e escreva $\alpha = \alpha_1 + \alpha_2$, com $\mathrm{supp}(\alpha_1) \subseteq \mathcal{Z}(G)$ e $\mathrm{supp}(\alpha_2) \cap \mathcal{Z}(G) = \varnothing$. Se $\alpha \in (RG)_\varphi$, então $\alpha = \alpha_1 + \alpha_2 = \varphi(\alpha_1 + \alpha_2) = \alpha_1 + s\alpha_2$. Logo, $\alpha_2 = s\alpha_2$. Assim, $\alpha_2 = \sum_{g \notin \mathcal{Z}(G)} a_g g = \sum_{g \notin \mathcal{Z}(G)} a_g sg$ e $a_g = a_{sg}$. Colocando estes coeficientes em evidência, temos que $\alpha_2 = \sum_{g \notin \mathcal{Z}(G)} a_g(g + sg)$. Logo, $\alpha_2 \in \mathcal{Z}(RG)$ e assim $\alpha \in \mathcal{Z}(RG)$. Portanto, $(RG)_\varphi$ é comutativo e $\mathcal{Z}(RG) = (RG)_\varphi$.

Em particular, suponha que $\varphi = *$ é a inversão de G. Se $(RG)_*$ é comutativo, então G é um SLC-grupo. Pela Proposição 3.9, G é um 2-grupo Hamiltoniano. Reciprocamente, suponha agora que G é um 2-grupo Hamiltoniano. Pelo Teorema 3.8, $G \cong K_8 \times E$, onde E é um 2-grupo abeliano

elementar. Logo, $RG = R(K_8 \times E) \cong (RE)K_8$. Pelo Exemplo 2.10, K_8 é um SLC-grupo com um único comutador não-trivial e pelo Exemplo 3.1 $((RE)K_8)_*$ é comutativo. □

Condições necessárias e suficientes para que $(RG)_\varphi$ seja comutativo quando $\text{car}(R) = 2$ podem ser encontradas em [3].

3.2 Comutatividade de $(RG)_{\sigma\varphi}$

Nesta seção, determinaremos condições necessárias e suficientes para que o conjunto $(RG)_{\sigma\varphi}$ (Definição 1.42) seja comutativo.

Sejam R um anel comutativo com identidade, G um grupo, φ uma involução em G e σ uma orientação não-trivial de G. Vimos na Seção 1.3.3 que se $\varphi(\ker(\sigma)) = \ker(\sigma)$, então a aplicação $\sigma\varphi : RG \to RG$ definida por

$$\sigma\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \sigma(g)\varphi(g)$$

é uma involução em RG, chamada de *involução orientada* em RG. Observe que a hipótese $\varphi(\ker(\sigma)) = \ker(\sigma)$ implica que $g\varphi(g) \in \ker(\sigma), \forall\, g \in G$.

Denotaremos $N = \ker(\sigma)$ e $G_{\sigma\varphi} = \{g \in G : \sigma\varphi(g) = g\}$ o conjunto dos elementos $\sigma\varphi$-simétricos em G. Ressaltamos que se σ é uma orientação não-trivial de G, então devemos ter $\text{car}(R) \neq 2$.

Seja $g \in G_{\sigma\varphi}$. Então $\sigma\varphi(g) = \sigma(g)\varphi(g) = g$. Logo, $\sigma(g) = 1$ e $\varphi(g) = g$. Assim, $G_{\sigma\varphi} = N \cap G_\varphi = N_\varphi$. Observe que, como $g\varphi(g) \in G_\varphi, \forall\, g \in G$, então $g\varphi(g) \in N_\varphi, \forall\, g \in G$.

Seja $\alpha = \sum_{g\in G} a_g g \in (RG)_{\sigma\varphi}$. Então $\sigma\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g\sigma(g)\varphi(g) = \sum_{g\in G} a_g g$. Logo, $a_{\varphi(g)} = \sigma(g)a_g, \forall\, g \in \text{supp}(\alpha)$. Com isso, $(RG)_{\sigma\varphi}$ é gerado como R-módulo pelo conjunto

$$\mathcal{S} = N_\varphi \cup \{g + \sigma\varphi(g) : g \in G\backslash N_\varphi\} =$$
$$N_\varphi \cup \{g + \varphi(g) : g \in N\backslash N_\varphi\} \cup \{g - \varphi(g) : g \in (G\backslash N)\backslash G_\varphi\}.$$

Portanto, $(RG)_{\sigma\varphi}$ é comutativo (logo, pelo Lema 1.43, um anel) se, e somente se, o conjunto $\mathcal{S}$ é comutativo.

No que segue, R é um anel comutativo com identidade de $\text{car}(R) \neq 2$ e $\sigma\varphi$ é uma involução orientada em RG.

Iniciaremos a demonstração de alguns lemas técnicos.

Lema 3.11. *Suponha que $(RG)_{\sigma\varphi}$ é comutativo e sejam $g \in (G\backslash N)\backslash G_\varphi$ e $h \in G$. Então:*

(i) $gh = hg$, ou

(ii) $\text{car}(R) = 4$ e $gh = \varphi(g)\varphi(h) = h\varphi(g) = \varphi(h)g$.

Além disso $g\varphi(g) = \varphi(g)g$.

Demonstração. Dividiremos a demonstração em 4 casos.

(a) $h \in N_\varphi$. Então

$$\begin{aligned} 0 &= [g + \sigma\varphi(g), h] \\ &= [g - \varphi(g), h] \\ &= gh - \varphi(g)h - hg + h\varphi(g) \end{aligned} \quad .$$

Temos que $gh \neq \varphi(g)h$, pois $g \notin G_\varphi$. Como $\text{car}(R) \neq 2$, devemos ter $gh = hg$ e segue (i). Agora, $g\varphi(g) \in N_\varphi$. Logo, g e $g\varphi(g)$ comutam e, com isso, $g\varphi(g) = \varphi(g)g$.

(b) $h \in (G\backslash N)\backslash G_\varphi$. Então

$$\begin{aligned} 0 &= [g + \sigma\varphi(g), h + \sigma\varphi(h)] \\ &= [g - \varphi(g), h - \varphi(h)] \\ &= gh - g\varphi(h) - \varphi(g)h + \varphi(g)\varphi(h) - hg + h\varphi(g) + \varphi(h)g - \varphi(h)\varphi(g). \end{aligned}$$

Logo,

$$gh + \varphi(g)\varphi(h) + h\varphi(g) + \varphi(h)g = g\varphi(h) + \varphi(g)h + hg + \varphi(h)\varphi(g).$$

Temos que $gh \neq g\varphi(h)$ e $gh \neq \varphi(g)h$, pois $g, h \notin G_\varphi$. Com isso, temos 4 possibilidades:

(1) $gh = hg$ ou

(2) $gh = \varphi(h)\varphi(g)$ ou

(3) $\mathrm{car}(R) = 3$ e gh é igual a dois elementos do conjunto $\{\varphi(g)\varphi(h), h\varphi(g), \varphi(h)g\}$ ou

(4) $\mathrm{car}(R) = 4$ e $gh = \varphi(g)\varphi(h) = h\varphi(g) = \varphi(h)g$.

Se (1) ou (4) ocorrem, o resultado segue.

Se (2) ocorre, então $gh = \varphi(h)\varphi(g) = \varphi(gh)$. Logo, $gh \in G_\varphi$. Como $g, h \notin N$, $gh \in N$. Logo, $gh \in N_\varphi$. Então, por (a), g e gh comutam e com isso $gh = hg$. Assim, (i) ocorre.

Se (3) ocorre, suponha que $gh = \varphi(g)\varphi(h) = h\varphi(g)$. Como $g, h \notin G_\varphi$, então $\varphi(h)g = g\varphi(h)$ ou $\varphi(h)g = \varphi(g)h$. Agora, $\varphi(h)g \neq g\varphi(h)$, pois como $gh = h\varphi(g)$, teríamos $\varphi(h)\varphi(g) = g\varphi(h)$, que por sua vez é igual a $\varphi(h)g$, contradição, já que $g \notin G_\varphi$. Logo, $\varphi(h)g = \varphi(g)h$. Assim, $\varphi(\varphi(h)g) = \varphi(g)h = \varphi(h)g$ e com isso $\varphi(h)g \in G_\varphi$. Como $g, h \notin N$, $\varphi(h)g \in N$. Logo, $\varphi(h)g \in N_\varphi$ e, por (a), $\varphi(g)h$ e g comutam. Logo, $g\varphi(g)h = \varphi(g)gh = \varphi(g)hg$ e assim $gh = hg$. Com isso, (i) ocorre. Analogamente, se $gh = \varphi(g)\varphi(h) = \varphi(h)g$ ou $gh = h\varphi(g) = \varphi(h)g$, obtemos $gh = hg$ e, assim, (i) ocorre.

(c) $h \in N \backslash G_\varphi$. Então

$$\begin{aligned} 0 &= [g + \sigma\varphi(g), h + \sigma\varphi(h)] \\ &= [g - \varphi(g), h + \varphi(h)] \\ &= gh + g\varphi(h) - \varphi(g)h - \varphi(g)\varphi(h) - hg + h\varphi(g) - \varphi(h)g + \varphi(h)\varphi(g). \end{aligned}$$

Logo,

$$gh + g\varphi(h) + h\varphi(g) + \varphi(h)\varphi(g) = \varphi(g)h + \varphi(g)\varphi(h) + hg + \varphi(h)g.$$

Temos que $gh \neq g\varphi(h), h\varphi(g) \neq \varphi(h)\varphi(g)$ e $gh \neq \varphi(g)h$, pois $g, h \notin G_\varphi$. Como $\mathrm{car}(R) \neq 2$, temos que gh é igual a $\varphi(g)\varphi(h)$ ou hg ou $\varphi(h)g$.

Se $gh = \varphi(h)g$, então $\varphi(gh) = \varphi(g)h$. Como $g \notin G_\varphi$, temos que $gh \notin G_\varphi$. Por outro lado, se $gh = \varphi(g)\varphi(h) = \varphi(hg)$, então $gh \in G_\varphi$ se, e somente se, $gh = hg$. Se $gh \in G_\varphi$, (i) ocorre. Suponha então que $gh \notin G_\varphi$. Como $gh \notin N$, pelo caso (b), temos que ou gh e g comutam ou $\mathrm{car}(R) = 4$ e $g^2h = \varphi(g)\varphi(h)\varphi(g) = gh\varphi(g) = \varphi(h)\varphi(g)g$. Logo, ou $gh = hg$, e (i) ocorre, ou $\mathrm{car}(R) = 4$ e $gh = \varphi(g)\varphi(h) = h\varphi(g) = \varphi(h)g$, e (ii) ocorre.

(d) $h \in (G\backslash N) \cap G_\varphi$.

Então $gh \in N$. Se $gh \in G_\varphi$, então $gh \in N_\varphi$ e, por (a), aplicado a gh e g, temos que $gh = hg$. Se $gh \notin G_\varphi$, por (c), aplicado a gh e g, ou gh e g comutam (e assim $gh = hg$) ou $\mathrm{car}(R) = 4$ e $g^2h = \varphi(g)\varphi(gh) = gh\varphi(g) = \varphi(gh)g$. Logo, $gh\varphi(g) = \varphi(h)\varphi(g)g = hg\varphi(g)$. Portanto, $gh = hg$ e, em ambos casos, (i) ocorre. □

Lema 3.12. *Suponha que $(RG)_{\sigma\varphi}$ é comutativo e sejam $g \in (G\backslash N) \cap G_\varphi$ e $h \in G$. Então:*

(i) $h \in N_\varphi$ e $gh = hg$, ou

(ii) $h \in N\backslash G_\varphi$ e $gh = hg$ ou $gh = \varphi(h)g$, ou

(iii) $h \in (G\backslash N)\backslash G_\varphi$ e $gh = hg$, ou

(iv) $h \in (G\backslash N) \cap G_\varphi$ e $gh = hg$ ou $g^2h = hg^2$.

Demonstração. (i) Seja $h \in N_\varphi$. Então $gh \notin N$. Se $gh \notin G_\varphi$, pela demonstração do Lema 3.11, caso (a), gh e h comutam e assim, $gh = hg$; se $gh \in G_\varphi$, então $gh = \varphi(gh) = \varphi(h)\varphi(g) = hg$.

(ii) Seja $h \in N\backslash G_\varphi$. Então $gh \notin N$. Se $gh \notin G_\varphi$, pela demonstração do Lema 3.11, caso (c), ou h e gh comutam (e assim $gh = hg$) ou $\mathrm{car}(R) = 4$ e $gh^2 = \varphi(gh)\varphi(h) = h\varphi(gh) = \varphi(h)gh$. Neste último caso, $\varphi(h)g\varphi(h) =$

$\varphi(h)gh$ e assim $\varphi(h) = h$, contradição, já que $h \notin G_\varphi$. Logo, $gh = hg$. Se $gh \in G_\varphi$, então $gh = \varphi(gh) = \varphi(h)g$.

(iii) Seja $h \in (G\backslash N)\backslash G_\varphi$. Pela demonstração do Lema 3.11, caso (d), $gh = hg$.

(iv) Seja $h \in (G\backslash N) \cap G_\varphi$. Então $gh \in N$. Se $gh \in G_\varphi$, então $gh \in N_\varphi$ e por (i), aplicado a g e gh, $gh = hg$. Se $gh \notin G_\varphi$, por (ii), g e gh comutam (e assim $gh = hg$) ou $g^2h = \varphi(gh)g = hg^2$. □

Suponha que $(RG)_{\sigma\varphi}$ seja comutativo. Então $(RN)_{\sigma\varphi} = (RN)_\varphi$ é comutativo e, pelo Teorema 3.10, temos que:

(A) N é abeliano ou

(B) N é um SLC-grupo com respeito à involução $\varphi|_N$.

Antes de seguirmos para o próximo resultado, convém fazer a seguinte observação: se σ é uma orientação não-trivial de G, então $[G : N] = 2$. Logo, $\forall\, g \in G\backslash N$, temos que $G = N \cup Ng$.

Lema 3.13. *Seja R um anel comutativo de característica 4 tal que $(RG)_{\sigma\varphi}$ é comutativo. Se $G \neq N \cup G_\varphi \cup \mathcal{Z}(G)$, então $(G\backslash N) \cap G_\varphi$ é vazio ou central em G.*

Demonstração. Como $G \neq N \cup G_\varphi \cup \mathcal{Z}(G)$, então $\exists\, g \in G \setminus (N \cup G_\varphi \cup \mathcal{Z}(G))$ e $h \in N$ tais que $gh \neq hg$. De fato, suponha que $gh = hg, \forall\, h \in N$. Como $G = N \cup Ng$, seja $\alpha \in Ng$. Logo, existe $n \in N$ tal que $\alpha = ng$ e $g^{-1}\alpha g = g^{-1}ngg = ng = \alpha$, o que implica $g \in \mathcal{Z}(G)$, absurdo. Com isso, pelo Lema 3.11, $gh = \varphi(g)\varphi(h) = h\varphi(g) = \varphi(h)g$ e assim, $\varphi(g) = h^{-1}gh$ e $\varphi(h) = g^{-1}hg$.

Agora, $h, gh \notin G_\varphi$. De fato, se $h \in G_\varphi$, então $gh = \varphi(g)\varphi(h) = \varphi(g)h$, o que implicaria $g \in G_\varphi$, contradição. Se $gh \in G_\varphi$, então $\varphi(h)\varphi(g) = \varphi(gh) = gh = \varphi(h)g$, o que implicaria $g \in G_\varphi$, contradição.

Suponha que exista $x \in (G\backslash N) \cap G_\varphi$. Pelo Lema 3.12, (iii), aplicado a x e g, temos que $gx = xg$. Como $gh \in (G\backslash N)\backslash G_\varphi$, aplicando novamente o Lema 3.12 (iii), temos que $x(gh) = (gh)x$. Logo, $xh = hx$.

Suponha que (A) ocorre. Como $xg, h \in N$, então $xgh = hgx = xhg$ e assim $gh = hg$, contradição. Então, se N é abeliano, $(G\backslash N) \cap G_\varphi = \varnothing$.

Suponha então que (B) ocorre. Observe que $N_\varphi = \mathcal{Z}(N)$. Pela demonstração do Lema 3.11, caso (a), g comuta com os elementos de N_φ. Vamos mostrar que N_φ é central em G. Sejam $\alpha \in G$ e $n \in N_\varphi = \mathcal{Z}(N)$. Temos que $G = N \cup Ng$. Se $\alpha \in N$, $\alpha n = n\alpha$, já que $n \in \mathcal{Z}(N)$; se $\alpha \in Ng, \exists\, n' \in N$ tal que $\alpha = n'g$ e $n\alpha = nn'g = n'ng = n'gn = \alpha n$, já que g comuta com N_φ. Com isso, como $xg = gx$, para mostrar que $(G\backslash N) \cap G_\varphi$ é central em G, basta mostrar que x comuta com os elementos de $N\backslash N_\varphi$.

Seja s o único comutador não-trivial de N. Já vimos que $h \notin G_\varphi$. Assim, $\varphi(h) = sh$. Como $gh = \varphi(g)\varphi(h) = h\varphi(g) = \varphi(h)g$, temos que $gh = shg$ e $\varphi(g) = sg = gs$. Logo, s é um elemento central em G

Seja $y \in N\backslash N_\varphi$. Temos que $hy = yh$ ou $hy = syh$, já que N é um SLC-grupo. Pelo Lema 3.11, temos que $gy = yg$ ou $gy = \varphi(y)g = syg$. Pelo Lema 3.12 (ii), temos que $xy = yx$ ou $xy = \varphi(y)x = syx$.

Suponha que $xy = syx$.

Se $gy \neq yg$, então $\varphi(gy) = \varphi(y)\varphi(g) = sysg = yg$ e $gy \notin N$. Logo, $yg \in (G\backslash N)\backslash G_\varphi$ e assim, pelo Lema 3.12, x e gy comutam. Logo, $xgy = gxy = gyx$ o que implica $xy = yx = syx$, contradição.

Então podemos supor que $gy = yg$.

Se $hy = syh$, então $\varphi(hgy) = sysgsh = sygh = sgyh = sgshy = ghy = shgy$ e $hgy \notin N$. Logo, $hgy \in (G\backslash N)\backslash G_\varphi$ e pelo Lema 3.12 x e hgy comutam. Assim, $xhgy = hgyx = hgsxy = shgxy = shxgy = sxhgy$ e com isso, $s = 1$, contradição.

Logo, $hy = syh$ não ocorre. Então $hy = yh$. Temos que $\varphi(hxy) = syxsh = yxh = yhx = hyx = shxy$ e $hxy \notin N$. Logo, $hxy \in (G\backslash N)\backslash G_\varphi$ e pelo Lema 3.12 x e hxy comutam. Assim, $xhxy = hxyx = xhsxy = sxhxy$ e com isso, $s = 1$, contradição.

Logo, $xy = syx$ não ocorre. Então $xy = yx$ e portanto $(G\backslash N) \cap G_\varphi$ é central em G. □

Vamos ao teorema principal do trabalho.

Teorema 3.14. *Sejam R um anel comutativo com identidade, G um grupo não-abeliano, φ uma involução em G e σ uma orientação não-trivial de G. Então $(RG)_{\sigma\varphi}$ é comutativo se, e somente se, uma das condições é verificada:*

(i) N é um grupo abeliano e $(G\backslash N) \subset G_\varphi$;

(ii) G e N são LC-grupos e existe um único comutador não-trivial s tal que a involução φ é dada por

$$\varphi(g) = \begin{cases} g & , \text{ se } g \in N \cap \mathcal{Z}(G) \text{ ou } g \in (G\backslash N)\backslash\mathcal{Z}(G) \\ sg & , \text{ caso contrário} \end{cases};$$

(iii) $\mathrm{car}(R) = 4$ e G é um SLC-grupo.

Demonstração. Suponha que $(RG)_{\sigma\varphi}$ é comutativo. Então $(RN)_\varphi$ é comutativo e (A) ou (B) ocorre. Temos dois casos a considerar:

(1) $(G\backslash N) \subset G_\varphi$

Neste caso, (A) ocorre. De fato, suponha que (B) ocorre. Sejam $x, y \in N$ tais que $xy \neq yx$. Logo, $x, y, xy \notin \mathcal{Z}(N)$. Assim $\varphi(x) = sx, \varphi(y) = sx$ e $\varphi(xy) = sxy$. Seja $g \in (G\backslash N) \subset G_\varphi$ (por hipótese). Então $xg \in (G\backslash N) \subset G_\varphi$ e $xg = \varphi(xg) = \varphi(g)\varphi(x) = gsx$. Da mesma forma, $yg = gsy$ e $xyg = gsxy$. Mas $sxy = g^{-1}xyg = (g^{-1}xg)(g^{-1}yg) = (sx)(sy) = xy$ e com isso $s = 1$, contradição. Logo, (i) ocorre.

(2) $(G\backslash N) \not\subset G_\varphi$

Dividiremos em 2 subcasos:

(2.1) $\mathrm{car}(R) \neq 4$.

Mostraremos que nesse caso, (ii) ocorre.

Seja $g \in (G\backslash N)\backslash G_{\varphi}$. Pelo Lema 3.11, $g \in \mathcal{Z}(G)$. Como $G = N \cup Ng$, se N é abeliano, então G é abeliano, já que $g \in \mathcal{Z}(G)$, contradição. Logo, (A) não ocorre. Assim, (B) ocorre.

Afirmação: G é um LC-grupo e $N' = G' = \{1, s\}$, onde s é o único comutador não-trivial de N.

Como $G = N \cup Ng, g \in \mathcal{Z}(G)$, para mostrar que G é um LC-grupo, temos que mostrar que, se $g_1, g_2 \in Ng$ e $g_1g_2 = g_2g_1$, então $g_1 \in \mathcal{Z}(G)$, ou $g_2 \in \mathcal{Z}(G)$, ou $g_1g_2 \in \mathcal{Z}(G)$, e que, se $g_1 \in N$ e $g_2 \in Ng$, com $g_1g_2 = g_2g_1$, então $g_1 \in \mathcal{Z}(G)$ ou $g_2 \in \mathcal{Z}(G)$ ou $g_1g_2 \in \mathcal{Z}(G)$. Vamos mostrar o primeiro caso. Sejam $x, y \in N$. Temos que $(xg)(yg) = (yg)(xg)$ se, e somente se, $xy = yx$, já que $g \in \mathcal{Z}(G)$. Como N é um LC-grupo, devemos ter $x \in \mathcal{Z}(N)$ ou $y \in \mathcal{Z}(N)$ ou $xy \in \mathcal{Z}(N)$. Vejamos que isso implica que $xg \in \mathcal{Z}(G)$ ou $yg \in \mathcal{Z}(G)$ ou $(xg)(yg) \in \mathcal{Z}(G)$. Suponha que $x \in \mathcal{Z}(N)$ e seja $h \in G$. Se $h \in N$, então $h^{-1}(xg)h = xg$, já que $g \in \mathcal{Z}(G)$ e $x \in \mathcal{Z}(N)$. Se $h \in Ng, \exists\, n \in N$ tal que $h = ng$. Então $h^{-1}(xg)h = g^{-1}n^{-1}xgng = xg$, já que $g \in \mathcal{Z}(G)$ e $x \in \mathcal{Z}(N)$. Logo, $xg \in \mathcal{Z}(G)$. De maneira análoga, mostra-se que, se $y \in \mathcal{Z}(N)$, então $yg \in \mathcal{Z}(G)$ e que se $xy \in \mathcal{Z}(N)$, então $(xg)(yg) \in \mathcal{Z}(G)$.

Agora, vamos mostrar que se $g_1 \in N$ e $g_2 \in Ng$, com $g_1g_2 = g_2g_1$, então $g_1 \in \mathcal{Z}(G)$ ou $g_2 \in \mathcal{Z}(G)$ ou $g_1g_2 \in \mathcal{Z}(G)$. Temos que $x(yg) = (yg)x$ se, e somente se, $xy = yx$, já que $g \in \mathcal{Z}(G)$. Como no caso anterior, devemos ter $x \in \mathcal{Z}(G)$ ou $yg \in \mathcal{Z}(G)$ ou $x(yg) \in \mathcal{Z}(G)$. Logo, G é um LC-grupo.

Para ver que $N' = G' = \{1, s\}$, sejam $x, y \in N$ tais que $xy \neq yx$. Temos que $(xg, yg) = (x, y) = s$, $(x, yg) = (x, y) = s$ e $(xg, y) = (x, y) = s$. Isto demonstra a afirmação.

Para finalizar, vamos mostrar que a involução φ é dada como no enunciado. Para isto, basta mostrar que $\mathcal{Z}(N) = N \cap \mathcal{Z}(G)$ e determinar φ em $G\backslash N$, já que N é um SLC-grupo.

Seja $h \in G\backslash N$. Se $h \notin \mathcal{Z}(G)$, pelo Lema 3.11, $h \in G_\varphi$. Se $h \in \mathcal{Z}(G)$, tome $x \in N\backslash\mathcal{Z}(N)$. Então $xh \in (G\backslash N)\backslash\mathcal{Z}(G)$ e, pelo Lema 3.11, $xh \in G_\varphi$. Logo $xh = \varphi(xh) = \varphi(h)sx$ e assim $\varphi(h) = sxhx^{-1} = sh$.

Agora, é claro que $N \cap \mathcal{Z}(G) \subseteq \mathcal{Z}(N)$. Seja $x \in \mathcal{Z}(N)\backslash\mathcal{Z}(G)$. Então $\varphi(x) = x$ e, pelo visto acima, $\exists\, y \in G\backslash N$ tal que $xy \neq yx$ e $\varphi(y) = y$. Assim, $xy \in (G\backslash N)\backslash\mathcal{Z}(G)$ e pelo Lema 3.11 $xy \in G_\varphi$. Com isso, $xy = \varphi(xy) = \varphi(y)\varphi(x) = yx$, contradição. Portanto, $\mathcal{Z}(N) = N \cap \mathcal{Z}(G)$ e segue (ii).

(2.2) $\mathrm{car}(R) = 4$.

Mostraremos que (ii) ou (iii) ocorre.

Se $G = N \cup G_\varphi \cup \mathcal{Z}(G)$, como $(G\backslash N) \not\subset G_\varphi$, temos que $(G\backslash N) \cap \mathcal{Z}(G) \neq \varnothing$. Logo, como em (2.1), mostra-se que (ii) ocorre.

Então suponha que $G \neq N \cup G_\varphi \cup \mathcal{Z}(G)$. Pelo Lema 3.13, se $g \in G\backslash N$ e $g \notin \mathcal{Z}(G)$, então $g \notin G_\varphi$.

Afirmação: Dados $g, h \in G$ tais que $gh \neq hg$, então $\varphi(g) = h^{-1}gh$.

De fato, se $g \in G\backslash N$ ou $h \in G\backslash N$, o Lema 3.11 nos garante que $\varphi(g) = h^{-1}gh$. Se $g, h \in N$, como N não é abeliano, (B) ocorre. Logo, $\varphi(g) = sg = (h, g^{-1})g = h^{-1}gh$. Isto demonstra a afirmação.

Com isso, temos que a involução φ possui a propriedade $h^{-1}gh \in \{g, \varphi(g)\}$. Portanto, pelo Teorema 2.7, G é um SLC-grupo e assim (iii) ocorre.

Sabemos que $(RG)_{\sigma\varphi}$ é gerado como R-módulo pelo conjunto $\mathcal{S} = N_\varphi \cup \{g + \varphi(g) : g \in N\backslash N_\varphi\} \cup \{g - \varphi(g) : g \in (G\backslash N)\backslash G_\varphi\}$. Vamos à recíproca.

Suponha que (i) ocorre. Então, se $g \in (G\backslash N) \subset G_\varphi$, $g - \varphi(g) = 0$. Logo, temos que $(RG)_{\sigma\varphi}$ é comutativo se, e somente se, $(RN)_\varphi$ é comutativo. Como N é abeliano, temos que $(RG)_{\sigma\varphi}$ é comutativo.

Suponha que (ii) ocorre. Vamos mostrar que a aplicação φ do enunciado é uma involução em G.

(1) $\varphi(\varphi(g)) = g, \forall\, g \in G$.

Como s é um elemento central de ordem 2, segue que $\varphi(\varphi(g)) = g, \forall\, g \in G$.

(2) $\varphi(gh) = \varphi(h)\varphi(g), \forall\, g, h \in G$.

Temos 2 casos a considerar.

1º caso) $gh \neq hg$. Então $gh = shg$ e $g, h, gh \notin \mathcal{Z}(G)$

Se $g, h \in N$, então $\varphi(gh) = sgh = hg = (sh)(sg) = \varphi(h)\varphi(g)$.

Se $g, h \notin N$, então $\varphi(gh) = sgh = hg = (sh)(sg) = \varphi(h)\varphi(g)$

Se $g \in N$ e $h \notin N$, então $\varphi(gh) = gh = shg = \varphi(h)\varphi(g)$. Análogo se $g \notin N$ e $h \in N$.

2º caso) $gh = hg$. Como G é um LC-grupo, devemos ter ou $g \in \mathcal{Z}(G)$ ou $h \in \mathcal{Z}(G)$ ou $gh \in \mathcal{Z}(G)$.

Se $g, h \in N$ e $g, h \in \mathcal{Z}(G)$, então $gh \in \mathcal{Z}(G)$. Logo $\varphi(gh) = gh = hg = \varphi(h)\varphi(g)$.

Se $g, h \in N$ e $g, h \notin \mathcal{Z}(G)$, então $gh \in \mathcal{Z}(G)$. Logo $\varphi(gh) = gh = hg = (sh)(sg) = \varphi(h)\varphi(g)$.

Se $g, h \in N$, $g \in \mathcal{Z}(G)$ e $h \notin \mathcal{Z}(G)$, então $gh \notin \mathcal{Z}(G)$. Logo, $\varphi(gh) = sgh = shg = \varphi(h)\varphi(g)$. Análogo se $g \notin \mathcal{Z}(G)$ e $h \in \mathcal{Z}(G)$.

Se $g, h \notin N$ e $g, h \in \mathcal{Z}(G)$, então $gh \in \mathcal{Z}(G)$. Logo $\varphi(gh) = gh = hg = (sh)(sg) = \varphi(h)\varphi(g)$.

Se $g, h \notin N$, $g \in \mathcal{Z}(G)$ e $h \notin \mathcal{Z}(G)$, então $gh \notin \mathcal{Z}(G)$. Logo, $\varphi(gh) = sgh = hsg = \varphi(h)\varphi(g)$. Análogo se $g \notin \mathcal{Z}(G)$ e $h \in \mathcal{Z}(G)$.

Se $g, h \notin N$ e $g, h \notin \mathcal{Z}(G)$, então $gh \in \mathcal{Z}(G)$. Logo, $\varphi(gh) = gh = hg = \varphi(h)\varphi(g)$.

Se $g \in N$, $h \notin N$ e $g, h \in \mathcal{Z}(G)$, então $gh \in \mathcal{Z}(G)$. Logo $\varphi(gh) = gh =$

$hg = (sh)(sg) = \varphi(h)\varphi(g)$. Análogo se $g \notin N$ e $h \in N$.

Se $g \in N$, $h \notin N$ e $g, h \notin \mathcal{Z}(G)$, então $gh \in \mathcal{Z}(G)$. Logo $\varphi(gh) = sgh = shg = \varphi(h)\varphi(g)$. Análogo se $g \notin N$ e $h \in N$.

Se $g \in N$, $h \notin N$, $g \in \mathcal{Z}(G)$ e $h \notin \mathcal{Z}(G)$, então $gh \notin \mathcal{Z}(G)$. Logo $\varphi(gh) = gh = hg = \varphi(h)\varphi(g)$. Análogo se $g \notin N$, $h \in N$ e g ou $h \notin \mathcal{Z}(G)$.

Assim, a aplicação φ do enunciado é uma involução em G. Observe que, neste caso, N é um SLC-grupo. Logo, podemos escrever $\mathcal{S}$ como

$$\mathcal{Z}(N) \cup \{g + sg : g \in N \backslash \mathcal{Z}(N)\} \cup \{g - sg : g \in (G \backslash N) \cap \mathcal{Z}(G)\}.$$

Observe que o conjunto $\{g - sg : g \in (G\backslash N) \cap \mathcal{Z}(G)\}$ é central em G. Como N é um SLC-grupo, pelo Corolário 2.12, o conjunto $\mathcal{Z}(N) \cup \{g + sg : g \in N\backslash\mathcal{Z}(N)\}$ é uma R-base de $\mathcal{Z}(RN)$, logo, comutativo. Portanto, o conjunto $\mathcal{S}$ é comutativo e assim $(RG)_{\sigma\varphi}$ é comutativo.

Finalmente, suponha que (iii) ocorre. Neste caso, podemos escrever $\mathcal{S}$ como

$$(N \cap \mathcal{Z}(G)) \cup \{g + gs : g \in N\backslash\mathcal{Z}(G)\} \cup \{g - sg : g \in (G\backslash N)\backslash\mathcal{Z}(G)\}.$$

Como G é um SLC-grupo, pelo Corolário 2.12, o conjunto $\mathcal{Z}(G) \cup \{g + sg : g \in G\backslash\mathcal{Z}(G)\}$ é uma R-base de $\mathcal{Z}(RG)$. Assim, os conjuntos $N \cap \mathcal{Z}(G)$ e $\{g + gs : g \in N\backslash\mathcal{Z}(G)\}$ são centrais em G. Logo, basta mostrar que o conjunto $\{g - sg : g \in (G\backslash N)\backslash\mathcal{Z}(G)\}$ é comutativo.

Sejam $g, h \in (G\backslash N)\backslash\mathcal{Z}(G)$. Então

$$[g - sg, h - sh] = 2(gh - hg) + 2(shg - sgh).$$

Se $gh = hg$, então $[g - sg, h - sh] = 0$. Se $gh \neq hg$, como G é um SLC-grupo, $gh = shg$. Logo, $[g - sg, h - sh] = 4(gh - hg) = 0$, já que $\mathrm{car}(R) = 4$. Portanto, o conjunto $\mathcal{S}$ é comutativo e assim $(RG)_{\sigma\varphi}$ é comutativo. □

Como caso particular do Teorema 3.14, vamos considerar a involução φ como sendo a inversão $*$ de G. Observe que, neste caso,

$$G_\varphi = G_* = \{g \in G : g^2 = 1\}.$$

Teorema 3.15. *Sejam R um anel comutativo com unidade, G um grupo não-abeliano, $*$ a inversão de G e σ uma orientação não-trivial de G. Então o conjunto $(RG)_{\sigma *}$ é comutativo se, e somente se, uma das condições é verificada:*

(1) *N é abeliano e $(G\backslash N)^2 = 1$;*

(2) *$N \cong \langle x, y : x^4 = 1, x^2 = y^2, x^y = x^{-1}\rangle \times E$ e $G \cong \langle x, y, g : x^4 = 1, x^2 = y^2 = g^2, x^y = x^{-1}, x^g = x, y^g = y\rangle \times E$, onde E é um 2-grupo abeliano elementar;*

(3) *$\mathrm{car}(R) = 4$ e G é um 2-grupo Hamiltoniano.*

Demonstração. Suponha que $(RG)_{\sigma *}$ é comutativo. Mostraremos que as condições $(i), (ii)$ e (iii) do Teorema 3.14 implicam as condições (1), (2) e (3) deste teorema, respectivamente.

Como $G_* = \{g \in G : g^2 = 1\}$, temos que (i) e (1) são equivalentes. Também, pela Proposição 3.9, temos que (iii) implica (3). Logo, basta mostrar que (ii) implica (2).

Assuma (ii). Pela Proposição 3.9, N é um 2-grupo Hamiltoniano. Logo, pelo Teorema 3.8 temos que $N \cong K_8 \times E$, onde K_8 denota o grupo dos quatérnios de ordem 8 e E é um 2-grupo abeliano elementar. Utilizaremos a apresentação $K_8 = \langle x, y : x^4 = 1, x^2 = y^2, x^y = x^{-1}\rangle$.

Pela definição de φ do enunciado do Teorema 3.14, temos que ou $(G\backslash N)^2 = 1$ ou $(G\backslash N) \cap \mathcal{Z}(G) \neq \varnothing$. De fato, se $(G\backslash N)^2 = 1$ e $(G\backslash N) \cap \mathcal{Z}(G) \neq \varnothing$, tome $g \in (G\backslash N) \cap \mathcal{Z}(G)$.

Então $g^{-1} = sg$, o que implicaria $s = 1$, já que $g^2 = 1$. Agora, não podemos ter $(G\backslash N)^2 = 1$. De fato, suponha que $(G\backslash N)^2 = 1$, e seja $g \in$

$G\backslash N$. Então $xg \in G\backslash N$ e assim $gxgx = 1$, i.e., $gxg = x^{-1}$. Da mesma forma, $gyg = g^{-1}$ e $g(xy)g = (xy)^{-1}$. Mas $g(xyg) = (gxg)(gyg) = x^{-1}y^{-1} = (yx)^{-1}$, o que nos dá $xy = yx$, contradição.

Com isso, temos que $(G\backslash N) \cap \mathcal{Z}(G) \neq \varnothing$. Seja $g \in (G\backslash N) \cap \mathcal{Z}(G)$. Como $N \cong K_8 \times E$, $G = N \cup Ng$ e $g \in \mathcal{Z}(G)$, temos que E é central em G, $\langle x, y, g\rangle \lhd G$ e $G = \langle x, y, g\rangle E$. Agora, temos que $g^{-1} = sg$ e $x^{-1} = sx$. Logo, $g^2 = x^2$ e $\langle x, y, g\rangle = \langle x, y, g : x^4 = 1, x^2 = y^2 = g^2, x^y = x^{-1}, x^g = x, y^g = y\rangle$. Com isso, basta mostrar que $\langle x, y, g\rangle \cap E = \{1\}$. Como $g^2 = x^2$, temos que $\langle x, y, g\rangle = \{zg : z \in \langle x, y\rangle\} \cup \langle x, y\rangle$. Mas $zg \notin N = \langle x, y\rangle \times E, \forall\, z \in \langle x, y\rangle$. Portanto, $\langle x, y, g\rangle \cap E = \{1\}$.

Reciprocamente, se (3) ocorre, pelo Teorema 3.8, $G \cong K_8 \times E$. Como E é abeliano, basta mostrar que $(RK_8)_{\sigma *}$ é comutativo. Pelo Exemplo 2.10, K_8 é um SLC-grupo com único comutador não-trivial s. Logo, como na demonstração do Teorema 3.14, $(RK_8)_{\sigma *}$ é comutativo.

Suponha que (2) ocorre. Seja $H = \langle x, y, g\rangle = \langle x, y, g : x^4 = 1, x^2 = y^2 = g^2, x^y = x^{-1}, x^g = x, y^g = y\rangle = \langle x, y\rangle \cup \langle x, y\rangle g = K_8 \cup K_8 g$. Como E é abeliano, basta mostrar que $(RH)_{\sigma *|_H}$ é comutativo. Como na demonstração do Teorema 3.14, parte (2.1), temos que H é um LC-grupo com um único comutador não-trivial s, já que K_8 é um SLC-grupo e g é central em H. O resultado segue do Teorema 3.14. □

Considerações Finais

Ao longo desta dissertação, buscamos condições necessárias e suficientes sobre o anel R e o grupo G para que o conjunto $(RG)_{\sigma\varphi}$ fosse comutativo, onde R é um anel de $\mathrm{car}(R) \neq 2$ e G é um grupo não-abeliano.

Como mencionamos na Introdução, podemos considerar o seguinte problema: se $(RG)_{\sigma\varphi}$ é Lie nilpotente (Lie n-Engel), então RG é Lie nilpotente (Lie m-Engel)? No caso que $\sigma = id$, existe uma resposta positiva.

Teorema 1. *[13, Teoremas A e B] Sejam K um corpo de $car(K) \neq 2$, G um grupo sem 2-elementos e φ uma involução (induzida) em KG. Então KG é Lie nilpotente (Lie n-Engel) se, e somente se, $(KG)_{\varphi}$ é Lie nilpotente (Lie m-Engel).*

Se $\sigma \neq id$ e $\varphi = *$, a inversão de G, existe uma resposta para o problema.

Teorema 2. *[15, Teoremas 3.1 e 3.2] Sejam K um corpo de $car(K) \neq 2$, G um grupo sem elementos de ordem 2 e σ uma orientação não-trivial de G. Então, KG é Lie nilpotente (Lie n-Engel) se, e somente se, $(KG)_{\sigma *}$ é Lie nilpotente (Lie m-Engel).*

Se a involução φ é qualquer, até o momento, não há uma resposta afirmativa para o problema.

Na busca da generalização do problema, introduzimos o conceito de *involuções orientadas não-lineares*. Sejam R um anel com identidade, G um

grupo, ψ uma involução em R, φ uma involução em G e σ uma orientação em G. Em RG, defina $\sigma\psi\varphi : RG \to RG$ por

$$\sigma\psi\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} \psi(a_g)\sigma(g)\varphi(g).$$

Se $\varphi(\ker(\sigma)) = \ker(\sigma)$, e usando o fato de $\sigma(g) \in R_\psi, \forall\, g \in G$ (Lema 1.3.4), como na Seção 1.3.3, mostra-se que a aplicação acima é uma involução em RG, chamada de *involução orientada não-linear*.

Sendo $\sigma\psi\varphi$ uma involução, podemos considerar o conjunto dos elementos $\sigma\psi\varphi$-simétricos $(RG)_{\sigma\psi\varphi}$. Os seguintes problemas, até o momento, continuam em aberto:

1) Quais condições sobre o anel R e o grupo G devemos impor para que o conjunto $(RG)_{\sigma\psi\varphi}$ seja comutativo?

2) Se $(RG)_{\sigma\psi\varphi}$ é Lie nilpotente, então RG é Lie nilpotente?

3) Se $(RG)_{\sigma\psi\varphi}$ é Lie n-Engel, então RG é Lie m-Engel?

A solução dos problemas apresentados nestas considerações é o objetivo de trabalhos futuros.

Referências Bibliográficas

[1] C. P. Milies, S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, 2002.

[2] C. P. Milies. *Anéis e Módulos*, Publicações do IME-USP, 1972.

[3] E. Jespers, M. Ruiz, *On symmetric elements and symmetric units in group rings*, Comm. Algebra, **34**, (2) (2006), 727-736.

[4] E. G. Goodaire, E. Jespers, C. P. Milies, *Alternative Loop Rings*, North Holland Math. Studies 184, Elsevier, Amsterdam, 1996.

[5] G. T. Lee, *Group Identities on Units and Symmetric Units of Group Rings*, Algebra and Aplications 12, Springer, 2010.

[6] J. Z. Gonçalves, D. S. Passman, *Involutions and free pairs of bicyclic units in integral group rings*, Journal of Group Theory 13, No. 5, 2010, 721-742.

[7] Knus et al, *The Book of Involutions*, AMS Colloquium Publications, Vol. 44, 1998, 593 pp.

[8] O. B. Cristo, C. P. Milies, *Symmetric elements under oriented involutions in group rings*, Communications in Algebra **34** (2006), 3347-3356.

[9] S. P. Novikov, *Algebraic construction and properties of hermitian analogues of K-theory over rings with involution from the viewpoint of Hamiltonian formalism, Applications to differential topology and the theory of characteristic classes II*, Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 475-500; English transl. in Math. USSR Izv., **4** (1970).

[10] S. A. Amitsur, *Rings with involutions*, Israel J. Math. **6** (1998), 99-106.

[11] I. M. Isaacs, D. S. Passman, *Groups with representations of bounded degree*, Canad. J. Math. **16** (1964), 299-309.

[12] D. S. Passman, *Group rings satisfying a polynomial identity*, J. Algebra **20** (1972) 221-225.

[13] A. Giambruno, C. P. Milies, S. K. Sehgal, *Lie properties of symmetric elements in group rings*, J. Algebra **321** (2009), nº 3, 890-902.

[14] N. Bourbaki, *Algèbre, Algèbre Lineaire, Chap. II*, Hermann, Paris, 1962.

[15] J. C. Gómez, C. P. Milies, *Lie properties of symmetric elements under oriented involutions*. Pré-print.