



ALCINDO TELES GALVÃO

Half-isomorfismos de Loops Automórficos Diedrais

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da UFAL –
Universidade Federal de Alagoas

Santo André, 2019



Universidade Federal do ABC

Centro de Matemática, Computação e Cognição

Alcindo Teles Galvão

Half-isomorfismos de Loops Automórficos Diedrais

Orientadora: Profa. Dra. Maria de Lourdes Merlini Giuliani

Tese de doutorado apresentada ao Centro de
Matemática, Computação e Cognição para
obtenção do título de Doutor em Matemática

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE
DEFENDIDA PELO ALUNO ALCINDO TELES GALVÃO,
E ORIENTADA PELA PROFA. DRA. MARIA DE LOURDES MERLINI GIULIANI.

Santo André, 2019

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Galvão, Alcindo Teles
Half-isomorfismos de Loops Automórficos Diedrais / Alcindo
Teles Galvão. — 2019.

82 fls. : il.

Orientadora: Maria de Lourdes Merlini Giuliani

Tese (Doutorado) — Universidade Federal do ABC, Programa de
Pós-Graduação em Matemática, Santo André, 2019.

1. Loops. 2. Loops Automórficos. 3. Half-isomorfismos. 4. Half
automorfismos. 5. Loops automórficos diedrais. I. Giuliani, Maria de
Lourdes Merlini. II. Programa de Pós-Graduação em Matemática,
2019. III. Título.



MINISTÉRIO DA EDUCAÇÃO

Fundação Universidade Federal do ABC

Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Tese de Doutorado do candidato, ALCINDO TELES GALVÃO realizada em 19 de Novembro 2019:

Prof.(a) Dr.(a) ALEXANDRE GRICHKOV
UNIVERSIDADE DE SÃO PAULO

Prof.(a) Dr.(a) DYLENE AGDA SOUZA DE BARROS
UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Prof.(a) Dr.(a) GILIARD SOUZA DOS ANJOS
UNIVERSIDADE DE SÃO PAULO

Prof.(a) Dr.(a) JUAN CARLOS GUTIERREZ FERNANDEZ
UNIVERSIDADE DE SÃO PAULO

Prof.(a) Dr.(a) LUIS ENRIQUE RAMIREZ
UNIVERSIDADE FEDERAL DO ABC

Prof.(a) Dr.(a) Orlando Stanley Juriaans
UNIVERSIDADE DE SÃO PAULO

Prof.(a) Dr.(a) MARIA DE LOURDES MERLINI GIULIANI
UNIVERSIDADE FEDERAL DO ABC - Presidente

* Por ausência do membro titular, foi substituído pelo membro suplente descrito acima: nome completo, instituição e assinatura



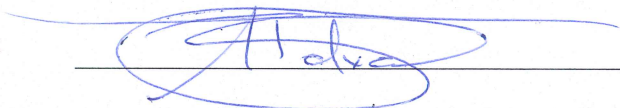
Universidade Federal do ABC

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do(a) autor(a) e com a anuência do(a) orientador(a).

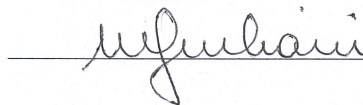
Santo André/SP

27 de 11 de 2019

Assinatura do(a) autor(a):



Assinatura do(a) orientador(a):



DEDICATÓRIA

Dedico essa tese aos meus pais José Ramos Galvão e Maria José Teles dos Santos.

AGRADECIMENTOS

Agradeço a Deus pela vida, aos meus pais pela minha criação e à tia Nancy pelo incentivo à minha escolarização.

À minha esposa Luciana e aos meus filhos, Adriano, Elaine, Aline, Luan e Laura, por suportarem minha ausência.

Aos amigos de fora e de dentro do mundo acadêmico pelas diversas formas de incentivos.

Na graduação e no mestrado destaco Gastão, Fernando, Romário, Zeneilton, Rinaldo, Steve e Wagner.

Na transição entre mestrado e doutorado agradeço ao subgrupo do verão da Unicamp. No doutorado agradeço a todos os colegas, destaco Bruno Rogério Locatteli dos Santos e Altemir Bortuli Junior, sendo que as afinidades fizeram do Altemir um irmão.

Agradeço aos Professores anteriores ao doutorado nos nomes de Adroaldo de Vasconcelos Dorvilé e José Adonai Pereira Seixas.

Agradeço aos governos do PT, na pessoa do presidente Luiz Inácio Lula da Silva, pelas criações do *Campus* da UFAL em Arapiraca, onde eu trabalho, e da UFABC, onde fiz meu doutorado.

No doutorado agradeço a todos os Professores nos nomes dos Professores Francisco César Polcino Milies e Igor Leite Freire.

Agradeço aos membros da banca, dos quais destaco Giliard Souza dos Anjos pela importante colaboração em todo o processo do desenvolvimento da tese.

Por fim, um agradecimento especial à minha orientadora Maria de Lourdes Merlini Giuliani, pela amizade, pela paciência e pela competência.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

"Deve-se escrever da mesma maneira como as lavadeiras lá de Alagoas fazem seu ofício. Elas começam com uma primeira lavada, molham a roupa suja na beira da lagoa ou do riacho, torcem o pano, molham-no novamente, voltam a torcer. Colocam o anil, ensaboam e torcem uma, duas vezes. Depois enxaguam, dão mais uma molhada, agora jogando a água com a mão. Batem o pano na laje ou na pedra limpa, e dão mais uma torcida e mais outra, torcem até não pingar do pano uma só gota. Somente depois de feito tudo isso é que elas dependuram a roupa lavada na corda ou no varal, para secar. Pois quem se mete a escrever devia fazer a mesma coisa. A palavra não foi feita para enfeitar, brilhar como ouro falso; a palavra foi feita para dizer."

- Da crônica *Linhas Tortas*, do Alagoano Graciliano Ramos, publicada em 1962.

RESUMO

Loops automórficos, ou A-loops, são loops nos quais todas as aplicações internas são automorfismos. Os loops automórficos diedrais abordados nesta tese formam uma classe de A-loops construídos a partir dos grupos cíclicos $\mathbb{Z}_m$ e C_p onde m é um número inteiro positivo par e p é um número primo, maior ou igual a 2. Denotamos tais loops por $L_\alpha = Dih(m, C_p, \alpha)$, onde α é um automorfismo de C_p . Um half-isomorfismo entre os loops L_α e L_β é uma função bijetora f tal que $f(x \cdot y) = f(x)f(y)$ ou $f(x \cdot y) = f(y)f(x)$, para quaisquer elementos $x, y \in L_\alpha$. Dizemos que o half-isomorfismo f é não trivial se f não é isomorfismo e nem anti-isomorfismo. Nesta tese descrevemos as propriedades e classificamos os half-isomorfismos não triviais entre os loops L_α e L_β . Provamos também que em L_J todos os half-automorfismos são triviais onde J é o automorfismo de C_p definido por $J(x) = x^{-1}$.

Palavras-chave: loops, loops automórficos, half-isomorfismos, half-automorfismos, loops automórficos diedrais.

ABSTRACT

Automorphic loops, or A -loops, are loops in which all inner mappings are automorphisms. The dihedral automorphic loops class considered in this thesis are constructed by taking the cyclic groups $\mathbb{Z}_m$ and C_p where m is an even positive integer and p is a prime number greater than or equal to 2. We denote such loops by $L_\alpha = Dih(m, C_p, \alpha)$, where α is an automorphism of C_p . A half-isomorphism between L_α and L_β is a bijection f such that $f(x \cdot y) = f(x)f(y)$ or $f(x \cdot y) = f(y)f(x)$, for any elements $x, y \in L_\alpha$. We say that f is nontrivial if f is neither isomorphism nor anti-isomorphism. In this thesis we describe the properties and classify all nontrivial half-isomorphisms between L_α and L_β . We also prove that in L_J all half-automorphisms are trivial where J is the automorphism of C_p defined by $J(x) = x^{-1}$.

Keywords: loops, automorphic loops, half-isomorphisms, half-automorphisms, dihedral automorphic loops.

CONTEÚDO

Introdução	1
1 LOOPS: CONCEITOS PRELIMINARES	5
1.1 Loops	5
1.2 Subloops	8
1.3 Half-isomorfismos de Loops	12
2 LOOPS AUTOMÓRFICOS	17
3 HALF-ISOMORFISMOS ENTRE OS A -LOOPS DIEDRAIS $Dih(m, C_p, \alpha)$: CASOS $m = 4$ E $m = 6$	23
3.1 Os A -Loops Diedrais $Dih(4, C_p, \alpha)$ e $Dih(6, C_p, \alpha)$	25
3.2 Half-Isomorfismos: para os casos $m = 4$ e $m = 6$	28
3.3 Half-Automorfismos: para os casos $m = 4$ e $m = 6$	44
3.4 Os A -Loops Diedrais $Dih(4, C_3, \alpha)$ e $Dih(6, C_3, \alpha)$	50
4 HALF-ISOMORFISMOS ENTRE OS A -LOOPS DIEDRAIS $Dih(m, C_p, \alpha)$: O CASO GERAL	63
4.1 Loops Automórficos Diedrais $Dih(m, C_p, \alpha)$	63
4.2 Half-Isomorfismos entre os Loops Automórficos Diedrais $Dih(m, C_p, \alpha)$	69
4.3 Half-Automorfismos entre os Loops Automórficos Diedrais $Dih(m, C_p, \alpha)$	76
Referência Bibliográfica	79

INTRODUÇÃO

Um loop é um conjunto L não vazio com uma operação binária $(\cdot)$ tal que para todo par de elementos $a, b \in L$, as equações $a \cdot x = b$ e $y \cdot a = b$ têm soluções únicas, para quaisquer $x, y \in L$, e existe um elemento neutro $1 \in L$ tal que $1 \cdot x = x \cdot 1 = x$ para todo $x \in L$. Grupos são exatamente loops associativos, e muitos dos resultados que são consolidados em teoria de grupos não são válidos para loops em geral, como por exemplo o teorema de Lagrange, o teorema de Cauchy e os teoremas de Sylow. No entanto o teorema do homomorfismo é válido para a categoria de loops.

A teoria de loops é relativamente jovem, tendo seu desenvolvimento ocorrido nos últimos oitenta anos. De fato, podemos dizer que o surgimento da teoria de loops se deu com a publicação de dois papers que por sua vez definiram duas importantes classes de loops que são conhecidas como "loops de Moufang" e "loops de Bol": *Zur Struktur von Alternativ Koerpern* por Ruth Moufang [Mou35], em 1935, e *Gewebe und Gruppen* por Gerrit Bol [Bol37], em 1937. Juntos esses dois papers marcaram o início formal da teoria de loops. Um loop de Moufang é um loop que satisfaz uma identidade que é uma aproximação da lei associativa: $(xy)(zx) = x((yz)x)$ a qual chamamos hoje de "identidade de Moufang". Ruth Moufang provou neste mesmo paper que esses loops são diassociativos, isto é, quaisquer dois elementos geram um subloop associativo.

Seja L um loop. Considere a bijeção $R_a : L \rightarrow L$, dada por $x \mapsto xa$, chamada translação à direita por a e, analogamente, $L_a : L \rightarrow L$, dada por $x \mapsto ax$, a translação à esquerda por a . Definimos o grupo das multiplicações de L , denotado por $Mlt(L)$, como sendo o grupo das permutações $Mlt(L) = \langle R_a, L_a; a \in L \rangle$. O grupo das aplicações internas, denotado por $Inn(L)$, é o subgrupo de $Mlt(L)$ que consiste das aplicações $f \in Mlt(L)$ tais que $f(1) = 1$. Dizemos que L é um loop automórfico se toda aplicação interna de L é um automorfismo de L , ou seja, $Inn(L)$ é um subgrupo do grupo $Aut(L)$, o grupo dos automorfismos de L . Convém ressaltar que grupos são loops automórficos mas a recíproca não é verdadeira.

Os loops automórficos (ou A -loops na notação de Bruck) foram definidos por Bruck e Paige em [BP56], onde eles mostraram que todo A -loop é potencialmente associativo, ou seja, cada elemento gera um grupo cíclico. Nesse mesmo artigo eles ainda conjecturaram que todo A -loop diassociativo é um loop de Moufang, fato que foi provado em 2002 [KKP02] com o uso de ferramentas computacionais.

Uma questão que aparece naturalmente é se loops automórficos têm uma expressão geral que os identifica. Loops automórficos de ordem p ou p^2 são grupos, onde p é um número primo, porém existem loops automórficos não associativos de ordem p^3 com núcleo trivial e expoente p . Em [KKPV16] os autores construíram uma classe de A -loops não associativos partindo de um grupo abeliano finito G e um automorfismo α de G generalizando a construção do grupo diedral e que tem ordem $2|G|$. Para esta classe deram o nome de *loop automórfico diedral* e denotaram por $Dih(m, G, \alpha)$. Esta classe tem uma característica importante, ela responde de certa forma um dos questionamentos: todo A -loop não associativo de ordem $2p$, onde p é um número primo é um loop automórfico diedral.

Um *half-isomorfismo* de loops é uma bijeção f entre os loops $(L, *)$ e $(L', \cdot)$ onde, para cada par de elementos $x, y \in L$, temos $f(x * y) \in \{f(x) \cdot f(y), f(y) \cdot f(x)\}$. Dizemos que um half-isomorfismo é *trivial* se ele é isomorfismo ou anti-isomorfismo (de maneira similar definimos half-isomorfismo não trivial). Em 1957 Scott [Sco57] provou que para grupos todo half-isomorfismo é um isomorfismo ou anti-isomorfismo.

Em teoria de grupos, o estudo de *determinante de grupo* levou Frobenius a desenvolver sua teoria de caracteres. Posteriormente, E. Formanek e D. Sibley [For91] provaram que um grupo finito é unicamente determinado pelo seu determinante. Isso foi feito usando o fato de que existe um half-isomorfismo entre dois grupos que possuem o mesmo determinante de grupo. Este fato junto com o resultado de Scott mostrou que dois grupos tendo determinantes equivalentes têm que ser isomorfos. Muitos especialistas em teoria de loops tem trabalhado na linha de investigação de half-isomorfismos, com o objetivo de identificar para quais categorias de loops o resultado de Scott pode ser estendido, este é o caso para loops de Moufang de ordem ímpar, provado por Giuliani e Gagola em [GG12]. Em caso de existência de half-automorfismo não trivial em uma classe de loops, é importante verificar se é possível identificar seu grupo de half-automorfismos.

O objetivo deste trabalho é investigar half-isomorfismos na classe de loops automórficos diedrais $Dih(m, G, \alpha)$. Inicialmente descrevemos por completo os loops diedrais

$Dih(m, C_p, \alpha)$, onde $\alpha : C_p \rightarrow C_p$ é um automorfismo do grupo cíclico de ordem p , com p primo maior ou igual a 2. Apresentamos dois casos particulares: os loops diedrais $Dih(4, C_p, \alpha)$ e $Dih(6, C_p, \alpha)$ com a descrição de seus half-isomorfismos. Por fim generalizamos os resultados obtidos nesses casos particulares descrevendo os half-isomorfismos dos loops automórficos diedrais $Dih(m, C_p, \alpha)$, para todo m par, positivo, e todo p primo maior ou igual a 2.

Este trabalho está dividido em quatro capítulos. No primeiro capítulo introduzimos as definições e resultados básicos sobre loops, subloops, half-isomorfismos de loops e suas propriedades mais conhecidas. O segundo capítulo estabelece o conceito de loops automórficos, além de resultados básicos relacionados a esse conceito, de forma geral.

No terceiro capítulo damos início à investigação dos loops automórficos diedrais $Dih(m, C_p, \alpha)$. Descrevemos todos os half-isomorfismos entre os loops diedrais $Dih(4, C_p, \alpha)$ e $Dih(4, C_p, \beta)$ e entre $Dih(6, C_p, \alpha)$ e $Dih(6, C_p, \beta)$, onde p é um número primo maior ou igual a 2. Além disso demonstramos que todos esses half-isomorfismos são não triviais.

No quarto capítulo apresentamos o caso geral $Dih(m, C_p, \alpha)$, para m inteiro par maior ou igual a 2. Descrevemos completamente os half-isomorfismos para essa classe de loops, determinamos as ordens dos elementos e a quantidade exata de half-isomorfismos para cada m e p dados. Mostramos também que todos os half-isomorfismos entre os loops $Dih(m, C_p, \alpha)$ e $Dih(m, C_p, \beta)$ são não triviais quando $\alpha \neq \beta$, onde α e β são iguais a I , a função identidade $I(x) = x$, ou J , a função inversão $J(x) = x^{-1}$. No entanto, mostramos que todos os half-automorfismos dos loops $Dih(m, C_p, J)$ são triviais.

1

LOOPS: CONCEITOS PRELIMINARES

Começaremos formalizando o conceito de loop, dando os primeiros exemplos e estabelecendo resultados básicos. Vamos omitir algumas demonstrações, pois muitas delas são fatos bem consolidados e podem ser encontradas na bibliografia citada para cada caso.

1.1 LOOPS

Definição 1.1. Um loop é um conjunto L , não vazio, dotado de uma operação binária $(\cdot)$, fechada em L , tal que dados $a, b \in L$ existem únicos $x, y \in L$ tais que $a \cdot x = b$ e $y \cdot a = b$, e com um elemento neutro $1 \in L$ tal que $1 \cdot x = x \cdot 1 = x$, para todo $x \in L$.

Denotamos o loop L com sua operação por $(L, \cdot)$. Caso não seja necessário identificar a operação diremos apenas "o loop L " e vamos escrever ab no lugar de $a \cdot b$.

No caso em que a operação de um loop L é associativa, temos que L é um grupo.

Uma consequência dessa definição é que vale a lei do cancelamento para a operação, ou seja, dados $a, b \in L$, $ax = bx$ ou $xa = xb$ se, e somente se, $a = b$, $\forall x \in L$. A lei do cancelamento é fundamental para a demonstração de várias propriedades de loops. A definição junto com a lei do cancelamento nos garante que se conhecemos dois elementos na igualdade $ab = c$, com $a, b, c \in L$, então o terceiro elemento é unicamente determinado.

Exemplo 1.2. O conjunto $L = \{1, 2, 3, 4, 5\}$ é um loop com a operação dada pela tabela

·	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

Observe que temos o elemento identidade $1 \in L$ e que cada elemento comparece apenas uma vez em cada coluna e em cada linha da tabela, garantindo a existência e a unicidade das soluções $x, y \in L$ de $ax = b$ e $ya = b$ para todo $a, b \in L$. Além disso L é um loop não associativo e não comutativo, pois temos, por exemplo, que $3 \cdot (3 \cdot 4) = 3 \cdot 2 = 5$, mas $(3 \cdot 3) \cdot 4 = 1 \cdot 4 = 4$ e $3 \cdot 4 = 2 \neq 5 = 4 \cdot 3$.

Seguem mais algumas definições:

Definição 1.3. Sejam L um loop e $a \in L$. Definimos a translação à direita por $a \in L$, $R_a : L \rightarrow L$, dada por $(x)R_a = xa$. Analogamente, definimos a translação à esquerda por $a \in L$, $L_a : L \rightarrow L$, dada por $(x)L_a = ax$. Decorre da definição de loops que essas funções são bijetoras.

Definição 1.4. Um loop $(L, \cdot)$ é dito potencialmente associativo quando o conjunto gerado por qualquer elemento de L é um grupo cíclico, ou seja, $(\langle x \rangle, \cdot)$ é associativo para todo $x \in L$.

Definição 1.5. Um loop $(L, \cdot)$ é dito diassociativo quando o conjunto gerado por quaisquer dois elementos de L é um grupo, ou seja, $(\langle x, y \rangle, \cdot)$ é associativo para todo par de elementos $x, y \in L$.

É simples verificar que um loop L ser diassociativo implica que L é potencialmente associativo.

Seja L um loop e $a \in L$. Como consequência da definição de loops, existem únicos $x, y \in L$ tais que $xa = 1$ e $ay = 1$. Esses elementos x e y são chamados, respectivamente, inverso à esquerda e inverso à direita de a e são denotados por x^λ e x^ρ . No caso em que $x^\lambda = x^\rho$, esse elemento é chamado inverso bilateral de a e denotado por x^{-1} .

Uma consequência imediata da definição (1.4), devido ao fato de $(\langle x \rangle, \cdot)$ ser grupo, $\forall x \in L$, é que se L é um loop potencialmente associativo, então todo elemento de L possui inverso bilateral.

Definição 1.6. Sejam $(L, \cdot)$ um loop e $x \in L$. Definimos as potências de x por

$$x^0 = 1 \quad \text{e} \quad x^{n+1} = x^n \cdot x, \text{ para } n \text{ número natural.}$$

No caso em que todo elemento de L possui inverso bilateral, podemos definir as potências negativas de cada elemento de x por $x^{-n} = (x^n)^{-1}$.

Definição 1.7. Um loop L é chamado loop com propriedade inversa à esquerda, quando dado $a \in L$, existe $a^\lambda \in L$ tal que $a^\lambda(ax) = x$, $\forall x \in L$. Denotamos esses loops por LIP-loops. Analogamente L é dito loop com propriedade inversa à direita, quando dado $a \in L$, existe $a^\rho \in L$ tal que $(xa)a^\rho = x$, $\forall x \in L$. Denotamos esses loops por RIP-loops.

Definição 1.8. Um loop L é chamado loop com propriedade inversa, ou IP-loop, quando ele é um LIP-loop e um RIP-loop.

Os loops que são abordados nesta tese são potencialmente associativos, mas não são IP-loops. Concluiremos a seção com um teorema que estabelece propriedades de IP-loops.

Teorema 1.9. ([Pfl90], Teorema I.4.1) Seja L um IP-loop, então temos os seguintes resultados:

- (a) $(a^\lambda)^\lambda = a$ e $(a^\rho)^\rho = a$;
- (b) $ax = b$ e $ya = b$ tem soluções $a^\lambda b$ e ba^ρ , respectivamente;
- (c) $(ab)^\lambda = b^\rho a^\rho$ e $(ab)^\rho = b^\lambda a^\lambda$;
- (d) $R_a^{-1} = R_{a^\rho}$ e $L_a^{-1} = L_{a^\lambda}$;
- (e) sendo J_λ e J_ρ de L em L dadas por $J_\lambda(x) = x^\lambda$ e $J_\rho(x) = x^\rho$, temos que

$$J_\lambda R_a J_\rho = L_{a^\lambda},$$

$$J_\rho R_a J_\lambda = L_{a^\rho},$$

$$J_\lambda L_a J_\rho = R_{a^\lambda} \text{ e}$$

$$J_\rho L_a J_\lambda = R_{a^\rho}.$$

Note que a definição de loop garante a unicidade de x^λ e de x^ρ , mas não necessariamente a igualdade. No exemplo (1.2) temos que $x \cdot x = 1$, $\forall x \in L$, então $x^\rho = x^\lambda = x$, $\forall x \in L$. Porém, $(2 \cdot 3) \cdot 3 \neq 2$ e $2 \cdot (2 \cdot 3) \neq 3$. Logo, L não é IP-loop.

1.2 SUBLOOPS

Definição 1.10. *Um subconjunto não vazio H de um loop $(L, \cdot)$ é um subloop de L se $(H, \cdot)$ também é um loop.*

O resultado a seguir nos dá uma condição necessária e suficiente para que um subconjunto de um loop L seja subloop de L .

Proposição 1.11. *([GJM96]) Seja H um subconjunto de um loop L , então H é subloop de L se, e somente se as seguintes condições se verificam:*

- (a) *se x e y pertencem a H , então xy pertence a H ;*
- (b) *se x e z pertencem a H e $xy = z$, então y pertence a H e*
- (c) *se y e z pertencem a H e $xy = z$, então x pertence a H .*

Assim como na teoria de grupos alguns subloops se destacam quando pretendemos estudar as propriedades de um dado loop L .

Definição 1.12. *Sejam a e b elementos de um loop L . O comutador de a e b é o único elemento $(a, b) \in L$ que satisfaz $ab = (ba)(a, b)$.*

Definição 1.13. *Sejam a , b e c elementos de um loop L . O associador de a , b e c é o único elemento $(a, b, c) \in L$ que satisfaz $a(bc) = \{(ab)c\}(a, b, c)$.*

Podemos então denotar por (X, Y, Z) e (X, Y) o conjunto dos associadores da forma (x, y, z) e dos comutadores da forma (x, y) , respectivamente. Com essa notação descrevemos os seguintes conjuntos, que são subloops.

- Definição 1.14.**
- (i) *O conjunto $D(L) = \langle (L, L, L), (L, L) \rangle$ é o associador-comutador de um loop L .*
 - (ii) *O conjunto $N_\lambda(L) = \{a \in L \mid (a, x, y) = 1, \forall x, y \in L\}$ é o núcleo à esquerda de um loop L .*
 - (iii) *O conjunto $N_\rho(L) = \{a \in L \mid (x, y, a) = 1, \forall x, y \in L\}$ é o núcleo à direita de um loop L .*
 - (iv) *O conjunto $N_\mu(L) = \{a \in L \mid (x, a, y) = 1, \forall x, y \in L\}$ é o núcleo central de um loop L .*
 - (v) *O conjunto $N(L) = N_\lambda \cap N_\rho \cap N_\mu$ é o núcleo de um loop L .*

(vi) O conjunto $Z(L) = \{a \in N(L) \mid (a, x) = 1, \forall x \in L\}$ é o centro de um loop L .

Proposição 1.15. ([Pfl90]). *Todo núcleo de um loop é um subloop associativo e, portanto, um grupo. O centro do loop é um grupo abeliano.*

Definição 1.16. *Sejam L um loop e S um subconjunto não vazio de L . Seja T o conjunto de todos os subloops H de L tais que $S \subseteq H$, então o conjunto $\bigcap_{H \in T} H$ é chamado subloop gerado por S . Denotaremos esse conjunto por $\langle S \rangle$.*

Sabemos que o teorema de Lagrange não vale para loops em geral. Vejamos um exemplo.

Exemplo 1.17. *O conjunto $L = \{1, 2, 3, 4, 5, 6, 7\}$ é um loop com a operação dada pela tabela*

$\cdot$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	1	7	6	5	3
3	3	1	5	6	7	2	4
4	4	6	7	2	1	3	5
5	5	7	6	1	3	4	2
6	6	3	4	5	2	7	1
7	7	5	2	3	4	1	6

Veja que L é um loop de ordem 7 que tem um subloop, $H = \{1, 6, 7\}$, de ordem 3.

Alguns conceitos de teoria de grupos se traduzem de maneira similar no contexto de loops, como é o caso de classes laterais.

Definição 1.18. *Sejam L um loop, H subloop de L e $K \subseteq L$, então K é uma classe lateral à esquerda de H (respectivamente à direita) quando $K = aH$ (respectivamente $K = Ha$) para algum $a \in L$.*

Dizemos que L tem uma decomposição em classes laterais à direita (à esquerda) módulo H se o conjunto de todas as classes laterais à direita (à esquerda) de H for uma partição de L . Ou seja, L é a união de todas as classes laterais à direita (à esquerda) de H e a interseção entre duas classes laterais de H distintas é vazia.

Mas, naturalmente, dado um subloop H qualquer, não garantimos a existência da decomposição em classes laterais de H , como ocorre com o loop do exemplo (1.2). Note

que, naquele exemplo, $H = \{1, 2\}$ é subloop do loop L , $1H = \{1, 2\} = 2H$, $3H = \{3, 5\}$, $4H = \{3, 4\}$ e $5H = \{4, 5\}$. Logo, o conjunto formado por essas classes não formam uma partição de L , pois, por exemplo, $3H \cap 4H \neq \emptyset$ e assim $3H \neq 4H$.

Precisamos então da seguinte proposição.

Proposição 1.19. ([Pfl90], Teorema I.2.12) *Sejam L um loop e H um subloop de L , então L tem uma decomposição em classes laterais à esquerda (respectivamente à direita) módulo H se, e somente se, $(a \cdot h)H = aH$, (respectivamente $H(h \cdot a) = Ha$) para todo $h \in H$ e todo $a \in L$.*

Aqui é importante introduzir as seguintes definições.

Definição 1.20. *Sejam L um loop finito e H subloop de L . Dizemos que H é tipo-Lagrange quando $|H|$ divide $|L|$, ou seja, a ordem de H divide a ordem de L .*

Definição 1.21. *Seja L um loop finito. Dizemos que L satisfaz a propriedade fraca de Lagrange quando todo subloop H de L é tipo-Lagrange.*

Definição 1.22. *Seja L um loop finito. Dizemos que L satisfaz a propriedade forte de Lagrange quando todo subloop H de L satisfaz a propriedade fraca de Lagrange.*

É natural que possamos ter um loop que satisfaz a propriedade fraca de Lagrange sem satisfazer a propriedade forte de Lagrange. Esse é o caso no loop L do exemplo abaixo.

Exemplo 1.23. *O conjunto $L = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ é um loop com a operação dada pela tabela*

$\cdot$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	1	4	5	3	7	8	9	10	6
3	3	5	1	2	4	8	9	10	6	7
4	4	3	5	1	2	9	10	6	7	8
5	5	4	2	3	1	10	6	7	8	9
6	6	7	8	9	10	1	2	3	4	5
7	7	8	9	10	6	2	1	4	5	3
8	8	9	10	6	7	3	5	1	2	4
9	9	10	6	7	8	4	3	5	1	2
10	10	6	7	8	9	5	4	2	3	1

De fato, nesse exemplo temos um loop L , contendo subloops $H = \{1, 2\}$ e $K = \{1, 2, 3, 4, 5\}$, tais que H é subloop de K e ambos são subloops de L , onde $|L| = 10$, $|H| = 2$ e $|K| = 5$. Assim, as ordens de H e K dividem a ordem de L , mas $|H| = 2$ não divide $|K| = 5$.

Por fim, o resultado que mais nos aproxima do teorema de Lagrange nesse contexto é o seguinte.

Teorema 1.24. ([Pfl90], Teorema I.2.16) *Sejam L um loop finito e H subloop de L . Se L tem uma decomposição em classes laterais à esquerda (respectivamente à direita) módulo H , então H é tipo-Lagrange.*

Definição 1.25. *Um loop L é um loop de Moufang se satisfaz uma das seguintes identidades equivalentes:*

- (i) $((xy)x)z = x(y(xz))$, a identidade de Moufang à esquerda,
- (ii) $((xy)z)y = x(y(zy))$, a identidade de Moufang à direita,
- (iii) $(xy)(zx) = (x(yz))x$, a identidade de Moufang central.

A equivalência dessas identidades pode ser vista em [GJM96].

Convém destacar que o teorema de Lagrange vale para a classe dos loops de Moufang. Este resultado foi provado por A. Grishkov e A. Zavarnitsine em [GZ04].

Concluimos a seção com as definições importantes de subloops normais e subloops característicos.

Definição 1.26. *Seja H um subloop de L , tal que L tenha uma decomposição (à direita e à esquerda) módulo H , então H é chamado um subloop normal de L quando*

$$xH = Hx, \quad (xH)y = x(Hy) \quad \text{e} \quad x(yH) = (xy)H,$$

para todo $x, y \in L$.

Observação 1.27. *No capítulo 2 vamos estabelecer uma condição necessária e suficiente para que um subloop seja normal.*

Definição 1.28. *Sejam os loops $(L_1, \cdot)$ e $(L_2, *)$ e $f : L_1 \rightarrow L_2$ uma função. Diremos que f é um homomorfismo de loops quando $f(x \cdot y) = f(x) * f(y)$, para todo $x, y \in L_1$.*

De maneira inteiramente análoga à teoria de grupos definimos isomorfismos e endomorfismos de loops.

Definição 1.29. *Sejam L um loop e $f : L \rightarrow L$ uma função bijetora. Diremos que f é um automorfismo de L quando $f(xy) = f(x)f(y)$, para todo $x, y \in L$.*

O conjunto dos automorfismos de L será denotado por $\text{Aut}(L)$.

Definição 1.30. *Seja H um subloop de L . Diremos que H é subloop característico de L quando $\varphi(H) = H$, para todo $\varphi \in \text{Aut}(L)$.*

1.3 HALF-ISOMORFISMOS DE LOOPS

Introduziremos aqui o conceito de *half-isomorfismo* de loops destacando suas principais propriedades.

Definição 1.31. *Sejam $(L, \cdot)$ e $(L', *)$ loops. Um half-isomorfismo de L em L' é uma função bijetora f tal que $f(x \cdot y) = f(x) * f(y)$ ou $f(x \cdot y) = f(y) * f(x)$, para todos os elementos $x, y \in L$.*

No caso em que $L = L'$ e f é um half-isomorfismo, diremos que f é um half-automorfismo.

Se $f(x \cdot y) = f(x) * f(y)$, para todo $x, y \in L$, então temos um isomorfismo e se $f(x \cdot y) = f(y) * f(x)$, para todo $x, y \in L$, então temos um anti-isomorfismo. No caso em que o half-isomorfismo é isomorfismo ou anti-isomorfismo diremos que ele é um half-isomorfismo trivial. Para grupos, todos os half-isomorfismos são triviais como foi mostrado por Scott [Sco57]. Em geral, para loops a situação é diferente: existem loops de Moufang com half-isomorfismos que não são nem isomorfismos nem anti-isomorfismos. No entanto o resultado de Scott foi extendido para a classe de loops de Moufang finitos de ordem ímpar. Em 2013 Giuliani e Gagola mostraram que nessa classe todos os half-isomorfismos são triviais [GG13].

Exemplo 1.32. *Consideremos novamente o loop L descrito no exemplo (1.17). Consideremos também a função inversão $J : L \rightarrow L$, definida por $J(x) = x^{-1}$, $\forall x \in L$. Podemos verificar, usando o GAP ([Gro]), por exemplo, que J é um half-automorfismo de L . Observe então que*

$$J(2 \cdot 4) = J(7) = J(4) \cdot J(2) = 6 \neq J(2) \cdot J(4) = 7$$

e

$$J(5 \cdot 6) = J(4) = J(5) \cdot J(6) = 5 \neq J(6) \cdot J(5) = 3.$$

Logo, J é um half-automorfismo de L que não é isomorfismo e não é anti-isomorfismo, portanto é um half-automorfismo não trivial.

As proposições a seguir estabelecem resultados fundamentais para a categoria de A -loops, que definiremos formalmente no próximo capítulo. Devido a importância nesse trabalho decidimos incluir as demonstrações de algumas dessas proposições.

Proposição 1.33. ([dA18]) *Sejam $f : L \rightarrow L'$ um half-isomorfismo de loops, onde $1_L \in L$ e $1'_{L'} \in L'$ são os elementos identidades, e K subloop de L' . Então*

- (a) $f(1_L) = 1'_{L'}$;
- (b) $f^{-1}(K)$ é subloop de L ;
- (c) se K é comutativo, então $f^{-1}(K)$ é comutativo e $f^{-1}(K) \cong K$;
- (d) se K é grupo abeliano, então $f^{-1}(K)$ é grupo abeliano;
- (e) se L' é comutativo, então $L \cong L'$.

Demonstração. Demonstraremos os itens (a) e (b).

- (a) Temos $f(1_L) = f(1_L \cdot 1_L) = f(1_L) * f(1_L)$. Logo, $f(1_L) = 1'_{L'}$.
- (b) Considere $x, y \in f^{-1}(K)$, então $f(x), f(y) \in K$. Logo,

$$\{f(x \cdot y), f(y \cdot x)\} \subseteq \{f(x) * f(y), f(y) * f(x)\} \subseteq K.$$

Assim, $x \cdot y \in f^{-1}(K)$.

Agora sejam $z, w \in L$ tais que $z \cdot x = y$ e $x \cdot w = y$, então

$$f(y) = f(x \cdot w) \in \{f(x) * f(w), f(w) * f(x)\}$$

e

$$f(y) = f(z \cdot x) \in \{f(z) * f(x), f(x) * f(z)\}.$$

Como $f(x), f(y) \in K$, temos que $f(z), f(w) \in K$ também. Assim, $z, w \in f^{-1}(K)$. Portanto, pela proposição (1.11), $f^{-1}(K)$ é subloop de L .

□

Proposição 1.34. ([dA18], Proposição 3.2.10) *Sejam $f : L \rightarrow L'$ um half-isomorfismo e H subloop de L . Suponha que $f^{-1} : L' \rightarrow L$ também seja half-isomorfismo. Então*

- (a) $f(H)$ é subloop de L' ;
- (b) se H é comutativo, então $f(H)$ é comutativo e $f(H)$ é isomorfo a H ;
- (c) se H é grupo abeliano, então $f(H)$ é grupo abeliano;
- (d) se L é comutativo, então L é isomorfo a L' .

Proposição 1.35. ([dA18]) Seja $f : L \rightarrow L'$ um half-isomorfismo de loops tal que todo elemento de L' tem inverso bilateral. Então todo elemento $x \in L$ tem inverso bilateral $x^{-1} = f^{-1}((f(x))^{-1})$.

Demonstração. Considere $x \in L$, visto que $f(x) \in L'$ temos que $f(x)^{-1} \in L'$. Como

$$\{f(x \cdot y), f(y \cdot x)\} \subseteq \{f(x) * f(y), f(y) * f(x)\}, \quad \forall x, y \in L,$$

temos que

$$\{f(x \cdot f^{-1}((f(x))^{-1})), f(f^{-1}((f(x))^{-1}) \cdot x)\} \subseteq \{f(x) * (f(x))^{-1}, (f(x))^{-1} * f(x)\} = \{1_{L'}\}.$$

Logo, $f(x \cdot f^{-1}((f(x))^{-1})) = f(f^{-1}((f(x))^{-1}) \cdot x) = 1_{L'}$. Como f é bijetora, pelo item (a) da proposição (1.33), $x \cdot f^{-1}((f(x))^{-1}) = 1_L$. Portanto, $x^{-1} = f^{-1}((f(x))^{-1})$. $\square$

Proposição 1.36. ([dA18]) Seja $f : L \rightarrow L'$ um half-isomorfismo de loops e L' potencialmente associativo. Então

- (a) $f(x^n) = (f(x))^n$, para todo $x \in L$ e todo $n \in \mathbb{Z}$;
- (b) L é potencialmente associativo;
- (c) se $x \in L$ é tal que a ordem de $f(x)$, $o(f(x))$, é finita, então $o(f(x)) = o(x)$.

Demonstração. Demonstraremos os itens (a) e (c).

- (a) Seja $x \in L$. Pelo item (a) da proposição (1.33), $f(x^0) = (f(x))^0$
Suponha $f(x^n) = (f(x))^n$ para algum n natural, então

$$f(x^{n+1}) = f(x^n \cdot x) \in \{(f(x))^n * f(x), f(x) * (f(x))^n\} = \{(f(x))^{n+1}\},$$

pois L' é potencialmente associativo. Assim, $f(x^{n+1}) = (f(x))^{n+1}$, logo $f(x^n) = (f(x))^n$, para todo n natural.

Agora, como L' é potencialmente associativo temos que $\langle y \rangle \subseteq L'$ é um grupo para todo $y \in L'$. Logo, todo elemento de L' tem inverso bilateral, então, da proposição

(1.35), temos que todo elemento de L também tem inverso bilateral. Portanto, para n natural, temos

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

Logo, $f((x)^{-n}) = (f(x^n))^{-1} = ((f(x))^n)^{-1} = (f(x))^{-n}$. Isso mostra que $f(x^n) = (f(x))^n$, para todo n inteiro.

(c) Seja $x \in L$ com $o(f(x))$ finita, então, do item (a), temos que

$$f(x^{o(f(x))}) = (f(x))^{o(f(x))} = 1_L.$$

Como f é bijetora $x^{o(f(x))} = 1_L$. Assim, $o(x) \leq o(f(x))$.

Por outro lado, usando novamente o item (a), temos que $(f(x))^{o(x)} = f(x^{o(x)}) = f(1_L) = 1_L$. Logo, $o(f(x)) \leq o(x)$. Portanto, $o(f(x)) = o(x)$.

□

O item (c) da proposição (1.36) será muito útil para os estudos dos loops automórficos diedrais dos capítulos (3) e (4).

Concluimos destacando algumas propriedades da composição de half-isomorfismos de loops.

Proposição 1.37. ([dA18], Proposições 3.2.13 e 3.2.14) *Sejam $(L, *)$, $(L', \cdot)$ e $(L'', \bullet)$ loops e $f : L \rightarrow L'$ e $g : L' \rightarrow L''$ half-isomorfismos, então*

- (a) *a composição $g \circ f : L \rightarrow L''$ é um half-isomorfismo;*
- (b) *se f e g são isomorfismos, então a composição $g \circ f$ é um isomorfismo;*
- (c) *se f e g são anti-isomorfismos, então a composição $g \circ f$ é um isomorfismo;*
- (d) *se f é um isomorfismo e g é um anti-isomorfismo, então a composição $g \circ f$ é um anti-isomorfismo;*
- (e) *se f é um anti-isomorfismo e g é um isomorfismo, então a composição $g \circ f$ é um anti-isomorfismo;*
- (f) *se f é um half-isomorfismo não trivial e g é um half-isomorfismo trivial, então a composição $g \circ f$ é um half-isomorfismo não trivial;*
- (g) *se f é um half-isomorfismo trivial e g é um half-isomorfismo não trivial, então a composição $g \circ f$ é um half-isomorfismo não trivial.*

A partir dessa proposição, podemos obter importantes conclusões sobre o conjuntos dos half-automorfismos de L , denotado por $\text{Half}(L)$, e dos half-automorfismos triviais de L , denotado por $\text{Half}_T(L)$.

Proposição 1.38. *Seja L um loop. Então $\text{Half}_T(L)$ é um grupo e $\text{Aut}(L)$ é um subgrupo normal de $\text{Half}_T(L)$.*

Demonstração. Da proposição (1.37) temos que $\text{Half}(L)$ e $\text{Half}_T(L)$ são fechados para a composição. Além disso, é fácil ver que a função inversa de um automorfismo é também um automorfismo e que a função inversa de anti-automorfismo é também um anti-automorfismo. Dessa forma $\text{Half}_T(L)$ é também fechado para inversos, logo é um grupo.

Temos também da proposição (1.37) que sendo f automorfismo e g anti-automorfismo, $g^{-1} \circ f \circ g$ é um automorfismo e assim $\varphi^{-1} \text{Aut}(L) \varphi \subseteq \text{Aut}(L)$, para todo $\varphi \in \text{Half}_T(L)$. Portanto, $\text{Aut}(L)$ é subgrupo normal de $\text{Half}_T(L)$. $\square$

Proposição 1.39. *Seja L um loop. O conjunto $\text{Half}(L)$ é um grupo se, e somente se para todo half-automorfismo $f : L \rightarrow L$, temos que $f^{-1} : L \rightarrow L$ é também half-automorfismo.*

Demonstração. Primeiro vamos supor que $\text{Half}(L)$ é um grupo. Então é imediato que toda inversa de um half-automorfismo de L pertence também a $\text{Half}(L)$, ou seja, toda inversa de um half-automorfismo de L é também um half-automorfismo.

Para demonstrarmos a recíproca, observe que, pela proposição (1.37), temos que $\text{Half}(L)$ é fechado para a composição. Logo, se toda inversa de um half-automorfismo de L é também um half-automorfismo, então $\text{Half}(L)$ é também fechado para a inversão de seus elementos, portanto é um grupo. $\square$

2

LOOPS AUTOMÓRFICOS

Neste capítulo introduzimos os conceitos e propriedades fundamentais de loops automórficos. Os resultados aqui apresentados são consolidados e alguns deles serão demonstrados, para outros colocaremos apenas as referências.

Definimos anteriormente as translações R_a e L_a . Desde que R_a e L_a são permutações em L , podemos considerá-las como elementos do grupo simétrico $S(L)$, o grupo das permutações de L . O conjunto de todas as L_a e suas inversas L_a^{-1} geram um subgrupo de $S(L)$. Analogamente, o conjunto de todas as R_a e suas inversas R_a^{-1} geram um subgrupo de $S(L)$. Esses grupos são chamados, respectivamente, de grupo das multiplicações à esquerda e à direita de L . Naturalmente, o grupo gerado por todas as multiplicações à esquerda e à direita e suas inversas é chamado grupo das multiplicações de L e denotado por $Mlt(L)$.

Note que consideramos o conjunto "gerado" pelas multiplicações, pois, no caso de loops, o produto de duas translações não é necessariamente uma translação, mas para grupos temos $(x)R_a R_b = (xa)b = x(ab) = (x)R_{ab}$, como consequência da associatividade. Ou seja, o produto de translações em grupos é novamente uma translação. Definimos o *grupo das aplicações internas* de L e denotamos por $Inn(L)$ como sendo o subgrupo de $Mlt(L)$ das funções que fixam o elemento identidade 1.

Bruck provou em [Bru71] que em qualquer loop L

$$Inn(L) = \langle R_{(x,y)}, L_{(x,y)}, T_{(x)} \mid x, y \in L \rangle,$$

onde

$$R_{(x,y)} = R_x R_y R_{xy}^{-1}, \quad L_{(x,y)} = L_x L_y L_{yx}^{-1} \quad \text{e} \quad T_{(x)} = R_x L_x^{-1},$$

para todo $x, y \in L$

Como dissemos na observação (1.27), vamos provar que um subloop é normal se ele é invariante por qualquer aplicação interna.

Proposição 2.1. *Seja H um subloop de L , então H é normal se, e somente se $(H)\varphi = H$ para todo $\varphi \in Inn(L)$.*

Demonstração. Vamos supor H subloop normal de L e mostrar que $(H)R_{(x,y)} = H$. Como H é normal, dado $h_i \in H$, temos

$$h_i R_{(x,y)} = h_i R_x R_y R_{xy}^{-1} = ((h_i x) y) R_{xy}^{-1} = (h_j (xy)) R_{xy}^{-1} = h_j,$$

para algum $h_j \in H$. Logo $(H)R_{(x,y)} = H$.

De maneira análoga podemos mostrar que $(H)L_{(x,y)} = H$ e $(H)T_{(x)} = H$. Como H é invariante para os geradores de $\text{Inn}(L)$, então H é invariante para todo $\varphi \in \text{Inn}(L)$.

Reciprocamente, assuma que $(H)\varphi = H$, então, de $(H)T_{(x)} = H$, segue-se $(H)R_x = (H)L_x$, ou seja, $Hx = xH$. De $(H)R_{(x,y)} = H$, temos $(H)R_x R_y R_{xy}^{-1} = H$, ou seja, $(Hx)y = H(xy)$. De $(H)L_{(x,y)} = H$ temos $(H)L_x L_y L_{yx}^{-1} = H$, ou seja, $y(xH) = (xy)H$. Combinando esses três resultados temos

$$(xH)y = (Hx)y = H(xy) = (xy)H = x(yH) = x(Hy).$$

Portanto, H é subloop normal de L . □

Seguiremos com a principal definição desse capítulo.

Definição 2.2. Um loop L é dito loop automórfico, ou simplesmente um A -Loop, quando toda aplicação interna de L é um automorfismo. Ou seja, quando temos $\text{Inn}(L) \subset \text{Aut}(L)$.

Assim, como $\text{Inn}(L)$ é gerado por $R_{(x,y)}$, $L_{(x,y)}$ e $T_{(x)}$, temos que L é A -loop se, e somente se

$$R_{(x,y)} = R_x R_y R_{xy}^{-1}, \quad L_{(x,y)} = L_x L_y L_{yx}^{-1} \quad \text{e} \quad T_{(x)} = R_x L_x^{-1}$$

são automorfismos de L para todo $x, y \in L$.

Exemplo 2.3. Seja $L = \{1, 2, 3, 4, 5, 6\}$ e $*$ a operação dada pela seguinte tabela:

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	1	3	2
5	5	6	4	2	1	3
6	6	4	5	3	2	1

O loop $(L, *)$ é o A -loop não associativo de menor ordem possível, e este é único a menos de isomorfismo.

Definição 2.4. *Seja L um loop. Diremos que L tem a propriedade inversa antiautomórfica quando ele tem inverso bilateral e satisfaz a equação*

$$(xy)^{-1} = y^{-1}x^{-1} \text{ para todo } x, y \in L.$$

Nesse caso diremos que L é um AAIP-loop.

Lema 2.5. ([KKPV16], Proposição 2.5) *Todo loop automórfico é AAIP-loop.*

As proposições a seguir resumem as relações entre A -loops e seus subloops além de estabelecer propriedades dos A -loops.

Proposição 2.6. ([BP56]) *Seja L um A -loop, então*

- (a) *se H é subloop de L , temos que H é A -loop;*
- (b) *se H é subloop normal de L , então L/H é A -loop;*
- (c) *L é potencialmente associativo;*
- (d) *L tem a propriedade flexível, ou seja, $x(yx) = (xy)x$, para todo $x, y \in L$;*
- (e) *se H é subloop característico de L , então H é subloop normal de L ;*
- (f) $N_\mu(L) \supseteq N_\lambda(L)$ e $N_\mu(L) \supseteq N_\rho(L)$.

Demonstração. Vamos demonstrar os itens (a) e (e).

- (a) *Seja H um subloop de L . Como os geradores de $\text{Inn}(L)$, $R_{(x,y)}$, $L_{(x,y)}$ e $T_{(x)}$, são automorfismos internos de L , restritos a H , para $x, y \in H$, são os geradores dos automorfismos internos de H , $\text{Inn}(H)$. Portanto, $\text{Inn}(H)$ consiste de automorfismos de H . Logo H é A -loop.*
- (e) *Seja H subloop característico de L , então $(H)\varphi = H$, para todo $\varphi \in \text{Inn}(L) \subseteq \text{Aut}(L)$, então, pela proposição (2.1), H é subloop normal de L .*

□

Corolário 2.7. *Seja L um A -loop, então os núcleos $N_\lambda(L)$, $N_\rho(L)$, $N_\mu(L)$ e $N(L)$ são subloops normais de L .*

Demonstração. Vamos demonstrar primeiro a inclusão $N_\lambda(L) \subseteq \varphi(N_\lambda(L))$, para todo $\varphi \in \text{Aut}(L)$. Considere $a \in N_\lambda(L)$, ou seja, $a(xy) = (ax)y$, para todo $x, y \in L$. Como φ é bijetora, existe $b \in L$ tal que $a = \varphi(b)$. Precisamos mostrar que $b \in N_\lambda(L)$. Sabemos que $\varphi^{-1}(a) = b$ e que $\varphi^{-1} \in \text{Aut}(L)$. Temos então, $\forall x, y \in L$,

$$\varphi^{-1}(a(xy)) = \varphi^{-1}((ax)y),$$

$$\varphi^{-1}(a)\varphi^{-1}(xy) = \varphi^{-1}(ax)\varphi^{-1}(y) \quad \text{e}$$

$$\varphi^{-1}(a)(\varphi^{-1}(x)\varphi^{-1}(y)) = (\varphi^{-1}(a)\varphi^{-1}(x))\varphi^{-1}(y).$$

Logo, $b = \varphi^{-1}(a) \in N_\lambda(L)$. Portanto, $a \in \varphi(N_\lambda(L))$ e assim $N_\lambda(L) \subseteq \varphi(N_\lambda(L))$.

Por outro lado, considerando novamente $a \in N_\lambda(L)$, temos, $\forall x, y \in L$,

$$\varphi(a(xy)) = \varphi((ax)y) \text{ e assim } \varphi(a)\varphi(xy) = \varphi(ax)\varphi(y).$$

Dessa forma,

$$\varphi(a)(\varphi(x)\varphi(y)) = (\varphi(a)\varphi(x))\varphi(y).$$

Portanto, $\varphi(a) \in N_\lambda(L)$ e temos a outra inclusão, $\varphi(N_\lambda(L)) \subseteq N_\lambda(L)$.

Demonstramos assim que $N_\lambda(L) = \varphi(N_\lambda(L))$, ou seja, $N_\lambda(L)$ é subloop característico de L . Pelo item (e) da proposição (2.6), $N_\lambda(L)$ é subloop normal de L .

As demonstrações de que $N_\rho(L)$ e $N_\mu(L)$ também são subloops normais de L são análogas.

Por fim, não é difícil mostrar, que a interseção de subloops normais também é um subloop normal. Logo, $N(L)$ também é um subloop normal de L . $\square$

Proposição 2.8. ([KKPV16]) *Seja L um A -loop, então*

- (a) $(ax)b = a(xb)$, para todo $a, b \in N_\mu(L)$ e para todo $x \in L$;
- (b) $N_\lambda(L) = N_\rho(L) = N(L)$;
- (c) $\text{Inn}(L) = \langle L_{(x,y)}, T_x \mid x, y \in L \rangle$;
- (d) (Teorema de Lagrange) se a ordem de L é ímpar e H é subloop de L , então $|H| \mid |L|$;
- (e) (Teorema de Cauchy) se a ordem de L é ímpar e p é um primo que divide a ordem de L , então existe $x \in L$ tal que $o(x) = p$.

Demonstração. Vamos demonstrar o item (b).

(b) Pelo lema (2.5), L é *AAIP*-loop. Logo, a condição $ax \cdot y = a \cdot xy$ é equivalente a

$$y^{-1} \cdot x^{-1}a^{-1} = y^{-1}x^{-1} \cdot a^{-1},$$

então $N_\lambda(L) = N_\rho(L)$.

A outra igualdade é consequência direta do item (f) da proposição anterior (2.6), pois se $N_\mu(L) \supseteq N_\lambda(L)$ e $N_\mu(L) \supseteq N_\rho(L)$ com $N_\lambda(L) = N_\rho(L)$, então

$$N_\lambda(L) \cap N_\rho(L) \cap N_\mu(L) = N(L) = N_\lambda(L) = N_\rho(L).$$

□

3

HALF-ISOMORFISMOS ENTRE OS A-LOOPS DIEDRAIS $Dih(m, C_p, \alpha)$: CASOS $m = 4$ E $m = 6$

Iniciamos com a definição dos loops diedrais $Dih(m, G, \alpha)$.

Definição 3.1. *Sejam $m \in \mathbb{Z}$, $m > 1$, G um grupo abeliano e $\alpha : G \rightarrow G$ um automorfismo. Considere o conjunto $\mathbb{Z}_m \times G$ com a operação $*$ definida por*

$$(i, u) * (j, v) = (i + j, (u^{(-1)^j} v) \alpha^{ij})$$

onde $u, v \in G$ e $i, j \in \mathbb{Z}_m$. Vamos denotar esse conjunto munido da operação $*$ por $Dih(m, G, \alpha)$.

Vojtěchovský, et alii, mostraram que $Dih(m, G, \alpha)$ é um loop automórfico ([KKPV16]).

O Teorema abaixo amplia a discussão sobre o loop $Dih(m, G, \alpha)$ e fornece condições para que este seja um loop automórfico.

Teorema 3.2. ([Abo14], Teorema 3.13) *Sejam $m > 1$ um número inteiro, G um grupo abeliano e α um automorfismo de G . Seja $Q = Dih(m, G, \alpha)$ definido em (3.1).*

- (i) *Se $m = 2$, então Q é um loop automórfico.*
- (ii) *Se $m > 2$ é par, então Q é um loop automórfico se, e somente se, $\alpha^2 = I$, onde I representa o automorfismo identidade.*
- (iii) *Se $m > 2$ é ímpar, então Q é um loop automórfico se, e somente se, $\alpha = I$ e $2(G) = 0$, neste caso Q é um grupo.*

Além disso, Mouna Aboras e Petr Vojtěchovský, em ([AbVo16]), mostraram que o loop diedral $Dih(m, G, \alpha)$ é um grupo se, e somente se, $\alpha = I$.

Tendo em vista a definição (3.1) e o Teorema (3.2), podemos estabelecer formalmente a definição dos loops que serão os principais objetos do nosso estudo.

Definição 3.3. *Sejam C_p o grupo cíclico de ordem p , tal que $p \geq 2$ é um número primo, m um inteiro par positivo e $\alpha : C_p \rightarrow C_p$ um automorfismo. Considere o conjunto $\mathbb{Z}_m \times C_p$ com a*

operação $*$ definida por

$$(i, u) * (j, v) = (i + j, (u^{(-1)^j} v) \alpha^{ij}),$$

onde $u, v \in C_p$ e $i, j \in \mathbb{Z}_m$. Esse conjunto munido da operação $*$ é um loop automórfico diedral e vamos denotá-lo por $Dih(m, C_p, \alpha)$.

As proposições a seguir são fatos conhecidos, mas são de importância fundamental no desenvolvimento deste trabalho. Assim, decidimos incluir as demonstrações.

Proposição 3.4. *Seja G um grupo cíclico de ordem par, então G tem apenas um elemento de ordem dois.*

Demonstração. Seja $G = \langle a \rangle = \{e, a, a^2, \dots, a^{m-1}\}$ um grupo cíclico de ordem par $m = 2k$, onde k é um inteiro positivo. Sabemos que $a^m = e$. Sabemos também que $g = a^k \neq e$, pois $0 < k < m$. Porém $g^2 = a^{2k} = a^m = e$. Logo, g tem ordem 2.

Suponha agora $h \in G$, $h \neq a^k$ e $h \neq e$, então $h = a^j \neq e$, $j \neq k$ onde j é um inteiro positivo. Temos portanto dois casos a considerar.

Caso 1: $0 < j < k$. Logo, $0 < 2j < 2k = m$ e assim $h^2 = a^{2j} \neq e$. Logo, $h = a^j$ não tem ordem 2.

Caso 2: $k < j < m$. Dessa forma, $m = 2k < 2j < 2m$, assim $0 < 2j - m < m$ e $h^2 = a^{2j} = a^m a^{2j-m} = a^{2j-m} \neq e$. Logo, $h = a^j$ não tem ordem 2.

Portanto, $g = a^k$ é o único elemento de ordem 2. □

Proposição 3.5. *Seja C_p um grupo cíclico de ordem p , onde p é um número primo. Então o grupo de automorfismos de C_p , $Aut(C_p)$, é isomorfo ao grupo cíclico C_{p-1} de ordem $p - 1$.*

Demonstração. Seja $G = C_p = \langle x \rangle$. Sabemos que $x^p = e$ e que todo elemento de G , diferente de e , é gerador de G .

Se $\varphi \in Aut(G)$, então φ deve levar x em outro gerador de G . Ou seja $\varphi(x) = x^k$, com $1 \leq k \leq p - 1$. E ainda note que $\varphi(x^n) = \varphi^n(x)$.

Podemos então enumerar os elementos de $Aut(G)$ por φ_i , onde $\varphi_i(x) = x^i$, com $1 \leq i \leq p - 1$. Logo, $|Aut(G)| = p - 1$.

Mostremos que $Aut(G)$ é abeliano. Sejam $\varphi_i, \varphi_j \in Aut(G)$. Temos $\varphi_i(x) = x^i$ e $\varphi_j(x) = x^j$. Logo, $\varphi_i \circ \varphi_j(x) = \varphi_i(x^j) = x^{ji} = x^{ij} = \varphi_j \circ \varphi_i(x)$.

Falta mostrar que $Aut(G)$ é cíclico. Para isso, mostraremos que $Aut(G)$ é isomorfo ao conjunto $\mathbb{Z}_p^*$ com a multiplicação. Como $\mathbb{Z}_p$ é corpo, $(\mathbb{Z}_p^*, \cdot)$ é cíclico e assim $Aut(G)$ é cíclico.

Considere $\varphi_i, \varphi_j \in \text{Aut}(G)$, $\varphi_i(x) = x^i$ e $\varphi_j(x) = x^j$. Temos $\varphi_i \circ \varphi_j(x) = x^{ij} = \varphi_{ij}$. Podemos definir $\tau : \text{Aut}(G) \rightarrow \mathbb{Z}_p^*$, dada por $\tau(\varphi_m) = \overline{m}$. Dessa forma

$$\tau(\varphi_m \circ \varphi_k) = \tau(\varphi_{mk}) = \overline{mk} = \overline{m}\overline{k} = \tau(\varphi_m)\tau(\varphi_k).$$

Além disso, τ está bem definida, pois se $\overline{m} \neq \overline{k}$ em $\mathbb{Z}_p^*$, com $1 \leq m, k \leq p-1$, então $\varphi_m \neq \varphi_k$. A sobrejetividade decorre diretamente da definição e se $\overline{m} = \overline{k}$ então $\varphi_m = \varphi_k$, logo τ é injetora, portanto τ é bijetora.

Concluimos que ϕ é um isomorfismo. $\square$

Segue imediatamente do Teorema (3.2) que, para o loop diedral $Dih(m, C_p, \alpha)$ ser automórfico, o automorfismo α , na definição (3.3), deve ser tal que $\alpha^2 = I$.

Em vista das proposições (3.4) e (3.5) temos apenas dois automorfismos de C_p a ser considerados daqui para frente. São eles $\alpha = I$ e $\alpha = J$, onde J é a função inversão, dada por $J(x) = x^{-1}$.

Nas próximas seções serão abordados os loops diedrais tomando $m = 4$ e $m = 6$. A análise desses casos fornecerá subsídios para a obtenção dos resultados no caso geral, quando m é um inteiro par positivo.

3.1 OS A-LOOPS DIEDRAIS $Dih(4, C_p, \alpha)$ E $Dih(6, C_p, \alpha)$

Vamos descrever aqui os loops automórficos diedrais $Dih(4, C_p, \alpha)$ e $Dih(6, C_p, \alpha)$.

Agora consideraremos as notações $C_p = \{e, u, u^2, \dots, u^{p-1}\}$, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ e $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ e teremos os conjuntos

$$\begin{aligned} \mathbb{Z}_4 \times C_p = \{ & (0, e), (0, u), (0, u^2), \dots, (0, u^{p-1}), (1, e), (1, u), (1, u^2), \dots, (1, u^{p-1}), \\ & (2, e), (2, u), (2, u^2), \dots, (2, u^{p-1}), (3, e), (3, u), (3, u^2), \dots, (3, u^{p-1}) \}. \end{aligned}$$

e

$$\begin{aligned} \mathbb{Z}_6 \times C_p = \{ & (0, e), (0, u), (0, u^2), \dots, (0, u^{p-1}), (1, e), (1, u), (1, u^2), \dots, (1, u^{p-1}), \\ & (2, e), (2, u), (2, u^2), \dots, (2, u^{p-1}), (3, e), (3, u), (3, u^2), \dots, (3, u^{p-1}), \\ & (4, e), (4, u), (4, u^2), \dots, (4, u^{p-1}), (5, e), (5, u), (5, u^2), \dots, (5, u^{p-1}) \}. \end{aligned}$$

No que segue

L_I representará o loop $Dih(m, C_p, I)$

e

L_J representará o loop $Dih(m, C_p, J)$,

onde tomaremos convenientemente $m = 4$ ou $m = 6$ e quando não especificarmos estaremos considerando a discussão para ambos.

Será natural no decorrer do texto escrevermos $(i, u)(j, v)$ no lugar de $(i, u) * (j, v)$.

É imediato notar que em ambos, L_I e L_J , $o((0, e)) = 1$, não importando o valor de m . Além disso, $o(x) = p$ para todo $x \in C_p$, $x \neq e$. Como consequência da definição segue que o conjunto $(0, C_p) = \{(0, x) \mid x \in C_p\}$ é isomorfo a C_p .

Continuaremos descrevendo as ordens dos elementos de L_I e L_J nas próximas proposições destacando as diferenças e semelhanças para os casos $m = 4$ e $m = 6$.

Proposição 3.6. *Seja $(2, C_p) = \{(2, x) \mid x \in C_p\}$, subconjunto de $\mathbb{Z}_4 \times C_p$. Então $o((2, e)) = 2$ e os elementos $(2, x) \in (2, C_p)$, tais que $x \neq e$, têm ordem $2p$ em ambos, L_I e L_J .*

Demonstração. Primeiro veja que $(2, e)(2, e) = (0, e)$, ou seja, $o((2, e)) = 2$. Agora considere $(2, x) \in (2, C_p)$, $x \neq e$. Veja que, tanto em L_I como em L_J ,

$$(2, x)(2, x) = (0, x^2), \quad (0, x^2)(2, x) = (2, x^3),$$

$$(2, x^3)(2, x) = (0, x^4), \quad \text{e} \quad (0, x^4)(2, x) = (2, x^5).$$

Como p é ímpar, temos $(2, x)^p = (0, x^{(p-1)})(2, x) = (2, x^p) = (2, e)$. Dessa forma, como $x^n \neq e$, para todo $n \in \{1, 2, \dots, p-1\}$ e $o((2, e)) = 2$, temos que $(2, x)^p = (2, e)$ implica que $o((2, x)) = 2p$. $\square$

Proposição 3.7. *Seja $(3, C_p) = \{(3, x) \mid x \in C_p\}$, subconjunto de $\mathbb{Z}_6 \times C_p$. Então todos os elementos de $(3, C_p)$ têm ordem 2 em ambos, L_I e L_J .*

Demonstração. De fato, dado $(3, x) \in (3, C_p)$, temos $(3, x)(3, x) = (0, (x^{-1}x)\alpha^{ij}) = (0, e)$, para ambos, $\alpha = I$ ou $\alpha = J$. Ou seja, $o((3, x)) = 2$, para todo $(3, x) \in (3, C_p)$. $\square$

Proposição 3.8. *Sejam*

$$(1, C_p) = \{(1, x) \mid x \in C_p\} \quad \text{e} \quad (3, C_p) = \{(3, x) \mid x \in C_p\},$$

subconjuntos de $\mathbb{Z}_4 \times C_p$. Então os elementos de $(1, C_p)$ e $(3, C_p)$ têm ordem 4 em ambos L_I e L_J .

Demonstração. Veja que em ambos os loops, L_I e L_J ,

$$(1, x)(1, x) = (2, x^{-1}x) = (2, e) \text{ e } (3, x)(3, x) = (2, e), \text{ para todo } x \in C_p.$$

Como $o((2, e)) = 2$, $(2, e)(1, x) = (3, x) \neq (0, e)$ e $(2, e)(3, x) = (1, x) \neq (0, e)$, temos $o((1, x)) = o((3, x)) = 4$. $\square$

Proposição 3.9. *Sejam*

$$(1, C_p) = \{(1, x) \mid x \in C_p\} \text{ e } (5, C_p) = \{(5, x) \mid x \in C_p\},$$

subconjuntos de $\mathbb{Z}_6 \times C_p$. Então os elementos de $(1, C_p)$ e $(5, C_p)$ têm ordem 6 em ambos L_I e L_J .

Demonstração. Veja que em ambos os loops, L_I e L_J ,

$$(1, x)(1, x) = (2, x^{-1}x) = (2, e), \text{ logo } (1, x)^3 = (2, e)(1, x) = (3, x) \text{ para todo } x \in C_p$$

e

$$(5, x)(5, x) = (4, x^{-1}x) = (4, e), \text{ logo } (5, x)^3 = (4, e)(5, x) = (3, x) \text{ para todo } x \in C_p.$$

Como, pela proposição (3.7), $o((3, x)) = 2$, temos $o((1, x)) = 6$ e $o((5, x)) = 6$, para todo $x \in C_p$. $\square$

Dessa forma, para $m = 4$ e $m = 6$, temos em ambos os loops L_I e L_J um elemento de ordem 1, o par $(0, e)$, e temos $p - 1$ elementos de ordem p , que são os pares

$$(0, u), (0, u^2), \dots, (0, u^{p-1}).$$

No entanto para $m = 4$ temos um elemento de ordem 2, que é o par $(2, e)$, $p - 1$ elementos de ordem $2p$, que são os pares

$$(2, u), (2, u^2), \dots, (2, u^{p-1}),$$

e $2p$ elementos de ordem 4, que são os pares

$$(1, e), (1, u), \dots, (1, u^{p-1}) \text{ e } (3, e), (3, u), \dots, (3, u^{p-1}).$$

Diferentemente para $m = 6$, temos exatamente p elementos de ordem 2, que são os pares

$$(3, e), (3, u), (3, u^2), \dots, (3, u^{p-1}),$$

e, de forma semelhante ao caso $m = 4$, temos $2p$ elementos de ordem 6, que são os pares

$$(1, e), (1, u), \dots, (1, u^{p-1}) \text{ e } (5, e), (5, u), \dots, (5, u^{p-1}).$$

Agora, considerando que os half-isomorfismos $f : L_I \rightarrow L_J$ preservam as ordens dos elementos (pela proposição 1.36), podemos começar a investigação desses half-isomorfismos, que é o objetivo principal da próxima seção.

3.2 HALF-ISOMORFISMOS: PARA OS CASOS $m = 4$ E $m = 6$

Nesta seção vamos considerar as seguintes notações:

L_α representará o loop $Dih(m, C_p, \alpha)$ e

L_β representará o loop $Dih(m, C_p, \beta)$,

para $m = 4$ ou $m = 6$, onde $\alpha = I$ ou $\alpha = J$ e, igualmente, $\beta = I$ ou $\beta = J$.

Na primeira seção desse capítulo observamos que, para $m = 4$ e $m = 6$, em ambos os loops, L_I e L_J , o elemento de ordem 1 e os elementos de ordem p aparecem em

$$(0, C_p) = \{(0, x) \mid x \in C_p\}.$$

Porém, no caso em que $m = 6$, os conjuntos $(2, C_p)$ e $(4, C_p)$ possuem elementos de ordem 3. Assim, no caso em que $p = 3$ os elementos de ordem p não estão somente em $(0, C_p)$, como acontece para $m = 4$. No entanto, vale ressaltar que se $f : L_\alpha \rightarrow L_\beta$, com $\alpha \neq \beta$, é um half-isomorfismo, então temos apenas duas possibilidades

$$f((1, x)) = (1, y) \quad \text{ou} \quad f((1, x)) = (5, y), \quad \text{para } x, y \in C_p.$$

Sendo assim,

$$f((2, e)) = f((1, x)(1, x)) = f((1, x))f((1, x)) = (1, y)(1, y) = (2, e), \quad \text{logo } f((4, e)) = (4, e),$$

ou

$$f((2, e)) = f((1, x)(1, x)) = f((1, x))f((1, x)) = (5, y)(5, y) = (4, e), \quad \text{logo } f((4, e)) = (2, e).$$

Mais ainda,

$$f((3, x)) = f((1, x)(2, e)) = \begin{cases} f((1, x))f((2, e)) = (1, y)(2, e), \\ f((2, e))f((1, x)) = (2, e)(1, y). \end{cases} = (3, y),$$

$$f((4, e)) = f((1, x)(3, x)) = \begin{cases} f((1, x))f((3, x)) = (1, y)(3, y), \\ f((3, x))f((1, x)) = (3, y)(1, y). \end{cases} = (4, e)$$

e

$$f((5, x)) = f((1, x)(4, e)) = \begin{cases} f((1, x))f((4, e)) = (1, y)(4, e), \\ f((4, e))f((1, x)) = (4, e)(1, y). \end{cases} = (5, y),$$

Além disso, fixamos $f((1, e)) = (1, y)$ e temos

$$f((2, x)) = f((1, e)(1, x)) = \begin{cases} f((1, e))f((1, x)), \\ f((1, x))f((1, e)), \end{cases} = \begin{cases} (1, y)(1, b), \\ (1, b)(1, y), \end{cases} = \begin{cases} (2, y^{-1}b), \\ (2, b^{-1}y), \end{cases}$$

onde consideramos $f(1, x) = (1, b)$.

Por fim, fixamos $f((1, e)) = (5, y)$ e temos

$$f((2, x)) = f((1, e)(1, x)) = \begin{cases} f((1, e))f((1, x)), \\ f((1, x))f((1, e)), \end{cases} = \begin{cases} (5, y)(5, c), \\ (5, c)(5, y), \end{cases} = \begin{cases} (4, y^{-1}c), \\ (4, c^{-1}y), \end{cases}$$

onde consideramos $f(1, x) = (1, c)$.

No caso em que $m = 4$ o elemento $(2, e)$ tem ordem 2 e os outros elementos do conjunto

$$(2, C_p) = \{(2, x) \mid x \in C_p\}$$

têm ordem $2p$. No entanto, no caso em que $m = 6$, temos que todos os elementos do conjunto

$$(3, C_p) = \{(3, x) \mid x \in C_p\}$$

têm ordem 2 e esses são os únicos com essa ordem.

A partir da discussão acima, juntamente com as proposições (1.34) e (1.36), podemos enunciar os seguintes lemas.

Lema 3.10. *Dado um half-isomorfismo $f : L_\alpha \rightarrow L_\beta$, temos que $f((i, C_p)) = (i, C_p)$ para $i = 0 \in \mathbb{Z}_4$ e para $m = i \in \mathbb{Z}_4$.*

Lema 3.11. *Dado um half-isomorfismo $f : L_\alpha \rightarrow L_\beta$, temos que $f((i, C_p)) = (i, C_p)$ para $i = 0 \in \mathbb{Z}_6$ e para $i = 3 \in \mathbb{Z}_6$.*

Podemos apresentar também a definição a seguir que é válida para ambos os casos, $m = 4$ e $m = 6$.

Definição 3.12. *Seja $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo, então definimos a seguinte função bijetora: $f' : C_p \rightarrow C_p$, dada por $x \mapsto f'(x)$, tal que $f((0, x)) = (0, f'(x))$.*

Observe que f' está bem definida, pois se $f'(x) = y$ e $f'(x) = z$, então $f(0, x) = (0, y) = (0, z)$, logo $y = z$. O fato de f' ser bijetora é consequência do fato de que f também é bijetora.

Note também que $(0, f'(xy)) = f(0, xy) = f((0, x) * (0, y)) = f(0, x)f(0, y) = (0, f'(x)) * (0, f'(y)) = (0, f'(x)f'(y))$, logo $f'(xy) = f'(x)f'(y)$, ou seja, f' é um automorfismo de C_p . Consequentemente temos $p - 1$ possibilidades para f' .

Considere agora o seguinte lema, válido para $m = 4$.

Lema 3.13. *Sejam $m = 4$ e $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo. Então $f((2, x)) = (2, f'(x))$, para todo $x \in C_p$.*

Demonstração. Veja que se $i \neq 0$ e $i + i = 0$ em $\mathbb{Z}_4$, então $i = 2$ e se $x \neq e$, então $x^n \neq e$, para todo $x \in C_p$ e $0 < n < p$. Dessa forma $(2, e)$ é o único elemento de ordem dois em ambos, L_I e L_J . Consequentemente $f((2, e)) = (2, e) = (2, f'(e))$, pois $f'(e) = e$, visto que f' é automorfismo de C_p . Considere $(2, x) \in (2, C_p)$ com $x \neq e$, então

$$f((2, x)(2, x)) = f((0, x^2)) = (0, f'(x^2)) = (0, (f'(x))^2).$$

Por outro lado, façamos $f((2, x)) = (2, a)$ e teremos

$$f((2, x)(2, x)) = f((2, x))f((2, x)) = (2, a)(2, a) = (0, a^2).$$

Dessa forma, $(0, (f'(x))^2) = (0, a^2)$. Logo, $(f'(x))^2 = a^2 \in C_p$. Portanto, $f'(x) = a$ e assim $f((2, x)) = (2, a) = (2, f'(x))$. $\square$

De maneira análoga ao que foi feito para $m = 4$ vamos estabelecer os resultados para $m = 6$.

Lema 3.14. *Sejam $m = 6$ e $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo. Então $f((2, x)) = (2, f'(x))$ e $f((4, x)) = (4, f'(x))$ ou $f((2, x)) = (4, f'(x))$ e $f((4, x)) = (2, f'(x))$, para todo $x \in C_p$.*

Demonstração. Observemos primeiro que $(2, e)(4, e) = (4, e)(2, e) = (0, e)$. Assim,

$$f((0, e)) = f((2, e)(4, e)) = \begin{cases} f((2, e))f((4, e)) = (0, e), \\ f((4, e))f((2, e)) = (0, e). \end{cases}$$

Dessa forma $f((2, e)) = (2, e)$ e $f((4, e)) = (4, e)$ ou $f((2, e)) = (4, e)$ e $f((4, e)) = (2, e)$.

Portanto, tomando $f((2, e)) = (2, e)$ e $f((4, e)) = (4, e)$, temos

$$f((2, x)) = f((2, e)(0, x)) = \begin{cases} f((2, e))f((0, x)) = (2, e)(0, f'(x)) = (2, f'(x)), \\ f((0, x))f((2, e)) = (0, f'(x))(2, e) = (2, f'(x)), \end{cases}$$

e

$$f((4, x)) = f((4, e)(0, x)) = \begin{cases} f((4, e))f((0, x)) = (4, e)(0, f'(x)) = (4, f'(x)), \\ f((0, x))f((4, e)) = (0, f'(x))(4, e) = (4, f'(x)). \end{cases}$$

Agora tomando $f((2, e)) = (4, e)$ e $f((4, e)) = (2, e)$, temos

$$f((2, x)) = f((2, e)(0, x)) = \begin{cases} f((2, e))f((0, x)) = (4, e)(0, f'(x)) = (4, f'(x)), \\ f((0, x))f((2, e)) = (0, f'(x))(4, e) = (4, f'(x)), \end{cases}$$

e

$$f((4, x)) = f((4, e)(0, x)) = \begin{cases} f((4, e))f((0, x)) = (2, e)(0, f'(x)) = (2, f'(x)), \\ f((0, x))f((4, e)) = (0, f'(x))(2, e) = (2, f'(x)). \end{cases}$$

□

Para concluirmos as caracterizações dos half-isomorfismos $f : L_\alpha \rightarrow L_\beta$ precisamos do seguinte lema, que demonstraremos inicialmente para o caso $m = 4$.

No que segue a é um elemento de C_p arbitrário porém fixado.

Lema 3.15. *Sejam $m = 4$, $g_a^1 : L_\alpha \rightarrow L_\beta$ e $g_a^2 : L_\alpha \rightarrow L_\beta$ dadas por*

$$g_a^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (1, af'(x^s)), & \text{se } i = 1, \\ (3, af'(x^t)), & \text{se } i = 3, \end{cases} \quad g_a^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (3, af'(x^t)), & \text{se } i = 1, \\ (1, af'(x^s)), & \text{se } i = 3, \end{cases}$$

onde s e t são inteiros distintos, $0 \leq s \leq p-1$ e $0 \leq t \leq p-1$.

Então, para cada $a \in C_p$, g_a^1 e g_a^2 não são half-isomorfismos de L_α em L_β .

Demonstração. (i) Temos

$$g_a^1((1, x)(3, x)) = g_a^1((0, (x^{-1}x)\alpha^3)) = g_a^1((0, e)) = (0, e), \text{ para todo } x \in C_p.$$

Porém,

$$\begin{aligned} g_a^1((1, x))g_a^1((3, x)) &= (1, af'(x^s))(3, af'(x^t)) = (0, (a^{-1}f'(x^{-s})af'(x^t))\beta^3) = \\ &= \begin{cases} (0, f'(x^{-s})f'(x^t)), & \\ (0, f'(x^{-t})f'(x^s)). & \end{cases} = \begin{cases} (0, f'(x^{s-t})), & \\ (0, f'(x^{t-s})). & \end{cases} \neq (0, e), \text{ se } x \neq e \text{ e } s \neq t. \end{aligned}$$

Além disso,

$$\begin{aligned} g_a^1((3, x))g_a^1((1, x)) &= (3, af'(x^t))(1, af'(x^s)) = (0, (a^{-1}f'(x^{-t})af'(x^s))\beta^3) = \\ &= \begin{cases} (0, f'(x^{-s})f'(x^t)), & \\ (0, f'(x^{-t})f'(x^s)). & \end{cases} = \begin{cases} (0, f'(x^{s-t})), & \\ (0, f'(x^{t-s})). & \end{cases} \neq (0, e), \text{ se } x \neq e \text{ e } s \neq t. \end{aligned}$$

Logo, $g_a^1 : L_\alpha \rightarrow L_\beta$ não é half-isomorfismo.

(ii) Temos

$$g_a^2((1, x)(3, x)) = g_a^2((0, (x^{-1}x)\alpha^3)) = g_a^2((0, e)) = (0, e), \text{ para todo } x \in C_p.$$

Porém,

$$\begin{aligned} g_a^2((1, x))g_a^2((3, x)) &= (3, af'(x^t))(1, af'(x^s)) = (0, (a^{-1}f'(x^{-t})af'(x^s))\beta^3) = \\ &= \begin{cases} (0, f'(x^{-t})f'(x^s)), & \\ (0, f'(x^{-s})f'(x^t)). & \end{cases} = \begin{cases} (0, f'(x^{t-s})), & \\ (0, f'(x^{s-t})). & \end{cases} \neq (0, e), \text{ se } x \neq e \text{ e } t \neq s. \end{aligned}$$

Além disso,

$$\begin{aligned} g_a^2((3, x))g_a^2((1, x)) &= (1, af'(x^s))(3, af'(x^t)) = (0, (a^{-1}f'(x^{-t})af'(x^s))\beta^3) = \\ &= \begin{cases} (0, f'(x^{-t})f'(x^s)), & \\ (0, f'(x^{-s})f'(x^t)). & \end{cases} = \begin{cases} (0, f'(x^{t-s})), & \\ (0, f'(x^{s-t})). & \end{cases} \neq (0, e), \text{ se } x \neq e \text{ e } t \neq s. \end{aligned}$$

Logo, $g_a^2 : L_I \rightarrow L_J$ não é half-isomorfismo.

□

Para o caso $m = 6$ temos o seguinte lema.

Lema 3.16. *Sejam $m = 6$, $g_a^1 : L_\alpha \rightarrow L_\beta$ e $g_a^2 : L_\alpha \rightarrow L_\beta$ dadas por*

$$g_a^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (4, f'(x)), & \text{se } i = 4, \\ (1, af'(x^r)), & \text{se } i = 1, \\ (3, af'(x^s)), & \text{se } i = 3, \\ (5, af'(x^t)), & \text{se } i = 5, \end{cases} \quad g_a^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (4, f'(x)), & \text{se } i = 2, \\ (2, f'(x)), & \text{se } i = 4, \\ (5, af'(x^t)), & \text{se } i = 1, \\ (3, af'(x^s)), & \text{se } i = 3, \\ (1, af'(x^r)), & \text{se } i = 5, \end{cases}$$

com $a \in C_p$ e r, s e t inteiros, dois a dois distintos, e $0 \leq r, s, t \leq p - 1$.

Então, para cada $a \in C_p$, g_a^1 e g_a^2 não são half-isomorfismos de L_α em L_β .

Demonstração. (i) Temos

$$g_a^1((1, x)(5, x)) = g_a^1((0, (x^{-1}x)\alpha^5)) = g_a^1((0, e)) = (0, e), \text{ para todo } x \in C_p.$$

Porém,

$$\begin{aligned} g_a^1((1, x))g_a^1((5, x)) &= (1, af'(x^r))(5, af'(x^t)) = (0, (a^{-1}f'(x^{-r})af'(x^t))\beta^5) = \\ &= \begin{cases} (0, f'(x^{-r})f'(x^t)), \\ (0, f'(x^{-t})f'(x^r)). \end{cases} = \begin{cases} (0, f'(x^{r-t})), \\ (0, f'(x^{t-r})). \end{cases} \neq (0, e), \text{ se } x \neq e \text{ e } r \neq t. \end{aligned}$$

Além disso,

$$\begin{aligned} g_a^1((5, x))g_a^1((1, x)) &= (5, af'(x^t))(1, af'(x^r)) = (0, (a^{-1}f'(x^{-t})af'(x^r))\beta^5) = \\ &= \begin{cases} (0, f'(x^{-r})f'(x^t)), \\ (0, f'(x^{-t})f'(x^r)). \end{cases} = \begin{cases} (0, f'(x^{r-t})), \\ (0, f'(x^{t-r})). \end{cases} \neq (0, e), \text{ se } x \neq e \text{ e } r \neq t. \end{aligned}$$

Logo, $g_a^1 : L_\alpha \rightarrow L_\beta$ não é half-isomorfismo.

(ii) Temos

$$g_a^2((1, x)(5, x)) = g_a^2((0, (x^{-1}x)\alpha^5)) = g_a^2((0, e)) = (0, e), \text{ para todo } x \in C_p.$$

Porém,

$$\begin{aligned} g_a^2((1, x))g_a^2((5, x)) &= (5, af'(x^t))(1, af'(x^r)) = (0, (a^{-1}f'(x^{-t})af'(x^r))\beta^5) = \\ &= \begin{cases} (0, f'(x^{-t})f'(x^r)), \\ (0, f'(x^{-r})f'(x^t)). \end{cases} = \begin{cases} (0, f'(x^{t-r})), \\ (0, f'(x^{r-t})). \end{cases} \neq (0, e), \text{ se } x \neq e \text{ e } t \neq r. \end{aligned}$$

Além disso,

$$\begin{aligned} g_a^2((5, x))g_a^2((1, x)) &= (1, af'(x^r))(5, af'(x^t)) = (0, (a^{-1}f'(x^{-r})af'(x^t))\beta^5) = \\ &= \begin{cases} (0, f'(x^{-t})f'(x^r)), \\ (0, f'(x^{-r})f'(x^t)). \end{cases} = \begin{cases} (0, f'(x^{t-r})), \\ (0, f'(x^{r-t})). \end{cases} \neq (0, e), \text{ se } x \neq e \text{ e } t \neq r. \end{aligned}$$

Logo, $g_a^2 : L_I \rightarrow L_J$ não é half-isomorfismo.

Os casos $r \neq s$ e $s \neq t$ são análogos aos dois casos apresentados aqui. $\square$

Observação 3.17. É importante ressaltar que os lemas 3.15 e 3.16 estabelecem uma condição necessária para a descrição dos half-isomorfismo que queremos apresentar.

Agora podemos dar um passo significativo na direção de caracterizar todos os half-isomorfismos de L_α em L_β , para $m = 4$ e $m = 6$, e mostrar que todos são não triviais, quando $\alpha \neq \beta$.

(1) No caso $m = 4$:

Teorema 3.18. *Sejam $m = 4$ e $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo. Então existe $a \in C_p$ tal que:*

$$f((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (1, af'(x^{\delta_a})), & \text{se } i = 1 \text{ e } \delta_a \in \{1, -1\}, \\ (3, af'(x^{\delta_a})), & \text{se } i = 3 \text{ e } \delta_a \in \{1, -1\} \end{cases}$$

ou

$$f((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (3, af'(x^{\delta_a})), & \text{se } i = 1 \text{ e } \delta_a \in \{1, -1\}, \\ (1, af'(x^{\delta_a})) & \text{se } i = 3 \text{ e } \delta_a \in \{1, -1\}. \end{cases}$$

Demonstração. Pelo lema 3.13 e pela definição de f' , temos que

$$f(0, x) = (0, f'(x)) \text{ e } f(2, x) = (2, f'(x)),$$

qualquer que seja $x \in C_p$.

Sabemos também, pela ordem dos elementos, que

$$f(1, e) = (1, a) \text{ ou } f(1, e) = (3, a),$$

para algum $a \in C_p = \{e, u, u^2, \dots, u^{p-1}\}$.

Então, vamos dividir a demonstração da existência de a em dois casos.

(i) Fixemos primeiro $f(1, e) = (1, a)$, para algum $a \in C_p$.

Temos então

$$\begin{aligned} f(1, x) &= f((1, e) * (0, x)) \in \{f((1, e))f((0, x)), f((0, x))f((1, e))\} = \\ &= \{(1, a)(0, f'(x)), (0, f'(x))(1, a)\} = \\ &= \{(1, af'(x)), (1, af'(x^{-1}))\} \end{aligned}$$

e

$$\begin{aligned} f(3, x) &= f((1, e) * (2, x)) \in \{f((1, e))f((2, x)), f((2, x))f((1, e))\} = \\ &= \{(1, a)(2, f'(x)), (2, f'(x))(1, a)\} = \\ &= \{(3, af'(x)), (3, af'(x^{-1}))\} \end{aligned}$$

(ii) Fixemos agora $f(1, e) = (3, a)$.

Teremos então

$$\begin{aligned} f(1, x) &= f((1, e) * (0, x)) \in \{f((1, e))f((0, x)), f((0, x))f((1, e))\} = \\ &= \{(3, a)(0, f'(x)), (0, f'(x))(3, a)\} = \\ &= \{(3, af'(x)), (3, af'(x^{-1}))\} \end{aligned}$$

e

$$\begin{aligned} f(3, x) &= f((1, e) * (2, x)) \in \{f((1, e))f((2, x)), f((2, x))f((1, e))\} = \\ &= \{(3, a)(2, f'(x)), (2, f'(x))(3, a)\} = \\ &= \{(1, af'(x)), (1, af'(x^{-1}))\} \end{aligned}$$

Dessa forma, tendo em vista o lema (3.15), concluímos a demonstração. $\square$

(2) No caso $m = 6$:

Teorema 3.19. *Sejam $m = 6$ e $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo. Então existe $a \in C_p$ tal que:*

$$f((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (4, f'(x)), & \text{se } i = 4, \\ (1, af'(x^{\delta_a})), & \text{se } i = 1 \text{ e } \delta_a \in \{1, -1\}, \\ (3, af'(x^{\delta_a})), & \text{se } i = 3 \text{ e } \delta_a \in \{1, -1\}, \\ (5, af'(x^{\delta_a})), & \text{se } i = 5 \text{ e } \delta_a \in \{1, -1\}, \end{cases}$$

ou

$$f((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (4, f'(x)), & \text{se } i = 2, \\ (2, f'(x)), & \text{se } i = 4, \\ (5, af'(x^{\delta_a})), & \text{se } i = 1 \text{ e } \delta_a \in \{1, -1\}, \\ (3, af'(x^{\delta_a})), & \text{se } i = 3 \text{ e } \delta_a \in \{1, -1\}, \\ (1, af'(x^{\delta_a})), & \text{se } i = 5 \text{ e } \delta_a \in \{1, -1\}. \end{cases}$$

Demonstração. Pelo lema 3.14 e pela definição de f' , temos

$$f(0, x) = (0, f'(x))$$

e

$$f(2, x) = (2, f'(x)) \text{ e } f(4, x) = (4, f'(x))$$

ou

$$f(2, x) = (4, f'(x)) \text{ e } f(4, x) = (2, f'(x)),$$

qualquer que seja $x \in C_p$.

Sabemos também, pela ordem dos elementos, que

$$f(3, e) = (3, a) \text{ e } f(1, e) = (1, a) \text{ ou } f(1, e) = (5, a),$$

para algum $a \in C_p = \{e, u, u^2, \dots, u^{p-1}\}$.

Então, vamos dividir a demonstração da existência de a em três casos.

(i) Fixemos primeiro $f(3, e) = (3, a)$, para algum $a \in C_p$.

Temos então

$$\begin{aligned} f(3, x) &= f((3, e) * (0, x)) \in \{f((3, e))f((0, x)), f((0, x))f((3, e))\} \\ &= \{(3, a)(0, f'(x)), (0, f'(x))(3, a)\} = \\ &= \{(3, af'(x)), (3, af'(x^{-1}))\}. \end{aligned}$$

(ii) Fixemos $f(1, e) = (1, a)$.

Neste caso temos,

$$\begin{aligned} f(1, x) &= f((1, e) * (0, x)) \in \{f((1, e))f((0, x)), f((0, x))f((1, e))\} \\ &= \{(1, a)(0, f'(x)), (0, f'(x))(1, a)\} = \\ &= \{(1, af'(x)), (1, af'(x^{-1}))\} \end{aligned}$$

e

$$\begin{aligned} f(5, x) &= f((1, e) * (4, x)) \in \{f((1, e))f((4, x)), f((4, x))f((1, e))\} = \\ &= \{(1, a)(4, f'(x)), (4, f'(x))(1, a)\} = \\ &= \{(5, af'(x)), (5, af'(x^{-1}))\} \end{aligned}$$

(iii) Fixemos agora $f(1, e) = (5, a)$.

Assim,

$$f(1, x) = f((1, e) * (0, x)) \in \{f((1, e))f((0, x)), f((0, x))f((1, e))\} =$$

$$\begin{aligned}
&= \{(5, a)(0, f'(x)), (0, f'(x))(5, a)\} = \\
&= \{(5, af'(x)), (5, af'(x^{-1}))\}
\end{aligned}$$

e

$$\begin{aligned}
f(5, x) &= f((1, e) * (4, x)) \in \{f((1, e))f((4, x)), f((4, x))f((1, e))\} = \\
&= \{(5, a)(2, f'(x)), (2, f'(x))(5, a)\} = \\
&= \{(1, af'(x)), (1, af'(x^{-1}))\}
\end{aligned}$$

Dessa forma, tendo em vista o lema (3.16), concluímos a demonstração. $\square$

Até aqui, independentemente do valor de m , se $f : L_\alpha \rightarrow L_\beta$ é um half-isomorfismo, então, pelas proposições (1.34), (1.36) e da definição de f' , temos $f((0, e)) = (0, e)$ e $f((0, x)) = (0, f'(x))$, para todo $x \in C_p$. Além disso, para $m = 4$, $f((2, e)) = (2, e)$, pois $(2, e)$ é o único elemento de ordem 2, $f(2, x) = (2, f'(x))$, pelo lema (3.13), e do Teorema (3.18), temos que se

$$f(1, x) = (1, af'(x^{\delta_a})),$$

então

$$f(3, x) = (3, af'(x^{\delta_a})), \text{ com } \delta_a \in \{1, -1\},$$

e se

$$f(1, x) = (3, af'(x^{\delta_a})),$$

então

$$f(3, x) = (1, af'(x^{\delta_a})), \text{ com } \delta_a \in \{1, -1\},$$

para cada $a \in C_p$ e para todo $x \in C_p$.

Por outro lado, para $m = 6$, do lema (3.14) temos que $f((2, x)) = (2, f'(x))$ e $f((4, x)) = (4, f'(x))$ ou $f((2, x)) = (4, f'(x))$ e $f((4, x)) = (2, f'(x))$, para todo $x \in C_p$. Além disso, do Teorema (3.19), temos $f(3, x) = (3, af'(x^{\delta_a}))$. Ainda mais, se

$$f(1, x) = (1, af'(x^{\delta_a})),$$

então

$$f(5, x) = (5, af'(x^{\delta_a})), \text{ com } \delta_a \in \{1, -1\}$$

e se

$$f(1, x) = (5, af'(x^{\delta_a})),$$

então

$$f(5, x) = (1, af'(x^{\delta_a})), \text{ com } \delta_a \in \{1, -1\},$$

para cada $a \in C_p$ e para todo $x \in C_p$.

Concluimos então que, para ambos os casos $m = 4$ e $m = 6$, descrevemos

$$2 \times 2 \times (p - 1) \times p = 4(p - 1)p$$

possibilidades para os half-isomorfismos. De fato, temos $p - 1$ possibilidades para f' . Temos ainda dois valores possíveis para δ_a , duas sentenças que definem f e a pode ser qualquer um dos p elementos de C_p .

Sendo assim, podemos melhorar a notação identificando as $4 \times (p - 1) \times p$ possibilidades de f em quatro famílias com $(p - 1) \times p$ half-isomorfismos cada, pelas seguintes expressões.

(1) Para $m = 4$:

$$f_{+a}^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (1, af'(x)), & \text{se } i = 1, \\ (3, af'(x)), & \text{se } i = 3. \end{cases} \quad f_{-a}^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (1, af'(x^{-1})), & \text{se } i = 1, \\ (3, af'(x^{-1})), & \text{se } i = 3. \end{cases}$$

$$f_{+a}^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (3, af'(x)), & \text{se } i = 1, \\ (1, af'(x)), & \text{se } i = 3. \end{cases} \quad f_{-a}^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (3, af'(x^{-1})), & \text{se } i = 1, \\ (1, af'(x^{-1})), & \text{se } i = 3. \end{cases}$$

(2) Para $m = 6$:

$$f_{+a}^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (4, f'(x)), & \text{se } i = 4, \\ (1, af'(x)), & \text{se } i = 1, \\ (3, af'(x)), & \text{se } i = 3, \\ (5, af'(x)), & \text{se } i = 5. \end{cases} \quad f_{-a}^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (4, f'(x)), & \text{se } i = 4, \\ (1, af'(x^{-1})), & \text{se } i = 1, \\ (3, af'(x^{-1})), & \text{se } i = 3, \\ (5, af'(x^{-1})), & \text{se } i = 5. \end{cases}$$

$$f_{+a}^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (4, f'(x)), & \text{se } i = 2, \\ (2, f'(x)), & \text{se } i = 4, \\ (5, af'(x)), & \text{se } i = 1, \\ (3, af'(x)), & \text{se } i = 3, \\ (1, af'(x)), & \text{se } i = 5. \end{cases} \quad f_{-a}^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (4, f'(x)), & \text{se } i = 2, \\ (2, f'(x)), & \text{se } i = 4, \\ (5, af'(x^{-1})), & \text{se } i = 1, \\ (3, af'(x^{-1})), & \text{se } i = 3, \\ (1, af'(x^{-1})), & \text{se } i = 5. \end{cases}$$

De fato, em ambos os casos, são quatro famílias com $(p-1)p$ funções, pois a pode assumir um dos p valores de C_p e f' é um dos $p-1$ automorfismos de C_p . Logo, temos $(p-1)p$ half-isomorfismos em cada uma das famílias de funções f_{+a}^1 , f_{-a}^1 , f_{+a}^2 e f_{-a}^2 .

Podemos então enunciar o principal resultado dessa seção, para ambos os casos $m = 4$ e $m = 6$.

Teorema 3.20. *Seja $f' : C_p \rightarrow C_p$ um automorfismo. Então, para cada $a \in C_p$,*

$$f_{+a}^1 : L_I \rightarrow L_J, \quad f_{-a}^1 : L_I \rightarrow L_J, \quad f_{+a}^2 : L_I \rightarrow L_J \quad \text{e} \quad f_{-a}^2 : L_I \rightarrow L_J$$

são half-isomorfismo não triviais.

Demonstração. Vamos demonstrar para o caso em que $m = 4$, o caso em que $m = 6$ é análogo com as devidas adaptações.

Provaremos caso a caso.

(i) Para a família de funções f_{+a}^1 .

Considere $j \in \{0, 2\}$.

Se $i = 0$ ou $i = 2$, então temos:

$$\begin{aligned} f_{+a}^1((i, u)(j, v)) &= f_{+a}^1((i+j, uv)) = (i+j, f'(uv)) = (i+j, f'(u)f'(v)) = \\ &= (i, f'(u))(j, f'(v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)).$$

Agora, se $i = 1$ ou $i = 3$, então temos:

$$\begin{aligned} f_{+a}^1((i, u)(j, v)) &= f_{+a}^1((i+j, uv)) = (i+j, af'(uv)) = (i+j, af'(u)f'(v)) = \\ &= (i, af'(u))(j, f'(v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)).$$

Considere agora $j \in \{1, 3\}$.

Se $i = 0$ ou $i = 2$, então temos:

$$\begin{aligned} f_{+a}^1((i, u)(j, v)) &= f_{+a}^1((i + j, u^{-1}v)) = (i + j, af'(u^{-1}v)) = (i + j, af'(u^{-1})f'(v)) = \\ &= (i, f'(u))(j, af'(v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)).$$

Se $i = 1$ ou $i = 3$, então temos:

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((i + j, u^{-1}v)) = (i + j, f'(u^{-1}v)) = (i + j, f'(u^{-1})f'(v)).$$

Por outro lado,

$$f_{+a}^1((j, v))f_{+a}^1((i, u)) = (j, af'(v))(i, af'(u)) = (i + j, (a^{-1}f'(v^{-1})af'(u))f) = (i + j, f'(u^{-1})f'(v)).$$

Logo, diferentemente dos casos anteriores, temos

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((j, v))f_{+a}^1((i, u)).$$

Assim, está demonstrado que f_{+a}^1 é uma família com $(p - 1)p$ half-isomorfismos não triviais.

Para as demais famílias as demonstrações são análogas, seguiremos analisando caso a caso.

(ii) Para a família de funções f_{-a}^1 .

Considere $j \in \{0, 2\}$.

Se $i = 0$ ou $i = 2$, então temos:

$$\begin{aligned} f_{-a}^1((i, u)(j, v)) &= f_{-a}^1((i + j, uv)) = (i + j, f'(uv)) = (i + j, f'(u)f'(v)) = \\ &= (i, f'(u))(j, f'(v)) = f_{-a}^1((i, u))f_{-a}^1((j, v)). \end{aligned}$$

Ou seja,

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((i, u))f_{-a}^1((j, v)).$$

Se $i = 1$ ou $i = 3$, então temos:

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((i + j, uv)) = (i + j, af'(v^{-1}u^{-1})) = (i + j, af'(v^{-1})f'(u^{-1})).$$

Por outro lado,

$$\begin{aligned} f_{-a}^1((j, v))f_{-a}^1((i, u)) &= (j, f'(v))(i, af'(u^{-1})) = \\ &= (i + j, f'(v^{-1})af'(u^{-1})) = (i + j, af'(v^{-1})f'(u^{-1})). \end{aligned}$$

Assim, temos

$$f_{-a}^1((i, u)(j, v)) = f_{+a}^1((j, v))f_{+a}^1((i, u)).$$

Considere $j \in \{1, 3\}$.

Se $i = 0$ ou $i = 2$, então temos:

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((i + j, u^{-1}v)) = (i + j, af'(v^{-1}u)) = (i + j, af'(v^{-1})f'(u)).$$

Por outro lado,

$$f_{-a}^1((j, v))f_{-a}^1((i, u)) = (j, af'(v^{-1}))(i, f'(u)) = (i + j, af'(v^{-1})f'(u)).$$

Temos então

$$f_{-a}^1((i, u)(j, v)) = f_{+a}^1((j, v))f_{+a}^1((i, u)).$$

Se $i = 1$ ou $i = 3$, então temos:

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((i + j, u^{-1}v)) = (i + j, f'(u^{-1}v)) = (i + j, f'(u^{-1})f'(v)).$$

Por outro lado,

$$\begin{aligned} f_{-a}^1((i, u))f_{-a}^1((j, v)) &= (i, af'(u^{-1}))(j, af'(v^{-1})) = \\ &= (i + j, (a^{-1}f'(u)af'(v^{-1}))J) = (i + j, f'(u^{-1})f'(v)). \end{aligned}$$

Portanto, diferentemente dos dois últimos casos,

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((i, u))f_{-a}^1((j, v)).$$

Concluimos assim a demonstração de que f_{-a}^1 também é uma família com $(p - 1)p$ half-isomorfismos não triviais.

Para as famílias de funções f_{+a}^2 e f_{-a}^2 usaremos as seguintes notações:

$$\left\{ \begin{array}{ll} \widetilde{i + j} = 4 - l, & \text{se } i + j = l, \\ \widetilde{i} = 4 - l, & \text{se } i = l, \\ \widetilde{j} = 4 - l, & \text{se } j = l, \end{array} \right.$$

onde $l = 1$ ou $l = 3$.

(iii) Para a família de funções f_{+a}^2

Considere $j \in \{0, 2\}$.

Se $i = 0$ ou $i = 2$, então temos:

$$\begin{aligned} f_{+a}^2((i, u)(j, v)) &= f_{+a}^2((i + j, uv)) = (i + j, f'(uv)) = (i + j, f'(u)f'(v)) = \\ &= (i, f'(u))(j, f'(v)) = f_{+a}^2((i, u))f_{+a}^2((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i, u))f_{+a}^2((j, v)).$$

Fazendo agora $i = 1$ ou $i = 3$ temos

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i + j, uv)) = (\widetilde{i + j}, af'(uv)) = (\widetilde{i + j}, af'(u)f'(v)).$$

Por outro lado,

$$f_{+a}^2((i, u))f_{+a}^2((j, v)) = (\widetilde{i}, af'(u))(j, f'(v)) = (\widetilde{i + j}, af'(u)f'(v)),$$

pois, nesse caso, $\widetilde{i + j} = \widetilde{i} + j$.

Logo, temos

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i, u))f_{+a}^2((j, v)).$$

Considere $j \in \{1, 3\}$.

Se $i = 0$ ou $i = 2$, então temos:

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i + j, u^{-1}v)) = (\widetilde{i + j}, af'(u^{-1}v)) = (\widetilde{i + j}, af'(u^{-1})f'(v)).$$

Por outro lado,

$$f_{+a}^2((i, u))f_{+a}^2((j, v)) = (i, f'(u))(\widetilde{j}, af'(v)) = (\widetilde{i + j}, af'(u^{-1})f'(v)),$$

pois, nesse caso, $i + \widetilde{j} = \widetilde{i + j}$.

Novamente temos

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i, u))f_{+a}^2((j, v)).$$

Se $i = 1$ ou $i = 3$, então temos:

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i + j, u^{-1}v)) = (i + j, f'(u^{-1}v)) = (i + j, f'(u^{-1})f'(v)).$$

Por outro lado,

$$f_{+a}^2((j, v))f_{+a}^2((i, u)) = (\widetilde{j}, af'(v))(\widetilde{i}, af'(u)) = (\widetilde{i} + \widetilde{j}, (a^{-1}f'(v^{-1})af'(u))J) = (i + j, f'(u^{-1})f'(v)),$$

pois, nesse caso, $\widetilde{i} + \widetilde{j} = i + j$.

Logo, nesses casos, diferentemente dos casos anteriores, temos

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((j, v))f_{+a}^2((i, u)).$$

Demonstramos então que f_{+a}^2 é uma família com $(p - 1)p$ half-isomorfismos que são não triviais.

(iv) Para a família de funções f_{-a}^2

Considere $j \in \{0, 2\}$.

Se $i = 0$ ou $i = 2$, então temos:

$$\begin{aligned} f_{-a}^2((i, u)(j, v)) &= f_{-a}^2((i + j, uv)) = (i + j, f'(uv)) = (i + j, f'(u)f'(v)) = \\ &= (i, f'(u))(j, f'(v)) = f_{-a}^2((i, u))f_{-a}^2((j, v)). \end{aligned}$$

Ou seja,

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((i, u))f_{-a}^2((j, v)).$$

Se $i = 1$ ou $i = 3$, então temos:

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((i + j, uv)) = (\widetilde{i + j}, af'(v^{-1}u^{-1})) = (\widetilde{i + j}, af'(v^{-1})f'(u^{-1})).$$

Por outro lado,

$$\begin{aligned} f_{-a}^2((j, v))f_{-a}^2((i, u)) &= (j, f'(v))(\widetilde{i}, af'(u^{-1})) = \\ &= (\widetilde{i + j}, af'(v^{-1})f'(u^{-1})) = (\widetilde{i + j}, af'(v^{-1})f'(u^{-1})). \end{aligned}$$

Assim,

$$f_{-a}^2((i, u)(j, v)) = f_{+a}^2((j, v))f_{+a}^2((i, u)).$$

Considere $j \in \{1, 3\}$.

Se $i = 0$ ou $i = 2$, então temos:

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((i + j, u^{-1}v)) = (\widetilde{i + j}, af'(v^{-1}u)) = (\widetilde{i + j}, af'(v^{-1})f'(u)).$$

Por outro lado,

$$f_{-a}^2((j, v))f_{-a}^2((i, u)) = (\widetilde{j}, af'(v^{-1}))(i, f'(u)) = (i + \widetilde{j}, af'(v^{-1})f'(u)) = (\widetilde{i + j}, af'(v^{-1})f'(u)).$$

Logo,

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((j, v))f_{-a}^2((i, u)).$$

Se $i = 1$ ou $i = 3$, então temos:

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((i + j, u^{-1}v)) = (i + j, f'(u^{-1}v)) = (i + j, f'(u^{-1})f'(v)).$$

Por outro lado,

$$\begin{aligned} f_{-a}^2((i, u))f_{-a}^2((j, v)) &= (\tilde{i}, af'(u^{-1}))(\tilde{j}, af'(v^{-1})) = \\ &= (\tilde{i} + \tilde{j}, (a^{-1}f'(u)af'(v^{-1}))J) = (i + j, f'(u^{-1})f'(v)). \end{aligned}$$

Portanto,

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((i, u))f_{-a}^2((j, v)).$$

Demonstramos assim que f_{-a}^2 é uma família com $(p - 1)p$ half-isomorfismos não triviais.

Assim concluímos a demonstração. $\square$

É importante observar que no Teorema (3.20) tomamos as funções de L_I em L_J , mas o resultado também é válido se tomarmos as funções, definidas pelas mesmas leis de formação, de L_J em L_I , com uma demonstração totalmente análoga.

3.3 HALF-AUTOMORFISMOS: PARA OS CASOS

$$m = 4 \text{ E } m = 6$$

Os procedimentos para a caracterização dos half-automorfismos do loop diedral $L_J = Dih(m, C_p, J)$, nos casos em que $m = 4$ e $m = 6$, são totalmente análogos aos realizados para caracterizar os half-isomorfismos de $L_\alpha = Dih(m, C_p, \alpha)$ em $L_\beta = Dih(m, C_p, \beta)$ na seção anterior. Consequentemente vamos obter as mesmas leis de formação f_{+a}^1 , f_{-a}^1 , f_{+a}^2 e f_{-a}^2 , dadas tanto para $m = 4$ como para $m = 6$. Entretanto, nesse caso, vamos demonstrar que todos os half-automorfismos de L_J são triviais.

Podemos então enunciar o principal resultado dessa seção.

Teorema 3.21. *Seja $f' : C_p \rightarrow C_p$ um automorfismo. Então, para cada $a \in C_p$,*

$$f_{+a}^1 : L_J \rightarrow L_J, \quad f_{-a}^1 : L_J \rightarrow L_J, \quad f_{+a}^2 : L_J \rightarrow L_J \quad \text{e} \quad f_{-a}^2 : L_J \rightarrow L_J$$

são half-automorfismo triviais de L_J .

Vamos demonstrar para o caso $m = 6$.

Demonstração. Provaremos caso a caso.

(i) Para a família de funções f_{+a}^1 .

Considere $j \in \{0, 2, 4\}$.

Sejam $i = 0$ ou $i = 2$ ou $i = 4$, então temos:

$$\begin{aligned} f_{+a}^1((i, u)(j, v)) &= f_{+a}^1((i + j, uv)) = (i + j, f'(uv)) = (i + j, f'(u)f'(v)) = \\ &= (i, f'(u))(j, f'(v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)).$$

Agora, sejam $i = 1$ ou $i = 3$ ou $i = 5$, então temos:

$$\begin{aligned} f_{+a}^1((i, u)(j, v)) &= f_{+a}^1((i + j, uv)) = (i + j, af'(uv)) = (i + j, af'(u)f'(v)) = \\ &= (i, af'(u))(j, f'(v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)).$$

Considere então $j \in \{1, 3, 5\}$.

Sejam $i = 0$ ou $i = 2$ ou $i = 4$, então temos:

$$\begin{aligned} f_{+a}^1((i, u)(j, v)) &= f_{+a}^1((i + j, u^{-1}v)) = (i + j, af'(u^{-1}v)) = (i + j, af'(u^{-1})f'(v)) = \\ &= (i, f'(u))(j, af'(v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)).$$

Por fim, sejam $i = 1$ ou $i = 3$ ou $i = 5$, então temos:

$$\begin{aligned} f_{+a}^1((i, u)(j, v)) &= f_{+a}^1((i + j, (u^{-1}v)J)) = f_{+a}^1((i + j, v^{-1}u)) = \\ &= (i + j, f'(v^{-1}u)) = (i + j, f'(v^{-1})f'(u)). \end{aligned}$$

Por outro lado,

$$f_{+a}^1((i, u))f_{+a}^1((j, v)) = (i, af'(u))(j, af'(v)) = (i + j, (a^{-1}f'(u^{-1})af'(v))J) = (i + j, f'(v^{-1})f'(u)).$$

Logo, temos

$$f_{+a}^1((i, u)(j, v)) = f_{+a}^1((i, u))f_{+a}^1((j, v)).$$

Dessa forma demonstramos que f_{+a}^1 é uma família com $(p-1)p$ isomorfismos de L_J .

(ii) Para a família de funções f_{-a}^1 .

Considere $j \in \{0, 2, 4\}$.

Sejam $i = 0$ ou $i = 2$ ou $i = 4$, então temos:

$$\begin{aligned} f_{-a}^1((i, u)(j, v)) &= f_{-a}^1((i+j, uv)) = (i+j, f'(uv)) = (i+j, f'(u)f'(v)) = \\ &= (i, f'(u))(j, f'(v)) = f_{-a}^1((i, u))f_{-a}^1((j, v)) = f_{-a}^1((j, v))f_{-a}^1((i, u)). \end{aligned}$$

Ou seja,

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((j, v))f_{-a}^1((i, u)).$$

Sejam $i = 1$ ou $i = 3$ ou $i = 5$, então temos:

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((i+j, uv)) = (i+j, af'(v^{-1}u^{-1})) = (i+j, af'(v^{-1})f'(u^{-1})).$$

Por outro lado,

$$\begin{aligned} f_{-a}^1((j, v))f_{-a}^1((i, u)) &= (j, f'(v))(i, af'(u^{-1})) = \\ &= (i+j, f'(v^{-1})af'(u^{-1})) = (i+j, af'(v^{-1})f'(u^{-1})). \end{aligned}$$

Assim, temos

$$f_{-a}^1((i, u)(j, v)) = f_{+a}^1((j, v))f_{+a}^1((i, u)).$$

Agora, considere $j \in \{1, 3, 5\}$.

Sejam $i = 0$ ou $i = 2$ ou $i = 4$, então temos:

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((i+j, u^{-1}v)) = (i+j, af'(v^{-1}u)) = (i+j, af'(v^{-1})f'(u)).$$

Por outro lado,

$$f_{-a}^1((j, v))f_{-a}^1((i, u)) = (j, af'(v^{-1}))(i, f'(u)) = (i+j, af'(v^{-1})f'(u)).$$

Temos então

$$f_{-a}^1((i, u)(j, v)) = f_{+a}^1((j, v))f_{+a}^1((i, u)).$$

Sejam, por fim, $i = 1$ ou $i = 3$ ou $i = 5$, então temos:

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((i+j, (u^{-1}v)J)) = f_{-a}^1((i+j, v^{-1}u)) =$$

$$= (i + j, f'(v^{-1}u)) = (i + j, f'(v^{-1})f'(u)).$$

Por outro lado,

$$\begin{aligned} f_{-a}^1((j, v))f_{-a}^1((i, u)) &= (j, af'(v^{-1}))(i, af'(u^{-1})) = \\ &= (i + j, (a^{-1}f'(v)af'(u^{-1}))J) = (i + j, f'(v^{-1})f'(u)). \end{aligned}$$

Portanto, temos

$$f_{-a}^1((i, u)(j, v)) = f_{-a}^1((j, v))f_{-a}^1((i, u)).$$

Concluimos então que f_{-a}^1 é uma família com $(p - 1)p$ anti-isomorfismos.

Para as próximas famílias de funções usaremos as seguintes notações:

$$\begin{cases} \widetilde{i + j} = 6 - l, & \text{se } i + j = l, \\ \widetilde{i} = 6 - l, & \text{se } i = l, \\ \widetilde{j} = 6 - l, & \text{se } j = l, \end{cases}$$

onde l é um inteiro entre 0 e 5.

Vale observar que para todos os possíveis valores de i e j temos que $\widetilde{i + j} = \widetilde{i} + \widetilde{j}$.

(iii) Para a família de funções f_{+a}^2

Considere $j \in \{0, 2, 4\}$.

Sejam $i = 0$ ou $i = 2$ ou $i = 4$, então temos:

$$\begin{aligned} f_{+a}^2((i, u)(j, v)) &= f_{+a}^2((i + j, uv)) = (\widetilde{i + j}, f'(uv)) = (\widetilde{i + j}, f'(u)f'(v)) = \\ &= (\widetilde{i}, f'(u))(\widetilde{j}, f'(v)) = f_{+a}^2((i, u))f_{+a}^2((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i, u))f_{+a}^2((j, v)).$$

Agora, seja $i = 1$ ou $i = 3$ ou $i = 5$, então temos:

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i + j, uv)) = (\widetilde{i + j}, af'(uv)) = (\widetilde{i + j}, af'(u)f'(v)),$$

Por outro lado,

$$f_{+a}^2((i, u))f_{+a}^2((j, v)) = (\widetilde{i}, af'(u))(\widetilde{j}, f'(v)) = (\widetilde{i + j}, af'(u)f'(v)).$$

Logo,

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i, u))f_{+a}^2((j, v)).$$

Considere $j \in \{1, 3, 5\}$.

Seja $i = 0$ ou $i = 2$ ou $i = 4$, então temos:

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i + j, u^{-1}v)) = (\widetilde{i + j}, af'(u^{-1}v)) = (\widetilde{i + j}, af'(u^{-1})f'(v)).$$

Por outro lado,

$$f_{+a}^2((i, u))f_{+a}^2((j, v)) = (\widetilde{i}, f'(u))(\widetilde{j}, af'(v)) = (\widetilde{i + j}, af'(u^{-1})f'(v)).$$

Então, temos

$$f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i, u))f_{+a}^2((j, v)).$$

Por fim, sejam $i = 1$ ou $i = 3$ ou $i = 5$, então temos:

$$\begin{aligned} f_{+a}^2((i, u)(j, v)) &= f_{+a}^2((i + j, (u^{-1}v))J) = f_{+a}^2((i + j, v^{-1}u)) = \\ &= (\widetilde{i + j}, f'(v^{-1}u)) = (\widetilde{i + j}, f'(v^{-1})f'(u)). \end{aligned}$$

Por outro lado,

$$f_{+a}^2((i, u))f_{+a}^2((j, v)) = (\widetilde{i}, af'(u))(\widetilde{j}, af'(v)) = (\widetilde{i + j}, (a^{-1}f'(u^{-1})af'(v))J) = (\widetilde{i + j}, f'(v^{-1})f'(u)).$$

Logo, nesse caso temos $f_{+a}^2((i, u)(j, v)) = f_{+a}^2((i, u))f_{+a}^2((j, v))$

Novamente, como no caso de f_{+a}^1 , demonstramos que f_{+a}^2 é uma família com $(p - 1)p$ isomorfismos.

(iv) Para a família de funções f_{-a}^2

Considere $j \in \{0, 2, 4\}$.

Sejam $i = 0$ ou $i = 2$ ou $i = 4$, então temos:

$$\begin{aligned} f_{-a}^2((i, u)(j, v)) &= f_{-a}^2((i + j, uv)) = (\widetilde{i + j}, f'(uv)) = (\widetilde{i + j}, f'(u)f'(v)) = \\ &= (\widetilde{i}, f'(u))(\widetilde{j}, f'(v)) = f_{-a}^2((i, u))f_{-a}^2((j, v)) = f_{-a}^2((j, v))f_{-a}^2((i, u)). \end{aligned}$$

Ou seja,

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((j, v))f_{-a}^2((i, u)).$$

Sejam agora $i = 1$ ou $i = 3$ ou $i = 5$, então temos:

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((i + j, uv)) = (\widetilde{i + j}, af'(v^{-1}u^{-1})) = (\widetilde{i + j}, af'(v^{-1})f'(u^{-1})).$$

Por outro lado,

$$\begin{aligned} f_{-a}^2((j, v))f_{-a}^2((i, u)) &= (\widetilde{j}, f'(v))(\widetilde{i}, af'(u^{-1})) = \\ &= (\widetilde{i} + \widetilde{j}, af'(v^{-1})f'(u^{-1})) = (\widetilde{i} + \widetilde{j}, af'(v^{-1})f'(u^{-1})). \end{aligned}$$

Assim, temos

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((j, v))f_{-a}^2((i, u)).$$

Considere $j \in \{1, 3, 5\}$.

Sejam $i = 0$ ou $i = 2$ ou $i = 4$, então temos:

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((i + j, u^{-1}v)) = (\widetilde{i} + \widetilde{j}, af'(v^{-1}u)) = (\widetilde{i} + \widetilde{j}, af'(v^{-1})f'(u)).$$

Por outro lado,

$$f_{-a}^2((j, v))f_{-a}^2((i, u)) = (\widetilde{j}, af'(v^{-1}))(\widetilde{i}, f'(u)) = (\widetilde{i} + \widetilde{j}, af'(v^{-1})f'(u)) = (\widetilde{i} + \widetilde{j}, af'(v^{-1})f'(u)).$$

Dessa vez temos

$$f_{-a}^2((i, u)(j, v)) = f_{+a}^2((j, v))f_{+a}^2((i, u)).$$

Por fim, sejam $i = 1$ ou $i = 3$, ou $i = 5$, então temos:

$$\begin{aligned} f_{-a}^2((i, u)(j, v)) &= f_{-a}^2((i + j, (u^{-1}v)J)) = f_{-a}^2((i + j, v^{-1}u)) = \\ &= (\widetilde{i} + \widetilde{j}, f'(v^{-1}u)) = (\widetilde{i} + \widetilde{j}, f'(v^{-1})f'(u)). \end{aligned}$$

Por outro lado,

$$\begin{aligned} f_{-a}^2((j, v))f_{-a}^2((i, u)) &= (\widetilde{j}, af'(v^{-1}))(\widetilde{i}, af'(u^{-1})) = \\ &= (\widetilde{i} + \widetilde{j}, (a^{-1}f'(v))af'(u^{-1})) = (i + j, f'(v^{-1})f'(u)). \end{aligned}$$

Portanto,

$$f_{-a}^2((i, u)(j, v)) = f_{-a}^2((j, v))f_{-a}^2((i, u)).$$

Novamente, como no caso de f_{-a}^1 , demonstramos que f_{-a}^2 é uma família com $(p - 1)p$ anti-isomorfismos. $\square$

Obtivemos assim a caracterização de todos os half-automorfismos de L_J , que são apenas esses $4 \times (p - 1) \times p$ descritos no Teorema (3.21). Além disso, demonstramos nessa seção que *todos são half-automorfismos triviais de L_J* .

3.4 OS A -LOOPS DIEDRAIS $Dih(4, C_3, \alpha)$ E $Dih(6, C_3, \alpha)$

Até o momento foram caracterizados todos os half-isomorfismos para os loops $Dih(m, C_p, \alpha)$, com $m = 4$ ou $m = 6$. A seguir analisaremos, como exemplos, dois casos particulares quando $p = 3$. Serão apresentados todos os half-isomorfismos entre $Dih(4, C_3, \alpha)$ e $Dih(4, C_3, \beta)$ e também entre $Dih(6, C_3, \alpha)$ e $Dih(6, C_3, \beta)$.

Fixando as notações $C_3 = \{e, u, u^2\}$, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ e $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ teremos os conjuntos

$$\mathbb{Z}_4 \times C_3 = \{(0, e), (0, u), (0, u^2), (1, e), (1, u), (1, u^2), (2, e), (2, u), (2, u^2), (3, e), (3, u), (3, u^2)\}.$$

e

$$\mathbb{Z}_6 \times C_3 = \{(0, e), (0, u), (0, u^2), (1, e), (1, u), (1, u^2), (2, e), (2, u), (2, u^2), (3, e), (3, u), (3, u^2),$$

$$(4, e), (4, u), (4, u^2), (5, e), (5, u), (5, u^2)\}.$$

Nessa seção

L_I representará o loop $Dih(m, C_3, I)$

e

L_J representará o loop $Dih(m, C_3, J)$,

para $m = 4$ ou $m = 6$.

Vamos então descrever as tabelas de multiplicação dos loops L_I e L_J , para $m = 4$.

Tendo em vista diminuir um pouco as dimensões das tabelas de multiplicação desses loops, faremos uma adaptação da notação usada até aqui. Usaremos a notação

$$\mathbb{Z}_4 \times C_3 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\},$$

de forma que os elementos

$$(0, e), (0, u), (0, u^2), \dots, (3, u), (3, u^2)$$

vão ser substituídos por $1, 2, 3, \dots, 11, 12$, respectivamente.

Loop L_I :	$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12
	1	1	2	3	4	5	6	7	8	9	10	11	12
	2	2	3	1	6	4	5	8	9	7	12	10	11
	3	3	1	2	5	6	4	9	7	8	11	12	10
	4	4	5	6	7	8	9	10	11	12	1	2	3
	5	5	6	4	9	7	8	11	12	10	3	1	2
	6	6	4	5	8	9	7	12	10	11	2	3	1
	7	7	8	9	10	11	12	1	2	3	4	5	6
	8	8	9	7	12	10	11	2	3	1	6	4	5
	9	9	7	8	11	12	10	3	1	2	5	6	4
	10	10	11	12	1	2	3	4	5	6	7	8	9
	11	11	12	10	3	1	2	5	6	4	9	7	8
	12	12	10	11	2	3	1	6	4	5	8	9	7

Loop L_J :	$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12
	1	1	2	3	4	5	6	7	8	9	10	11	12
	2	2	3	1	6	4	5	8	9	7	12	10	11
	3	3	1	2	5	6	4	9	7	8	11	12	10
	4	4	5	6	7	9	8	10	11	12	1	3	2
	5	5	6	4	8	7	9	11	12	10	2	1	3
	6	6	4	5	9	8	7	12	10	11	3	2	1
	7	7	8	9	10	11	12	1	2	3	4	5	6
	8	8	9	7	12	10	11	2	3	1	6	4	5
	9	9	7	8	11	12	10	3	1	2	5	6	4
	10	10	11	12	1	3	2	4	5	6	7	9	8
	11	11	12	10	2	1	3	5	6	4	8	7	9
	12	12	10	11	3	2	1	6	4	5	9	8	7

Observando as tabelas acima é imediato notar que temos em ambos os loops apenas um elemento de ordem 1, o par $(0, e)$, e apenas um de ordem 2, que é o par $(2, e)$. Temos dois elementos de ordem 3, correspondentes aos pares $(0, u)$ e $(0, u^2)$, confirmando que $(0, C_3) = \{(0, x) | x \in C_3\}$, em L_I e L_J , são isomorfos a C_3 . Existem seis elementos de ordem 4, correspondentes aos pares $(1, e), (1, u), (1, u^2), (3, e), (3, u)$ e $(3, u^2)$, e dois elementos de ordem 6, que são os pares $(2, u)$ e $(2, u^2)$.

Como a classificação dos grupos de ordem 12 é conhecida, concluímos, pelas ordens dos elementos, que L_I é isomorfo ao grupo $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$, o produto semidireto de $\mathbb{Z}_4$ por $\mathbb{Z}_3$.

Agora, por tudo que foi estabelecido na seção (3.1) temos que se $f : L_I \rightarrow L_J$ é um half-isomorfismo, então $f((0, e)) = ((0, e))$, pois $(0, e)$ é o único elemento de ordem 1, e $f((2, e)) = ((2, e))$, pois $(2, e)$ é o único elemento de ordem 2. Da definição de f' e da demonstração do lema (3.13) temos que $f((0, x)) = (0, f'(x))$ e $f((2, x)) = (2, f'(x))$, para todo $x \in C_3$, com $f' : C_3 \rightarrow C_3$, sendo $f' = I$ ou $f' = J$, dadas por $I(x) = x$ e $J(x) = x^{-1}$.

Além disso, do Teorema (3.18), temos que se

$$f(1, x) = (1, af'(x^{\delta_a})),$$

então

$$f(3, x) = (3, af'(x^{\delta_a})), \text{ com } \delta_a \in \{1, -1\},$$

e se

$$f(1, x) = (3, af'(x^{\delta_a})),$$

então

$$f(3, x) = (1, af'(x^{\delta_a})), \text{ com } \delta_a \in \{1, -1\},$$

para cada $a \in C_3$.

Considerando ainda o lema (3.15), podemos então descrever todos os half-isomorfismos f em quatro famílias com 6 half-isomorfismos cada, pelas seguintes expressões:

$$f_{+a}^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (1, af'(x)), & \text{se } i = 1, \\ (3, af'(x)), & \text{se } i = 3. \end{cases} \quad f_{-a}^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (1, af'(x^{-1})), & \text{se } i = 1, \\ (3, af'(x^{-1})), & \text{se } i = 3. \end{cases}$$

$$f_{+a}^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (3, af'(x)), & \text{se } i = 1, \\ (1, af'(x)), & \text{se } i = 3. \end{cases} \quad f_{-a}^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (3, af'(x^{-1})), & \text{se } i = 1, \\ (1, af'(x^{-1})), & \text{se } i = 3. \end{cases}$$

De fato, são 6 half-isomorfismos para cada uma das famílias de funções f_{+a}^1 , f_{-a}^1 , f_{+a}^2 e f_{-a}^2 , totalizando 24 half-isomorfismos, pois temos duas possibilidades para f' , I ou J , e temos três possibilidades para a , pois a pode ser qualquer um dos elementos em C_3 .

A proposição abaixo é similar ao Teorema (3.20) com as devidas adaptações.

Proposição 3.22. *Seja $f' : C_3 \rightarrow C_3$, $f' = I$ ou $f' = J$, dadas por $I(x) = x$ e $J(x) = x^{-1}$. Então, para cada $a \in C_3$, temos que*

$$f_{+a}^1 : L_I \rightarrow L_J, \quad f_{-a}^1 : L_I \rightarrow L_J, \quad f_{+a}^2 : L_I \rightarrow L_J \quad \text{e} \quad f_{-a}^2 : L_I \rightarrow L_J$$

são half-isomorfismos não triviais.

Por fim listamos todos os half-isomorfismos descritos até agora usando a notação clássica de permutações.

(i) Para f_{+a}^1 .

Fixando $f' = I$ temos,

- para $a = e$, $f_1 = (1)$, é a função identidade em $\mathbb{Z}_4 \times C_3$;
- para $a = u$, $f_2 = (4 \ 5 \ 6)(10 \ 11 \ 12)$;
- para $a = u^2$, $f_3 = (4 \ 6 \ 5)(10 \ 12 \ 11)$.

Fixando $f' = J$ temos,

- para $a = e$, $f_4 = (2 \ 3)(8 \ 9)$;
- para $a = u$, $f_5 = (2 \ 3)(8 \ 9)(4 \ 5 \ 6)(10 \ 11 \ 12)$;
- para $a = u^2$, $f_6 = (2 \ 3)(8 \ 9)(4 \ 6 \ 5)(10 \ 12 \ 11)$.

(ii) Para f_{-a}^1 .

Fixando $f' = I$ temos,

- para $a = e$, $f_7 = (5 \ 6)(11 \ 12)$;
- para $a = u$, $f_8 = (4 \ 5)(10 \ 11)$;
- para $a = u^2$, $f_9 = (4 \ 6)(10 \ 12)$.

Fixando $f' = J$ temos,

- para $a = e$, $f_{10} = (2 \ 3)(8 \ 9)(5 \ 6)(11 \ 12)$;
- para $a = u$, $f_{11} = (2 \ 3)(8 \ 9)(4 \ 5)(10 \ 11)$;
- para $a = u^2$, $f_{12} = (2 \ 3)(8 \ 9)(4 \ 6)(10 \ 12)$.

(iii) Para f_{+a}^2 .

Fixando $f' = I$ temos,

- para $a = e$, $f_{13} = (4\ 10)(5\ 11)(6\ 12)$;
- para $a = u$, $f_{14} = (4\ 11\ 6\ 10\ 5\ 12)$;
- para $a = u^2$, $f_{15} = (4\ 12\ 5\ 10\ 6\ 11)$.

Fixando $f' = J$ temos,

- para $a = e$, $f_{16} = (2\ 3)(8\ 9)(4\ 10)(5\ 11)(6\ 12)$;
- para $a = u$, $f_{17} = (2\ 3)(8\ 9)(4\ 11\ 6\ 10\ 5\ 12)$;
- para $a = u^2$, $f_{18} = (2\ 3)(8\ 9)(4\ 12\ 5\ 10\ 6\ 11)$.

(iv) Para f_{-a}^2 .

Fixando $f' = I$ temos,

- para $a = e$, $f_{19} = (4\ 10)(5\ 12)(6\ 11)$;
- para $a = u$, $f_{20} = (4\ 11)(5\ 10)(6\ 12)$;
- para $a = u^2$, $f_{21} = (4\ 12)(5\ 11)(6\ 10)$.

Fixando $f' = J$ temos,

- para $a = e$, $f_{22} = (2\ 3)(8\ 9)(4\ 10)(5\ 12)(6\ 11)$;
- para $a = u$, $f_{23} = (2\ 3)(8\ 9)(4\ 11)(5\ 10)(6\ 12)$;
- para $a = u^2$, $f_{24} = (2\ 3)(8\ 9)(4\ 12)(5\ 11)(6\ 10)$.

Analisando esses half-isomorfismos é simples verificar que eles formam um grupo com a operação composição.

Temos então um grupo com 24 elementos onde f_1 é a identidade, logo tem ordem 1. Além disso, f_2 e f_3 têm ordem 3. Os elementos

$$f_4, f_7, f_8, f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{16}, f_{19}, f_{20}, f_{21}, f_{22}, f_{23} \text{ e } f_{24}$$

têm ordem 2 e os elementos

$$f_5, f_6, f_{14}, f_{15}, f_{17} \text{ e } f_{18}$$

têm ordem 6. Pelas ordens dos elementos, vemos que esse grupo é isomorfo ao grupo $C_2 \times C_2 \times S_3$.

Ao obtermos esses half-isomorfismos temos que as funções $f_i^{-1} : L_J \rightarrow L_I$, para todo i , $1 \leq i \leq 24$, são os half-isomorfismos de L_J em L_I . Portanto o grupo desses half-isomorfismos é o mesmo descrito acima.

Concluimos observando que, por considerações totalmente análogas as que foram feitas nas seções anteriores, podemos enunciar uma proposição similar ao Teorema (3.21).

Proposição 3.23. *Seja $f' : C_3 \rightarrow C_3$ um automorfismo e $a \in C_3$, então*

$$f_{+a}^1 : L_J \rightarrow L_J, \quad f_{-a}^1 : L_J \rightarrow L_J, \quad f_{+a}^2 : L_J \rightarrow L_J \quad \text{e} \quad f_{-a}^2 : L_J \rightarrow L_J$$

são half-automorfismos triviais para todo $a \in C_3$. Além disso f_{+a}^1 e f_{+a}^2 determinam 6 isomorfismos cada, enquanto que f_{-a}^1 e f_{-a}^2 determinam 6 anti-isomorfismos cada.

Por fim vale ressaltar que as leis de formação dos half-isomorfismos de $f : L_\alpha \rightarrow L_\beta$, no caso em que $L_\alpha = Dih(4, C_3, \alpha)$ e $L_\beta = Dih(4, C_3, \beta)$, onde naturalmente $\alpha = I$ ou $\alpha = J$ e $\beta = I$ ou $\beta = J$, são exatamente as que estão descritas nessa seção.

Vamos tratar agora o caso $m = 6$. Relembremos o conjunto

$$\mathbb{Z}_6 \times C_3 = \{(0, e), (0, u), (0, u^2), (1, e), (1, u), (1, u^2), (2, e), (2, u), (2, u^2), (3, e), (3, u), (3, u^2), \\ (4, e), (4, u), (4, u^2), (5, e), (5, u), (5, u^2)\}.$$

Novamente faremos uma adaptação da notação usada até aqui, escrevendo

$$\mathbb{Z}_6 \times C_3 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 14, 15, 16, 17, 18\},$$

de forma que os elementos

$$(0, e), (0, u), (0, u^2), (1, e), \dots, (5, e), (5, u) \text{ e } (5, u^2)$$

vão ser substituídos por $1, 2, 3, \dots, 17, 18$, respectivamente.

Loop L_I :

$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	3	1	6	4	5	8	9	7	12	10	11	14	15	13	18	16	17
3	3	1	2	5	6	4	9	7	8	11	12	10	15	13	14	17	18	16
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	1	2	3
5	5	6	4	9	7	8	11	12	10	15	13	14	17	18	16	3	1	2
6	6	4	5	8	9	7	12	10	11	14	15	13	18	16	17	2	3	1
7	7	8	9	10	11	12	13	14	15	16	17	18	1	2	3	4	5	6
8	8	9	7	12	10	11	14	15	13	18	16	17	2	3	1	6	4	5
9	9	7	8	11	12	10	15	13	14	17	18	16	3	1	2	5	6	4
10	10	11	12	13	14	15	16	17	18	1	2	3	4	5	6	7	8	9
11	11	12	10	15	13	14	17	18	16	3	1	2	5	6	4	9	7	8
12	12	10	11	14	15	13	18	16	17	2	3	1	6	4	5	8	9	7
13	13	14	15	16	17	18	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	13	18	16	17	2	3	1	6	4	5	8	9	7	12	10	11
15	15	13	14	17	18	16	3	1	2	5	6	4	9	7	8	11	12	10
16	16	17	18	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	16	3	1	2	5	6	4	9	7	8	11	12	10	15	13	14
18	18	16	17	2	3	1	6	4	5	8	9	7	12	10	11	14	15	13

Loop L_J :

$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	3	1	6	4	5	8	9	7	12	10	11	14	15	13	18	16	17
3	3	1	2	5	6	4	9	7	8	11	12	10	15	13	14	17	18	16
4	4	5	6	7	9	8	10	11	12	13	15	14	16	17	18	1	3	2
5	5	6	4	8	7	9	11	12	10	14	13	15	17	18	16	2	1	3
6	6	4	5	9	8	7	12	10	11	15	14	13	18	16	17	3	2	1
7	7	8	9	10	11	12	13	14	15	16	17	18	1	2	3	4	5	6
8	8	9	7	12	10	11	14	15	13	18	16	17	2	3	1	6	4	5
9	9	7	8	11	12	10	15	13	14	17	18	16	3	1	2	5	6	4
10	10	11	12	13	15	14	16	17	18	1	3	2	4	5	6	7	9	8
11	11	12	10	14	13	15	17	18	16	2	1	3	5	6	4	8	7	9
12	12	10	11	15	14	13	18	16	17	3	2	1	6	4	5	9	8	7
13	13	14	15	16	17	18	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	13	18	16	17	2	3	1	6	4	5	8	9	7	12	10	11
15	15	13	14	17	18	16	3	1	2	5	6	4	9	7	8	11	12	10
16	16	17	18	1	3	2	4	5	6	7	9	8	10	11	12	13	15	14
17	17	18	16	2	1	3	5	6	4	8	7	9	11	12	10	14	13	15
18	18	16	17	3	2	1	6	4	5	9	8	7	12	10	11	15	14	13

Das tabelas dos loops L_I e L_J , é imediato notar que $o((0, e)) = 1$ e $o((3, e)) = o((3, u)) = o((3, u^2)) = 2$. Além disso, o conjunto

$$\{(0, x) \mid x \in C_3\}, \text{ que vamos indicar por } (0, C_3),$$

é isomorfo a C_3 .

Note também que, em ambos os loops L_I e L_J , os elementos dos conjuntos $(1, C_3) = \{(1, x) \mid x \in C_3\}$ e $(5, C_3) = \{(5, x) \mid x \in C_3\}$ têm ordem 6 e os elementos dos conjuntos $(2, C_3) = \{(2, x) \mid x \in C_3\}$ e $(4, C_3) = \{(4, x) \mid x \in C_3\}$ têm ordem 3.

Como a classificação dos grupos de ordem 18 é conhecida, concluímos, pelas ordens dos elementos, que L_I é isomorfo ao grupo $C_3 \times S_3$.

Agora, observemos que se $f : L_I \rightarrow L_J$ é um half-isomorfismo, então $f((0, e)) = ((0, e))$, da definição de f' e da demonstração do lema (3.13), temos que $f((0, x)) = (0, f'(x))$, $f((2, x)) = (2, f'(x))$ e $f((4, x)) = (4, f'(x))$ ou $f((2, x)) = (4, f'(x))$ e $f((4, x)) = (2, f'(x))$, para todo $x \in C_3$, com $f' : C_3 \rightarrow C_3$, sendo $f' = I$ ou $f' = J$.

Além disso, do Teorema (3.19), temos que $f((3, x)) = (3, af'(x))$ e se

$$f(1, x) = (1, af'(x^{\delta_a})),$$

então

$$f(5, x) = (5, af'(x^{\delta_a})), \text{ com } \delta_a \in \{1, -1\},$$

e se

$$f(1, x) = (5, af'(x^{\delta_a})),$$

então

$$f(5, x) = (1, af'(x^{\delta_a})), \text{ com } \delta_a \in \{1, -1\},$$

para cada $a \in C_3$.

Observe então que isso também resume a descrição de $8 \times 3 = 24$ possibilidades para os half-isomorfismos que estamos procurando e que podemos identificar as possibilidades de f em quatro famílias com 6 half-isomorfismos cada, pelas seguintes expressões:

$$f_{+a}^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (4, f'(x)), & \text{se } i = 4, \\ (1, af'(x)), & \text{se } i = 1, \\ (3, af'(x)), & \text{se } i = 3, \\ (5, af'(x)), & \text{se } i = 5. \end{cases} \quad f_{-a}^1((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 2, \\ (4, f'(x)), & \text{se } i = 4, \\ (1, af'(x^{-1})), & \text{se } i = 1, \\ (3, af'(x^{-1})), & \text{se } i = 3, \\ (5, af'(x^{-1})), & \text{se } i = 5. \end{cases}$$

$$f_{+a}^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 4, \\ (4, f'(x)), & \text{se } i = 2, \\ (5, af'(x)), & \text{se } i = 1, \\ (3, af'(x)), & \text{se } i = 3, \\ (1, af'(x)), & \text{se } i = 5. \end{cases} \quad f_{-a}^2((i, x)) = \begin{cases} (0, f'(x)), & \text{se } i = 0, \\ (2, f'(x)), & \text{se } i = 4, \\ (4, f'(x)), & \text{se } i = 2, \\ (5, af'(x^{-1})), & \text{se } i = 1, \\ (3, af'(x^{-1})), & \text{se } i = 3, \\ (1, af'(x^{-1})), & \text{se } i = 5. \end{cases}$$

De fato, são quatro famílias com 6 funções cada, pois a pode assumir um dos três valores de C_3 , e , u ou u^2 e f' pode ser igual a I ou J , logo temos $3 \times 2 = 6$ possibilidades para cada uma das famílias de funções f_{+a}^1 , f_{-a}^1 , f_{+a}^2 e f_{-a}^2 .

A proposição abaixo é similar ao Teorema (3.20) com as devidas adaptações.

Proposição 3.24. *Sejam $f' : C_3 \rightarrow C_3$ um automorfismo e $a \in C_3$, então*

$$f_{+a}^1 : L_I \rightarrow L_J, \quad f_{-a}^1 : L_I \rightarrow L_J, \quad f_{+a}^2 : L_I \rightarrow L_J \quad \text{e} \quad f_{-a}^2 : L_I \rightarrow L_J$$

são half-isomorfismos não triviais para todo $a \in C_3$.

Por fim listamos todos os half-isomorfismos descritos no caso em que $m = 6$ usando a notação clássica de permutações.

(i) Para f_{+a}^1 .

Fixando $f' = I$ temos,

- para $a = e$, $f_1 = (1)$, é a função identidade em $\mathbb{Z}_6 \times C_3$;
- para $a = u$, $f_2 = (4 \ 5 \ 6)(10 \ 11 \ 12)(16 \ 17 \ 18)$;
- para $a = u^2$, $f_3 = (4 \ 6 \ 5)(10 \ 12 \ 11)(16 \ 18 \ 17)$.

Fixando $f' = J$ temos,

- para $a = e$, $f_4 = (2 \ 3)(8 \ 9)(14 \ 15)(5 \ 6)(11 \ 12)(17 \ 18)$;
- para $a = u$, $f_5 = (2 \ 3)(8 \ 9)(14 \ 15)(4 \ 5)(10 \ 11)(16 \ 17)$;
- para $a = u^2$, $f_6 = (2 \ 3)(8 \ 9)(14 \ 15)(4 \ 6)(10 \ 12)(16 \ 18)$.

(ii) Para f_{-a}^1 .

Fixando $f' = I$ temos,

- para $a = e$, $f_7 = (5 \ 6)(11 \ 12)(17 \ 18)$;

- para $a = u$, $f_8 = (4\ 5)(10\ 11)(16\ 17)$;
- para $a = u^2$, $f_9 = (4\ 6)(10\ 12)(16\ 18)$.

Fixando $f' = J$ temos,

- para $a = e$, $f_{10} = (2\ 3)(8\ 9)(14\ 15)$;
- para $a = u$, $f_{11} = (2\ 3)(8\ 9)(14\ 15)(4\ 5\ 6)(10\ 11\ 12)(16\ 17\ 18)$;
- para $a = u^2$, $f_{12} = (2\ 3)(8\ 9)(14\ 15)(4\ 6\ 5)(10\ 12\ 11)(16\ 18\ 17)$.

(iii) Para f_{+a}^2 .

Fixando $f' = I$ temos,

- para $a = e$, $f_{13} = (4\ 16)(5\ 17)(6\ 18)(7\ 13)(8\ 14)(9\ 15)$;
- para $a = u$, $f_{14} = (4\ 17\ 6\ 16\ 5\ 18)(10\ 11\ 12)(7\ 13)(8\ 14)(9\ 15)$;
- para $a = u^2$, $f_{15} = (4\ 18\ 5\ 16\ 6\ 17)(10\ 12\ 11)(7\ 13)(8\ 14)(9\ 15)$.

Fixando $f' = J$ temos,

- para $a = e$, $f_{16} = (2\ 3)(7\ 13)(8\ 15)(9\ 14)(4\ 16)(5\ 18)(6\ 17)(11\ 12)$;
- para $a = u$, $f_{17} = (2\ 3)(7\ 13)(8\ 15)(9\ 14)(4\ 17)(5\ 16)(6\ 18)(10\ 11)$;
- para $a = u^2$, $f_{18} = (2\ 3)(7\ 13)(8\ 15)(9\ 14)(4\ 18)(5\ 17)(6\ 16)(10\ 12)$.

(iv) Para f_{-a}^2 .

Fixando $f' = I$ temos,

- para $a = e$, $f_{19} = (7\ 13)(8\ 14)(9\ 15)(4\ 16)(5\ 18)(6\ 17)(11\ 12)$;
- para $a = u$, $f_{20} = (7\ 13)(8\ 14)(9\ 15)(4\ 17)(5\ 16)(6\ 18)(10\ 11)$;
- para $a = u^2$, $f_{21} = (7\ 13)(8\ 14)(9\ 15)(4\ 18)(5\ 17)(6\ 16)(10\ 12)$.

Fixando $f' = J$ temos,

- para $a = e$, $f_{22} = (2\ 3)(14\ 15)(8\ 9)$;
- para $a = u$, $f_{23} = (2\ 3)(7\ 13)(8\ 15)(9\ 14)(10\ 11\ 12)(4\ 17\ 6\ 16\ 5\ 18)$;
- para $a = u^2$, $f_{24} = (2\ 3)(7\ 13)(8\ 15)(9\ 14)(10\ 12\ 11)(4\ 18\ 5\ 16\ 6\ 17)$.

Analisando esses half-isomorfismos é simples verificar que eles formam um grupo com a operação composição.

Temos então um grupo com 24 elementos onde f_1 é a identidade, logo tem ordem 1. Além disso, f_2 e f_3 têm ordem 3. Os elementos

$$f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{13}, f_{16}, f_{17}, f_{18}, f_{19}, f_{20}, f_{21} \text{ e } f_{22}$$

têm ordem 2 e os elementos

$$f_{11}, f_{12}, f_{14}, f_{15}, f_{23} \text{ e } f_{24}$$

têm ordem 6. Novamente, pelas ordens dos elementos, vemos que esse grupo é isomorfo ao grupo $C_2 \times C_2 \times S_3$.

Análogo ao que observamos para o loop $Dih(4, C_3, \alpha)$, ao obtermos esses half-isomorfismos temos que as funções $f_i^{-1} : L_J \rightarrow L_I$, para todo i , $1 \leq i \leq 24$, são os half-isomorfismos de L_J em L_I . Portanto o grupo desses half-isomorfismos é o mesmo descrito acima.

Concluimos observando que, por considerações totalmente análogas as que foram feitas nas seções anteriores, podemos enunciar, também para esse loop, uma proposição similar ao Teorema (3.21).

Proposição 3.25. *Seja $f' : C_3 \rightarrow C_3$ um automorfismo e $a \in C_3$, então*

$$f_{+a}^1 : L_J \rightarrow L_J, \quad f_{-a}^1 : L_J \rightarrow L_J, \quad f_{+a}^2 : L_J \rightarrow L_J \text{ e } f_{-a}^2 : L_J \rightarrow L_J$$

são half-automorfismos triviais para todo $a \in C_3$. Além disso f_{+a}^1 e f_{+a}^2 determinam 6 isomorfismos cada, enquanto que f_{-a}^1 e f_{-a}^2 determinam 6 anti-isomorfismos cada.

Por fim, também vale ressaltar que as leis de formação dos half-isomorfismos de $f : L_\alpha \rightarrow L_\beta$, no caso em que $L_\alpha = Dih(6, C_3, \alpha)$ e $L_\beta = Dih(6, C_3, \beta)$, onde naturalmente $\alpha = I$ ou $\alpha = J$ e $\beta = I$ ou $\beta = J$, são exatamente as que estão descritas nessa seção.

4

HALF-ISOMORFISMOS ENTRE OS A-LOOPS DIEDRAIS $Dih(m, C_p, \alpha)$: O CASO GERAL

Neste capítulo vamos generalizar os resultados obtidos no capítulo 3. Consideraremos os loops $Dih(m, C_p, \alpha)$, onde $p > 2$ é um número primo e m é um inteiro par maior ou igual a 2.

4.1 LOOPS AUTOMÓRFICOS DIEDRAIS $Dih(m, C_p, \alpha)$

Iniciaremos reapresentando a definição (3.3).

Definição 4.1. *Sejam C_p o grupo cíclico de ordem p , tal que $p > 2$ é primo, m um inteiro par positivo e $\alpha : C_p \rightarrow C_p$ um automorfismo. Definimos o loop diedral $Dih(m, C_p, \alpha)$ com a operação $*$ sobre $\mathbb{Z}_m \times C_p$, dada por*

$$(i, u) * (j, v) = (i + j, (u^{(-1)^j} v) \alpha^{ij}),$$

onde $u, v \in C_p$ e $i, j \in \mathbb{Z}_m$.

Como observamos no início do capítulo 3, os automorfismos de C_p a serem considerados são apenas $\alpha = I$ e $\alpha = J$, onde I é a função identidade e $J(x) = x^{-1}$ é a função inversão.

Agora consideraremos as notações $C_p = \{e, u, u^2, \dots, u^{p-1}\}$ e $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ e teremos o conjunto

$$\begin{aligned} \mathbb{Z}_m \times C_p = \{ & (0, e), (0, u), (0, u^2), \dots, (0, u^{p-1}), (1, e), (1, u), (1, u^2), \dots, (1, u^{p-1}), \dots \\ & \dots, (m-2, u^{p-1}), (m-1, e), (m-1, u), (m-1, u^2), \dots, (m-1, u^{p-1}) \}. \end{aligned}$$

Nessa seção

L_I representará o loop $Dih(m, C_p, I)$

e

L_J representará o loop $Dih(m, C_p, J)$.

É imediato notar que em ambos, L_I e L_J , $o((0, e)) = 1$ e como $(\frac{m}{2}, e)(\frac{m}{2}, e) = (0, e)$, temos $o((\frac{m}{2}, e)) = 2$.

Além disso $o(x) = p$, para todo $x \in C_p$, $x \neq e$, e assim $o((0, x)) = o(x) = p$ para todo $(0, x) \in (0, C_p)$, $(0, x) \neq (0, e)$. Logo, o conjunto $(0, C_p) = \{(0, x) \mid x \in C_p\}$ é isomorfo a C_p .

Doravante as próximas proposições seguirão estabelecendo mais informações sobre as ordens dos elementos de L_I e L_J .

Proposição 4.2. *Seja $(\frac{m}{2}, C_p) = \{(\frac{m}{2}, x) \mid x \in C_p\}$, subconjunto de $\mathbb{Z}_m \times C_p$. Então em ambos, L_I e L_J , os elementos $(\frac{m}{2}, x)$, tais que $x \neq e$, têm ordem $2p$ quando $\frac{m}{2}$ for par e têm ordem 2 quando $\frac{m}{2}$ for ímpar.*

Demonstração. Considere $(\frac{m}{2}, x) \in (\frac{m}{2}, C_p)$, $x \neq e$. Veja que, tanto em L_I como em L_J , se $\frac{m}{2}$ for par, temos

$$\left(\frac{m}{2}, x\right) \left(\frac{m}{2}, x\right) = (0, x^2),$$

e se $\frac{m}{2}$ for ímpar, temos

$$\left(\frac{m}{2}, x\right) \left(\frac{m}{2}, x\right) = (0, x^{-1}x) = (0, e).$$

Dessa forma a ordem de $(\frac{m}{2}, x)$ é 2, para $\frac{m}{2}$ ímpar, $\forall x \in C_p$.

Para $\frac{m}{2}$ par, vamos provar que a ordem de $(\frac{m}{2}, x)$, $x \neq e$, é $2p$. Provaremos primeiro que

$$\left(\frac{m}{2}, x\right)^\lambda = (0, x^\lambda), \text{ se } \lambda \text{ é um número natural par,}$$

e

$$\left(\frac{m}{2}, x\right)^\lambda = \left(\frac{m}{2}, x^\lambda\right), \text{ se } \lambda \text{ é um número natural ímpar.}$$

Faremos por indução sobre λ . Temos

$$\left(\frac{m}{2}, x\right)^2 = \left(\frac{m}{2}, x\right) \left(\frac{m}{2}, x\right) = (0, x^2).$$

Suponhamos

$$\left(\frac{m}{2}, x\right)^\lambda = (0, x^\lambda),$$

para λ número natural par maior do que 2. Temos então:

$$(0, x^\lambda) \left(\frac{m}{2}, x \right) = \left(\frac{m}{2}, x^{\lambda+1} \right)$$

e assim

$$\left(\frac{m}{2}, x \right)^{\lambda+2} = \left(\frac{m}{2}, x^{\lambda+1} \right) \left(\frac{m}{2}, x \right) = (0, x^{\lambda+2}).$$

Isso demonstra o que queríamos para λ par.

Vejamos agora que

$$\left(\frac{m}{2}, x \right)^1 = \left(\frac{m}{2}, x^1 \right)$$

e que

$$\left(\frac{m}{2}, x \right)^3 = (0, x^2) \left(\frac{m}{2}, x \right) = \left(\frac{m}{2}, x^3 \right).$$

Suponhamos que

$$\left(\frac{m}{2}, x \right)^\lambda = \left(\frac{m}{2}, x^\lambda \right),$$

para λ número natural ímpar maior do que 3. Temos então:

$$\left(\frac{m}{2}, x \right)^{\lambda+1} = \left(\frac{m}{2}, x^\lambda \right) \left(\frac{m}{2}, x \right) = (0, x^{\lambda+1})$$

e assim

$$\left(\frac{m}{2}, x \right)^{\lambda+2} = (0, x^{\lambda+1}) \left(\frac{m}{2}, x \right) = \left(\frac{m}{2}, x^{\lambda+2} \right).$$

Isso demonstra o que queríamos para λ ímpar.

Concluimos que $\left(\frac{m}{2}, x \right)^\lambda = (0, e)$, se $\frac{m}{2}$ e λ são ambos pares e $x^\lambda = e$. Assim, como p é primo, o menor valor de λ que satisfaz essas condições é $\lambda = 2p$, pois $x^\lambda \neq e$ para todo λ tal que $1 < \lambda < p$ ou $p+1 < \lambda < 2p$. Portanto a ordem de $\left(\frac{m}{2}, x \right)$ é $2p$, para $\frac{m}{2}$ par. $\square$

Lema 4.3. *Sejam (i, x) e $(m-i, x)$, com $i \neq 0$, elementos de $Dih(m, C_p, \alpha)$. Então, em ambos, L_I e L_J , temos que*

- se i é ímpar,

$$(i, x)^\lambda = (\lambda i, e) \quad e \quad (m-i, x)^\lambda = (m-\lambda i, e), \text{ quando } \lambda \geq 2 \text{ é um inteiro par;}$$

e

$$(i, x)^\lambda = (\lambda i, x) \quad e \quad (m-i, x)^\lambda = (m-\lambda i, x), \text{ quando } \lambda \geq 3 \text{ é um inteiro ímpar;}$$

- se i é par,

$$(i, x)^\lambda = (\lambda i, x^\lambda) \quad e \quad (m-i, x)^\lambda = (m-\lambda i, x^\lambda), \text{ quando } \lambda \geq 3 \text{ é um inteiro positivo qualquer.}$$

Demonstração. (i) Para i ímpar vamos mostrar que

$$(i, x)^\lambda = (\lambda i, e), \text{ se } \lambda \text{ é par,}$$

e

$$(i, x)^\lambda = (\lambda i, x), \text{ se } \lambda \text{ é ímpar.}$$

Faremos por indução sobre λ . Vejamos que se $\lambda = 2$,

$$(i, x)^2 = (i, x)(i, x) = (2i, x^{-1}x) = (2i, e).$$

Suponhamos $(i, x)^\lambda = (\lambda i, e)$, para λ um número par maior do que 2. Como

$$(i, x)^{\lambda+1} = (\lambda i, e)(i, x) = (\lambda i + i, x),$$

temos

$$(i, x)^{\lambda+2} = (\lambda i + i, x)(i, x) = (\lambda i + 2i, e) = ((\lambda + 2)i, e).$$

Isso demonstra o que queríamos para λ par.

Observemos agora que se $\lambda = 1$, então $(i, x)^1 = (1 \cdot i, x)$. Suponhamos $(i, x)^\lambda = (\lambda i, x)$, para λ número ímpar maior do que 1. Como

$$(i, x)^{\lambda+1} = (\lambda i, x)(i, x) = (\lambda i + i, e),$$

temos

$$(i, x)^{\lambda+2} = (\lambda i + i, e)(i, x) = (\lambda i + 2i, x) = ((\lambda + 2)i, x).$$

Isso demonstra o que queríamos para λ ímpar.

Note que se i é ímpar, então $m - i$ também é ímpar. Portanto, do que foi demonstrado até aqui, temos que

$$(m - i, x)^\lambda = (\lambda(m - i), e) = (m - \lambda i, e), \text{ se } \lambda \text{ é par,}$$

e

$$(m - i, x)^\lambda = (\lambda(m - i), x) = (m - \lambda i, x), \text{ se } \lambda \text{ é ímpar.}$$

(ii) Para i par vamos mostrar que $(i, x)^\lambda = (\lambda i, x^\lambda)$. Faremos também por indução sobre λ . Vejamos que se $\lambda = 1$, $(i, x)^1 = (1 \cdot i, x^1)$. Suponhamos $(i, x)^\lambda = (\lambda i, x^\lambda)$, para λ número natural maior do que 1. Logo, como

$$(i, x)^{\lambda+1} = (\lambda i, x^\lambda)(i, x) = (\lambda i + i, x^{\lambda+1}),$$

temos

$$(i, x)^{\lambda+2} = (\lambda i + i, x^{\lambda+1})(i, x) = (\lambda i + 2i, x^{\lambda+2}) = ((\lambda + 2)i, x^{\lambda+2}).$$

Isso demonstra o que queríamos para i par.

Por fim temos que $(m - i, x)^\lambda = (m - \lambda i, x^\lambda)$, pois $m - i$ é par quando i é par. $\square$

Proposição 4.4. Para cada $i \in \mathbb{Z}_m$, $i \neq 0$, consideremos os subconjuntos de $\mathbb{Z}_m \times C_p$,

$$(i, C_p) = \{(i, x) \mid x \in C_p\} \text{ e } (m - i, C_p) = \{(m - i, x) \mid x \in C_p\}.$$

Então, em ambos, L_I e L_J , os elementos $(i, x) \in (i, C_p)$ e $(m - i, x) \in (m - i, C_p)$, têm as mesmas ordens.

Demonstração. (i) Consideremos primeiro i ímpar. Pelo lema (4.3), temos que $\lambda = o((i, x))$ é par, pois se λ fosse ímpar teríamos

$$(i, x)^\lambda = (\lambda i, x) \text{ e } (m - i, x)^\lambda = (m - \lambda i, x);$$

e assim $(\lambda i, x) \neq (0, e)$ e $(m - \lambda i, x) \neq (0, e)$, visto que se λi é ímpar e m é par, então $\lambda i \not\equiv 0 \pmod{m}$.

Logo, $o((i, x)) = o((m - i, x))$ é o menor número λ par tal que $\lambda i \equiv 0 \pmod{m}$. O fato de ser o menor número com essa propriedade garante a unicidade de λ .

(ii) Consideremos agora i par. Novamente pelo lema (4.3), temos que se $\lambda = o((i, x))$, então $(\lambda i, x^\lambda) = (0, e)$ e se $\lambda = o((m - i, x))$, então $(m - \lambda i, x^\lambda) = (0, e)$. Portanto, basta que tenhamos $\lambda i \equiv 0 \pmod{m}$, pois dessa forma teremos que $x^\lambda = e$. Novamente, $\lambda = o((i, x)) = o((m - i, x))$ é o menor número natural positivo, portanto o único, tal que $\lambda i \equiv 0 \pmod{m}$. $\square$

Corolário 4.5. As ordens dos elementos $(1, x)$ e $(m - 1, x)$, para $x \in C_p$, são iguais a m .

Demonstração. Pelo lema 4.3, se $\lambda = o((1, x))$, devemos ter $(1, x)^\lambda = (\lambda, e) = (0, e)$. Ou seja, devemos ter que λ é o menor natural positivo tal que $\lambda \equiv 0 \pmod{m}$. Logo, $\lambda = m$. Pela proposição anterior temos o resultado. $\square$

Teorema 4.6. Sejam $o((i, x))$, a ordem do elemento (i, x) em $Dih(m, C_p, \alpha)$, e $o(i)$, a ordem do elemento i em $\mathbb{Z}_m$. Então,

- $o((i, e)) = o(i)$, $\forall i \in \mathbb{Z}_m$;

- se i é ímpar, temos que

$$o((i, x)) = o(i) \text{ é um número natural par;}$$

- e se i é par temos que

$$o((i, x)) = o(i), \forall i \neq 0, \text{ quando } p \text{ divide } m,$$

e

$$o((i, x)) = o(i) \cdot p, \forall x \neq e, \text{ quando } p \text{ não divide } m.$$

Demonstração. Inicialmente observemos que, devido ao lema 4.3, $(i, e)^\lambda = (\lambda i, e)$, para qualquer número natural λ . Dessa forma, se $\lambda = o((i, x))$, então $\lambda i \equiv 0 \pmod{m}$, logo $\lambda = o((i, x)) = o(i)$.

Consideremos a seguir os outros dois casos.

Caso (i): i é ímpar.

Considerando novamente o lema 4.3, para $\lambda \geq 2$ par, temos que se $\lambda = o((i, x))$, então $(i, x)^\lambda = (\lambda i, e) = (0, e)$, ou seja, temos que $\lambda i \equiv 0 \pmod{m}$, mas isso significa exatamente que $\lambda = o(i)$. Portanto, $\lambda = o((i, x)) = o(i)$ é um número natural par.

Agora se $\lambda \geq 3$ também é ímpar, teríamos $(i, x)^\lambda = (\lambda i, x)$. Logo, se $\lambda = o((i, x))$ teríamos $(\lambda i, x) = (0, e)$ e novamente $\lambda i \equiv 0 \pmod{m}$, mas isso não é possível para m par e λ e i ímpares.

Caso (ii): i é par.

Consideremos que p divide m . Se $i \neq 0$, temos que $(i, x)^\lambda = (\lambda i, x^\lambda)$. Dessa forma, se $\lambda = o((i, x))$, devemos ter $(\lambda i, x^\lambda) = (0, e)$, ou seja, devemos ter $\lambda i \equiv 0 \pmod{m}$ e $x^\lambda = e$. Note então que $o(i)i \equiv 0 \pmod{m}$ e, como p divide m , temos $x^{o(i)i} = x^m = x^{kp} = e$, onde k é um número natural. Portanto, $\lambda = o((i, x)) = o(i)$.

Consideremos agora que p não divide m . Suponhamos $x \neq e$ e $i \neq 0$. Se $\lambda = o((i, x))$, temos

$$(i, x)^\lambda = (\lambda i, x^\lambda) = (0, e),$$

ou seja, devemos ter $\lambda i \equiv 0 \pmod{m}$ e $x^\lambda = e$. Mas, se $0 < \lambda < o(i)$, temos que $\lambda i \not\equiv 0 \pmod{m}$ e se $0 < \lambda < p$, temos que $x^\lambda \neq e$. Portanto, como p não divide m , o menor inteiro λ tal que $\lambda i \equiv 0 \pmod{m}$ e $x^\lambda = e$ é $\lambda = o((i, x)) = o(i) \cdot p$. $\square$

4.2 HALF-ISOMORFISMOS ENTRE OS LOOPS AUTOMÓRFICOS DIEDRAIS $Dih(m, C_p, \alpha)$

Como já fizemos anteriormente, vamos considerar as seguintes notações:

L_α representará o loop $Dih(m, C_p, \alpha)$,

L_β representará o loop $Dih(m, C_p, \beta)$,

onde $\alpha = I$ ou $\alpha = J$ e, igualmente, $\beta = I$ ou $\beta = J$.

Convém ressaltar que L_I é grupo e que Scott, em ([Sco57]), mostrou que todos os half-automorfismos de grupos são triviais.

Na primeira seção do capítulo observamos que em ambos os loops, L_I e L_J ,

$$(0, C_p) = \{(0, x) \mid x \in C_p\}$$

é isomorfo a C_p . Além disso, se $\frac{m}{2}$ for ímpar, em

$$\left(\frac{m}{2}, C_p\right) = \left\{\left(\frac{m}{2}, x\right) \mid x \in C_p\right\},$$

todos os elementos tem ordem 2. No entanto, para o caso em que $\frac{m}{2}$ é par, $(\frac{m}{2}, e)$ tem ordem 2, mas os outros elementos em $(\frac{m}{2}, C_p)$ têm ordem $2p$.

O lema a seguir é consequência desses fatos e da proposição (1.36).

Lema 4.7. *Dado um half-isomorfismo $f : L_\alpha \rightarrow L_\beta$, temos que $f((n, C_p)) = (n, C_p)$ para $n = 0 \in \mathbb{Z}_m$ e para $n = \frac{m}{2} \in \mathbb{Z}_m$.*

Considerando esse lema, podemos apresentar a definição a seguir, análoga a definição (3.12), porém válida para o caso geral.

Definição 4.8. *Seja $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo, então definimos a seguinte função bijetora: $f' : C_p \rightarrow C_p$, dada por $x \mapsto f'(x)$, tal que $f((0, x)) = (0, f'(x))$.*

Os fatos de que f' está bem definida, é bijetora e é um automorfismo de C_p verificam-se de forma totalmente análoga ao que foi feito para a definição (3.12).

Começaremos destacando uma peculiaridade do caso em que $\frac{m}{2}$ é par.

Lema 4.9. *Seja $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo, se $\frac{m}{2}$ é par, então $f((\frac{m}{2}, x)) = (\frac{m}{2}, f'(x))$, para todo $x \in C_p$.*

Demonstração. Considere $(\frac{m}{2}, x) \in (\frac{m}{2}, C_p)$, então,

$$f\left(\left(\frac{m}{2}, x\right)\left(\frac{m}{2}, x\right)\right) = f(0, x^2) = (0, f'(x^2)) = (0, (f'(x))^2).$$

Por outro lado, devido ao lema (4.7) podemos fazer $f\left(\left(\frac{m}{2}, x\right)\right) = \left(\frac{m}{2}, b\right)$, com $b \in C_p$, e teremos

$$f\left(\left(\frac{m}{2}, x\right)\left(\frac{m}{2}, x\right)\right) = f\left(\left(\frac{m}{2}, x\right)\right)f\left(\left(\frac{m}{2}, x\right)\right) = \left(\frac{m}{2}, b\right)\left(\frac{m}{2}, b\right) = (0, b^2).$$

Dessa forma, $(0, (f'(x))^2) = (0, b^2)$. Logo, $(f'(x))^2 = b^2 \in C_p$. Portanto, $f'(x) = b$ e assim $f\left(\left(\frac{m}{2}, x\right)\right) = \left(\frac{m}{2}, b\right) = \left(\frac{m}{2}, f'(x)\right)$. $\square$

Na próxima proposição vamos definir os half-isomorfismos $f : L_\alpha \rightarrow L_\beta$ por

$$f(i, u) = (f_1(i), f_2(i, u)).$$

Observe que, se $f(i, e) = (j, v)$, então temos

$$f(i, u) = f((i, e)(0, u)) = \begin{cases} (j, v)(0, f'(u)) = (j, v f'(u)), \\ (0, f'(u))(j, v) = (j, (f'(u))^{(-1)^j} v), \end{cases}$$

Note que f_1 não depende de u . Dessa forma f_1 está bem definida em consequência de f ser um half-isomorfismo.

Segue então a proposição:

Proposição 4.10. *Seja $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo dado por $f((i, u)) = (f_1(i), f_2(i, u))$. Então $f_1 : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ é um automorfismo.*

Demonstração. Por definição

$$f((i, u)(j, v)) = f((i + j, (u^{(-1)^j} v) \alpha^{ij})) = (f_1(i + j), f_2(i + j, (u^{(-1)^j} v) \alpha^{ij})).$$

Além disso,

$$f((i, u)(j, v)) = f((i, u))f((j, v)) \tag{1}$$

ou

$$f((i, u)(j, v)) = f((j, v))f((i, u)) \tag{2}$$

Assim, em (1), temos

$$\begin{aligned} f((i, u)(j, v)) &= f((i, u))f((j, v)) = (f_1(i), f_2(i, u))(f_1(j), f_2(j, v)) = \\ &= (f_1(i) + f_2(j), (f_2(i, u))^{(-1)^{f_1(j)}} f_2(j, v)) \beta^{f_1(i)f_1(j)}), \end{aligned}$$

logo $f_1(i + j) = f_1(i) + f_1(j)$.

Em (2) temos

$$\begin{aligned} f((i, u)(j, v)) &= f((j, v))f((i, u)) = (f_1(j), f_2(j, v))(f_1(i), f_2(i, u)) = \\ &= (f_1(j) + f_1(i), (f_2(j, v))^{(-1)^{f_1(i)}} f_2(i, u)) \beta^{f_1(j)f_1(i)}), \end{aligned}$$

e novamente $f_1(i + j) = f_1(i) + f_1(j)$.

O fato de f_1 ser bijetora decorre do fato de f ser bijetora. $\square$

O próximo Teorema caracteriza $f((i, x))$, onde $f : L_\alpha \rightarrow L_\beta$ é um half-isomorfismo, para o caso em que i é par.

Teorema 4.11. *Seja $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo, então, para todo $x \in C_p$ e para todo i par, $f((i, x)) = (f_1(i), f'(x))$, onde $f_1 : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ é um automorfismo.*

Demonstração. Do lema (4.9), quando $(\frac{m}{2})$ é par, temos que $f(\frac{m}{2}, x) = (\frac{m}{2}, f'(x))$ para todo $x \in C_p$. Então considere $i = \frac{m}{2} + k$, onde k é um inteiro par. Logo, $(i, x) = (\frac{m}{2} + k, x)$. Façamos então

$$f(i, x) = f\left(\left(\frac{m}{2} + k, x\right)\right) = f\left(\left(\frac{m}{2}, x\right)(k, e)\right).$$

Teremos então

$$\begin{aligned} f(i, x) &= f\left(\left(\frac{m}{2}, x\right)\right) f((k, e)) = \left(\frac{m}{2}, f'(x)\right) (f_1(k), e) = \\ &= \left(f_1\left(\frac{m}{2}\right) + f_1(k), f'(x)\right) = (f_1(i), f'(x)), \end{aligned}$$

ou então teremos,

$$\begin{aligned} f(i, x) &= f((k, e)) f\left(\left(\frac{m}{2}, x\right)\right) = (f_1(k), e) \left(\frac{m}{2}, f'(x)\right) = \\ &= \left(f_1\left(\frac{m}{2}\right) + f_1(k), f'(x)\right) = (f_1(i), f'(x)). \end{aligned}$$

$\square$

Para concluirmos as caracterizações dos half-isomorfismos $f : L_\alpha \rightarrow L_\beta$ precisamos do próximo lema.

Daqui para frente a representa um elemento de C_p arbitrário, porém fixado.

Lema 4.12. *Seja $g_a : L_\alpha \rightarrow L_\beta$ definida por*

$$g_a((i, x)) = \begin{cases} (f_1(i), f'(x)), & \text{se } i \text{ é par,} \\ (f_1(i), af'(x^{\delta_a})), & \text{se } i \text{ é um número ímpar e } \delta_a \in \{1, -1\}, \end{cases}$$

então, se $g_a((i, x)) = (f_1(i), af'(x))$ e $g_a((j, y)) = (f_1(j), af'(y^{-1}))$, onde $i \neq j$ são ímpares, temos que g_a não é half-isomorfismo de L_α em L_β , para qualquer $a \in C_p$.

Demonstração. Mostraremos para o caso em que $\beta = J$, o caso em que $\beta = I$ é análogo. Vejamos primeiro que

$$g_a((i, x)(j, y)) = g_a((i + j, (x^{-1}y)J)) = g_a((i + j, y^{-1}x)) = (f_1(i + j), f'(y^{-1}x)).$$

Por outro lado,

$$\begin{aligned} g_a((i, x))g_a((j, y)) &= (f_1(i), af'(x))(f_1(j), af'(y^{-1})) = (f_1(i + j), (a^{-1}f'(x^{-1})af'(y^{-1}))J) = \\ &= (f_1(i + j), f'(y)f'(x)) = (f_1(i + j), f'(yx)) \end{aligned}$$

e

$$\begin{aligned} g_a((j, y))g_a((i, x)) &= (f_1(j), af'(y^{-1}))(f_1(i), af'(x)) = (f_1(i + j), (a^{-1}f'(y)af'(x))J) = \\ &= (f_1(i + j), f'(x^{-1})f'(y^{-1})) = (f_1(i + j), f'(x^{-1}y^{-1})). \end{aligned}$$

Dessa forma, se $g_a((i, x)(j, y)) = g_a((i, x))g_a((j, y))$, então $f'(y^{-1}x) = f'(yx)$ e assim $f'(y^{-1}) = f'(y)$, logo $y^{-1} = y$. Outrossim, se $g_a((i, x)(j, y)) = g_a((j, y))g_a((i, x))$, então $f'(y^{-1}x) = f'(y^{-1}x^{-1})$ e assim $f'(x) = f'(x^{-1})$, logo $x = x^{-1}$. Portanto, basta tomar $x, y \in C_p$ tal que $x \neq e$ ou $y \neq e$. Logo, $g_a : L_\alpha \rightarrow L_\beta$ não é half-isomorfismo. $\square$

Agora podemos dar um passo significativo na direção de caracterizar todos os half-isomorfismos de L_α em L_β , com $\alpha \neq \beta$, e mostrar que todos são não triviais.

Teorema 4.13. *Sejam $f : L_\alpha \rightarrow L_\beta$ um half-isomorfismo denotado por $f(i, u) = (f_1(i), f_2(u))$ onde $f_1 : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ é um automorfismo. Então existe $a \in C_p$ tal que:*

$$f((i, x)) = \begin{cases} (f_1(i), f'(x)), & \text{se } i \text{ é par,} \\ (f_1(i), af'(x^{\delta_a})), & \text{se } i \text{ é ímpar e } \delta_a \in \{1, -1\}. \end{cases}$$

Demonstração. Pelo Teorema (4.11) temos que

$$f((i, x)) = (f_1(i), f'(x)), \text{ se } i \text{ é par,}$$

qualquer que seja $x \in C_p$.

Segundo a proposição (4.10), podemos considerar $f(i, e) = (f_1(i), a)$ para algum $a \in C_p = \{e, u, u^2, \dots, u^{p-1}\}$.

Sendo assim, para i ímpar, temos

$$\begin{aligned} f(i, x) &= f((i, e)(0, x)) \in \{f((i, e))f((0, x)), f((0, x))f((i, e))\} = \\ &= \{(f_1(i), a)(0, f'(x)), (0, f'(x))(f_1(i), a)\} = \\ &= \{(f_1(i), af'(x)), (f_1(i), af'(x^{-1}))\}. \end{aligned}$$

Tendo em vista o lema (4.12), concluímos a demonstração. $\square$

Com a finalidade de descrever todos os half-isomorfismos entre L_α e L_β faz-se necessário destacar alguns fatos. Note que $|Aut \mathbb{Z}_m| = \varphi(m)$, onde $\varphi(m)$ é a função de Euler que nos dá a quantidade de números inteiros relativamente primos com m e menores do que m . Além disso, temos $\varphi(p) = p - 1$ valores de f' , 2 valores de δ_a e p valores de a , que são os elementos de C_p . Dessa forma, a quantidade total de half-isomorfismos entre os loops automórficos diedrais L_α e L_β é

$$2 \times \varphi(p) \times \varphi(m) \times p = 2\varphi(m)(p - 1)p.$$

Podemos portanto melhorar a notação identificando as possibilidades de f , em 2 famílias com $\varphi(m)(p - 1)p$ half-isomorfismos cada, pelas seguintes expressões:

$$f_{+a}((i, x)) = \begin{cases} (f_1(i), f'(x)), & \text{se } i \text{ é par,} \\ (f_1(i), af'(x)), & \text{se } i \text{ é ímpar,} \end{cases}$$

e

$$f_{-a}((i, x)) = \begin{cases} (f_1(i), f'(x)), & \text{se } i \text{ é par,} \\ (f_i(i), af'(x^{-1})), & \text{se } i \text{ é ímpar.} \end{cases}$$

Chegamos então ao principal resultado dessa seção.

Teorema 4.14. *Sejam $f' : C_p \rightarrow C_p$ e $f_1 : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ automorfismos. Então*

$$f_{+a} : L_\alpha \rightarrow L_\beta \text{ e } f_{-a} : L_\alpha \rightarrow L_\beta$$

são half-isomorfismos não triviais para cada $a \in C_p$, quando $\alpha \neq \beta$.

Demonstração. Provaremos caso a caso.

(i) Para a família de funções f_{+a} .

Considere j par.

Se i também é par, então temos:

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}((i + j, uv)) = (f_1(i + j), f'(uv)) = \\ &= (f_1(i), f'(u))(f_1(j), f'(v)) = f_{+a}((i, u))f_{+a}(j, v), \end{aligned}$$

ou seja,

$$f_{+a}((i, u)(j, v)) = f_{+a}((i, u))f_{+a}(j, v).$$

Agora, considere i ímpar, então temos:

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}((i + j, uv)) = (f_1(i + j), af'(uv)) = \\ &= (f_1(i), af'(u))(f_1(j), f'(v)) = f_{+a}((i, u))f_{+a}(j, v) \end{aligned}$$

ou seja

$$f_{+a}((i, u)(j, v)) = f_{+a}((i, u))f_{+a}(j, v)$$

Considere agora j ímpar.

Se i é par, então temos:

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}((i + j, u^{-1}v)) = (f_1(i + j), af'(u^{-1}v)) = (f_1(i) + f_1(j), af'(u^{-1})f'(v)) = \\ &= (f_1(i), f'(u))(f_1(j), af'(v)) = f_{+a}((i, u))f_{+a}((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}((i, u)(j, v)) = f_{+a}((i, u))f_{+a}((j, v)).$$

Se i é também ímpar, para o caso $L_I \rightarrow L_J$, temos

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}((i + j, u^{-1}v)) = (f_1(i + j), f'(u^{-1}v)) = (f_1(i) + f_1(j), f'(u^{-1})f'(v)) = \\ &= (f_1(i) + f_1(j), (a^{-1}f'(v^{-1})af'(u))J) = (f_1(j), af'(v))(f_1(i), af'(u)) = f_{+a}((j, v))f_{+a}((i, u)). \end{aligned}$$

Para o caso $L_J \rightarrow L_I$, temos

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}((i + j, (u^{-1}v)J)) = (f_1(i + j), f'(v^{-1}u)) = (f_1(i) + f_1(j), f'(v^{-1})f'(u)) = \\ &= (f_1(j) + f_1(i), a^{-1}f'(v^{-1})af'(u)) = (f_1(j), af'(v))(f_1(i), af'(u)) = f_{+a}((j, v))f_{+a}((i, u)) \end{aligned}$$

Logo, diferentemente dos casos anteriores, temos

$$f_{+a}((i, u)(j, v)) = f_{+a}((j, v))f_{+a}((i, u)).$$

Assim, está demonstrado que f_{+a} é uma família com $\varphi(m)(p-1)p$ half-isomorfismos não triviais.

(ii) Para a família de funções f_{-a} .

Considere j par.

Se i também é par, então temos:

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i+j, uv)) = (f_1(i+j), f'(uv)) = (f_1(i) + f_1(j), f'(u)f'(v)) = \\ &= (f_1(i), f'(u))(f_1(j), f'(v)) = f_{-a}((i, u))f_{-a}((j, v)). \end{aligned}$$

Ou seja,

$$f_{-a}((i, u)(j, v)) = f_{-a}((i, u))f_{-a}((j, v)).$$

Se i é ímpar, então temos:

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i+j, uv)) = (f_1(i+j), af'(v^{-1}u^{-1})) = (f_1(i) + f_1(j), af'(v^{-1})f'(u^{-1})) = \\ &= (f_1(j), f'(v))(f_1(i), af'(u^{-1})) = f_{-a}((j, v))f_{-a}((i, u)). \end{aligned}$$

Assim, diferente do caso em que i é par, temos

$$f_{-a}((i, u)(j, v)) = f_{-a}((j, v))f_{-a}((i, u)).$$

Considere j ímpar.

Se i é par, então temos

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i+j, u^{-1}v)) = (f_1(i+j), af'(v^{-1}u)) = (f_1(i) + f_1(j), af'(v^{-1})f'(u)) = \\ &= (f_1(j), af'(v^{-1}))(f_1(i), f'(u)) = f_{-a}((j, v))f_{-a}((i, u)). \end{aligned}$$

Temos então

$$f_{-a}((i, u)(j, v)) = f_{-a}((j, v))f_{-a}((i, u)).$$

Se i também é ímpar, então, para $L_I \rightarrow L_J$, temos

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i+j, u^{-1}v)) = (f_1(i+j), f'(u^{-1}v)) = \\ &= (f_1(i) + f_1(j), f'(u^{-1})f'(v)) = (f_1(j) + f_1(i), (a^{-1}f'(v^{-1})af'(u))J) = \end{aligned}$$

$$= (f_1(j), af'(v))(f_1(i), af'(u)) = f_{-a}((j, v))f_{-a}((i, u)).$$

Para $L_J \rightarrow L_I$ temos

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i + j, (u^{-1}v)J)) = f_{-a}((i + j, v^{-1}u)) = \\ &= (f_1(i + j), f'(u^{-1}v)) = (f_1(i) + f_1(j), f'(u^{-1})f'(v)) = (f_1(i) + f_1(j), (a^{-1}f'(v^{-1})af'(u))J) = \\ &= (f_1(j), af'(v))(f_1(i), af'(u)) = f_{-a}((j, v))f_{-a}((i, u)). \end{aligned}$$

Portanto,

$$f_{-a}((i, u)(j, v)) = f_{-a}((j, v))f_{-a}((i, u)).$$

Concluimos a demonstração de que f_{-a} também é uma família com $\varphi(m)(p - 1)p$ half-isomorfismos não triviais.

Demonstramos assim que ambas as famílias têm $\varphi(m)(p - 1)p$ half-isomorfismos não triviais quando $\alpha \neq \beta$. $\square$

4.3 HALF-AUTOMORFISMOS ENTRE OS LOOPS AUTOMÓRFICOS DIEDRAIS $Dih(m, C_p, \alpha)$

Se $\alpha = I$, então L_α é grupo e portanto todo half-isomorfismo é trivial. Os procedimentos para a caracterização dos half-automorfismos de um loop diedral, $L_J = Dih(m, C_p, J)$ no caso geral, também são totalmente análogos aos praticados para caracterizar os half-isomorfismos de $L_\alpha = Dih(m, C_p, \alpha)$ em $L_\beta = Dih(4, C_p, \beta)$, com $\alpha \neq \beta$, consequentemente vamos obter as mesmas leis de formação f_{+a} e f_{-a} . Entretanto, nesse caso, vamos demonstrar que todos os half-automorfismos de L_J são triviais.

Vale lembrar que

$$f_{+a}((i, x)) = \begin{cases} (f_1(i), f'(x)), & \text{se } i \text{ é par,} \\ (f_1(i), af'(x)), & \text{se } i \text{ é ímpar,} \end{cases}$$

e

$$f_{-a}((i, x)) = \begin{cases} (f_1(i), f'(x)), & \text{se } i \text{ é par,} \\ (f_1(i), af'(x^{-1})), & \text{se } i \text{ é ímpar.} \end{cases}$$

Podemos então enunciar o principal resultado dessa seção.

Proposição 4.15. *Sejam $f' : C_p \rightarrow C_p$ e $f_1 : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ automorfismos. Então*

$$f_{+a} : L_J \rightarrow L_J \text{ e } f_{-a} : L_J \rightarrow L_J$$

são half-isomorfismos triviais para cada $a \in C_p$.

Demonstração. Provaremos caso a caso.

(i) Para a família de funções f_{+a} .

Considere j par.

Se i é par, então temos:

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}(((i + j), uv)) = (f_1(i + j), f'(uv)) = (f_1(i) + f_1(j), f'(u)f'(v)) = \\ &= (f_1(i), f'(u))(f_1(j), f'(v)) = f_{+a}((i, u))f_{+a}((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}((i, u)(j, v)) = f_{+a}((i, u))f_{+a}((j, v)).$$

Agora, considere i ímpar, então temos:

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}((i + j, uv)) = (f_1(i + j), af'(uv)) = (f_1(i) + f_1(j), af'(u)f'(v)) = \\ &= (f_1(i), af'(u))(f_1(j), f'(v)) = f_{+a}((i, u))f_{+a}((j, v)). \end{aligned}$$

Ou seja,

$$f_{+a}((i, u)(j, v)) = f_{+a}((i, u))f_{+a}((j, v)).$$

Considere então j ímpar.

Seja i par, então temos:

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}((i + j, u^{-1}v)) = (f_1(i + j), af'(u^{-1}v)) = (f_1(i) + f_1(j), af'(u^{-1})f'(v)) = \\ &= (f_1(i), f'(u))(f_1(j), af'(v)) = f_{+a}((f_1(i), u))f_{+a}((f_1(j), v)). \end{aligned}$$

Ou seja,

$$f_{+a}((i, u)(j, v)) = f_{+a}((i, u))f_{+a}((j, v)).$$

Por fim, considere i também ímpar, então temos

$$\begin{aligned} f_{+a}((i, u)(j, v)) &= f_{+a}((i + j, (u^{-1}v)J)) = f_{+a}((i + j, v^{-1}u)) = \\ &= (f_1(i + j), f'(v^{-1}u)) = (f_1(i) + f_1(j), f'(v^{-1})f'(u)) = \\ &= (f_1(i), af'(u))(f_1(j), af'(v)) = f_{+a}((i, u))f_{+a}((j, v)). \end{aligned}$$

Logo, temos

$$f_{+a}((i, u)(j, v)) = f_{+a}((i, u))f_{+a}((j, v)).$$

Dessa forma demonstramos que f_{+a} é uma família com $\varphi(m)(p-1)p$ isomorfismos de L_J .

(ii) Para a família de funções f_{-a} .

Considere j par.

Seja i também par, então temos:

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i+j, uv)) = (f_1(i+j), f'(uv)) = (f_1(i) + f_1(j), f'(u)f'(v)) = \\ &= (f_1(i), f'(u))(f_1(j), f'(v)) = f_{-a}((i, u))f_{-a}((j, v)) = f_{-a}((j, v))f_{-a}((i, u)). \end{aligned}$$

Ou seja,

$$f_{-a}((i, u)(j, v)) = f_{-a}((j, v))f_{-a}((i, u)).$$

Considere agora i ímpar, então temos:

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i+j, uv)) = (f_1(i+j), af'(v^{-1}u^{-1})) = (f_1(i) + f_1(j), af'(v^{-1})f'(u^{-1})) = \\ &= (j, f'(v))(i, af'(u^{-1})) = f_{-a}((j, v))f_{-a}((i, u)). \end{aligned}$$

Assim, temos

$$f_{-a}((i, u)(j, v)) = f_{-a}((j, v))f_{-a}((i, u)).$$

Agora, considere j ímpar.

Se i é par, então temos:

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i+j, u^{-1}v)) = (f_1(i) + f_1(j), af'(v^{-1}u)) = (f_1(i) + f_1(j), af'(v^{-1})f'(u)) = \\ &= (f_1(j), af'(v^{-1}))(f_1(i), f'(u)) = f_{-a}((j, v))f_{-a}((i, u)). \end{aligned}$$

Temos então

$$f_{-a}((i, u)(j, v)) = f_{-a}((j, v))f_{-a}^1((i, u)).$$

Seja, por fim, i também ímpar, então temos

$$\begin{aligned} f_{-a}((i, u)(j, v)) &= f_{-a}((i+j, (u^{-1}v))I) = f_{-a}((i+j, v^{-1}u)) = \\ &= (f_1(i+j), f'(v^{-1}u)) = (f_1(i) + f_1(j), f'(v^{-1})f'(u)) = \\ &= (f_1(j), af'(v^{-1}))(f_1(i), af'(u^{-1})) = f_{-a}((j, v))f_{-a}((i, u)). \end{aligned}$$

Portanto, temos

$$f_{-a}((i, u)(j, v)) = f_{-a}((j, v))f_{-a}((i, u)).$$

Concluimos que f_{-a} é uma família com $\varphi(m)(p-1)p$ anti-isomorfismos de L_J .

Demonstramos então que ambas as famílias descrevem $\varphi(m)(p-1)p$ half-automorfismos triviais de L_J .

□

BIBLIOGRAFIA

- [Abo14] M. Aboras, *Dihedral-Like constructions of automorphic loops*, Comment. Math. Univ. Carolin. 55,3(2014), 269 – 284.
- [AbVo16] M. Aboras, P. Vojtěchovský; *Automorphisms of Dihedral-Like Automorphic Loops*, Communications in Algebra, 44 : 613 – 627, 2016.
- [Bol37] G. Bol, *Gewebe und Gruppen*, Math. Ann. 114, 1937, n^o 1, 414 – 431.
- [BP56] R. H. Bruck, L. J. Page; *Loops whose inner mappings are automorphisms*, Ann. Math, 63 : 308 – 323, 1956.
- [Bru71] R. H. Bruck; *Survey of Binary Systems*, Terceira Edição, Springer, 1971.
- [dA18] G. S. dos Anjos; *Half-isomorfismos de Loops Automórficos*, Tese de Doutorado - USP, 2018.
- [For91] E. Formanek, D. Sibley; *The group determinant determines the group*, Proc. Amer. Math. Soc., 112 : 649 – 656, 1991.
- [GdA17] M. L. Merlini Giuliani, G. S. dos Anjos; *On the structure of the automorphism group of certain automorphic loop*, Communications in Algebra, 45 : 2245 – 2255, 2017.
- [GGRS16] A. Grishkov, M. L. Merlini Giuliani, M. Rasskazova, L. Sabinina; *Half-isomorphisms of Finite Automorphic Moufang Loops*, Communications in Algebra, 44 : 4252 – 4261, 2016.
- [GZo4] A. Grishkov, A. Zavarnitsine; *Lagrange's Theorem for Moufang Loops*, Math. Proc. Camb. Phil. Soc., 139 : 41 – 57, 2005.
- [GJM96] E. G. Goodaire, E. Jespers, C. P. Milies; *Alternative Loops Rings*, Elsevier Science B.V., 1996.
- [Gro] The GAP Group; *Group, Algorithms and Programming*, Versão 4.8.7., 2017, (<http://www.gap-system.org>).

- [GG12] S. Gagola III, M. L. Merlini Giuliani; *Half-isomorphisms of Moufang Loops of Odd Order*, Journal of Algebra and Its Applications, vol.11, 2012.
- [GG13] S. Gagola III, M. L. Merlini Giuliani; *On Half-isomorphisms of Certain Moufang Loops With Even Order*, Journal of Algebra and Its Applications, 386 : 131 – 141, 2013.
- [KKPo2] M. K. Kinyon, K. Kunen, J. D. Phillips; *Every Diassociative A-Loop is Moufang*, Proc. Amer. Math. Soc., 130 : 619 – 624, 2002.
- [KKPV16] M. K. Kinyon, K. Kunen, J. D. Phillips, P. Vojtechovsky; *The Structure of Automorphic Loops*, Transactions of The American Mathematical Society, 368 : 8901 – 8927, 2016.
- [Mou35] R. Moufang; *Zur Structur Von Alternativ Korpern*, Math Ann., 110 : 416 – 430, 1935.
- [Pfl90] H. O. Pflugfelder; *Quasigroups and Loops: Introduction*, Volume 7 of Sigma Series in Pure Mathematics, Heldermann Verlag Berlin, 1990.
- [Sco57] W. R. Scott; *Half-homomorphisms of Groups*, Proc. Amer. Math. Soc., 8 : 1141 – 1144, 1957.