Estrutura e exemplos de A-Loops comutativos finitos

Dylene Agda Souza de Barros

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Mestre em Ciências

Programa: Matemática

Orientador: Prof. Dr. Alexandre Grichkov

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES/CNPq

São Paulo, fevereiro de 2010

Estrutura e exemplos de A-loops comutativos finitos

Esta versão definitiva da dissertação
contém as correções e alterações sugeridas pela
Comissão Julgadora durante a defesa realizada
por Dylene Agda Souza de Barros em 03/03/2010.

Comissão Julgadora:

- Prof. Dr. Alexandre Grichkov (orientador) - IME-USP
- Prof. Dr. Henrique Guzzo Junior - IME-USP
- Prof. Dr. Alexandr Zubkov - OMSK STATE

Dedico esse trabalho à minha sobrinha Sarah,
in memorian.

Agradecimentos

Para mim é impossível começar esse trabalho sem agradecer a Deus por... tudo. Quero agradecer aos meus pais, Raimundo e Maria Creuza, por me darem amor e suporte para correr atrás dos meus sonhos, e aos meus irmãos, Marco, Marcelo, Denyse e Matheus, simplismente por fazerem parte da minha vida, contribuindo, cada um da sua forma, com a pessoa que sou. Um especial muito obrigada a minha irmã Denyse por, mesmo com a distância, estar sempre tão presente.

Quero agradecer aos meus professores da gradução do IME-UFG, em especial à professora Shirlei, ao professor Romildo e ao professor Walterson, por todas as lições dadas. Todas elas me ajudaram muito durante o mestrado. Falando em IME-UFG, tenho aqui que lembrar dos meus amigos queridos Marcelo, Poliana, Thaynara, Bira, Eduardo, Arianny, Adriana, Lidiane, Wender, Sunamita, Tarcísio, Vanessa e, é claro, da minha flor de Canella, Ju. Eu sinto muita saudade de todos vocês.

Muito obrigada a todos os funcionários e professores do IME-USP, por me receberem tão bem, em especial ao meu orientador, professor Alexandre Grichkov, por tanta paciência e por todos os ensinamentos durante esses dois anos.

Aos meus amigos do IME-USP, Gustavo, Rose, Diego, Maurício, Débora, Humberto, Juliano, Graciele, Taty, Fran, Big, Bruno, Arlane, André, Bernardo, eu não sei nem o que dizer para agradecer. Vocês fizeram toda a diferença nesses dois anos, desde a piada sem graça que mesmo assim alegra ao silêncio que compreende, passando sempre pelo abraço que conforta. Meus dias aqui foram mais felizes por causa de vocês...

Resumo

Esse trabalho trata um pouco da teoria de A-loops comutativos finitos.

No primeiro capítulo estudamos propriedades básicas de loops em geral e exibimos exemplos de loops não associativos. No capítulo 2 falamos de A-loops em geral e mesmo sem assumirmos comutatividade obtivemos resultados importantes, um exemplo é que A-loop associa potências. Também determinamos quando um isótopo e K^*-holomorfo de um A-loop é um A-loop.

No capítulo 3, nossos únicos objetos de estudo foram os A-loops comutativos finitos. Vimos que tais estruturas têm proriedades muito interessantes, por exemplo, para um A-loop comutativo finito valem os teoremas de Lagrange, Cauchy. Também, um A-loop comutativo finito, Q, tem ordem potência de um primo p se e somente se todo elemento de Q tem ordem potência de p. Mais ainda, todo A-loop comutativo finito de ordem ímpar é solúvel. No último capítulo, apresentamos algumas maneira de se construir um A-loop.

Palavras-chave: A-loops, Aplicações internas, Decomposição, A-loops comutativos de oredem ímpar, A-loops comutativos de expoente 2, Extensões centrais, A-loops comutativos de ordem p^3.

Abstract

This work is about finite commutative A-loops.

In the first chapter we studied basic properties of general loops and we showed some examples of nonassociative loops. In chapter 2, we talked about general A-loops (without commutativity) and even that we obtained important results, for instance, that any A-loop is power-associative. We also determined when an isotope and a K^*-holomorph of an A-loop is an A-loop.

In chapter 3 we dealt only with finite commutative A-loops. We saw that such structures have very interesting properties, for example, for a finite commutative A-loop, Lagrange, Cauchy's theorems apply. Also a finite commutative A-loop, Q, has order a power of a prime p if and only if every element of Q has order a power of p. Moreover, finite commutative A-loops of odd order are solvable. In the last chapter we introduce some ways to construct a commutative A-loop

Keywords: A-loops, Inner mappings, Decomposition, Commutative A-loops of odd order, Commutative A-loops of exponent 2, Central extension, Commutative A-loop of order p^3.

Sumário

Capítulo 1

Loops

1.1 Conceitos e Proriedades Básicas

Daremos, neste capítulo, a definição, exemplos e algumas propriedades básicas de loops.

Definição 1.1.1. *Um conjunto não vazio L munido de uma operação binária é um* ***quase-grupo*** *se as equações $ax = b$, $xa = b$ têm uma única solução em L quaisquer que sejam $a, b \in L$.*

Um ***loop*** *é um quase-grupo L tal que existe $1 \in L$ com a propriedade que*

$$1a = a1 = a \quad \textit{para todo} \quad a \in L.$$

Salvo menção contrária, L denotará um loop.

Dado $a \in L$, a equação $ax = 1$ tem única solução $x = a^{\rho}$ que é chamado de ***inverso à direita*** de a; da mesma forma a equação $xa = 1$ tem única solução $x = a^{\lambda}$ que é chamado de ***inverso à esquerda*** de a. Se em L valer a propreidade associativa, obtemos um grupo, pois $a^{\rho} = a^{\lambda}$ para todo $a \in L$. Em outras palavras, um grupo é um loop associativo.

Notemos que se $a, b, c \in L$ são tais que $ab = ac = d$, pela unicidade da solução da

equação $ax = d$ temos que $b = c$, e se, por outro lado, $ba = ca = f$ temos, pelo mesmo argumento, que $b = c$. Ou seja, em um loop L vale a lei do cancelamento.

Seja $a \in L$ e defina $R_a : L \longrightarrow L$ por $R_a(x) = xa$ e $L_a : L \longrightarrow L$ por $L_a(x) = ax$. Temos que R_a e L_a são bijeções de L e consideremos $\mathcal{M}(L) = \langle R_x, L_x | x \in L \rangle$ subgrupo de $\mathcal{A}(L)$ chamado ***grupo das multiplicações de L***, onde $\mathcal{A}(L)$ é o grupo das permutações do conjunto L.

Definição 1.1.2. *Um subconjunto não vazio $H \subseteq L$ é um subloop se, com a operação de L restrita a H, H tiver estrutura de loop.*

Note que, se $H \subseteq L$ for um subloop, a equação $hx = h$, onde $h \in H$, tem única solução em H e em L. Portanto $1_H = 1_L$.

Proposição 1.1.3. *Seja $H \subseteq L$ un subconjunto não vazio de um loop L. São equivalentes:*

a) H é um subloop de L;

b) Se $x, y \in H$, então $xy, R_y^{-1}(x)$ e $L_y^{-1}(x)$ estão em H;

c) Se $x, y, z \in L$ com $xy = z$ e dois destes elementos estão em H, então o terceiro elemneto também está em H.

Demonstração. *Vamos supor verdadeiro o ítem a, isto é H subloop de L e sejam $x, y \in H$. Como H é fechado pela operação de L, temos $xy \in H$. Temos que $z = R_y^{-1}(x) \in L$ é a única solução da equação $zy = x$, portanto está em H. Da mesma maneira, $w = L_y^{-1}(x)$ está em H pois é a ínica solução da equação $yw = x$. Agora supondo o ítem b, sejam $x, y, z \in L$ com $xy = z$. Se $x, y \in H$, segue que $z \in H$. Se $x, z \in H$ temos $y = L_x^{-1}(z) \in H$ e se $y, z \in H$ temos $x = R_y^{-1}(z) \in H$. Finalmente, supondo o ítem c sejam $x, y \in H$. Então temos $z = xy \in H$. Como existem únicos $w, v \in L$ tais que $xw = y$ e $vx = y$ seguem e que $w, v \in H$ e então H é um quase-grupo. Finalmente para todo $x \in H$, $1x = x$ donde segue que $1 \in H$. Logo H é um subloop de L, como queíamos demonstrar.*

Notemos que se H for um subloop de L, então a^ρ e a^λ estão em H para todo $a \in H$.

Definição 1.1.4. *Sejam H um subloop do loop L e $x \in L$. Os conjuntos $Hx = \{hx :\in H\}$ e $xH = \{xh :\in H\}$ são chamados, de* ***classe lateral à direita de H por x*** *e* ***classe lateral à esquerda de H por x****.*

Suponha, H subloop de L e $x, y \in L$ tais que $Hx = Hy$. Então para qualquer que seja $h \in H$, existem $h_1, h_2 \in H$ tais que $hx = h_1 y$ e $hy = h_2 x$, isto é, $x = L_h^{-1}(L_{h_1}(y))$ e $y = L_h^{-1}(L_{h_2}(x))$. Reciprocamente se $x, y \in L$ são tais que, para todo $h \in L$ existem $h_1, h_2 \in H$ satisfazendo $x = L_h^{-1}(L_{h_1}(y))$ e $y = L_h^{-1}(L_{h_2}(x))$, então $Hx = Hy$. Analogamente $xH = yH$ se e somente se, para todo $h \in H$ existem $h_1, h_2 \in H$ tais que $x = R_h^{-1}(R_{h_1}(y))$ e $y = R_h^{-1}(R_{h_2}(x))$. Assim temos que $xH = H = 1H$ e $Hx = H = H1$ se e somente se $x \in H$

Existe uma bijeção natural ente Hx e H. Daí temos que $|H| = |Hx|$ para todo $x \in L$. Da mesma forma $|H| = |xH|$ para todo $x \in H$. Então temos que, se L for um loop finito e puder ser escrito como reunião disjunta de classes laterais à direira (ou à esquerda) do subloop H, a ordem de H divide a ordem de L.

Proposição 1.1.5. *Sejam L um loop, H um subloop de L e $x, y \in L$. São equivalentes:*

a) $Hx \cap Hy \neq \emptyset$ implica que $Hx = Hy$;

b) $H(hx) = Hx$ para todo $h \in H$.

Demonstração. *Vamos supor que valha o ítem b e sejam $h_1 x = h_2 y \in Hx \cap Hy$. Então segue que $Hx = H(h_1 x) = H(h_2 y) = Hy$. Reciprocamente, para todo $h \in H$, $hx \in H(hx) \cap Hx$ logo $H(hx) = Hx$.* □

Definição 1.1.6. *Sejam $a, b.c \in L$. O* ***comutador*** *de a e b é o único elemento $(a, b) \in L$ tal que $ab = ba(a, b)$. O* ***associador*** *de a, b e c é o único elemento $(a, b, c) \in L$ tal que $(ab)c = [a(bc)](a, b, c)$.*

Definição 1.1.7. *Seja L um loop. Os conjuntos*

$$\mathcal{N}_\lambda(L) = \{a \in L : (a, x, y) = 1 \quad \textit{para todos} \quad x, y \in L\},$$

$$\mathcal{N}_\rho(L) = \{a \in L : (x, y, a) = 1 \quad \textit{para todos} \quad x, y \in L\}$$

e

$$\mathcal{N}_\mu(L) = \{a \in L : (x, a, y) = 1 \quad \textit{para todos} \quad x, y \in L\}$$

são cahamdos, respectivamente, ***núcleo à esquerda, núcleo à direita*** *e* ***núcleo intermediário*** *de L.*
O ***núcleo*** *de L é o conjunto* $\mathcal{N}(L) = \mathcal{N}_\lambda(L) \cap \mathcal{N}_\mu(L) \cap \mathcal{N}_\rho(L)$ *e o* ***centro*** *de L é o conjunto*

$$\mathcal{Z}(L) = \{a \in \mathcal{N}(L) : (a, x) = 1 \quad \textit{para todo} \quad x \in L\}.$$

Proposição 1.1.8. *Cada um dos núcleos de um loop é um subloop associativo e, portanto, um grupo. Em particular, o centro de um loop é um grupo abeliano.*

Demonstração. *Seja L um loop. Desde que* $1 \in \mathcal{N}_\mu(L)$ *temos* $\mathcal{N}_\mu(L) \neq \emptyset$. *Para quaisquer* $a, b \in \mathcal{N}_\mu(L)$ *e* $x, y \in L$*temos*

$$[x(ab)]\, y = [(xa)b]\, y = (xa)(by) = x\,[a(by)] = x\,[(ab)y]$$

Portanto $ab \in \mathcal{N}_\mu(L)$. *Além disso* $(a^\rho a)a^\rho = a^\rho(aa^\rho) = a^\rho 1 = 1a^\rho$ *e, pela lei do cancelamento, temos* $a^\rho a = 1$ *que implica* $a^\lambda = a^\rho$. *Logo, qualquer* $a \in \mathcal{N}_\mu(L)$ *possui inverso bilateral, denotado por* a^{-1}. *Mais ainda, se* $a \in \mathcal{N}_\mu(L)$ *então* $R_a^{-1} = R_{a^{-1}}$, *pois* $(xa)a^{-1} = x(aa^{-1}) = x$ *qualquer que seja* $x \in L$ *e, da mesma forma,* $L_a^{-1} = L_{a^{-1}}$. *Para quaisquer* $x, y \in L$, *podemos escrever* $x = ta$ *para algum* $t \in L$ *e então temos:*

$$(xa^{-1})y = \left[(ta)a^{-1}\right] y = \left[t(aa^{-1})\right] y = ty$$

e

$$x(a^{-1}y) = (ta)(a^{-1}y) = t\left[a(a^{-1}y)\right] = t\,[L_a L_{a^{-1}}(y)] = ty.$$

Ou seja, $a^{-1} \in \mathcal{N}_\mu(L)$. *Como* $a(bc) = (ab)c$, *para quaisquer que sejam* $a, b, c \in \mathcal{N}_\mu(L)$, *obetmos que* $\mathcal{N}_\mu(L)$*é um grupo.*

Consideremos agora, $\mathcal{N}_\lambda(L)$. É fácil ver que $1 \in \mathcal{N}_\lambda(L)$ e que $ab \in \mathcal{N}_\lambda(L)$ quaisquer que sejam $a, b \in \mathcal{N}_\lambda(L)$. Para $a \in \mathcal{N}_\lambda(L)$, temos $(aa^\lambda)a = a(a^\lambda a) = a1 = 1a$ e, portanto a possui um inverso bilateral em L, que será denotado por a^{-1}. Além disso, qualquer que seja $x \in L$, $a(a^{-1}x) = (aa^{-1})x = 1x = x$, o que implica que $L_a^{-1} = L_{a^{-1}}$. Tome $x, y \in L$, então

$$a\left[(a^{-1}x)y\right] = \left[a(a^{-1}x)\right]y = L_a L_{a^{-1}}(x)y = xy$$

e

$$a\left[a^{-1}(xy)\right] = (aa^{-1})(xy) = xy.$$

Assim, pela lei do cancelamento, obtemos $(a^{-1}x)y = a^{-1}(xy)$ para quaisquer $x, y \in L$, ou seja, $a^{-1} \in \mathcal{N}_\lambda(L)$ e, portanto, este é um subloop de L. Como $(ab)c = a(bc)$ para todos $a, b, c \in \mathcal{N}_\lambda(L)$, temos que este é um grupo.
Para $\mathcal{N}_\rho(L)$, observemos que, se $(L, .)$ é um loop, fazendo $x * y = yx$, temos um loop $(L, *)$ que será chamado de loop oposto a $(L, .)$ e denotado por L^{op}. Além disso $\mathcal{N}_\rho(L) = \mathcal{N}_\lambda(L^{op})$. Logo $\mathcal{N}_\rho(L)$ é um grupo.
Por definição, $\mathcal{N}(L) = \mathcal{N}_\mu(L) \cap \mathcal{N}_\lambda(L) \cap \mathcal{N}_\rho(L)$, donde segue, facilmente, que $\mathcal{N}(L)$ é um subgrupo de L.
Finalmente, para $\mathcal{Z}(L)$, basta observarmos que se $a, b \in \mathcal{Z}(L) \subset \mathcal{N}(L)$ então $ab \in \mathcal{Z}(L)$. De fato,

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab),$$

o que completa a demonstração.

Temos que a condição b) da proposição 1.1.5 vale se o subloop H for um dos núcleos ou o centro do loop L. Portanto se L for um loop finito, então os números $|\mathcal{N}_\lambda(L)|$, $|\mathcal{N}_\mu(L)|$, $|\mathcal{N}_\rho(L)|$, $|\mathcal{N}(L)|$, e $|\mathcal{Z}(L)|$ dividem $|L|$.

Definição 1.1.9. *Seja L um loop. Um subloop H de L é dito* ***normal*** *se para quaisquer $x, y \in L$ temos*

$$Hx = xH, \quad H(xy) = (Hx)y, \quad (xH)y = x(Hy), \quad e \quad (yx)H = y(xH).$$

Usaremos a notação $H \lhd L$ para indicar que o subloop H é normal em L.

Sejam L um loop e $H \lhd L$ e consideremos o conjunto $L/H = \{xH : x \in L\}$. Vamos definir a seguinte operação binária em L/H: para $xH, yH \in L/H$,

$$(xH)(yH) = (xy)H.$$

Notemos que se $xH = x^{'}H$ e $yH = y^{'}H$ então

$$(xy)H = H(xy) = (Hx)y = (xH)y = (x^{'}H)y =$$
$$= x^{'}(Hy) = x^{'}(yH) = x^{'}(y^{'}H) = x^{'}(Hy^{'}) =$$
$$= (x^{'}H)y^{'} = (Hx^{'})y^{'} = H(x^{'}y^{'}) = (x^{'}y^{'})H.$$

Ou seja, a operação definida acima está bem definida. É de fácil verificação que esta operação dá a L/H uma estrutura de loop cujo elemento neutro é $1H = H$.

Definição 1.1.10. *O loop L/H é chamado de **loop quociente de** L **por** H.*

Se $H \lhd L$, então temos $H(hx) = (Hh)x = Hx$ para todo $x \in L$ e todo $h \in H$. Assim, as distintas classes laterais de H em L são disjuntas. Então, se L for um loop finito, teremos que $|H|$ divide $|L|$ e $|L/H| = \frac{|L|}{|H|}$.

Definição 1.1.11. *Sejam $L, L^{'}$ loops e uma aplicação $f : (L, .) \longrightarrow (L^{'}, *)$. Dizemos que f é um **homomorfismo** se $f(x.y) = f(x) * f(y)$ quaisquer que sejam $x, y \in L$. Um **isomorfismo** entre os loops $L, L^{'}$ é um homomorfismo bijetivo. Um **automorfismo** do loop L é um isomorfismo de L em L.*

Observação. *As oprerações de L e $L^{'}$ terão a mesma notação embora elas sejam, eventualmente, diferentes.*

Definição 1.1.12. *O **kernel** de um homomorfismo de loops $f : L \longrightarrow L^{'}$ é o conjunto*

$$ker(f) = \{x \in L : f(x) = 1\}$$

*e a **imagem** de f é o conjunto*

$$f(L) = \left\{y = f(x) \in L^{'} : x \in L\right\}.$$

Lema 1.1.13. *Se $f : L \longrightarrow L'$ for um homomorfismo de loops, então $ker(f)$ é um subloop de L.*

Demonstração. *Como $f(1) = (1.1) = f(1)f(1)$ temos que $f(1) = 1$, e portanto, $K = ker(f) \neq \emptyset$. Sejam $x, y, z \in L$ com $xy = z$. Então*

- *Se $x, y \in K$ vale $f(z) = f(xy) = f(x)f(y) = 1$, ou seja $z \in K$;*
- *Se $y, z \in K$ vale $f(x) = f(x)f(y) = f(xy) = f(z) = 1$, ou seja $x \in K$;*
- *Se $x, z \in K$ vale $f(y) = f(x)f(y) = f(xy) = f(z) = 1$, ou seja $y \in K$.*

Segue, portanto, do item c) da proposição 1.1.3 que K é um suloop de L.

Lema 1.1.14. *Se $f : L \longrightarrow L'$ for um homomorfismo de loops, então $K = ker(f)$ é um subloop normal em L.*

Demonstração. *No lema anterior mostramos que K é um subloop de L. Sejam $x, y \in L$.*

- *Vamos mostrar que $Kx = xK$.*
  Seja $xk \in xK$ um elemento arbitrário. Existe um único elemento $a \in L$ que satifaz a equação $ax = xk$ e nosso objetivo é mostrar que $a \in K$. De fato temos que $f(a)f(x) = f(ax) = f(xk) = f(x)f(k) = f(x)$. Logo, aplicando a lei do cancelamento, temos $f(a) = 1$, como desejado. Analogamente se $a \in L$ satisfaz a equação $xa = kx$, para um lemento $k \in K$ arbitrário, vamos ter, necessariamente, $a \in K$. Portanto $Kx = xK$.
- *Considere $d = k(xy) \in K(xy)$ e a equação $(zx)y = d$. Existe um único $a \in L$ tal que $(ax)y = d = k(xy)$. Quermos mostrar que $a \in K$. Temos $f(xy) = f(k)f(xy) = f(k(xy)) = f((ax)y) = f(ax)f(y)$, e assim, $f(x)f(y) = (f(a)f(x))f(y)$. Então $f(a)f(x) = f(x)$, isto é, $f(a) = 1$.*
  Da mesma forma considerando $d = (kx)y \in (Kx)y$ e a equação $z(xy) = d$ temos que existe um único $a \in L$ tal que $a(xy) = (kx)y$ e assim $f(a)f(xy) =$

$f(a(xy)) = f((kx)y) = (f(k)f(x))f(y) = f(x)f(y) = f(xy)$ *e então* $f(a) = 1$. *Logo* $(Kx)y = K(xy)$.

- *A prova de que* $(xK)y = x(Ky)$ *é feita de maneira inteiramenta análoga à prova de que* $(Kx)y = K(xy)$.

- *Finalmente* $(yx)K = K(yx) = (Ky)x = (yK)x = y(Kx) = y(xK)$.

Logo K *é um subloop normal de* L.

Lema 1.1.15. *Um subloop* $H \leq L$ *é normal em* L *se e somente se for kernel de um homomorfismo com domínio* L.

Demonstração. *No lema anterior, vimos que se* $K = Ker(f)$ *para algum homomorfismo de loops* $f : L \longrightarrow L^{'}$ *então* K *é um subloop normal de* L. *Reciprocamente se* K *é um subloop normal de* L *então a aplicação* $\pi : L \longrightarrow L/K$ *dada por* $\pi(a) = aK$ *é um homomorfismo de loops com* $ker(\pi) = K$.

Definição 1.1.16. *O conjunto*

$$\mathcal{I}(L) = \{f \in \mathcal{M}(L) : f(1) = 1\}$$

é chamado grupo das aplicações internas de L.

Claramente $\mathcal{I}(L)$ é um subgrupo de $\mathcal{M}(L)$. Exibiremos uma caracterização bastante útil para o grupo $\mathcal{I}(L)$.

Proposição 1.1.17. *O grupo das aplicações internas* $\mathcal{I}(L)$ *é gerado pelas aplicações da forma*

$$T_{(x)} = L_x^{-1} R_x,$$

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

e

$$L_{(x,y)} = L_{yx}^{-1} L_y L_x$$

para $x, y \in L$.

Demonstração. *Considere* $F = \left\{R_{(x,y)}, L_{(x,y)}, T_x; x, y \in L\right\} \subset \mathcal{M}(L)$. *Queremos mostrar que* $\mathcal{I}(L) = \langle F\rangle$.
Considere o conjunto $K = \left\{g \in \mathcal{M}(L); g \in R_{g(1)}\langle F\rangle\right\}$, *onde* $R_{g(1)}\langle F\rangle$ *denota a classe lateral do subgrupo* $\langle F\rangle$ *em* $\mathcal{M}(L)$. *Se* $g(1) = t$, *para cada* $x \in L$ *temos*

$$R_x(g(1)) = R_x(t) = tx.$$

Para cada $g \in K$ *existe* $\phi \in \langle F\rangle$ *tal que*

$$g = R_{g(1)}\phi = R_t\phi.$$

Assim temos

$$R_x g = R_x R_t\phi = R_{tx}R_{(t,x)}\phi = R_{R_x(g(1))}R_{(t,x)}\phi.$$

Ou seja $R_x g \in K$.
Temos que, se

$$L_x(g(1)) = L_x(t) = xt,$$

então

$$L_x g = L_x R_t\phi = R_{L_x(g(1))}T_{xt}^{-1}L_{(t,x)}T_t\phi,$$

isto é $L_x g \in K$. *Do memso modo temos que* $L_x^{-1}g \in K$ *e* $R_x^{-1}g \in K$. *Assim* $\mathcal{M}(L)K \subset K \subset \mathcal{M}(L) \subset \mathcal{M}(L)K$. *Em outras palavras, para toda aplicção* $f \in \mathcal{M}(L)$, $f \in R_{f(1)}\langle F\rangle$. *Se* $f \in \mathcal{I}(L)$ *temos* $f(1) = 1$ *e assim* $f \in \langle F\rangle$.
Reciprocamnte, vamos mostrar que para quaisquer $x, y \in L$ *temmos*

$$R_{(x,y)}(1) = R_{xy}^{-1}R_yR_x(1) = R_{xy}^{-1}(xy) = 1,$$

$$L_{(x,y)}(1) = L_{yx}^{-1}L_yL_x(1) = L_{yx}^{-1}(yx) = 1$$

e

$$T_x(1) = L_x^{-1}R_x(1) = L_x^{-1}(x) = 1.$$

Então $\mathcal{I}(L) = \langle F\rangle$. □

Lema 1.1.18. *Um subloop $H \leq L$ é normal em L se e somente se $f(H) \subset H$, para qualquer $f \in \mathcal{I}(L)$.*

Demonstração. *Sejam $x, y \in L$ e $h \in H$. Como $R_{(x,y)}(h) = R_{xy}^{-1} R_y R_x(h) = R_{xy^{-1}}((hx)y)$ temos que $R_{(x,y)}(h) \in H$ se e somente se $(Hx)y = H(xy)$. Da mesma forma temos que $L_{(x,y)}(h) \in H$ se e somente se $y(xH) = (xy)H$ e $T_x(h) \in H$ se e somente se $xH = Hx$. Para completar, a demosntração basta observar que se para um subloop H de L valerem as propriedades $(Hx)y = H(xy), y(xH) = (xy)H$ e $xH = Hx$ para quaisquer $x, y \in L$ temos*

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

para quaisquer $x, y \in L$. $\square$

Para um automorfismo artrário S de L, é fácil ver que, para quaisquer $x, y \in L$,

$$SR_xS^{-1} = R_{S(x)} \quad \text{e} \quad SL_xS^{-1} = L_{S(x)} \tag{1.1}$$

$$SR_{(x,y)}S^{-1} = R_{(S(x),S(y))} \quad \text{e} \quad SL_{(x,y)}S^{-1} = L_{(S(x),S(y))} \tag{1.2}$$

$$ST_xS^{-1} = T_{S(x)} \tag{1.3}$$

1.2 Loops com a Propriedade do Inverso

Definição 1.2.1. *Um loop L é dito ser um **loop com a propriedade do inverso** se para cada $x \in L$ existe um inverso bilateral x^{-1}, isto é $xx^{-1} = x^{-1}x = 1$, e ainda*

$$x^{-1}(xy) = y$$

e

$$(yx)x^{-1} = y$$

para todos $x, y \in L$.

Para simplificar a liguagem, chamaremos um loop com a proriedade do inverso L de PI-loop. Para um PI-loop L definimos $J : L \longrightarrow L$ por $J(x) = x^{-1}$.

Proposição 1.2.2. *Sejam L um PI-loop e $I : L \longrightarrow L$ a aplicação identidade. Então:*

1. $J^2 = I$;
2. $R_x^{-1} = R_{x^{-1}}$ *e* $L_x^{-1} = L_{x^{-1}}$ *para todo* $x \in L$;
3. $(xy)^{-1} = y^{-1}x^{-1}$ *para todos* $x, y \in L$;
4. $JL_xJ = R_{x^{-1}}$ *e* $JR_xJ = L_{x^{-1}}$.

Demonstração.

1. *De* $xx^{-1} = x^{-1}x = 1$, *para qualquer que seja* x *no PI-loop L, temos que* $(x^{-1})^{-1} = x$ *donde segue* $J^2 = I$.
2. *Temos que* $(yx)x^{-1} = y$ *para todos* $x, y \in L$ *se e somente se* $R_{x^{-1}}R_x = I$ *para todo* $x \in L$. *Da definição de PI-loop e do item 1, segue que* $R_xR_{x^{-1}} = I$ *pois* $(yx^{-1})x = (yx^{-1})(x^{-1})^{-1}$. *Logo* $R_x^{-1} = R_{x^{-1}}$. *Da modo análogo, obtemos* $L_x^{-1} = L_{x^{-1}}$ *para todo* $x \in L$.
3. *Basta notar que se* $xy = z$ *então* $x = (xy)y^{-1} = zy^{-1}$ *e, assim,* $y^{-1} = z^{-1}(zy^{-1}) = z^{-1}x$. *Logo* $z^{-1} = (z^{-1}x)x^{-1} = y^{-1}x^{-1}$.
4. *Para* $x, y \in L$ *temos* $JL_xJ(y) = JL_x(y^{-1}) = J(xy^{-1}) = yx^{-1} = R_{x^{-1}}(y)$ *e* $JR_xJ(y) = JR_x(y^{-1}) = J(y^{-1}x) = x^{-1}y = L_{x^{-1}}(y)$, *o que completa a demonstração.*

Corolário 1.2.3. *Um subconjunto não vazio H de um PI-loop L é um subloop se e somente se* $xy, x^{-1} \in H$ *para quaisquer* $x, y \in H$.

Proposição 1.2.4. *Se L for um PI-loop então $\mathcal{N}_\lambda(L) = \mathcal{N}\mu(L) = \mathcal{N}_\rho(L)$. Consequentemente, todos os núcleos de um PI-loop são iguais.*

Demonstração. *Seja $x \in \mathcal{N}_\lambda(L)$. Então $x^{-1} \in \mathcal{N}_\lambda(L)$, pois este é um grupo. Assim para $a, b \in L$ temos que $(x^{-1}a^{-1})b^{-1} = x^{-1}(a^{-1}b^{-1})$ e tomando o iverso nessa igualdade temos que $b(ax) = (ba)x$, isto é, $x \in \mathcal{N}_\rho(L)$. Portanto $\mathcal{N}_\lambda(L) \subset \mathcal{N}_\rho(L)$. Da mesma maneira, se $x \in \mathcal{N}_\rho(L)$ então $(a^{-1}b^{-1})x^{-1} = a^{-1}(b^{-1}x^{-1})$ o que implica que $x(ba) = (xb)a$ para quaisquer $a, b \in L$. Logo, $\mathcal{N}_\rho(L) \subset \mathcal{N}_\lambda(L)$ e assim $\mathcal{N}_\rho(L) = \mathcal{N}_\lambda(L)$.*
Para $x \in \mathcal{N}_\mu(L)$, temos $(ax)b = a(xb)$ para todos $a, b \in L$, isto é

$$b = (ax)^{-1}[a(xb)] = (x^{-1}a^{-1})[a(xb)]$$

. Para quaisquer $a, c \in L$ existe $b \in L$ tal que $c = a(xb)$ e então $b = (x^{-1}a^{-1})c$. Por outro lado, $x^{-1}(a^{-1}c) = x^{-1}(xb) = b$. Portanto

$$(x^{-1}a^{-1})c = x^{-1}(a^{-1}c),$$

ou seja, $x^{-1} \in \mathcal{N}_\lambda(L)$, e com isso $x \in \mathcal{N}_\lambda(L)$. Logo $\mathcal{N}_\mu(L) \subset \mathcal{N}_\lambda(L)$. Reciprocamente, se $x \in \mathcal{N}_\lambda(L)$, $(xa)b = x(ab)$ para todos $a, b \in L$. Assim

$$b = (a^{-1}x^{-1})[x(ab)].$$

Para $a, c \in L$, existe $b \in L$ tal que $x(ab) = c$ e assim $b = (a^{-1}x^{-1})c$. Também temos $a^{-1}(x^{-1}c) = a^{-1}(ab) = b$. Assim

$$a^{-1}(x^{-1}c) = (a^{-1}x^{-1})c$$

então $x^{-1} \in \mathcal{N}_\mu(L)$ e, então $x \in \mathcal{N}_\mu(L)$. Logo $\mathcal{N}_\lambda(L) \subset \mathcal{N}_\mu(L)$ e assim, $\mathcal{N}_\lambda(L) = \mathcal{N}_\mu(L)$. □

Definição 1.2.5. *O **índice do subloop** H **em** L é o número minimal de classes laterais à direita de H cuja reunião é igual a L.*

Vamos denotar o índice de H em L por $[L : H]$.

Suponhamos L um PI-loop e $H \subset L$ um subloop. Desde que $\{h^{-1} : h \in H\} = H$ temos que $Hx \mapsto x^{-1}H$ é uma bijeção entre a família de classes laterais à direita de H e a família de classes laterais à esquerda de H. Então, o índice de H em L é o número minimal de classes laterais à esquerda de H cuja reunião é igual a L. Além disso se L for finito e puder ser escrito como reunião disjunta de classes laterais de H teremos $[L : H] = \frac{|L|}{|H|}$.

1.3 Exemplos de Loops

No início deste capítulo, mencionamos que um loop associoativo é um grupo. Daremos agora dois exemplos de loops que não são associativos.

Exemplo 1.3.1. *Considere o conjunto $S = \{1, 2, 3, 4, 5\} \subset \mathbb{N}$, munido da operação binária descrita na tabela abaixo.*

$*$	**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

Como cada elemento de S aparece uma vez, e somente uma vez, temos que $(S, *)$ é um quase-grupo. Além disso, 1 é o elemento neutro de S. Entretanto $3 * (3 * 4) = 3 * 2 = 5$ e $(3 * 3) * 4 = 1 * 4$, portanto $(S, *)$ não é associativo.

Exemplo 1.3.2. *Sejam G um grupo não abeliano, u uma indetreminada e considere o conjunto formal $Gu = \{gu : g \in G\}$. Vamos definir $L = G \cup Gu$ onde esta reunião é disjunta e vamos estender a operação de G a L da seguinte maneira:*

$$g(hu) = (hg)u,$$

$$(gu)h = (gh^{-1})u$$

e

$$(gu)(hu) = h^{-1}g,$$

para quaisquer $g, h \in G$.
Afirmamos que L *é um loop. De fato, seja a equação* $ax = b$ *com* $a, b \in L$.

- *Se* $a, b \in G$ *então a equação tem única solução em* $G \subset L$;
- *Se* $a = g_1u \in Gu$ *e* $b \in G$, *façamos* $x = g_1b^{-1}u$ *e, assim* $(g_1u)(g_1b^{-1}u) = (g_1b^{-1})^{-1}g_1 = b$. *Portanto* $x = g_1b^{-1}u \in Gu \subset L$ *é uma solução de* $ax = b$. *Se* y *for uma outra solução de* $ax = b$, y *deve pertencer a* Gu, *pois* $b \in G$ *e* $a \in Gu$. *Assim* $y = g_2u$ *com* $g_2 \in G$ *e* $b = (g_1u)(g_2u) = g_2^{-1}g_1$, *o que implica que,* $g_2 = g_1b^{-1}$ *e, logo, a solução é única.*
- *Supondo* $a \in G$, $b = h_1u \in Gu$ *e fazendo* $x = (h_1a^{-1})u \in Gu$ *temos que* $ax = a(h_1a^{-1}u) = h_1a^{-1}au = b$ *e, assim, a equação tem solução. Se* $y = h_2u \in Gu$ *for outra solução de* $ax = b$ *(qualquer solucão de* $ax = b$ *está em* Gu *pois* $a \in G$ *e* $b \in G$*)temos* $h_1u = a(h_2u) = h_2au$, *ou seja,* $h_2 = h_1a^{-1}$ *e a solução é única.*
- *Agora, se* $a = a_1x, b = b_1u \in Gu$ *onde* $a_1, b_1 \in G$, *faça* $x = b_1^{-1}a_1 \in G$ *e então* $(a_1u)(b_1^{-1}a_1) = a_1(b_1^{-1}a_1)^{-1}u = b_1u = b$, *o que implica que a equação* $ax = b$ *tem solução. E a solução é unica pois se* $g \in G$ *for outra solução teremos* $b_1u = (a_1u)g = (a_1g^{-1})u$ *e assim* $g = b_1^{-1}a_1$.

De maneira inteiremente análoga, prova-se que a equação $xa = b$ *tem única solução em* L, *quaisquer que sejam* $a, b \in L$. *Também é de fácil verificação que* $ea = ae = a$ *para todo* $a \in L$, *onde* e *é o elemento neutro de* G. *Com isso temos que* L *é um loop. Verifiquemos agora que* L *não é um grupo. Para isso, tomemos* $gu, hu, lu \in Gu$. *Temos que*

$$(gu)((hu)(lu)) = (gu)(l^{-1}h) = (gh^{-1}l)u$$

e

$$((gu)(hu))(lu) = (h^{-1}g)(lu) = (lh^{-1}g)u.$$

Assim $(gu)((hu)(lu)) = ((gu)(hu))(lu)$ *se, e somente se,*

$$gh^{-1}l = lh^{-1}g. \tag{1.4}$$

Tomando $h = e$, $g \in G\backslash Z(G)$ *e* $l \in G\backslash C_G(g)$, *temos que a igualdade 1.4 não se verifica e, portanto,* L *não é associativo. Logo* L *não é um grupo.*

Capítulo 2

A-loops

Neste capítulo estudaremos um importante tipo de loop, loops cujas aplicações internas são automorfismos.

2.1 Propriedades Gerais

Definição 2.1.1. *Um loop L é chamado* ***A-loop*** *se cada elemento $f \in \mathcal{I}(L)$ for um automorfismo de L.*

Definição 2.1.2. *Um subloop $H \leq L$ é um subloop* ***característico*** *de L se $f(H) \subset H$, para todo automorfismo f de L.*

Teorema 2.1.3. *Seja L um A-loop. Então:*

1. *Todo subloop de L é um A-loop;*
2. *Todo subloop característico de L é um subloop normal de L;*
3. *Os núcleos e o centro de L são subloops normais de L;*
4. *Se $H \lhd L$, então L/H é um A-loop.*

Demonstração.

1. *Seja* $H \leq L$. *Temos que* $\mathcal{I}(H) = \langle R_{(x,y)}, L_{(x,y)}, T_{(x)} | x, y \in H \rangle$. *Como* L *é um A-loop temos que* $\mathcal{I}(H) \subset \mathcal{I}(L) \subset Aut(L)$ *e, por isso,* $R_{(x,y)}|_H, L_{(x,y)}|_H, T_{(x)}|_H$ *são homomorfismos injetivos de* H *para quaisquer* $x, y \in H$. *Para* $b \in H$, *existe* $a \in L$ *tal que* $R_{(x,y)}(a) = R_{xy}^{-1} R_y R_x(a) = R_{xy}^{-1}(ax.y) = b$, *ou seja,* $b(xy) = (ax)y$. *Então* $ax \in L$ *é a única solução da equação* $zy = b(xy)$ *e, como* b, x *e* y *são elementos do loop* H, *podemos concluir que* $ax = h \in H$. *Assim* a *é a única solução de* $zx = h$ *e, pelo mesmo argumento, concluimos que* $a \in H$. *Portanto* $R_{(x,y)} : H \longrightarrow H$ *é um automorfismo de* H, *para todos* $x, y \in H$. *Analogamente, concluímos que* $L_{(x,y)}, T_{(x)} \in Aut(H)$ *para todos* $x, y \in H$. *Logo,* H *é um A-loop.*

2. *Se* $H \leq L$ *é um subloop característico de* L, *temos, por definição, que* $f(H) \subset H$ *para toda* $f \in Aut(L)$. *Assim* $f(H) \subset H$ *para qualquer* $f \in \mathcal{I}(L) \subset Aut(L)$ *e, portanto,* H *é um subloop normal de* L.

3. *Sejam* $f \in Aut(L)$ *e* $x, y \in L$. *Então existem* $u, v \in L$ *tais que* $f(u) = x$ *e* $f(v) = y$. *Se* $a \in \mathcal{N}_\lambda(L)$, *temos* $(af^{-1}(u))f^{-1}(v) = a(f^{-1}(u)f^{-1}(v))$ *e assim* $f((af^{-1}(u))f^{-1}(v)) = f(a(f^{-1}(u)f^{-1}(v)))$ *ou, equivalentemente,* $f(a)x.y = f(a).xy$. *Portanto* $f(a) \in \mathcal{N}_\lambda(L)$, *e então,* $\mathcal{N}_\lambda(L)$ *é um subloop característico de* L. *Logo* $\mathcal{N}_\lambda(L)$ *é um subloop normal de* L. *De maneira análoga temos que* $\mathcal{N}_\mu(L)$ *e* $\mathcal{N}_\rho(L)$ *são subloops normais de* L.
   Se $a \in \mathcal{N}(L) = \mathcal{N}_\lambda(L) \cap \mathcal{N}_\mu(L) \cap \mathcal{N}_\rho(L)$ *então* $f(a) \in \mathcal{N}_\lambda(L) \cap \mathcal{N}_\mu(L) \cap \mathcal{N}_\rho(L)$. *Então* $\mathcal{N}(L)$ *é um subloop característico de* L *e, portanto, um subloop normal de* L.
   Para $a \in \mathcal{Z}(L) \subset \mathcal{N}(L)$ *temos que* $f(a) \in \mathcal{N}(L)e$, *além disso, como* $f^{-1}(u)a = af^{-1}(u)$ *temos* $f(a)x = xf(a)$, *o que implica que* $f(a) \in \mathcal{Z}(L)$. *Logo* $\mathcal{Z}(L)$ *é um subloop característico e, portamto, normal de* L.

4. *Para cada* $f \in \mathcal{I}(L)$, *defina* $f' : L/H \longrightarrow L/H$ *onde* $f'(xH) = f(x)H$. *Sabemos* $xH = yH$ *se e somente se para todo* $h \in H$ *existem* $h_1, h_2 \in H$ *tais que* $xh = yh_1$ *e* $yh = xh_2$. *Como* $H \lhd L$ *e como* f *é um automorfismo de* L, *temos que*

$$f(x)f(h) = f(xh) = f(yh_1) = f(y)f(h_1)$$

e

$$f(y)f(h) = f(yh) = f(xh_2) = f(x)f(h_2)$$

onde $f(h), f(h_1), f(h_2) \in H$. *Assim teremos* $f(x)H = f(y)H$ *e então* $f^{'}$ *está bem definida.*
Além disso $f^{'}(H) = f^{'}(1H) = f(1)H = 1H = H$, *isto é* $f^{'} \in \mathcal{I}(L/H)$. *Nosso objetivo é mostrar que a aplicação* $\tau : \mathcal{I}(L) \longrightarrow \mathcal{I}(L/H)$, *definido por* $\tau(f) = f^{'}$ *é um homomorfismo sobrejetor de grupos.Para* $f, g \in \mathcal{I}(L)$ *e* $x \in L$ *temos*

$$(fg)^{'}(xH) = f(g(x))H = f^{'}(g(x)H) = f^{'}(g^{'}(xH)),$$

ou seja $(fg)^{'} = f^{'}g^{'}$ *e assim* τ *é um homomorfismo de grupos.*
Para $x, y \in L$ *considere* $R_{(xH,yH)}, L_{(xH,yH)}$ *e* T_{xH}. *Seja* $z \in L$,

$$R_{(xH,yH)}(zH) = R^{-1}_{(yx)H}(((zx)y)H) = wH$$

onde $(w(xy))H = ((zx)y)H$. *Por outro lado,*

$$R^{'}_{(x,y)}(zH) = (R_{(x,y)}(z))H = wH$$

onde $w(xy) = (zx)y$. *Portanto* $R^{'}_{(x,y)} = R_{(xH,yH)}$. *Da memsa forma,* $L^{'}_{(x,y)} = L_{(xH,yH)}$ $T^{'}_{x} = T_{xH}$. *Assim* τ *é um epimorfismo de grupos.*
Finalmente, para cada $f^{'} \in \mathcal{I}(L/H)$, *onde* $f \in \mathcal{I}(L)$, *e para quaisquer* $x, y \in L$ *vale*

$$f^{'}(xHyH) = f^{'}(xyH) = f(xy)H = (f(x)f(y))H = (f(x)H)(f(y)H) = f^{'}(xH)f^{'}(yH).$$

Logo $f^{'}$ *é um automorfismo de* L/H *e, portanto,* L/H *é um A-loop.* $\square$

Um subconjunto associativo (comutativo) $K \subset L$ é chamado ***subconjunto associativo (comutativo) maximal*** se K não estiver contido propriamente em nenhum subconjunto associativo (comutativo) de L. Pelo Lema de Zorn temos que qualquer subconjunto associativo (comutativo) de L está contido em,pelo menos, um subconjunto associativo (comutativo) maximal de L.

Lema 2.1.4. *Sejam L um loop, S um conjunto não vazio de automorfismos de L e H o subconjunto dos elementos de L que são fixos por todos os elementos de S, isto é, $H = \{x \in L : f(x) = x \quad para\ todo \quad f \in S\}$. Então H é um subloop de L.*

Demonstração. *É fácil ver que $H \neq \emptyset$ pois $1 \in H$. Sejam $x, y, z \in L$ com $xy = z$.*

- *Se $x, y \in H$, temos $f(z) = f(xy) = f(x)f(y) = xy = z$, logo $z \in H$.*
- *Se $x, z \in H$, temos $z = f(z) = f(xy) = f(x)f(y) = xf(y)$, logo $f(y) = y$ e $y \in H$.*
- *Se $y, z \in H$, temos $z = f(z) = f(xy) = f(x)f(y) = f(x)y$, logo $f(x) = x$ e $x \in H$.*

Concluímos, então, que H é um subloop de L.

Observação. *Notemos que para $x \in H$ temos $1 = f(1) = f(xx^\rho) = f(x)f(x^\rho) = xf(x^\rho)$ e $1 = f(1) = f(x^\lambda x) = f(x^\lambda)f(x) = f(x^\lambda)x$ para todo $f \in S$. Portanto $f(x^\rho) = x^\rho$ e $f(x^\lambda) = x^\lambda$ para todo $f \in S$. Logo $x^\lambda, x^\rho \in H$.*

Teorema 2.1.5. *Seja L um A-loop. Então*

1. *Todo subconjunto comutativo maximal, C, é um subloop de L.*
2. *Todo subconjunto associativo maximal, A, é um subloop de L.*
3. *L comuta potências, isto é, $x^m x^n = x^n x^m$, para todo $x \in L$ e todos $m, n \in \mathbb{Z}$.*
4. *L associa potências, isto é, $(x^m x^n)x^p = x^m(x^n x^p)$, para todo $x \in L$ e todos $m, n, p \in \mathbb{Z}$.*

Demonstração.

1. *Um elemento $c \in L$ pertence a C se e somente se $cx = xc$ para todo $x \in L$. Em outras palavras $c \in C$ se e somente se $c = L_x^{-1}(R_x(c)) = T_x(c)$ para todo $x \in L$. Como L é um A-loop, do lema anterior segue que C é um subloop de L.*

2. *Temos que $a \in L$ está em A se e somente se $(ax)y = a(xy)$, $(xa)y = x(ay)$ e $x(ya) = (yx)a$ para quaisquer $x, y \in L$. Ou seja $a \in A$ se e somente se $R_{(x,y)}(a) = a$, $R_y^{-1}L_x^{-1}R_yL_x(a) = a$ e $L_{(x,y)}(a) = a$ para todos $x, y \in L$. Notemos que $R_y^{-1}L_x^{-1}R_yL_x = T_y^{-1}L_{(y,x)}^{-1}T_{xy}R_{(x,y)}T_x^{-1} \in \mathcal{I}(L)$. Assim, pelo lema anterior temos que A é um subloop de L.*

3. *Seja $x \in G$, Como $\{x\}$ é um conjunto comutativo de L, existe C subloop comutativo maximal de L que contém $\{x\}$, donde segue que $x^m x^n = x^n x^m$ para todos $m, n \in \mathbb{Z}$.*

4. *Para $x \in L$ temos, do ítem anterior, que $\{x\}$ está contido num subloop comutativo maximal de L, e então $(xx)x = x(xx)$. Ou seja $\{x\}$ é um conjunto associativo de L, logo está contido num subloop associoativo maximal de L. Portanto $(x^m x^n)x^p = x^m(x^n x^p)$ para todos $m, n, p \in \mathbb{Z}$.*

Lema 2.1.6. *Sejam L um A-loop e $f, g \in \mathcal{M}(L)$. Suponha $f(1) = g(1)$ e $f(a) = g(a)$ para $a \in G$. Então $f(a^n) = g(a^n)$ para todo $n \in \mathbb{Z}$.*

Demonstração. *Para $f, g \in \mathcal{M}(L)$, tal que $f(1) = g(1)$, temos $g^{-1}(f(1)) = 1$, isto é $g^{-1}f \in \mathcal{I}(L)$. Como $g^{-1}(f(a)) = a$, pelo lema 2.1.4, a pertence ao subloop de L que consiste nos elementos que são fixos pelo automorfismo $g^{-1}f$. Logo $g^{-1}(f(a^n)) = a^n$, para todo $n \in \mathbb{Z}$.*□

Teorema 2.1.7. *Seja L um A-loop. Então:*

1. *$x^m(x^n y) = x^n(x^m y)$ para todos $x, y \in L$ e $m, n \in \mathbb{Z}$.*

2. *$(yx^m)x^n = (yx^n)x^m$ para todos $x, y \in L$ e $m, n \in \mathbb{Z}$.*

3. *$(x^m y)x^n = x^m(yx^n)$ para todos $x, y \in L$ e $m, n \in \mathbb{Z}$.*

4. *Se $(xy)z = x(yz)$, então $(x^m y^n)z^p = x^m(y^n z^p)$ para todos $m, n, p \in \mathbb{Z}$.*

5. *Se $xy = yx$, então $x^m y^n = y^n x^m$ para todos $m, n \in \mathbb{Z}$.*

6. $x[(yx)(zx)] = [(xy)(xz)]x$ *para todos* $x, y, z \in L$.

Demonstração. *Sejam* $x, y \in L$

1. *A equação* $R_{xy}(z) = L_x R_y(z)$ *é satisfeita por* $z = 1$ *e por* $z = x$. *Então pelo lema 2.1.6 temos que* $R_{xy}(x^n) = L_x R_y(x^n)$, *ou seja* $x^n(xy) = x(x^n y)$, *para todo* $n \in \mathbb{Z}$. *Fixe* $n \in \mathbb{Z}$ *arbitrariamente e considere a equação* $R_{x^n y}(z) = L_{x^n} R_y(z)$. *Esta última equação é satisfeita por* $z = 1$ *e por* $z = x$, *portanto* $R_{x^n y}(x^m) = L_{x^n} R_y(x^m)$, *para todo* $m \in \mathbb{Z}$. *Ou seja* $x^m(x^n y) = x^n(x^m y)$ *para todos* $m, n \in \mathbb{Z}$

2. *Temos que* $z = 1$ *e* $z = x$ *são soluções da equação* $L_{yx}(z) = R_x L_y(z)$, *logo, pelo lema 2.1.6 temos que* $(yx)x^n = (yx^n)x$ *para todo* $n \in \mathbb{Z}$. *Fixado* $n \in \mathbb{Z}$ *arbitrário, temos que* $z = 1$ *e* $z = x$ *são soluções de* $L_{yx^n}(z) = R_{x^n} L_y(z)$, *e novamente pelo lema 2.1.6 temos* $(yx^n)x^m = (yx^m)x^n$ *para todos* $n, m \in \mathbb{Z}$.

3. *Para provar esse ítem, basta seguir os mesmos passos da demonstração dos ítens 1 e 2, mas considerando a equação* $L_{xy}(z) = R_x R_y(z)$.

4. *Se* $(xy)z = x(yz)$ *temos que* $L_{xy}(z) = L_x L_y(z)$. *Como* $L_{xy}(1) = L_x L_y(1)$ *temos que* $L_{xy}(z^p) = L_x L_y(z^p)$, *para todo* $p \in \mathbb{Z}$, *ou seja* $(xy)z^p = x(yz^p)$. *Assim, temos que* $R_{z^p} L_x(y) = L_x R_{z^p}(y)$ *e então, devido a* $R_{z^p} L_x(1) = L_x R_{z^p}(1)$, *temos* $(xy^m)z^p = x(y^m z^p)$, *para quaisquer* $m, p \in \mathbb{Z}$. *Agora, desde que* $R_{z^p} R_{y^m}(x) = R_{y^m z^p}(x)$ *e* $R_{z^p} R_{y^m}(1) = R_{y^m z^p}(1)$ *temos* $(x^n y^m)z^p = x^n(y^m z^p)$, *para todos* $n, m, p \in \mathbb{Z}$.

5. *Do mesmo modo que o ítem anterior, se* $xy = yx$, *temos a equação* $R_y(z) = L_y(z)$ *satisfeita por* $z = 1$ *e* $z = x$, *portanto* $yx^n = x^n y$ *para todo* $n \in \mathbb{Z}$. *Agora temos* $R_{x^n}(y) = L_{x^n}(y)$ *e assim, como* $R_{x^n}(1) = L_{x^n}(1)$, *temos* $y^m x^n = x^n y^m$ *para quaisquer* $m, n \in \mathbb{Z}$

6. *Temos que* $T_x = L_x^{-1} R_x$ *é um automorfismo de* L *temos que, para todo* $y \in L$,

$$T_x L_x(y) = T_x(yx) = T_x(x) T_x(y) = x T_x(y) = L_x T_x(y).$$

Assim $L_xL_x^{-1}R_x = L_x^{-1}R_xL_x$, *isto é,* $R_xL_x = L_xR_x$ *para todo* $x \in L$. *Desta última igualdade, temos que* $T_x = L_x^{-1}R_x = R_xL_x^{-1}$ *e, portanto, para quaisquer* $y, z \in L$,

$$(R_xL_x^{-1}(y))(R_xL_x^{-1}(z)) = T_x(y)T_x(z) = T_x(yz) = R_xL_x^{-1}(yz). \tag{2.1}$$

Na equação 2.1, substitua y *por* xy *e* z *por* xz, *e então termos*

$$(R_xL_x^{-1}(xy))(R_xL_x^{-1}(xz)) = R_xL_x^{-1}((xy)(xz))$$

$$R_x(y)R_x(z) = R_xL_x^{-1}((xy)(xz))$$

$$(yx)(zx) = L_x^{-1}R_x((xy)(xz))$$

$$(yx)(zx) = L_x^{-1}([(xy)(xz)]x)$$

e, finalmente,

$$x[(yx)(zx)] = [(xy)(xz)]x$$

para todos $x, y, z \in L$.

Consideremos $\mathcal{M}_\rho(L) = \langle R_x : x \in L\rangle$ e $\mathcal{M}_\lambda(L) = \langle L_x : x \in L\rangle$ subgrupos de $\mathcal{M}(L)$.

Teorema 2.1.8. *Seja* L *um A-loop. Então.*

1. *Para cada* $x \in L$, *o conjunto* $\{R_{x^m}, L_{x^n} : n, m \in \mathbb{Z}\}$ *gera um grupo abeliano.*
2. $\mathcal{M}_\rho(L)$ *e* $\mathcal{M}_\lambda(L)$ *são subgrupos normais de* $\mathcal{M}(L)$.

Demonstração.

1. *Seja* $x \in L$. *Do teorema 2.1.7 temos que, para todo* $m, n \in \mathbb{Z}$, $L_{x^n}R_{x^m} = R_{x^m}L_{x^n}$, $L_{x^n}L_{x^m} = L_{x^m}L_{x^n}$ *e* $R_{x^n}R_{x^m} = R_{x^m}R_{x^n}$. *Portanto* $\langle R_{x^m}, L_{x^n} : n, m \in \mathbb{Z}\rangle$ *é um grupo abeliano.*

2. *Sejam $x, y \in L$. Segue do ítem 6 do teorema 2.1.7 que $x[(yx)(zx)] = [(xy)(xz)]x$ para todo $z \in L$. Então $L_x L_{yx} R_x = R_x L_{xy} L_x$, ou seja $L_x L_{yx} L_x^{-1} = R_x L_{xy} R_x^{-1}$. Fixando x e fazendo y variar em L, temos que $R_x \mathcal{M}_\lambda(L) R_x^{-1} \subset \mathcal{M}_\lambda$ para todo $x \in L$. Como $\mathcal{M}(L) = \langle \mathcal{M}_\lambda(L), \mathcal{M}_\rho(L) \rangle$, temos que $\mathcal{M}_\lambda(L)$ é normal em $\mathcal{M}(L)$.*

   Novamente de $x[(yx)(zx)] = [(xy)(xz)]x$ temos que $L_x R_{zx} R_x = R_x R_{xz} L_x$, que é o mesmo que $R_x^{-1} R_{zx} R_x = L_x^{-1} R_{xz} L_x$ para todo $x, z \in L$. De modo análogo ao acima temos que $\mathcal{M}_\rho(L)$ é um subgrupo normal de $\mathcal{M}(L)$.

Para $x, y \in L$, definimos $C(x, y) = L_y^{-1} R_x^{-1} L_y R_x$. Como

$$C(x,y) = (L_y^{-1}R_y)(R_y^{-1}R_x^{-1}R_{yx})(R_{yx}^{-1}L_{yx})(L_{yx}^{-1}L_yL_x)(L_x^{-1}R_x) = T_yR_{(y,x)}^{-1}T_{yx}^{-1}L_{(x,y)}T_x,$$

temos que $C(x, y) \in \mathcal{I}(L)$ para todos $x, y \in L$.

Considere $\mathcal{I}_\rho(L) = \langle R_{(x,y)} : x, y \in L \rangle$, $\mathcal{I}_\lambda(L) = \langle L_{(x,y)} : x, y \in L \rangle$ e $\mathcal{I}_\mu(L) = \langle C(x, y) : x, y \in L \rangle$ subgrupos de $\mathcal{I}(L)$. Para cada $a \in L$, temos que $a \in \mathcal{N}_\rho(L)$ se e somente se $(xy)a = x(ya)$, para todos $x, y \in L$ que é equivalente a $L_{xy}^{-1} L_x L_y(a) = a$ para todos $x, y \in L$. Em outras palavras $a \in \mathcal{N}_\rho(L)$ se e somente se $f(a) = a$ para toda $f \in \mathcal{I}_\lambda(L)$. Do mesmo modo, temos $a \in \mathcal{N}_\lambda(L)$ se e somente se $f(a) = a$ para toda $f \in \mathcal{I}_\rho(L)$ e $a \in \mathcal{N}_\mu(L)$ se e somente se $f(a) = a$ para toda $f \in \mathcal{I}_\mu(L)$.

Lema 2.1.9. *Seja L um A-loop. Então*

1. *$C(x, y) = T_x^{-1} L_{(y,x)}^{-1} L_{(x,y)} T_x$ para quaisquer $x, y \in L$.*
2. *$C(x, y) = T_y R_{(y,x)}^{-1} R_{(x,y)} T_y^{-1}$ para quaisquer $x, y \in L$.*
3. *$C(x, y) = T_y R_{(y,x)}^{-1} T_{yx}^{-1} L_{(x,y)} T_x$ para quaisquer $x, y \in L$.*

Demonstração. *Temos que o ítem 3 foi demonstrado acima. Vamos agora mostrar os ítens 1 e 2.*

1. *Temos que $C(x, y) = L_y^{-1} T_x^{-1} L_x^{-1} L_{yx} L_{(x,y)} T_x$ e, como T_x é um automorfismo de L pela equação 1.2 temos $C(x, y) = L_y^{-1} L_{T_x^{-1}(x)}^{-1} L_{T_x^{-1}(yx)} T_x^{-1} L_{(x,y)} T_x$, ou seja*

$$C(x, y) = L_{(y,x)}^{-1} T_x^{-1} L_{(x,y)} T_x \tag{2.2}$$

pois $T_x^{-1}(x) = x$ *e* $T_x^{-1}(yx) = xy$. *Por outro lado, temos* $L_{(y,x)}(x) = L_{xy}^{-1}(x(yx)) = L_{xy}^{-1}((xy)x) = x$, *desde que, pelo ítem 3 do teorema 2.1.7 temos* $x(yx) = (xy)x$. *Como* $L_{(y,x)}$ *é um automorfismo de* L *temos* $L_{(y,x)}(zx) = L_{(y,x)}(z).x$, *para todo* $z \in L$, *isto é,* $L_{(y,x)}R_x = R_xL_{(y,x)}$ *para todo* $x, y \in L$. *Agora, fazendo* $L_{(y,x)}(xz) = x.L_{(y,x)}(z)$, *obtemos* $L_{(y,x)}L_x = L_xL_{(y,x)}$ *para todo* $x, y \in L$. *Daí segue que* $L_{(y,x)}T_x = T_xL_{(y,x)}$, *e então, na equação 2.2 temos* $C(x, y) = T_x^{-1}L_{(y,x)}^{-1}L_{(x,y)}T_x$ *para quaisquer* $x, y \in L$.

2. *Podemos escrever* $C(x, y) = T_yR_y^{-1}R_x^{-1}T_y^{-1}R_yR_x = T_yR_y^{-1}R_x^{-1}T_y^{-1}R_{xy}T_yT_y^{-1}R_{xy}^{-1}R_yR_x$. *Ou seja,* $C(x, y) = T_yR_{(y,x)}^{-1}T_y^{-1}R_{(x,y)}$, *pois* $T_y^{-1}(xy) = yx$. *Como* $R_{(x,y)}T_y = T_yR_{(x,y)}$, *para todo* $x, y \in L$, *obtemos* $C(x, y) = T_yR_{(y,x)}^{-1}R_{(x,y)}T_y^{-1}$ *para quaisquer* $x, y \in L$. □

Corolário 2.1.10. *Se* L *for um A-loop então* $\mathcal{N}_\rho(L) \subset \mathcal{N}_\mu(L)$ *e* $\mathcal{N}_\lambda(L) \subset \mathcal{N}_\mu(L)$. *Em particular,* $\mathcal{N}(L) = \mathcal{N}_\rho(L) \cap \mathcal{N}_\lambda(L)$

Demonstração. *Basta observar que, pelos ítens 1 e 2 do lema 2.1.9 e pelas equações 1.2 e 1.3 temos*

$$C(x, y) = L_{(T_x(y)^{-1},T_x(x)^{-1})}^{-1}L_{(T_x(x)^{-1},T_x(y)^{-1})} = R_{(T_y(y),T_y(x))}^{-1}R_{(T_y(x),T_y(y))},$$

para quaisquer $x, y \in L$.

2.2 *A*-loops Diassociativos

Definição 2.2.1. *Um loop* L *é chamado* ***diassociativo*** *se, para quaisquer* $x, y \in L$ *o subloop gerado por* x, y, $\langle x, y\rangle$, *for associativo (e, portanto, um grupo).*

Teorema 2.2.2. *Seja* L *um A-loop. As seguintes propriedades são equivalentes.*

1. L *é diassociativo.*

2. $(yx)x = yx^2$ *e* $x(xy) = x^2y$, *para quaisquer* $x, y \in L$.

3. L é um PI-loop.

As identidades do ítem 2 do teorema 2.2.2 são chamadas de ***leis alternativas***.

Demonstração. *Supondo o ítem 2 verdadairo, vamos provar o ítem 1. Como, pelo teorema 2.1.7, $(xy)x = x(yx)$ para quaisquer x, y em qualquer A-loop L, temos que $\{x, y\}$ é um subconjunto associativo de L. Logo está contido num subconjunto associativo maximal de L, que é um grupo. Assim, $\langle x, y\rangle$ é um grupo.*

Agora vamos ter por hipótese o ítem 3. Temos que cada elemento $x \in L$ possui um inverso bilateral x^{-1} e que $x^{-1}(xy) = y = (yx)x^{-1}$ para todo $y \in L$. Do ítem 4 do teorema 2.1.7, temos que $x^{-1}(xy) = y = (x^{-1}x)y$ e $(yx)x^{-1} = y = y(xx^{-1})$ implicam que $x(xy) = x^2y$ e que $(yx)x = yx^2$, o que prova o ítem 2.

Assumindo o ítem 1, vale que $\langle x, y\rangle$ é um grupo, para quaisquer $x, y \in L$. Assim $x^\lambda = x^\rho = x^{-1} \in \langle x, y\rangle$ e $x^{-1}(xy) = y = (yx)x^{-1}$. Com isso, provamos o ítem 3, o que completa a demonstração.

Teorema 2.2.3. *Seja L um A-loop diassociativo e sejam $a, b, c \in L$ tais que $(ab)c = a(bc)$. Então o subloop $H = \langle a, b, c\rangle$ é associativo.*

Demonstração. *Nosso objetivo é mostrar que os elementos a, b, c associam-se em qualquer ordem. Com isso $\{a, b, c\}$ será um subconjunto associativo de L e estará contido num subgrupo de L.*

Considere o conjunto $S = \{s \in H : (ab)s = a(bs)\}$. Como L é um A-loop, H também o é, e assim S é um subloop de H, pois $s \in S$ se e somente se $L_{(b,a)}(s) = s$. Mas, note que $c \in S$, por hipótese e $a, b \in S$ pela diassociatividade. Logo $S = H$ e

$$(ab)h = a(bh) \quad \textit{para todo} \quad h \in H. \tag{2.3}$$

Em 2.3, faça $h = b^{-1}c$, então $(ab)(b^{-1}c) = a(b(b^{-1}c)) = ac$ por diassociatividade. Consequentemente, $ab = (ac)(b^{-1}c)^{-1} = (ac)(c^{-1}b)$, e assim

$$ab = a(c(c^{-1}b)) = (ac)(c^{-1}b). \tag{2.4}$$

É fato que $H = \langle a, c, c^{-1}b\rangle$ *e por 2.4 temos que*

$$(ac)h = a(ch) \quad \textit{para todo} \quad h \in H. \tag{2.5}$$

As outras formas de associatividade seguem usando o mesmo raciocínio. Sendo $\{a, b, c\}$ *um subconjunto associativo de* L*, a demonstração está completa.*

Seja L um A-loop diassociativo. Vimos que, L é um PI-loop e então consideremos $J : L \longrightarrow L$ a aplicação definida por $J(x) = x^{-1}$. Vimos na proposição 1.2.2 que vale

$$L_x^{-1} = L_{x^{-1}}, \quad R_x^{-1} = R_{x^{-1}},$$

$$JL_xJ = R_{x^{-1}} \quad \text{e} \quad JR_xJ = L_{x^{-1}}$$

para todo $x \in L$. Se θ for um automorfismo de L, temos que

$$J\theta(x) = (\theta(x))^{-1} = \theta(x^{-1}) = \theta J(x),$$

para todo $x \in L$, ou seja $J\theta = \theta J$. Agora, em relação aos geradores de $\mathcal{I}(L)$, temos

$$L_{(x,y)} = L_{(x,y)}J^2 = JL_{(x,y)}J = JL_{yx}^{-1}L_yL_xJ = R_{(yx)^{-1}}^{-1}R_{y^{-1}}R_{x^{-1}} = R_{(x^{-1},y^{-1})}, \tag{2.6}$$

$$R_{(x,y)} = R_{(x,y)}J^2 = JR_{(x,y)}J = JR_{xy}^{-1}R_yR_xJ = L_{(xy)^{-1}}^{-1}L_{y^{-1}}L_{x^{-1}} = L_{(x^{-1},y^{-1})}, \tag{2.7}$$

$$T_x = JT_xJ = JL_x^{-1}JJR_xJ = R_xL_x^{-1} = R_{x^{-1}}^{-1}L_x^{-1} = (L_xR_{x^{-1}})^{-1} = T_{x^{-1}}^{-1}, \tag{2.8}$$

$$C(x, y) = JC(x, y)J = JR_xL_yR_x^{-1}L_y^{-1}J = C(y^{-1}, x^{-1})^{-1}. \tag{2.9}$$

Observação 2.2.4. *Para* p, q, r*, no subloop gerado por* $\{x, y\}$*, temos que* $R_{(q,r)}(p) = p$*, pois* L *é um loop diassociativo. Assim* $R_{(q,r)}(zp) = R_{(q,r)}(z)R_{(q,r)}(p) = R_{(q,r)}(z)p$ *para qualquer* $z \in L$*, logo*

$$R_pR_{(q,r)} = R_{(q,r)}R_p. \tag{2.10}$$

Lema 2.2.5. *Sejam* L *um A-loop diassociativo e* p, q, r *elementos do subloop* $\langle x, y\rangle$*. Então:*

1. $R_pR_{(q,r)} = R_{(q,r)}R_p$ *e* $L_pR_{(q,r)} = R_{(q,r)}L_p$*;*

2. $R_pL_{(q,r)} = L_{(q,r)}R_p$ *e* $L_pL_{(q,r)} = L_{(q,r)}L_p$;

3. $R_pC(q,r) = C(q,r)R_p$ *e* $L_pC(q,r) = C(q,r)L_p$;

4. $R_{(q,r)} = R_{(pqr,(qr)^{-1})}R_{(pq,r)}R_{(p,q)}$;

5. $L_{(q,r)} = L_{(rqp,(rq)^{-1})L_{(qp,r)}}L_{(p,q)}$.

Demonstração.

1. *Vimos que* $R_pR_{(q,r)} = R_{(q,r)}R_p$ *(equação 2.10). Para* $z \in L$ *temos, pela observação 2.2.4,*

$$R_{(q,r)}L_p(z) = R_{(q,r)}(pz) = R_{(q,r)}(p)R_{(q,r)}(z) = pR_{(q,r)}(z) = L_pR_{(q,r)}(z),$$

donde segue $R_{(q,r)}L_p = L_pR_{(q,r)}$.

2. *Como* $L_{(q,r)}(p) = L_{(rq)^{-1}}L_rL_q(p) = p$, *segue que, do mesmo modo feito no ítem 1,* $L_{(q,r)}R_p = R_pL_{(q,r)}$ *e* $L_{(q,r)}L_p = L_pL_{(q,r)}$.

3. *Vamos escrever* $T_q(p) = L_{q^{-1}}R_q(p) = q^{-1}pq$ *e* $T_q^{-1} = R_{q^{-1}}L_q(p) = qpq^{-1}$. *Do fato que* $C(q,r) = T_rR_{(r,q)}^{-1}T_(rq)^{-1}L_{(q,r)}T_q$ *temos que*

$$\begin{aligned} C(q,r)(p) &= T_rR_{(r,q)}^{-1}T_(rq)^{-1}L_{(q,r)}(q^{-1}pq) \\ &= T_rR_{(r,q)}^{-1}T_(rq)^{-1}(q^{-1}q) \\ &= T_rR_{(r,q)}^{-1}(rpr^{-1}) \\ &= T_r(rpr^{-1}) = p. \end{aligned}$$

Assim

$C(q,r)R_p(z) = C(q,r)(zp) = C(q,r)(z)C(q,r)(p) = C(q,r)(z)p = R_pC(q,r)(z)$

e

$C(q,r)L_p(z) = C(q,r)(pz) = C(q,r)(p)C(q,r)(z) = pC(q,r)(z) = L_pC(q,r)(z),$

para todo $z \in L$. *Logo* $R_pC(q,r) = C(q,r)R_p$ *e* $L_pC(q,r) = C(q,r)L_p$.

4. Do ítem 1, obtemos

$$\begin{aligned} R_{(q,r)} &= R_{p^{-1}} R_{(q,r)} R_p \\ &= R_{p^{-1}} R_{qr}^{-1} R_r R_q R_p \\ &= R_{p^{-1}} R_{qr}^{-1} R_r R_{pq} R_{pq}^{-1} R_q R_p \\ &= R_{p^{-1}} R_{qr}^{-1} R_r R_{pq} R_{(p,q)} \\ &= R_{p^{-1}} R_{qr}^{-1} R_{pqr} R_{pqr}^{-1} R_r R_{pq} R_{(p,q)} \\ &= R_{p^{-1}qr(qr^{-1})} R_{qr}^{-1} R_{pqr} R_{(pq,r)} R_{(p,q)} \\ &= R_{(pqr,(qr^{-1}))} R_{(pq,r)} R_{(p,q)}. \end{aligned}$$

5. A partir do ítem 2, obtems 5 do mesmo modo que obtemos o ítem 4. □

Do ítem 1 do lema 2.2.5 temos $R_{(q,r)}^{-1} = R_p^{-1} R_{(q,r)}^{-1} R_p$, para quaisquer p, q, r no subloop $\langle x, y \rangle$. Fazendo $p = xy$, $q = x$ e $r = y$, obtemos $R_{(x,y)}^{-1} = R_{(y^{-1},x^{-1})}$. Da mesma forma $L_{(x,y)}^{-1} = L_{(y^{-1},x^{-1})}$.

2.3 Isotopias de A-Loops

Nessa e na próxima seção, trataremos de como obter "novos" A-loops a partir de um A-loop dado. Durante tais seções, L, denotará o loop $(L, .)$. Aqui, nosso objetivo é determinar condições para que um isótopo de L também seja um A-loop.

Definição 2.3.1. *Um loop $(H, *)$ é dito **isótopo** do loop L se existirem bijeções $U, V.W : H \longrightarrow L$, tais que*

$$W(u * v) = U(u)V(v) \quad \textit{para quaisquer} \quad u, v \in H. \tag{2.11}$$

*Um loop $(L, \circ)$ é dito um **isótopo principal** do loop L, se existirem P, Q, permutações do conjunto L, tais que*

$$x \circ y = P(x)Q(y) \quad \textit{para quaisquer} \quad x, y \in L. \tag{2.12}$$

Em [Br] temos que todo loop isótopo de L é isomorfo a um isótopo principal $(L, \circ)$, cuja mltiplicação é dada por

$$x \circ y = R_f^{-1}(x) L_g^{-1}(y) \tag{2.13}$$

onde f, g são elemntos fixados de L e, além disso, gf é a identidade de $(L, \circ)$.

Agora vamos considerar $(L, *)$ o isótopo principal de L definido por

$$x * y = R_f^{-1}(x) y \quad \text{para todos} \quad x, y \in L. \tag{2.14}$$

Se definirmos o loop $(L, \circ)$ por

$$R_f(x \circ y) = R_f(x) * R_f(y) \tag{2.15}$$

então $(L, \circ)$ e $(L, *)$ serão isomorfos e, além disso,

$$x \circ y = R_f^{-1}(x R_f(y)) \quad \text{para quaisquer} \quad x, y \in L. \tag{2.16}$$

Afirmamos que L e $(L, \circ)$ têm a mesma identidade e $\mathcal{M}(L) = \mathcal{M}(L, \circ)$. De fato, para mostrar que 1 é a identidade de $(L, \circ)$, basta observar que

$$x \circ 1 = R_f^{-1}(x R_f(1)) = R_f^{-1}(R_f(x)) = x$$

e

$$1 \circ x = R_f^{-1}(1 R_f(x)) = x$$

. Para $x \in L$, denotaremos por L_x° e R_x° as translações à esquerda e à direita, respectivamente, em relação a $(L, \circ)$. Para qualquer que seja $y \in L$, temos

$$L_x^\circ(y) = x \circ y = R_f^{-1}(x R_f(y)) = R_f^{-1} L_x R_f(y)$$

e

$$R_x^\circ(y) = y \circ x = R_f^{-1}(y R_f(x)) = R_f^{-1}(y L_x(f)) = R_f^{-1} R_{L_x(f)}(y)$$

. Logo $\mathcal{M}(L,\circ) \subset \mathcal{M}(L)$. Para inclusão contrária, usaremos o fato que existem únicos $u, v \in L$ tais que $x = uf$ e $y = vf$ e, ainda, de $x * y = R_f^{-1}(x)y$ e $R_f(x \circ y) = R_f(x) * R_f(y)$ obtemos

$$xy = R_f^{-1}R_f(x)y = R_f(x) * y = R_f(x \circ R_f^{-1}(y)) = R_f R_v^{\circ}(x),$$

ou seja, $R_f^{-1}R_y = R_v^{\circ}$. Logo, para cada $y \in L$, $R_f^{-1}R_y \in \mathcal{M}(L,\circ)$. Fazendo $y = 1$ temos R_f^{-1} (e, portanto) $R_f \in \mathcal{M}(L,\circ)$, assim $R_y \in \mathcal{M}(L,\circ)$ para todo $y \in L$. Da memsa forma, $L_y \in \mathcal{M}(L,\circ)$ para todo $y \in L$. Portanto

$$\mathcal{M}(L) = \mathcal{M}(L,\circ). \tag{2.17}$$

Como consequência de 2.17 e do fato que as identidades de L e $(L,\circ)$ coincidem, segue $\mathcal{I}(L) = \mathcal{I}(L,\circ)$.

A partir de agora suponha L um A-loop. Se $(L,\circ)$, definido como em 2.16, também for um A-loop então para todo $U \in \mathcal{I}(L)$ vale que $U(x \circ y) = U(x) \circ U(y)$, ou

$$U(x \circ y) = U(R_f^{-1}(xR_f(y))) = R_{U(f)}^{-1}(U(x)R_f(y)) = R_{U(f)}^{-1}(U(xR_{U(f)}(U(y)))),$$

ou

$$R_f^{-1}(U(x)R_f(U(y))) = R_{U(f)}^{-1}(U(x)R_{U(f)}(U(y))) \quad \text{para todos} \quad x, y \in L. \tag{2.18}$$

Substituindo, em 2.18, x por $U^{-1}(x)$, y por $U^{-1}R_f^{-1}(y)$ e chamando $S = R_{U(f)R_f^{-1}}$ obtemos

$$S(xy) = xS(y) \quad \text{para todos} \quad x, y \in L. \tag{2.19}$$

Agora, faça $y = 1$, em 2.19, e denote $s = S(1)$. Então $S(x) = xs = R_s(x)$, qualquer que seja $x \in L$, isto é $S = R_s$. Voltando a 2.19, temos $R_s(xy) = xR_s(y)$ para todos $x, y \in L$, o que é equivalente a $s \in \mathcal{N}_\rho(L)$.

Concluimos que se $(L,\circ)$ for um A-loop então para cada $U \in \mathcal{I}(L)$ existirá $s \in \mathcal{N}_\rho(L)$ tal que $R_{U(f)} = R_s R_f$.

Reciprocamente, suponha que para cada $U \in \mathcal{I}(L)$ exista $s \in \mathcal{N}_\rho(L)$ tal que $R_{U(f)} = R_s R_f$. Como, para quaisquer $x, y \in L$, temos que $R_s(xy) = xR_s(y)$, vale que

$$\begin{aligned} U(x \circ y) &= U(R_f^{-1}(xR_f(y))) \\ &= R_{U(f)}^{-1}(U(x)R_{U(f)}(U(y))) \\ &= R_{U(f)}^{-1}(U(x)R_sR_f(U(y))) \\ &= R_{U(f)}^{-1}R_s(U(x)R_f(U(y))) \\ &= R_f^{-1}(U(x)R_f(U(y))) \\ &= U(x) \circ U(y) \end{aligned}$$

donde segue que $U \in Aut(L, \circ)$. Com isso, temos demosntrado o seguinte lema:

Lema 2.3.2. *Seja L um A-loop. Uma codição necessária e suficiente para que o iótopo principal $(L, \circ)$, definido por $x \circ y = R_f^{-1}(xR_f(y))$, para $x, y \in L$, seja um A-loop é que, para cada $U \in \mathcal{I}(L)$, exista $s \in \mathcal{N}_\rho(L)$ tal que $R_{U(f)} = R_sR_f$.*

Observação. *No lema acima, a condição $R_{U(f)} = R_sR_f$ é equivaente a $L_f^{-1}(U(f)) \in \mathcal{N}_\rho(L)$.*

O *subloop (centralmente) derivado*, L', é o subloop de L, definido pela interseção de todos os subloops $K \lhd L$, tais que L/K seja um grupo abeliano. Em [Br], Bruck provou que

$$L' = \langle R_x^{-1}(U(x)) : x \in L, U \in \mathcal{I}(L)\rangle = \langle L_x^{-1}(U(x)) : x \in L, U \in \mathcal{I}(L)\rangle. \qquad (2.20)$$

Assim, de 2.20, temos que um isótomo principal de um A-loop L do tipo 2.16 será um A-loop se e somente se $L' \subset \mathcal{N}_\rho(L)$. Definindo $(L, \star)$, isótopo principal de um A-loop L, por

$$x \star y = L_g^{-1}(L_g(x)y) \quad \text{para quaisquer} \quad x, y \in L, \qquad (2.21)$$

temos que, $(L, \star)$ será um A-loop se e somente se $L' \subset \mathcal{N}_\lambda(L)$.

A seguir, temos o principal teorema dessa seção.

Teorema 2.3.3. *Seja L um A-loop. Então todo loop isótopo de L será um A-loop se e somente se $L' \subset \mathcal{N}(L)$.*

Demonstração. *Se todos os isótopos de L são A-loops, em particular os isótopos dos tipos 2.16 e 2.21, também o são. Então $L' \subset \mathcal{N}_\rho(L)$ e $L' \subset \mathcal{N}_\lambda(L)$, donde temos $L' \subset \mathcal{N}(L) = \mathcal{N}_\rho(L) \cap \mathcal{N}_\lambda(L)$.*

Reciprocamente suponha $L' \subset \mathcal{N}(L)$ e seja $(L, \circ)$ um isótopo de L da forma

$$x \circ y = R_f^{-1}(x) L_g^{-1}(y).$$

Sabemos que gf é a identidade de $(L, \circ)$, $L_x^\circ(y) = L_{R_f^{-1}(x)} L_g(y)$, $R_y^\circ(x) = R_{L_g^{-1}(y)} R_f^{-1}(x)$ e $xy = R_f^{-1}(xf) L_g^{-1}(gy) = R_f(x) \circ L_g(y)$. Assim $\mathcal{M}(L) = \mathcal{M}(L, \circ)$.
Uma aplicação $T \in \mathcal{M}(L, \circ)$ será uma aplicação interna de $(L, \circ)$ se e somente se $T(gf) = gf$. De [Br] temos que existem $U \in \mathcal{I}(L)$ e $b \in L$ tais que $T = R_b U$. Temos que $L_{gf}^{-1}(U(gf)) = a \in \mathcal{N}(L)$, então $U(gf) = (gf)a$. Assim, $T \in \mathcal{I}(L, \circ)$ se e somente se

$$gf = T(gf) = R_b U(gf) = ((gf)a)b = (gf)(ab),$$

ou seja, $b = a^{-1}$. Também temos que $U(f) = fs$ e $U(g) = gt$, onde $s, t \in \mathcal{N}(L)$, assim, $g(fa) = (gf)a = U(gf) = U(g)U(f) = (gt)(fs) = g(t(fs))$, isto é, $fa = (tf)s$. Logo

$$\begin{aligned}
T(T^{-1}(x) \circ T^{-1}(y)) &= R_{a^{-1}} U(U^{-1} R_a(x) \circ U^{-1} R_a(y)) \\
&= R_{a^{-1}} U((R_f^{-1} U^{-1} R_a(x))(L_g^{-1} U^{-1} R_a(y))) \\
&= R_{a^{-1}} (U(R_f^{-1} U^{-1} R_a(x)) U(L_g^{-1} U^{-1} R_a(y)) \\
&= (R_{U(f)}^{-1}(R_a(x)) L_{U(g)}^{-1}(R_a(y))) a^{-1} \\
&= (R_{fs}^{-1}(R_a(x)) L_{gt}^{-1}(R_a(y))) a^{-1} \\
&= (R_{fs}^{-1} R_a(x))(L_{gt}^{-1} R_a(y).a^{-1}) \\
&= (R_{fs}^{-1} R_a(x))(R_{a^{-1}} L_{gt}^{-1} R_a(y)) \\
&= (R_{t^{-1} fa}^{-1} R_a(x)) L_{gt}^{-1}(y) \qquad (2.22) \\
&= R_t R_f^{-1}(x) L_t^{-1} L_g^{-1}(y) \\
&= R_f^{-1}(x) L_g^{-1}(y) = x \circ y,
\end{aligned}$$

onde, em 2.22 usamos o fato de que $a \in \mathcal{N}(L)$. Assim mostramos que T^{-1} é um automorfismo de $(L, \circ)$, consequentemete, $(L, \circ)$ é um A-loop, como queríamos demosntrar.

2.4 Holomorfos de A-loops

Agora discutiremos condições para que um tipo especial de holomorfo do A-loop L também seja um A-loop.

Definição 2.4.1. *Seja K^* um grupo de automorfismos de L. O K^*-**holomorfo** de L, denotado por $[K^*, L]$, é o loop formado por elementos $[S, x]$, onde $S \in K^*$ e $x \in L$, com multiplicação dada por*

$$[S, x][T, y] = [TS, T(x)y] \tag{2.23}$$

O conjunto $[K^*, L]$ é, de fato, um loop pois, para quaisquer $[A, a], [B, b] \in [K^*, L]$, temos que $[A^{-1}B, A^{-1}(R_a^{-1}(b))]$ e $[BA^{-1}, L_{BA^{-1}(a)}(b)]$ são, respectivamente, as únicas soluções de $[X, x][A, a] = [B, b]$ e de $[A, a][X, x] = [B, b]$. Além disso, está claro que $[Id_L, 1]$ é o elememto neutro de $[K^*, L]$.

Definição 2.4.2. *Um **automorfismo de centro** de um loop L é um automorfismo S de L, tal que $S(x) = x.c(x)$ onde $c(x)$ é um elemento de $\mathcal{Z}(L)$.*

Temos que se S for um automorfismo de centro de L, S^{-1} também será. De fato, se $S(x) = x.c(x)$, com $c(x) \in \mathcal{Z}(L)$, então $S^{-1}(x) = S^{-1}(S(x).c(x)^{-1}) = x.S^{-1}(c(x)^{-1})$. Como $S^{-1}(c(x)^{-1}) \in \mathcal{Z}(L)$, concluimos que S^{-1} é um automorfismo de centro de L.

Lema 2.4.3. *Se S for um automorfismo de centro de L, então $SU = US$ para toda aplicação interna U.*

Demonstração. *Notemos que, para quaisquer $x, y \in L$,*

$$(xy).c(xy) = S(xy) = S(x)S(y) = (x.c(x))(y.c(y)) = (xy).c(x)c(y),$$

ou seja, S induz um homomorfismo de L no grupo abeliano $\mathcal{Z}(L)$. Pelo Teorema do Homomorfismo, temos que $L/ker(c) \cong H \leq \mathcal{Z}(L)$, assim, $L' \subset ker(c)$. Como $L' = \langle L_x^{-1}(U(x)) : x \in L, U \in \mathcal{I}(L)\rangle$, temos que $c(L_x^{-1}U(x)) = 1$, quaisquer que sejam $x \in L$ e $U \in \mathcal{I}(L)$. Desde que, $U(x) = L_x L_x^{-1}U(x) = x.L_x^{-1}U(x)$ temos que $c(U(x)) = c(x.L_x^{-1}U(x)) = c(x)$.

Usando que $U(x.c(x)) = U(x).c(x)$, fato demonstrado por Bruck em [Br], temos que

$$U(S(x)) = U(x.c(x)) = U(x).c(x) = U(x).c(U(x)) = S(U(x)),$$

e, portanto, $US = SU$.

O próximo teorema, o resultado mais importante dessa seção, nos dá condições de caracterizar quando que um K^*-holomorfo de um loop é um A-loop, para um grupo particular de automorfismos, é um A-loop.

Teorema 2.4.4. *Seja K^* um grupo de automorfismos de centro de um loop L. Uma condição necessária e suficiente para que o K^*-holomorfo L seja um A-loop é que L seja um A-loop.*

Demonstração. *Suponha $[K^*, L]$ um A-loop.*

Desde que o conjunto $\{[Id_L, x]|x \in L\}$ é um subloop de $[K^*, L]$ isomorfo a L, temos que L é um A-loop.

Reciprocamente, suponha L um A-loop.

Sejam $[A, a], [B, b] \in [K^*, L]$. Queremos mostrar que $R_{([A,a],[B,b])}, L_{([A,a],[B,b])}$ e $T_{[A,a]}$ são automorfismos de $[K^*, L]$. Para qualquer $[S, x] \in [K^*, L]$ temos que

$$R_{([A,a],[B,b])}([S, x]) = [S, R_{(B(a),b)}(x)] \tag{2.24}$$

e

$$L_{([A,a],[B,b])}([S, x]) = [S, L_{(a,A(b))}(x)]. \tag{2.25}$$

Sejam $[S, x], [V, y] \in [K^*, L]$. De 2.24, temos que

$$R_{([A,a],[B,b])}([S, x][V, y]) = [VS, V(R_{(B(a),b)}(x))R_{(B(a),b)}(y)] \tag{2.26}$$

e, por outro lado,

$$R_{([A,a],[B,b])}([S,x]) = [S, R_{(B(a),b)}(x)] \quad e \quad R_{([A,a],[B,b])}([V,y]) = [V, R_{(B(a),b)}(y)]. \quad (2.27)$$

Assim, concluimos que

$$R_{([A,a],[B,b])}([S,x][V,y]) = R_{([A,a],[B,b])}([S,x])R_{([A,a],[B,b])}([V,y]),$$

donde temos que $R_{([A,a],[B,b])}$ *é um automorfismo de* $[K^*, L]$. *De maneira análoga temos que* $L_{([A,a],[B,b])}$ *também é um automorfismo de* $[K^*, L]$.

Finalmente vamos analisar o gerador $T_{[A,a]}$. *Fazendo*

$$T_{[A,a]}([S,x]) = L^{-1}_{[A,a]}R_{[A,a]}([S,x]) = [Z,z],$$

teremos $Z = ASA^{-1}$ *e* $A(x)a = ASA^{-1}(a)z$. *Como* ASA^{-1} *é um automorfismo de centro de* L, *temos que* $ASA^{-1}(a) = a.c_{ASA^{-1}}(a)$, *onde* $c_{ASA^{-1}}$ *é o homomorfismo de* L *em* $\mathcal{Z}(L)$ *induzido por* ASA^{-1}. *Assim*

$$A(x)a = (a.c_{ASA^{-1}}(a))z = a(c_{ASA^{-1}}(a)z),$$

ou seja, $z = T_a(A(x)).c_{ASA^{-1}}(a)^{-1}$, *portanto*

$$T_{[A,a]}([S,x]) = [ASA^{-1}, T_a(A(x)).c_{ASA^{-1}}(a)^{-1}]. \quad (2.28)$$

Vamos mostrar que $T_{[A,a]}$ *é um automorfismo de* $[K^*, L]$. *De 2.28 temos*

$$T_{[A,a]}([S,x][V,y]) = [AVSA^{-1}, T_aA(V(x)y).c_{AVSA^{-1}}(a)^{-1}] \quad (2.29)$$

e $T_{[A,a]}([S,x])T_{[A,a]}([V,y]) = [AVSA^{-1}, w]$, *onde*

$$w = AVA^{-1}(T_aA(x)c_{ASA^{-1}}(a^{-1}))T_aA(y)c_{AVA^{-1}}(a)^{-1}. \quad (2.30)$$

Agora notemos que

$$\begin{aligned} w &= T_aAV(x).T_aA(y).AVA^{-1}.(c_{ASA^{-1}}(a^{-1})).c_{AVA^{-1}}(a)^{-1} \\ &= T_aA(V(x)y).(AVA^{-1}(c_{ASA^{-1}}(a)^{-1}).c_{AVA^{-1}}(a)^{-1}). \end{aligned}$$

Portanto, $T_{[A,a]}$ será um automorfismo de $[K^*, L]$ se e somente se valer

$$AVA^{-1}(c_{ASA^{-1}}(a)^{-1}).c_{AVA^{-1}}(a)^{-1} = c_{AVSA^{-1}}(a)^{-1}. \tag{2.31}$$

É fato que

$$\begin{aligned} AVSA^{-1}(a) &= AVA^{-1}(ASA^{-1}(a)) \\ &= AVA^{-1}(a.c_{ASA^{-1}})(a) \\ &= AVA^{-1}(a)AVA^{-1}(c_{ASA^{-1}}(a)) \\ &= a.c_{AVA^{-1}}(a)AVA^{-1}(c_{ASA^{-1}}(a)). \end{aligned} \tag{2.32}$$

Por outro lado,

$$AVSA^{-1}(a) = a.c_{AVSA^{-1}}(a). \tag{2.33}$$

Então de 2.32 e 2.33 temos que vale a identidade 2.31. Logo $T_{[A,a]}$ é um automorfismo de $[K^*, L]$. Concluimos, então, que $[K^*, L]$ é um A-loop, como queríamos demonstrar.

2.5 Construção e Exemplos de A-Loops

Nessa seção apresentaremos uma nova maneira de se construir novos A-loops a partir de A-loops dados.

Sejam L um loop, S e T automorfismos de L. Considere o conjunto Q formado pelos pares $[A^i, x]$ onde $i = 0, 1$ e $x \in L$. Em Q, defina a seguinte multiplicação:

$$[1,x][1,y] = [1,xy] \quad [1,x][A,y] = [A,S(x)y]$$
$$[A,x][1,y] = [A,xy] \quad [A,x][A,y] = [1,xT(y)]$$

Vamos mostrar que com esta multiplicação, Q admite estrutura de loop. Para isso, primeiramente, mostremos que Q é um quase-grupo. Considere a equação $[A^i, a][A^j, x] = [A^k, b]$, com incógnita $[A^j, x]$ e onde $[A^i, a], [A^k, b] \in Q$.

1. Se $i = k = 1$, faça $j = 0$ e tome x a única solução da equação $ax = b$ em L. A unicidade de x nos garante a unicidade da solução $[1, x]$.

2. Se $i = 1$ e $k = 0$, tome $j = 1$ e x a única solução da equação $aT(x) = b$. A unicidade de $[A, x]$ segue do mesmo argumento do ítem 1.

3. Para o caso de $i = 0$ e $k = 1$, tome $j = 1$ e x a única solução de $S(a)x = b$.

4. Finalmente para $i = k = 0$, tome $j = 0$ e x a única solução de $ax = b$.

Para as equações $[A^j, x][A^i, a] = [A^k, b]$ onde $i, k = 0, 1$ usamos raciocínio análogo ao usado acima. Assim temos que Q éum quase-grupo. Para mostrar que Q é um loop, vamos mostrar que $[1, 1]$ é elemento neutro de Q. De fato,

$$[1,1][1,x] = [1,x] \quad [1,x][1,1] = [1,x]$$
$$[1,1][A,x] = [A,S(1)x] = [A,x] \quad [A,x][1,1] = [A,x]$$

para qualquer $x \in L$. Logo temos que Q é um loop.

Bruck e Paige, em [BP], mostraram o seguinte lema, do qual faremos uso na demosntração do próximo teorema.

Lema 2.5.1. *Sejam L um loop, S, T automorfismos de L tais que $T(x) = x^{-1}$ para todo $x \in \mathcal{Z}(L)$. Considere o loop Q como definido acima, e $M : Q \longrightarrow Q$ definida por*

$$M([1,x]) = [1,\alpha(x)] \quad M([A,x]) = [A,\beta(x)]$$

onde α, β são permutações de L. Então M será um automorfismo de Q se e somente se α for um automorfismo de L que comuta com S e T e $\beta(x) = c\alpha(x)$ onde $c \in \mathcal{Z}(L)$.

Teorema 2.5.2. *Seja G um grupo abeliano e S o automorfismo de G dado por $S(x) = x^{-1}$ para todo $x \in G$. Considere o loop $L = \{[S^i, x] : i = 0, 1 \quad x \in G\}$ sob a seguinte multiplicação*

$$[1,x][1,y] = [1,xy] \quad [1,x][S,y] = [A,S(x)y]$$
$$[S,x][1,y] = [A,xy] \quad [S,x][S,y] = [1,xS(y)].$$

Então L é um A-loop.

Demonstração. *Vamos aqui usar o lema 2.5.1. Para isso vamos mostrar que os geradores de $\mathcal{I}(L)$, satisfazem as condições da aplicação M desse lema. Tal demonstração será feita para apenas um gerador já que para os outros geradores o argumento é inteiramente análogo. Sejam $[S,a],[S,b] \in L$ e faça $R_{([S,a],[S,b])}([1,x]) = [Z,z]$. Assim temos que*

$$R^{-1}_{[S,a][S,b]} R_{[S,b]} R_{[S,a]}([1,x]) = [Z,z],$$

$$R_{[S,b]([1,x][S,a])} = [Z,z]([S,a][S,b]),$$

$$[S, x^{-1}a][S,b] = [Z,z][1.ab^{-1}],$$

$$[Z,z][1,ab^{-1}] = [1,(x^{-1}a)b^{-1}],$$

o que implica que $Z = 1$ e $z = R_{(a,b^{-1})}S(x)$, isto é,

$$R_{([S,a],[S,b])}([1,x]) = [1, R_{(a,b^{-1})}S(x)]. \tag{2.34}$$

Da mesma forma, obtemos

$$R_{([S,a],[S,b])}([S,x]) = [S, R_{b^2}R_{(a,b)}S(x)]. \tag{2.35}$$

Então aplicando o lema 2.5.1 para a aplicação $R_{([S,a],[S,b])}$, temos que esta é um automorfismo de L.

Bruck e Paige em [BP], mostraram um resultado mais geral para o teorema 2.5.2. Na verdade esse resultado vale se G for um A-loop, S um automorfismo de centro de L e $T = S^{-1}$. O próximo resultado nos fala de construções de A-loops através de extensões centrais.

Teorema 2.5.3. *Sejam Z um grupo abeliano e K um A-loop. Para cada par de elementos (p,q) de K determine um elemento $z(p,q) \in Z$, satisfazendo $z(p,1) = z(1,p) = 1$ (os elementos neutros de Z e K serão denotados por 1) e respeitando as segintes restrições:*

$$F(p,s,t)F(q,s,t)z(R_{(s,t)}(p), R_{(s,t)}(q)) = F(pq,s,t)z(p,q), \tag{2.36}$$

para todos $p, q, s, t \in K$*, onde,* $F(p,s,t) = z(R_{(s,t)}(p), st)^{-1} z(s,t)^{-1} z(ps,t) z(p,s)$*,*

$$G(p,s,t)G(q,s,t)z(L_{(s,t)}(p), L_{(s,t)}(q)) = G(pq,s,t)z(p,q), \tag{2.37}$$

para todos $p, q, s, t \in K$*, onde,* $G(p,s,t) = z(ts, L_{(s,t)}(p))^{-1} z(t,s)^{-1} z(t,sp) z(s,p)$ *e*

$$H(p,t)H(q,t)z(T_t(p), T_t(q)) = H(pq,t)z(p,q), \tag{2.38}$$

para todos $p, q, t \in K$*, onde,* $H(p,t) = z(t, T_t(p))^{-1} z(p,t)$*.*
Seja $G = K \ltimes_z Z$ *o cinjunto dos pares* $(p,x) \in K \times Z$ *munido da seguinte operação binária:*

$$(p,x)(q,y) = (pq, z(p,q)xy).$$

Então G *é um A-loop. Além disso, o conjunto dos pares* $(1,x), x \in Z$ *é um subloop normal de* G *contido no centro* $\mathcal{Z}(G)$ *e o loop quociente* $G/(1,Z)$ *é isomorfo a* K*.*

Demonstração. *As estruturas de grupo de* Z *e de loop de* K *fazem com que* G *tenha estrutura de loop com elemento neutro* $(1,1)$*. Antes de mostrar que* G *é um A-loop vamos determinar como os geradores de* $\mathcal{I}(G)$ *agem em* G*. Sejam* $(p,x), (q,y), (s,u) \in G$*. Faça* $R_{((p,x),(q,y))}(s,u) = (t,v)$*, então*

$$R^{-1}_{(p,x)(q,y)} R_{(q,y)} R_{(p,x)}(s,u) = (t,v),$$

$$R_{(q,y)}((s,u)(p,x)) = (t,v)((p,x)(q,y)),$$

$$(sp, z(s,p)ux)(q,y) = (t,v)(pq, z(p,q)xy),$$

$$(t(pq), z(t,pq)z(p,q)xyv) = ((sp)q, z(sp,q)z(s,p)uxy),$$

e assim $t = R_{(p,q)}(s)$ *e* $v = z(t,pq)^{-1} z(p,q)^{-1} z(sp,q) z(s,p) u$*, então*

$$R_{((p,x),(q,y))}(s,u) = (R_{(p,q)}(s), z(R_{(p,q)}(s), pq)^{-1} z(p,q)^{-1} z(sp,q) z(s,p) u). \tag{2.39}$$

Procedendo da mesma forma, obtemos

$$L_{((p,x),(q,y))}(s,u) = (L_{(p,q)}(s), z(qp, L_{(p,q)}(s))^{-1} z(q,p)^{-1} z(q,ps) z(s,p) u) \quad e \qquad (2.40)$$

$$T_{(p,x)}(s,u) = (T_p(s), z(p, T_p(s))^{-1} z(s,p) u). \qquad (2.41)$$

Agora é fácil ver que, pelas equações 2.39, 2.40 e 2.41, $R_{((p,x),(q,y))}, L_{((p,x),(q,y))}$ *e* $T_{(p,x)}$ *serão automorfismos de* G *se e somente se valerem as equações 2.36, 2.37 e 2.38, respectivamente. Portanto* G *é um A-loop.*

Agora vamos mostrar que o conjunto $(1,Z) = \{(1,x) : x \in Z\}$ *é um subloop normal de* G*. Como* $(1,1) \in (1,Z)$ *temos que esse conjunto é não vazio. Sejam* $(p,x),(q,y),(s,u) \in G$ *tais que* $(p,q)(q,y) = (s,u)$*.*

1. *Se* $(p,x),(q,y) \in (1,Z)$*, temos que* $p = q = 1$ *e assim* $(s,u) = (1,xy) \in (1,Z)$*,*
2. *se* $(p,x),(s,u) \in (1,Z)$*, temos que* $p = s = 1$ *e assim* $(q,y) = (1,x^{-1}u) \in (1,Z)$*,*
3. *se* $(s,u),(q,y) \in (1,Z)$*, temos que* $s = q = 1$ *e assim* $(p,x) = (1,uy^{-1}) \in (1,Z)$*.*

Assim $(1,Z)$ *é um subloop de* G*. Pelas equações 2.39, 2.40 e 2.41, temos que* $(1,Z)^{\varphi} = (1,Z)$ *para todo* $\varphi \in \mathcal{I}(L)$*. Logo* $(1,Z)$ *é um subloop normal de* G*. Finalmente vamos mostrar que* $G/(1,Z) \simeq K$*. Para isso considere a sobrejeção* $\Psi : G \longrightarrow K$ *definida por* $\Psi(p,x) = p$*. Note que*

$$\Psi((p,x)(q,y)) = \Psi(pq, z(p,q)xy) = pq = \Psi(p,x)\Psi(q,y),$$

assim Ψ *é um homomorfiso sobrejetor entre os loops* G *e* K*. Desde que* $\Psi(p,x) = 1$ *se e somente se* $(p,x) \in (1,Z)$ *temos* $ker(\Psi) = (1,Z)$*. Logo* $G/(1,Z) \simeq K$*.* $\square$

Capítulo 3

A-Loops Comutativos Finitos: Estrutura

Nesse capítulo estudaremos estrutura de um A-loop comutativo que, salvo meção contrária, denotaremos por Q. Para A-loops comutativos, têm-se muitos resultados interessantes dentre eles o Teorema da Ordem Ímpar que nos garante que todo A-loop comutativo finito de ordem ímpar é solúvel. Outro resultado bastante importante é o Teorema da Decomposição que afirma que todo A-loop comutativo finito é o produto direto de um A-loop de ordem ímpar por um A-loop de expoente 2. Encerraremos esse capítulo mostrando que valem os teoremas de Lagrange, Cauchy para A-loops comutativos finitos.

3.1 Notações e Fatos Básicos

Vamos agora estabelecer algumas noações e estabelecer alguns pequenos resultados que usaremos no decorrer do capítulo. Temos que $L_x : Q \longrightarrow Q$ é uma translação de Q e, associada a essa translação, vamos definir uma *divisão à esquerda* por $x\backslash y = L_x^{-1}(y)$. Definiremos também as *permutações de divisão* $D_x : Q \longrightarrow Q$ por $D_x(y) = y\backslash x$. Temos que $D_x^2 = id_Q$ para todo $x \in Q$. Como Q é comutativo temos

que $x^\rho = x^\lambda$ que denotaremos por x^{-1} e, assim, $x^{-1} = x\backslash 1 = L_x^{-1}(1)$ e ainda podemos definir $J : Q \longrightarrow Q$ por $J(x) = x^{-1}$.

Notemos que se $u, v \in Q$, $u\backslash v = w$ se e somente se, $uw = v$. Desde que $L_{(x,y)} = L_{yx}^{-1} L_y L_x \in \mathcal{I}(L)$, temos que $L_{(x,y)}(v) = L_{(x,y)}(uw) = (L_{(x,y)}(u))(L_{(x,y)}(w))$, ou seja

$$L_{(x,y)}(u\backslash v) = (L_{(x,y)}(u))\backslash(L_{(x,y)}v)) \tag{3.1}$$

para quaisquer $x, y, u, v \in Q$. Também temos que $JL_{(x,y)} = L_{(x,y)}J$, para todos $x, y \in Q$.

Para φ um automorfismo de Q, consideremos

$$Fix(\varphi) = \{x \in Q : \varphi(x) = x\}$$

. Pelo lema 2.1.4, temos que $Fix(\varphi)$ é um subloop de Q e que, portanto, se $x \in Fix(\varphi)$, o subgrupo de Q, gerado por x, é de fato, subgrupo de $Fix(\varphi)$. Agora, tomando $x \in Fix(\varphi)$ e $y \in Q$ notemos que

$$\varphi(L_x(y)) = \varphi(xy) = \varphi(x)\varphi(y) = x\varphi(y) = L_x(\varphi(y))$$

e

$$\varphi(D_x(y)) = \varphi(y\backslash x) = \varphi(y)\backslash\varphi(x) = \varphi(y)\backslash x = D_x(\varphi(y)).$$

Assim

$$L_x\varphi = \varphi L_x \quad \text{e} \quad D_x\varphi = \varphi D_x \tag{3.2}$$

para todo $x \in Fix(\varphi)$.

Lema 3.1.1. *Para quaisquer x, y, z em um A-loop comutativo Q, $x \in Fix(L_{(y,z)})$ se e somente se $L_xL_z(y) = L_zL_x(y)$ que é equivalente a $z \in Fix(L_{(y,x)})$.*

Demonstração. *Temos que $x \in Fix(L_{(y,z)})$ se e somente se $L_{zy}^{-1}L_zL_y(x) = x$, isto é $z(yx) = (zy)x$. Como Q é comutativo, esta última equação é o mesmo que $z(xy) = x(zy)$, ou seja $L_xL_z(y) = L_zL_x(y)$. Finalmente $z(xy) = x(zy)$ é equivalente a $L_{xy}(z) = L_xL_y(x)$, isto é, $z \in Fix(L_{(y,x)})$.* □

Do teorema 2.1.7 temos que, em Q, vale que

$$L_{(y,x^m)}(x^n) = x^n; \tag{3.3}$$

$$L_{x^m}L_{x^n} = L_{x^n}L_{x^m} \tag{3.4}$$

$$L_{x^n}L_{(y,x^m)} = L_{(y,x^m)}L_{x^n} \tag{3.5}$$

$$D_{x^n}L_{(y,x^m)} = L_{(y,x^m)}D_{x^n} \tag{3.6}$$

para quaisquer $x, y \in Q$ e $n, m \in \mathbb{Z}$. Ainda temos que Q associa potências, pelo teorema 2.1.5.

Lema 3.1.2. *Para quaisquer $x, y \in Q$, valem as seguintes propriedades:*

1. $L_{(y,x)}(y^n) = (xy\backslash x)^{-n}$, *para todo* $n \in \mathbb{Z}$
2. $xy^2 = (xy)(xy\backslash x)^{-1}$.

Demonstração. *Temos que $L_{(y,x)}(y^{-n}) = L_{(y,x)}((y^{-1})^n) = (L_{(y,x)}(y^{-1}))^n$ pois $L_{(y,x)}$ é um automorfismo de Q. Assim $L_{(y,x)}(y^{-n}) = (L_{xy}^{-1}L_xL_y(y^{-1}))^n = (L_{xy}^{-1}(x))^n = (xy\backslash x)^n$. Substituindo n por $-n$ obtemos a identidade 1.*
Temos que $L_{(y,x)}(y) = L_{xy}^{-1}L_xL_y(y) = L_{xy}^{-1}(y^2x) = (xy)\backslash(xy^2)$. Do ítem 1, temos que $(xy)\backslash(xy^2) = (xy\backslash x)^{-1}$, que nos dá o ítem 2. □

Pelo teorema 2.1.7, temos que todo A-loop comutativo Q, é um PI-loop, no sentido da definição dada no capítulo 1. Um loop L é dito ter a ***propriedade automórfica do inverso*** (AIP) e se todos os seus elementos possuirem inverso bilateral se, para todos $x, y \in L$

$$(xy)^{-1} = x^{-1}y^{-1} \quad \text{ou, equivalentemente} \quad L_xJ = JL_{x^{-1}}. \tag{3.7}$$

Lema 3.1.3. *Todo A-loop comutativo tem AIP.*

Demonstração. *Temos que* $L_xL_{x^{-1}} = L_{(x^{-1},x)}$ *é um automorfismo de* Q. *De 3.4 temos que*

$$JL_{x^{-1}}L_x(y) = JL_xL_{x^{-1}}(y) = L_xL_{x^{-1}}(y^{-1}) = L_x(x^{-1}y^{-1}) = L_xL_{y^{-1}}(x^{-1}) =$$

$$= [L_xL_y][L_y^{-1}L_{y^{-1}}](x^{-1}) = L_{xy}L_{xy}^{-1}L_xL_yL_{y^{-1}}L_y^{-1}(x^{-1}) = L_{xy}[L_{(y,x)}L_{y^{-1}}]L_y^{-1}(x^{-1}) =$$

$$= L_{xy}L_{L_{(y,x)}(y^{-1})}L_{(y,x)}L_y^{-1}(x^{-1})$$

. Pelo ítem 1 do lema 3.1.2 temos

$$L_{xy}[L_{L_{(y,x)}(y^{-1})}L_{(y,x)}L_y^{-1}(x^{-1})] = L_{xy}[(xy)^{-1}(xy\backslash x)] =$$

$$= L_{xy}L_{(xy)}^{-1}L_{(xy)^{-1}}(x) = L_{(xy)^{-1}}(x) = L_x(xy^{-1}) = L_xJL_x(y).$$

Daí temos que, $L_{x^{-1}}J = JL_x$ *para todo* $x \in L$

Lema 3.1.4. *Num A-loop comutativo* Q, *para quaisquer* $x, y \in Q$, *as seguintes identidades se verificam:*

1. $L_{(x,y)} = L_{(x^{-1},y^{-1})}$;
2. $L_{(x,y)} = L_yL_xL_{x^{-1}\backslash y}^{-1}$;
3. $L_{(x,y)} = L_xL_{x^{-1}\backslash y}^{-1}L_y$;
4. $L_{(x\backslash y,x)} = L_{((y\backslash x)^{-1},x)}$;
5. $L_{(x\backslash y)^{-1}\backslash x}^{-1}L_{x\backslash y} = L_y^{-1}L_{(y\backslash x)^{-1}}$.

Demonstração.

1. *Seja* $z \in Q$. *Temos que*

   $$(L_{(x,y)}(z))^{-1} = J(L_{(x,y)}(z)) = L_{(x,y)}J(z) = L_{yx}^{-1}L_yL_xJ(z) = JL_{(yx)^{-1}}^{-1}L_{y^{-1}}L_{x^{-1}}(z) =$$

   $$= J(L_{(x^{-1},y^{-1})}(z)) = (L_{(x^{-1},y^{-1})}(z))^{-1}.$$

   Ou seja, $L_{(x,y)} = L_{(x^{-1},y^{-1})}$.

2. *Temos que*

$$L_y L_x L^{-1}_{x^{-1}\backslash y} = L_{xy} L_{(x,y)} L^{-1}_{x^{-1}\backslash y} = L_{xy} L_{(x,y)} L^{-1}_{x^{-1}\backslash y} L^{-1}_{(x,y)} L_{(x,y)}.$$

Assim

$$L_y L_x L^{-1}_{x^{-1}\backslash y} = L_{xy} L^{-1}_{L_{(x,y)}(x^{-1}\backslash y)} L_{(x,y)} = L_{xy} L^{-1}_{L_{(x^{-1},y^{-1})}(x^{-1}\backslash y)} L_{(x,y)} = L_{(x,y)},$$

pois $L_{(x^{-1},y^{-1})}(x^{-1}\backslash y) = yx$.

3. *Como* $L_{(x,y)} L_y^{-1} = L_y^{-1} L_{(x,y)} = L_x L^{-1}_{x^{-1}\backslash y}$, *temos que* $L_{(x,y)} = L_x L^{-1}_{x^{-1}\backslash y} L_y$.

4. *Como* $x(y\backslash x) = y$ *e* $L_{(x\backslash y,x)}(x)x$, *temos*

$$L_{(x\backslash y,x)} = L^2_{(x\backslash y,x)} L^{-1}_{(x\backslash y,x)} = L_{(x\backslash y,x)} L^{-1}_{(x\backslash y)x} L_x L_{x\backslash y} L_{(x\backslash y,x)} L^{-1}_{(x\backslash y,x)} =$$

$$= L^{-1}_{L_{(x\backslash y,x)}((x\backslash y)x)} L_{L_{(x\backslash y,x)}(x)} L_{L_{(x\backslash y,x)}(y\backslash y)} L_{(x\backslash y,x)} L^{-1}_{(x\backslash y,x)} =$$

$$= L_{(L_{(x\backslash y,x)}(x\backslash y), L_{(x\backslash y,x)}(x))} L_{(x\backslash y,x)} L^{-1}_{(x\backslash y,x)} = L_{((y\backslash x)^{-1},x)}.$$

5. *Aplicando o ítem 2 na identidade* $L_{(x\backslash y,x)} = L_{((y\backslash x)^{-1},x)}$, *temos que*

$$L_{x\backslash y} L^{-1}_{(x\backslash y)^{-1}\backslash x} = L_{(y\backslash x)^{-1}} L^{-1}_{(y\backslash x)\backslash x}.$$

Notemos que $(y\backslash x)\backslash x = w\backslash x = u$ *onde* $yw = x$ *e* $wu = x$, *então pela lei do cancelamento* $u = y$. *Então*

$$L_{x\backslash y} L_{(x\backslash y)^{-1}\backslash x} = L_{(y\backslash x)^{-1}} L_y^{-1}.$$

Lema 3.1.5. *Para todos* x, y *em um A-loop comutativo* Q, *valem*

1. $D_{x^2} = D_x J D_x$;

2. $x^2 = D_x(y) D_x(y^{-1})$;

3. $x = D_{x^{-1}}(y^{-1}) D_{x^2}(y)$.

Demonstração.

1. *Para qualquer que seja $y \in Q$, temos*

$$D_{x^2}(y) = L_y^{-1}(x^2) = L_y^{-1}L_x(x) = L_{(x\backslash y,x)}L_{x\backslash y}^{-1}(x),$$

então

$$D_{x^2}(y) = L^{-1}_{L_{(x\backslash y,x)}(x\backslash y)}L_{(x\backslash y,x)}(x) = L^{-1}_{((x(x\backslash y))\backslash x)^{-1}}L_{(x\backslash y,x)}(x) =$$

$$= L^{-1}_{(y\backslash x)^{-1}}L_{(x\backslash y,x)}(x) = L^{-1}_{(y\backslash x)^{-1}}(x) = (y\backslash x)^{-1}\backslash x = D_x((y\backslash x)^{-1}) = D_xJD_x(y).$$

Assim $D_{x^2} = D - xJD_x$.

2. *De $D_{x^2} = D_xJD_x$, temos que $D_xJ = D_{x^2}D_x$ pois $D_x^2 = id_Q$. Então $D_x(y^{-1}) = D_{x^2}D_x(y) = L^{-1}_{D_x(y)}(x^2)$, ou seja $x^2 = D_x(y)D_x(y^{-1})$.*

3. *Temos que $D_{x^2}(y) = D_xJD_x(y) = L^{-1}_{JD_x(y)}(x)$. Como Q, tem AIP, segue que $x = JD_x(y)D_{x^2}(y) = D_{x^{-1}}(y^{-1})D_{x^2}(y)$.* □

3.2 A-loops Comutativos Finitos de Ordem Ímpar

O principal objetivo dessa seção é o Teorema da Ordem Ímpar que nos diz que todo A-loop comutativo finito de ordem ímpar é solúvel.

Definição 3.2.1. *Um loop L será dito* ***unicamente 2-divisível*** *se a aplicação $x \mapsto x^2$ for uma permutação de L.*

Lema 3.2.2. *Um loop finito, comutativo e que associa potências Q será unicamente 2-divisível se e somente se tiver ordem ímpar.*

Demonstração. *Vamos supor Q unicamente 2-divisível. Assim, $J(x) = x^{-1} = x$ se e somente se $x = 1$. Daí temos que o conjunto $Q\backslash\{1\}$ tem ordem par, ou seja Q tem ordem ímpar.*

Reciprocamente, suponha que Q tenha ordem ímpar, e fixe um elemento $c \in Q$. Considere os conjuntos

$$U = \{(x, y) \in Q \times Q : xy = c \quad e \quad x \neq y\}$$

e

$$V = \{(x, y) \in Q \times Q : xy = c\}.$$

Temos que $|V| = |Q|$ e, por comutatividade, U tem ordem par. Portanto $V \backslash U$ tem ordem ímpar e, assim, é não vazio. Logo a aplicação $x \mapsto x^2$ é sobrejetiva e então, como Q é finito, é bijetiva.

Definição 3.2.3. *Um subgrupo torcido de um grupo G é um subconjunto T que satisfaz:*

1. $1 \in T$;
2. $a^{-1} \in T$ *sempre que* $a \in T$;
3. $aba \in T$ *sempre que* $a, b \in T$

Um subgrupo torcido T de um grupo G será unicamente 2-divisível se a restrição da aplicação $x \mapsto x^2$ for uma bijeção de T (Note que de $a^2 = a1a \in T$ sempre que $a \in T$). Para a, b em um unicamente 2-divisível subgrupo torcido T, podemos definir $a \circ b = (ab^2a)^{\frac{1}{2}}$, onde $x^{\frac{1}{2}}$ denota a única raiz quadrada de $x \in T$. Temos que $(T, \circ)$ é um loop de Bol (à esquerda), isto é

$$x \circ (y \circ (x \circ z)) = (x \circ (y \circ x)) \circ z, \tag{3.8}$$

para quaisquer $x, y, z \in T$. Além disso, $(T, \circ)$ tem a propriedade (AIP). Em outras palavras, $(T, \circ)$ é um loop de Bruck à esquerda.

Para um loop de Bol Q, temos o conjunto $L_Q = \{L_x : x \in Q\}$ é um subgrupo torcido de $\mathcal{M}(L)$, o grupo das multiplicações de Q. No caso de Q ser unicamente 2-divisível L_Q tem estrutura de loop de Bruck à esquerda. Essa estrutura pode ser

passada isomorficamente para Q e assim o conjunto Q admite duas estruturas de loop: a estrutura de loop de Bol original e a estrutura de loop de Bruck. Um fato já conhecido é que potências nessas duas estruturas coincidem, assim é possível mostrar alguns resultados para o loop de Bol Q usando a estrutura de loop de Bruck do conjunto Q. Glauberman em [Gl-02] usou esse raciocínio para loops de Moufang. Nesse trabalho, não é de interesse o estudo de loops de Moufang tampouco loops de Bol, entretando usaremos essa idéia para mostrar alguns resultados para A-loops comutativos finitos.

Para cada x em um A-loop comutativo Q, definimos

$$P_x = L_x L_{x^{-1}}^{-1} = L_{x^{-1}}^{-1} L_x.$$

Temos que $P_Q = \{P_x : x \in Q\} \subset \mathcal{M}(Q)$ satisfaz as condições 1 e 2 da definição de subgrupo torcido, pois $id_Q = P_1$ e, como $P_x P_{x^{-1}} = id_Q$, $P_x^{-1} = P_{x^{-1}}$.

Lema 3.2.4. *Sejam Q um A-loop comutativo e $x, y \in Q$. Então:*

1. $P_{xy}(x^{-1}) = xy^2$;
2. $P_{xy} L_{x^{-1}} = L_x P_y$.

Demonstração. *Pelo ítem 2 do lema 3.1.2 temos que*

$$xy^2 = (xy)(xy\backslash x)^{-1} = (xy)J(xy\backslash x) = (xy)J(L_{xy}^{-1}(x)),$$

e, como Q tem AIP segue que

$$(xy)J(L_{xy}^{-1}(x)) = L_{xy} J L_{xy}^{-1}(x) = L_{xy} L_{(xy)^{-1}}^{-1} J(x) = P_{xy}(x^{-1}),$$

o que prova 1. Para provar 2, temos

$$P_{xy} L_{x^{-1}} = L_{xy} L(xy)^{-1^{-1}} L_{x^{-1}} = L_{xy} L_{x^{-1}y^{-1}}^{-1} L_{x^{-1}} = L_{xy} L_{x^{-1}y^{-1}}^{-1} L_{x^{-1}} L_{y^{-1}} L_{y^{-1}},$$

ou seja,

$$P_{xy} L_{x^{-1}} = L_{xy} L_{(y^{-1},x^{-1})} L_{y^{-1}} = L_{xy} L_{(y,x)} L_{y^{-1}} = L_x L_y L_{y^{-1}}^{-1} = L_x P_y.$$

Lema 3.2.5. *Para quaisquer $x, y \in Q$, $P_x P_y P_x = P_{P_x(y)}$. Em particular, P_Q é um subgrupo torcido de $\mathcal{M}(Q)$.*

Demonstração. *Primeiramente notemos que*

$$x^{-1}.P_x(y) = L_{x^{-1}} P_x(y) = L_{x^{-1}} L_{x^{-1}}^{-1} L_x(y) = L_x(y) = xy.$$

Pelo ítem 2 do lema anterior e esta última observação, temos que

$$P_x P_y P_x = L_{x^{-1}}^{-1} L_x P_y P_x = L_{x^{-1}}^{-1} P_{xy} L_{x^{-1}} P_x = L_{x^{-1}}^{-1} P_{xy} L_x = L_{x^{-1}}^{-1} P_{x^{-1} P_x(y)} L_x,$$

e assim, $P_x P_y P_x = L_{x^{-1}}^{-1} L_{x^{-1}} P_{P_x(y)} = P_{P_x(y)}$.

Lema 3.2.6. *Para todo x em um A-loop comutativo Q e para todo n em $\mathbb{Z}$,*

$$P_x^n = P_{x^n}$$

.

Demonstração. *Vamos proceder por indução sobre $n \in \mathbb{N}$. Para $n = 0$ ou $n = 1$ não há nada a fazer.*

Se $P_x^n = P_{x^n}$ vale para algum n, temos que $P_x^{n+2} = P_x P_x^n P_x = P_x P_{x^n} P_x = P_{P_x(x^n)} = P_x^{n+2}$, desde que $P_x(x^n) = x^{n+2}$. Por indução, temos que $P_x^n = P_{x^n}$ vale para todo $n \in \mathbb{N}$. Como $P_x^{-1} = P_{x^{-1}}$, segue que $P_x^n = P_{x^n}$ vale para todo $n \in \mathbb{Z}$.

Assumindo que Q seja um A-loop comutativo unicamente 2-divisível, pelo último lema temos que P_Q é um subgrupo torcido de $\mathcal{M}(Q)$ que também é unicamente 2-divisível. Para $x, y \in Q$, vamos definir

$$P_x \circ P_y = (P_x P_y^2 P_x)^{\frac{1}{2}} = (P_x P_{y^2} P_x)^{\frac{1}{2}} = (P_{P_x(y^2)})^{\frac{1}{2}} = P_{(P_x(y^2))^{\frac{1}{2}}}. \tag{3.9}$$

Assim, está definida em Q uma nova operação binária, a qual também denotaremos por $\circ$.

$$x \circ y = (P_x(y^2))^{\frac{1}{2}} = (x^{-1} \backslash x y^2)^{\frac{1}{2}}. \tag{3.10}$$

Lema 3.2.7. *Para um A-loop comutativo unicamente 2-divsível Q, $(Q, \circ)$ é um loop de Bruck. Além disso, as potências em Q coincidem com as potências em $(Q, \circ)$.*

Demonstração. *Vimos que P_Q é um subgrupo torcido de $\mathcal{M}(Q)$ e como $P_x^2 = P_{x^2}$ para todo $x \in Q$ e Q é unicamente 2-divisível, temos que P_Q também é unicamente 2-divisível. Em P_Q, definindo*

$$P_x \circ P_y = P_{(P_x(y^2))^{\frac{1}{2}}},$$

temos que P_Q é um loop de Bruck. A aplicação $x \mapsto P_x$ é, claramente, um homomorfismo sobrejetor de $(Q, \circ)$ em $(P_Q, \circ)$. Se $P_x = id_Q$, temos $x^2 = P_x(1) = 1$ o que implica que $x = 1$, pois Q é unicamente 2-divisível. Portanto $(Q, \circ)$ é um loop de Bruck. Para mostrar que as potências de $(Q, \circ)$ coincidem com as potências de Q, vamos usar o argumento de indução sobre n. Como Q associa potências temos que

$$x \circ x = (x^{-1} \backslash x^3)^{\frac{1}{2}} = (x^4)^{\frac{1}{2}} = x^2.$$

Agora assuma que $x \circ x^{n-1} = x^n$, então

$$x \circ x^n = (x^{-1} \backslash x x^{2n})^{\frac{1}{2}} = (x^{-1} \backslash x^{2n+1})^{\frac{1}{2}} = (x^{2n+2})^{\frac{1}{2}} = x^{n+1},$$

como queríamos demonstrar.

Definição 3.2.8. *Dizemos que o loop $(H, \star)$ é um B-loop se:*

a) $(H, \star)$ associa potências;

b) $(H, \star)$ satisfaz a identidade 3.8;

c) $(H, \star)$ tem (AIP);

d) Todo elemento de H tem ordem finita ímpar.

Temos que se Q for um A-loop comutativo, finito e unicamente 2-divisível, $(Q, \circ)$ será um B-loop.

Proposição 3.2.9. *Seja $A \leq B$ subloops de um A-loop comutativo finito Q, de ordem ímpar. Entã $|A|$ divide $|B|$. Em particular, a ordem de qualquer elemento de Q, divide a ordem de Q.*

Demonstração. *Glauberman em [Gl-01], provou o mesmo resultado para B-loops finitos. O que vamos fazer é mostrar que os subloops A e B de Q, nos dão subloops $(A, \circ)$ e $(B, \circ)$ de $(Q, \circ)$. Temos que A é não vazio e unicamente 2-divisível. Como A é finito, basta mostrarmos que A é fechado para a operação $\circ$. De fato, para $x, y \in A$, temos*

$$x \circ y = (x^{-1} \backslash xy^2)^{\frac{1}{2}} = (L_{x^{-1}}^{-1}(xy^2))^{\frac{1}{2}} \in A.$$

Logo $(A, \circ)$ é um subloop de $(Q, \circ)$. Do mesmo modo provamos que $(B, \circ)$ é um subloop de $(Q, \circ)$. Assim vale o resultado para Q.

Proposição 3.2.10 (Cauchy)**.** *Seja Q, um A-loop comutativo, finito de ordem ímpar. Se um primo p divide $|Q|$, então Q possui um elemento de oredm p.*

Demonstração. *Como Glauberman em [Gl-01] provou esse resultado para B-loops finitos, temos que essa proposição vale para $(Q, \circ)$. Desde que potências em Q e em $(Q, \circ)$ coincidem, segue o resultado para o loop Q.*

Para um conjunto de números primos positivos π, um número inteiro positivo n é dito um *π-número*, se $n = 1$ ou se n se escreve como produto de primos em π. Para cada inteiro positivo n, n_π denotará o maior π-número que divide n.

Definição 3.2.11. *Para um conjunto de números primos positivos π, um subloop K de um loop finito que associa potências L, é chamado* ***π-subloop de Hall*** *se $|K| = |L|_\pi$. Em particular, se $\pi = \{p\}$, dizemos que K é um* ***p-subloop de Sylow****.*

Jedlicka, Kinyon e Vojtechovsky suspeitam que para um A-loop comutativo finito de ordem ímpar, existam subloops de Hall e Sylow, mas não há prova para esse fato.

Lema 3.2.12. *Toda aplicação interna de um A-loop comutativo unicamente* 2*-divisível* Q*, age como um automorfismo para* $(Q, \circ)$*.*

Demonstração. *Vamos mostrar que os geradores de* $\mathcal{I}(L)$ *são automorfismos de* $(Q, \circ)$*. Para quaisquer* $x, y, a, b \in Q$*, temos*

$$\begin{aligned} L_{(x,y)}(a \circ b) &= L_{(x,y)}[(a^{-1} \backslash ab^2)^{\frac{1}{2}}] \\ &= [L_{(x,y)}(a^{-1} \backslash ab^2)]^{\frac{1}{2}} \\ &= [L_{(x,y)}(a)^{-1} \backslash (L_{(x,y)}(a) L_{(x,y)}(b)^2)]^{\frac{1}{2}} \\ &= L_{(x,y)}(a) \circ L_{(x,y)}(b). \end{aligned}$$

Lema 3.2.13. *Seja* Q*, um A-loop comutativo finito de ordem ímpar. Um subloop* K *de* $(Q, \circ)$ *é um subloop de* Q *se e somente se* $\varphi(K) = K$ *para cada* $\varphi \in X = \mathcal{I}(Q) \cap \langle L_x : x \in K \rangle$

Demonstração. *Claramente se* $K \leq (Q, \circ)$ *também for um subloop de* Q*, então* $\varphi(K) = K$ *para toda* $\varphi \in X$*. Reciprocamente vamos supor que, para qualquer* $\varphi \in X$ *temos* $\varphi(K) = K$*. Sejam* $u, v \in K$*, devemos mostrar que* $uv, L_u^{-1}(v) \in K$*. Como potências em* Q *e em* $(Q, \circ)$ *coincidem, temos que* $u^{-1}, v^{-1}, v^{\frac{1}{2}} \in K$*. Assim*

$$(u \circ v^{\frac{1}{2}})^2 = L_{u^{-1}}^{-1} L_u(v) = L_{u^{-1}}^{-1} L_u^{-1} L_u^2(v) = L_{(u^{-1},u)}^{-1} L_u^2(v) \in K.$$

Por hipótese $L_u^2(v) \in K$*. Por indução, já que* $L_u^2 \in X$*, temos que* $L_u^{2k}(v) \in K$*, para todo inteiro* $k \in \mathbb{Z}$*.*
Se $|u| = 2n + 1$*, temos* $L_u^{2n+1} \in \mathcal{I}(L)$*, pois* $L_u^{2n+1}(1) = u^{2n+1} = 1$*. Portanto,*

$$L_u^{2n+1} L_u^{-2n}(v) = uv \quad e \quad L_u^{2n+1} L_u^{2(-n-1)}(v) = L_u^{-1}(v)$$

estão em K*. Logo* K *é um subloop de* Q*.* $\square$

Lema 3.2.14. *Seja* Q *um A-loop comutativo e assuma que a identidade*

$$P_x(y^2) = P_y(x^2) \tag{3.11}$$

valha para todos $x, y \in Q$. Então para quaisquer $x, y \in Q$ temos

$$P_x(y^2) = x^2y^2. \tag{3.12}$$

Corolário 3.2.15. *Seja Q um A-loop comutativo unicamente 2-divisível. Então $(Q, \circ)$ será comutativo se e somente se $(Q, \circ)$ for isomorfo a Q.*

Demonstração. *De fato, supondo Q comutativo e unicamente 2-divisível, temos que se $(Q, \circ)$ for comutativo, a identidade 3.11 valerá para quaisquer $x, y \in Q$, e assim, 3.12 nos diz que a aplicação $x \mapsto x^2$ é um isomorfismo de $(Q, \circ)$ em Q. Claramente, se $(Q, \circ)$ for isomorfo a Q, aquele será comutativo.*

Demonstração (Demonstração do Lema 3.2.14)**.** *Primeiramente, vamos mostrar que*

$$P_x(xy^2) = P_y(x) \tag{3.13}$$

para quaisquer $x, y \in Q$. De fato, temos que

$$P_x(xy^2) = L_xL_{x^{-1}}^{-1}(xy^2) = L_xP_x(y^2) = L_xP_y(x^2).$$

Desde que $x^{-1}\backslash x = x^2$, temos

$$P_x(xy^2) = L_{x^{-1}}P_xPyP_x(1) = L_{x^{-1}}P_{P_x(y)}(1) = x^{-1}(P_x(y))^2 = P_{x^{-1}P_x(y)}(x),$$

e como, $x^{-1}P_x(y) = xy$, temos que $P_x(xy^2) = P_{xy}(x)$.

Também afirmamos que

$$P_{y^2}(x^{-1}) = L_xP_yP_{x^{-1}}(y^2) \quad \textit{para todos} \quad x, y \in Q. \tag{3.14}$$

Temos que

$$\begin{aligned}
P_{y^2}(x^{-1}) &= P_{x.x\backslash y^2}(x^{-1}) = x(x\backslash y^2)^2 = L_x((x\backslash y^2)^2) \\
&= L_xP_yP_{y^{-1}}((x\backslash y^2)^2) = L_xP_yP_{x\backslash y^2}(y^{-2}) \\
&= L_xP_yL_{x\backslash y^2}L_{(x\backslash y^2)^{-1}}^{-1}(y^{-2}) \\
&= L_xP_y((x\backslash y^2).(x\backslash y^2)^{-1}\backslash y^{-2}) \\
&= L_xP_y((x\backslash y^2).(x^{-1}\backslash y^{-2})\backslash y^{-2}) \\
&= L_xP_y(x^{-1}(x\backslash y^2)) = L_xP_yL_{x^{-1}}L_x^{-1}(y^2) = L_xP_yP_{x^{-1}}(y^2)
\end{aligned}$$

Agora, faça

$$\begin{aligned} L_xP_yP_x(y^2) &= L_xP_y^2(x^2) = L_{x^{-1}}P_xP_{y^2}(x^2) = L_{x^{-1}}P_xP_{y^2}P_x(1) \\ &= L_{x^{-1}}P_{P_x(y^2)} = x^{-1}(P_x(y^2))^2 = P_{x^{-1}P_x(y^2)}(x) \\ &= P_{xy^2}(x) = P_{xy^2}P_{xy}P_{x^{-1}y^{-1}}(x) = P_{xy^2}P_{xy}(x^{-1}y^{-2}) \\ &= P_{xy^2}P_{xy^2(xy^2\backslash xy}((xy^2)^{-1}) = P_{xy^2}((xy^2)(xy^2\backslash xy)^2) \\ &= P_{xy^2(xy^2\backslash xy)}(xy^2) = P_{xy}(xy^2) = P_{xy}^2(x^{-1}) = P_{(xy)^2}(x^{-1}) \\ &= L_xP_{xy}P_{x^{-1}}(xy^2). \end{aligned}$$

De, $L_xP_yP_x(y^2) = L_xP_{xy}P_{x^{-1}}(xy^2)$*, temos que*

$$P_yP_x(y^2) = P_{xy}P_{x^{-1}}(xy^2) = PxyP_{x^{-1}}P_{xy}(1) = P_{P_{xy}(x^{-1})}(1)P_{xy^2}(1) = (xy^2)^2,$$

assim,

$$P_x(y^2) = P_{y^{-1}}((xy^2)^2) = P_{y^2x}(y^{-2}) = y^2x^2,$$

o que conclui o lema.

Antes de ver o resultado mais importante dessa seção, vamos definir o que é um loop solúvel.

Definição 3.2.16. *Um loop* L *é dito solúvel se existirem subloops* $N_i \quad (i = 0, ..., r)$ *tais que*

$$\{1\} = N_r \leq N_{r-1} \leq ... \leq N_1 \leq N_0 = L,$$

onde $N_i \lhd N_{i-1}$ *para todo* $i = 1, ..., r$ *e* N_{i-1}/N_i *é um grupo abeliano.*

Teorema 3.2.17. *[Teorema da Oredem Ímpar] Todo A-loop comutativo e finito de ordem ímpar é solúvel.*

Demonstração. *Suponha que exista um A-loop comutativo, finito, de ordem ímpar, não solúvel. Seja* Q *o contra-exemplo de menor ordem. Desde que subloops normais e quocientes de* Q *também têm ordem ímpar, temos que* Q *deve ser simples.*

Tome N o subloop derivado de $(Q, \circ)$, isto é menor subloop normal de $(Q, \circ)$ tal que $(Q/N, \circ)$ é um grupo abeliano. Em [Gl-02] tem-se qualquer loop de Bruck finito de ordem ímpar é solúvel, donde tiramos que N é um subloop próprio. Como N é fixado por qualquer automorfismo de $(Q, \circ)$, pelo lema 3.2.12, temos que N é fixado por qualquer elemento de $\mathcal{I}(L)$. Assim pelo lema 3.2.13, temos que N é um subloop de Q. Além disso, $N \lhd Q$, pois $\varphi(N) = N$, para todo $\varphi \in \mathcal{I}(L)$.

Desde que Q é simples, temos $N = 1$ e assim $(Q, \circ)$ é um grupo abeliano. Assim, pelo corolário, 3.2.15, temos Q um grupo abeliano, que contradiz a suposição de Q ser não-solúvel. Logo, todo A-loop comutativo, finito e de ordem ímpar é solúvel.

3.3 Quadrados e Loop Associado

Durante essa seção, Q denotará um A-loop comutativo.

Ao contrário de grupos abelianos e loops de Moufang comutativos, onde o produto de dois quadrados ainda é um quadrado, em A-loops comutativos, nem sempre vale $(xy)^2 = x^2y^2$ para quaisquer x, y. Vamos, em Q, definir a seguinte operação binária: para quaisquer $x, y \in Q$ seja

$$x \circledast y = ((xy\backslash x)(yx\backslash y))^{-1}. \tag{3.15}$$

Desde que, em Q vale a (AIP) e, pelo lema 3.1.2, temos que a definição 3.15 pode ser reescrita como

$$x \circledast y = L_{(y,x)}(y)L_{(x,y)}(x) \tag{3.16}$$

A definição 3.16 é motivada no seguinte teorema:

Teorema 3.3.1. *Para quaisquer x, y em um A-loop comutativo, temos*

$$x^2y^2 = (x \circledast y)^2.$$

Para demonstrar o teorema 3.3.1, serão necessários alguns lemas.

Lema 3.3.2. *Para todos $x, y \in Q$, $x \divideontimes y = x^2(x\backslash(xy\backslash x)^{-1})$.*

Demonstração. *Como,*

$$L_{(x,y)}(x) = L_{yx}^{-1}(x^2y) = L_{yx}^{-1}L_{x^2}L_xL_x^{-1}(y) = L_{(y,x)}L_y^{-1}L_{x^2}L_x^{-1}(y),$$

temos que

$$\begin{aligned} x \divideontimes y &= L_{(y,x)}(y)L_{(x,y)}(x) = L_{(y,x)}(y)(L_{(y,x)}L_y^{-1}L_{x^2}L_x^{-1}(y)) \\ &= L_{(y,x)}(y.L_y^{-1}L_{x^2}L_x^{-1}(y)) = L_{(y,x)}L_{x^2}L_x^{-1}(y) \\ &= L_{x^2}L_x^{-1}L_{(y,x)}(y) = L_{x^2}L_x^{-1}(xy\backslash x)^{-1} \qquad (3.17) \\ &= x^2(x\backslash(xy\backslash x)^{-1}). \end{aligned}$$

Na passagem 3.17 usamos o lema 3.1.2.

Lema 3.3.3. *Para todos $x, y \in Q$, $x^{-1}\backslash(xy\backslash x) = y\backslash(yx\backslash y)^{-1}$.*

Demonstração. *Afirmamos que $x = L_{xy}L_{x^{-1}}(y\backslash(yx\backslash y)^{-1})$. De fato,*

$$\begin{aligned} L_{xy}L_{x^{-1}}(y\backslash(yx\backslash y)^{-1}) &= L_{xy}L_{x^{-1}}L_y^{-1}((yx\backslash y)^{-1}) = L_{xy}L_{x^{-1}}L_{x\backslash xy}^{-1}((yx\backslash y)^{-1}) \\ &= L_{(x^{-1},xy)}((yx\backslash y)^{-1}) = [L_{(x^{-1},xy)}(xy)\backslash L_{(x^{-1},xy)}(y)]^{-1} \\ &= [xy\backslash L_{(x^{-1},xy)}(y)]^{-1} = [xy\backslash L_{(x,(xy)^{-1})}(y)]^{-1} \\ &= [xy\backslash(x(xy)^{-1})^{-1}]^{-1} = [xy\backslash(x^{-1}(xy))]^{-1} \\ &= [xy\backslash L_{xy}(x^{-1})]^{-1} = (x^{-1})^{-1} = x. \end{aligned}$$

Portanto,

$$y\backslash(yx\backslash y)^{-1} = L_{x^{-1}}^{-1}L_{xy}^{-1}(x) = x^{-1}\backslash(xy\backslash x).$$

Agora, estamos em condições de demonstrar o teorema 3.3.1

Demonstração (Demonstração do Teorema 3.3.1)**.** *Faça $z = x \divideontimes y$. Então*

$$\begin{aligned} D_z(x^2) &= L_{x^2}^{-1}(z) = L_{x^2}^{-1}(x^2(x\backslash(xy\backslash x)^{-1})) = x\backslash(xy\backslash x)^{-1} \qquad (3.18) \\ &= J(x^{-1}\backslash(xy\backslash x)) = J(y\backslash(yx\backslash y)^{-1}) \qquad (3.19) \\ &= JL_{y^2}^{-1}(y^2(y\backslash(yx\backslash y)^{-1})) = JL_{y^2}^{-1}(z) = JD_z(y^2). \qquad (3.20) \end{aligned}$$

Onde, nas passagens 3.18 e 3.20 usamos o lema 3.3.2 e na passagem 3.19 usamos o lema 3.3.3. Assim,

$$x^2 = D_z^2(x^{^2}) = D_z J D_z(y^2) = D_{z^2}(y^2) = L_{y^2}^{-1}(z^2),$$

portanto $x^2y^2 = z^2$, como queríamos demonstrar.

Em $(Q, \divideontimes)$, usaremos a notação S_x para a translação a esquerda, isto é, $S_x : (Q, \divideontimes) \longrightarrow (Q, \divideontimes)$ é tal que $S_x(y) = x \divideontimes y$. Notemos que, pelo lema 3.3.2, temos que

$$S_x = L_{x^2} L_x^{-1} J D_x L_x. \tag{3.21}$$

Proposição 3.3.4. *Seja Q um A-loop comutativo e seja $\divideontimes$ como definida em 3.15. Então $(Q, \divideontimes)$ é um loop comutativo, que associa potências e possui o mesmo elemento neutro de Q. Além disso, potências em $(Q, \divideontimes)$ coincidem com potências em Q.*

Demonstração. *Primeiramente mostremos que a operação $\divideontimes$ é comutativa. Como Q é um loop comutativo, para quaisquer $x, y \in Q$, temos*

$$x \divideontimes y = ((xy\backslash x)(yx\backslash y))^{-1} = ((yx\backslash y)(xy\backslash x))^{-1} = y \divideontimes x.$$

Para qualquer que seja $x \in Q$, a identidade 3.21 implica que S_x é uma permutação de Q, donde segue que $(Q, \divideontimes)$ é um quase-grupo. Desde que

$$x \divideontimes 1 = ((x\backslash x).(x\backslash 1))^{-1} = (x^{-1})^{-1} = x$$

para todo $x \in Q$, temos que 1 é o elemento neutro de $(Q, \divideontimes)$.

Para mostrar que $(Q, \divideontimes)$ associa potências, façamos

$$(x^m \divideontimes x^n) \divideontimes x^l = ((x^m x^n \backslash x^m)(x^n x^m \backslash x^n))^{-1} \divideontimes x^l = ((x^{m+n} \backslash x^m)(x^{n+m} \backslash x^n))^{-1} \divideontimes x^l =$$

$$= (x^{-n} x^{-m})^{-1} \divideontimes x^l = x^{m+n} \divideontimes x^l = ((x^{m+n} x^l \backslash x^{m+n})(x^l x^{m+n} \backslash x^l))^{-1} =$$

$$= ((x^{m+n+l} \backslash x^{m+n})(x^{l+m+n} \backslash x^l))^{-1} = (x^{-l} x^{-m-n})^{-1} = x^{m+n+l}.$$

Por outro lado,

$$x^m \circledast (x^n \circledast x^l) = x^m \circledast ((x^n x^l \backslash x^n)(x^l x^n \backslash x^l))^{-1} = x^m \circledast ((x^{n+l} \backslash x^n)(x^{l+n} \backslash x^l))^{-1} =$$

$$= x^m \circledast (x^{-l} x^{-n})^{-1} = x^m \circledast x^{l+n} = ((x^m x^{l+n} \backslash x^m)(x^{l+n} x^m \backslash x^{l+n}))^{-1} =$$

$$= (x^{-l-n} x^{-m})^{-1} = (x^{-m-n-l})^{-1} = x^{m+n+l},$$

donde temos $(x^m \circledast x^n) \circledast x^l = x^m \circledast (x^n \circledast x^l)$*, para quaisquer* $x \in Q, m, n, l \in \mathbb{Z}$*.*

Finalmente, mostremos que potências em $(Q, \circledast)$ *coincidem com potências em* Q*. De fato,*

$$x^m = (x^{m-1} \circledast x) = ((x^{m-1} x \backslash x^{m-1})(x x^{m-1} \backslash x))^{-1} = (x^{-1} x^{-m+1})^{-1} = x^{m+1} x,$$

para todo $x \in Q$ *e todo* $m \in \mathbb{Z}$*.* □

Lema 3.3.5. *Para quaisquer* $x, y \in Q$ *e* $m, n \in \mathbb{Z}$*,* $L_{(y,x^m)} S_{x^n} = S_{x^n} L_{(y,x^m)}$*.*

Demonstração. *Desde que* $S_{x^n} = L_{x^{2n}} L_{x^n}^{-1} J D_{x^n} L_{x^n}$*, temos que*

$$\begin{aligned}
L_{(y,x^m)} S_{x^n} &= L_{(y,x^m)} L_{x^{2n}} L_{x^n}^{-1} J D_{x^n} L_{x^n} \\
&= L_{x^{2n}} L_{x^n}^{-1} L_{(y,x^m)} J D_{x^n} L_{x^n} \\
&= L_{x^{2n}} L_{x^n}^{-1} J L_{(y,x^m)} D_{x^n} L_{x^n} \\
&= L_{x^{2n}} L_{x^n}^{-1} J D_{x^n} L_{(y,x^m)} L_{x^n} \\
&= L_{x^{2n}} L_{x^n}^{-1} J D_{x^n} L_{x^n} L_{(y,x^m)} = S_{x^n} L_{(y,x^m)}. \quad \square
\end{aligned}$$

Para finalizar a seção, notemos um importante resultado.

Teorema 3.3.6. *Se* Q *for uma A-loop comutativo unicamente* 2*-divisível, então* $(Q, \circledast)$ *será isomorfo a* Q*.*

Demonstração. *Defina* $\varphi : (Q, \circledast) \longrightarrow Q$*, por* $\varphi(x) = x^2$*. Vamos mostrar que* φ *é um isomorfismo. De fato, como* $(x \circledast y)^2 = x^2 y^2$ *para quaisquer* $x, y \in Q$*,* φ *é um homomorfismo. Desde que* Q *é unicammente* 2*-divisível, temos que* φ *é sobrejetiva. Finalmente, se* $x^2 = 1$*, temos que* $x = 1$*, e assim,* φ *é injetiva. Portanto,* φ *é um isomorfismo.*

3.4 O Teorema de Decomposição

Nessa seção mostraremos que um A-loop comutativo finito pode ser escrito como produto direto de um subloop de ordem ímpar e um subloop cuja ordem de qualquer elemento é uma potênicia de 2. Ainda nessa seção, Q denota um A-loop comutativo finito. O seguinte teorema é o principal resultado dessa seção.

Teorema 3.4.1. *[Decomposição de um A-loop comutativo finito] Se Q for um A-loop comutativo finito, então $Q = K(Q) \times H(Q)$, onde $K(Q) = \{x \in Q : |x| \quad \text{é ímpar}\}$ e $H(Q) = \{x \in Q : x^{2^n} = 1 \quad \text{para algum} \quad n \in \mathbb{Z}\}$. Além disso, $K(Q)$ tem ordem ímpar e $H(Q)$ tem ordem potência de 2.*

Agora vamos nos concentrar em alguns resultados, que serão necessários para demonstrarmos o teorema 3.4.1.

Proposição 3.4.2. *O conjunto $K_1(Q) = \{x^2 : x \in Q\}$ é um subloop normal de Q.*

Demonstração. *Claramente $K_1(Q)$ é não vazio. Para quaisquer $x, y \in K_1(Q)$, temos, pelo teorema 3.3.1, $x^2y^2 = (x \divideontimes y)^2$. Logo $K_1(Q)$ é fechado pela multiplicação de Q. Além disso, pela proposição 3.3.4, temos que existe $z \in Q$ tal que $x \divideontimes z = y$ e, novamente pelo teorema 3.3.1, temos $x^2z^2 = y^2$. Como Q é comutativo, temos que $K_1(Q)$ é um subloop de Q.*

Resta-nos, agora, mostrar que $K_1(Q)$ é normal em Q. Como Q é um A-loop, temos que toda aplicaçaõ interna é um automorfismo de Q, logo preserva quadrados. Assim $K_1(Q)^\varphi = K_1(Q)$ para toda $\varphi \in \mathcal{I}(L)$. Logo $K_1(Q)$ é um subloop normal de Q.

Teorema 3.4.3. *Seja Q um A-loo comutativo. Para cada $n \in \mathbb{N}$, defina*

$$K_n(Q) = \{x^{2^n} : x \in Q\} \quad e \quad K(Q) = \bigcap_{n \geq 1} K_n(Q).$$

Então:

1. $K_{n+1}(Q) = \{x^n : x \in K_n(Q)\}$, *para todo* $n \geq 0$;

2. $K_{n+1}(Q)$ *é um subloop de* $K_n(Q)$, *para todo* $n \geq 0$;

3. $K_n(Q) \lhd Q$, *para todo* $n \geq 0$;

4. $K(Q) \lhd Q$;

5. *Se* Q *for finito, então* $K(Q) = \{x \in Q : |x| \quad \text{é ímpar}\}$ *e* $|K(Q)|$ *é ímpar.*

Demonstração.

1. *Se* $x \in K_n(Q)$, *temos que* $x = y^{2^n}$ *para algum* $y \in Q$. *Então* $x^2 = y^{2^n}y^{2^n} = y^{2^{n+1}} \in K_{n+1}(Q)$. *Reciprocamente, se* $x \in K_{n+1}(Q)$, *então,* $x = z^{2^{n+1}} = (z^{2^n})^2$ *para algum* $z \in Q$.

2. *Se* $x \in K_{n+1}(Q)$, *temos* $x = z^{2^{n+1}} = (z^2)^{2^n}$, *para algum* $z \in Q$. *Logo,* $K_{n+1}(Q) \subset K_n(Q)$. *Concluimos que* $K_{n+1}(Q)$ *é um subloop de* $K_n(Q)$ *pelo ítem 1 e pela proposião 3.4.2.*

3. *Para provar esse ítem, vamos proceder por indução sobre* n. *Pela proposição 3.4.2 temos* $K_1(Q) \lhd Q$. *Assuma que* $K_m(Q) \lhd Q$. *Queremos mostrar que* $K_{m+1}(Q)$ *é um subloop normal de* Q. *Como temos que* $K_{m+1}(Q)$ *é um subloop de* $K_m(Q)$, *segue* K_{m+1} *é um subloop de* Q. *Para mostrar que* $K_{m+1}(Q) \lhd Q$, *basta observar que qualquer aplicação interna de* Q *preserva potências, pois* Q *é um A-loop. Logo,* $K_n(Q) \lhd Q$, *para todo* $n \geq 0$.

4. *Esse ítem segue do fato de que interseção de uma família de subloops normais de* Q *é um subloop normal de* Q.

5. *Agora vamos assumir que* Q *é finito. Temos que*

$$Q \supset K_1(Q) \supset K_2(Q) \supset ... \supset K_n(Q) \supset ...$$

Assim existe $n \in \mathbb{N}$ tela que $K(Q) = K_i(Q)$, para todo $i \geq n$. Pelo ítem 1 temos que $K(Q) = \{x^2 : x \in K(Q)\}$. Donde temos que $K(Q)$ é um A-loop comutativo, finito, unicamente 2-divisível. Logo, pelo lema 3.2.2, $K(Q)$ tem oredem ímpar. Ainda pelo fato de $K_(Q)$ ser unicamete 2-divisível, a aplicação $x \mapsto x^2$ é uma bijeção que fixa apenas o elemento 1, assim nenhum elemento de $K_(Q)$ pode ter oredem par. Finalmente, seja $x \in Q$ cuja oredem é $2m+1$. para algum $m \in \mathbb{N}$. Como $x = x^{2m+2} = (x^{m+1})^2$, temos que $x \in K_1(Q)$. Pelo ítem 3, temos que $x^{m+1} \in K_1(Q)$ e qntão $x \in K_2(Q)$ e assim por diante. Logo, $x \in K(Q)$, e assim, $K(Q) = \{x \in Q : |x| \quad$ é ímpar$\}$.

Lema 3.4.4. *Para todos x, y em um A-loop comutativo Q,*

$$(x\backslash(y\backslash x))^2\backslash(y^{-1}\backslash(y\backslash x))^2 = (x\backslash y)^{-2}. \tag{3.22}$$

Demonstração. *Substitua y por $x\backslash y$ no item 2 do lema 3.1.2, temos*

$$x(x\backslash y)^2 = (x(x\backslash y))((x.x\backslash y)\backslash x)^{-1} = y(y\backslash x)^{-1}. \tag{3.23}$$

Novamente faça $y\backslash x$ no lugar de y e usando o fato que $(y\backslash x)\backslash x = y$, temos

$$x(x\backslash(y\backslash x))^2 = (y\backslash x)((y\backslash x)\backslash x)^{-1} = y^{-1}(y\backslash x). \tag{3.24}$$

Aplicando J nos dois lados da equação 3.24 e usando a propriedade (AIP), obtemos

$$x^{-1}(x\backslash(y\backslash x))^{-2} = y(y\backslash x)^{-1}. \tag{3.25}$$

Agora, junte as equações 3.23 e 3.25 afim de obter

$$(x\backslash y)^2(x\backslash(y\backslash x))^{-2} = D_{y(y\backslash x)^{-1}}(x)D_{y(y\backslash x)^{-1}}(x^{-1}) = (y(y\backslash x)^{-1})^2.$$

Finalmente, aplicando J na última equação e usando a (AIP), temos

$$(x\backslash y)^{-2}(x\backslash(y\backslash x))^2 = (y^{-1}(y\backslash x))^2,$$

e então $(x\backslash(y\backslash x))^2\backslash(y^{-1}(y\backslash x))^2 = (x\backslash y)^{-2}$. $\square$

Proposição 3.4.5. *Seja x em um A-loop comutativo finito Q, satisfazendo $x^{2^n} = 1$. Então, $(xy)^{2^n} = y^{2^n}$, para todo $y \in Q$.*

Demonstração. *Vamos proceder por indução sobre n. Para o caso $n = 0$, temos*

$$(xy)^{2^0} = (xy)^1 = x^1 y^1 = x^{2^0} y^{2^0} = y^{2^0}.$$

Agora assuma que a proposição valha para algum n e tome $x \in Q$ tal que $x^{2^{n+1}} = 1$. Desde que $1 = x^{2^{n+1}} = (x^2)^{2^{n+1}}$, temos

$$(x^2 y)^{2^n} = y^{2^n} = (x^2 (x^2 \backslash y)^{2^n}) = (x^2 \backslash y)^{2^n}, \tag{3.26}$$

para todo $y \in Q$.

Seja φ um automorfismo de Q. Aplicando φ na equação 3.26 e fazendo $z = y^\varphi$, obtemos

$$((x^\varphi)^2 z)^{2^n} = ((x^\varphi)^2 \backslash z)^{2^n} = z^{2^n}, \quad \textit{para todo} \quad z \in Q.$$

Como Q é um A-loop onde vale (AIP), podemos escolher $\varphi = L_{(x,x\backslash y)} J$. Note que

$$L_{(x,x\backslash y)} J(x) = L_{(x,x\backslash y)}(x^{-1}) = L_{y^{-1}} L_{x\backslash y} L_x (x^{-1}) = y \backslash (x \backslash y).$$

Portanto $(z(y\backslash(x\backslash y))^2)^{2^n} = z^{2^n}((y\backslash(x\backslash y))^2 \backslash z)^{2^n}$, para quaisquer $y, z \in Q$. Assim

$$\begin{aligned} y^{2^{n+1}} &= (y(y\backslash(x\backslash y))^2)^{2^{n+1}} \\ &= (x^{-1}(x\backslash y))^{2^{n+1}} \\ &= ((x^{-1}(x\backslash y))^2)^{2^n} \\ &= [(y\backslash(x\backslash y))^2 \backslash (x^{-1}(x\backslash y))^2]^{2^n} \\ &= (y\backslash x)^{-2^{n+1}}. \end{aligned}$$

Então, $(y^{-1})^{-2^{n+1}} = y^{2^{n+1}} = L_{(y,y^{-1})}(y^{2^{n+1}}) = (L_{(y,y^{-1})}(y\backslash x))^{-2^{n+1}} = (y^{-1}x)^{-2^{n+1}}$. Agora, basta tomar inversos e substituir y^{-1} por y, para obtermos o resultado desejado.

Teorema 3.4.6. *Seja Q um A-loop comutativo. Para $n \geq 0$, sejam*

$$H_n(Q) = \{x \in Q : x^{2^n} = 1\},$$

$$H(Q) = \bigcup_{n \geq 0} H_n(Q).$$

Então:

1. $H_{n+1}(Q) = \{x \in Q : x^2 \in H_n(Q)\}$, *para todo* $n \geq 0$;
2. $H_n(Q) \subset H_{n+1}(Q)$, *para todo* $n \geq 0$;
3. $H_n(Q) \lhd Q$, *para todo* $n \geq 0$;
4. $H(Q) \lhd Q$.

Demonstração.

1. *Se $x \in Q$, tal que $x^2 \in H_n(Q)$, então $x^{2^{n+1}} = (x^2)^{2^n} = 1$, portanto, $x \in H_{n+1}(Q)$. Reciprocamente se $x \in H_{n+1}(Q)$, temos $(x^2)^{2^n} = x^{2^{n+1}} = 1$, ou seja, $x^2 \in H_n(Q)$.*
2. *Se $x \in H_n(Q)$, então $x^{2^{n+1}} = (x^{2^n})^2 = 1$, isto é, $x \in H_{n+1}(Q)$.*
3. *Vamos mostrar que $H_n(Q) \leq Q$, para todo $n \geq 0$. Seja $n \in \mathbb{N}$. Claramente, $1 \in H_n(Q)$. Pela proposição 3.4.5, temos que, para quaisquer $x, y \in H_n(Q)$, $(xy)^{2^n} = y^{2^n} = 1$, ou seja $xy \in H_n(Q)$. Também temos que existe $z \in Q$, tal que $xz = y$. Assim $z^{2^n} = (xz)^{2^n} = y^{2^n} = 1$, donde temos que $z \in H_n(Q)$ e então, $H_n(Q)$ é um subloop de Q. Para mostrar normalidade, basta observar que, como Q é um A-loop, qualquer aplicação interna de Q é um automorfismo de Q e, portanto, preserva potências. Ou seja, $H_n(Q)^\varphi = H_n(Q)$ para todo $\varphi \in \mathcal{I}(L)$, logo $H_n(Q)$ é um subloop normal de Q.*
4. *Sejam $x, y \in H(Q)$. Então existem $n, m \geq 0$ tais que $x \in H_n(Q)$ e $y \in H_m(Q)$. Tome $k = max\{m, n\}$. Claramente $xy \in H(Q)$. Existe $z \in Q$, tal que, $xz = y$.*

Então, pela proposição 3.4.5 temos $z^{2^k} = (xz)^{2^k} = y^{2^k} = 1$, *ou seja,* $z \in H_k(Q) \subset H(Q)$, *logo* $H(Q)$ *é um subloop de* Q. *Pelo mesmo argumento do ítem 3, temos que* $H(Q)^\varphi = H(Q)$ *para todo* $\varphi \in \mathcal{I}(L)$, *isto é,* $H(Q)$ *é um subloop normal de* Q.

Demonstração (Demostração do Teorema 3.4.1)**.** *Pelos teoremas 3.4.3 e 3.4.6, temos que* $K(Q), H(Q) \lhd Q$ *e* $K(Q) \cap H(Q) = \{1\}$. *Resta-nos agora mostrar que* $Q = K(Q)H(Q)$. *Seja* $x \in Q$ *e faça* $|x| = n = 2^k.m$ *onde* $(2^k, m) = 1$. *Então existem* $a, b \in \mathbb{Z}$ *tais que* $1 = 2^k a + mb$. *Assim,*

$$x = x^1 = x^{2^k a + mb} = x^{2^k a}.x^m.$$

Logo $x_1 = x^{2^k a} \in K(Q)$ *e* $x_2 = x^{mb} \in H(Q)$, *como queríamos demonstrar.*

3.5 A-Loops Comutativos de Expoente 2

A definição de expoente para um loop finito é a mesma usada para grupos, isto é, o expoente de um loop finito é o mínimo múltiplo comum da ordem de seus elementos. A proposição abaixo nos motiva a estudar os A-loops comutativos de expoente 2.

Proposição 3.5.1. *Um A-loop comutativo, finito e simples ou é um grupo cíclico de ordem p, para algum número primo ímpar p, ou tem expoente* 2.

Demonstração. *Seja* Q *um A-loop comutativo finito e simples. Pelo Teorema 3.4.5,* $Q = K \times H$, *onde* K *tem ordem ímpar e* $H = \{x \in Q : x^{2^n} = 1 \quad \text{para algum} \quad n \geq 0\}$. *Como,* Q *é simples, temos que* $Q = K$ *ou* $Q = H$
Se $Q = K$, *pelo Teorema da Ordem Ímpar (3.2.17), temos que* Q *é solúvel. Assim,* Q *simples, solúvel e comutativo implica que* Q *é um grupo cíclico de oredem prima p. Agora assuma* $Q = H$, *então todo elemento de* Q *tem ordem potência de* 2. *Da proposição 3.4.2, que* $K_1(Q) \lhd Q$. *Como* Q *é simples, temos* $K_1(Q) = Q$ *ou* $K_1(Q) = \{1\}$. *Se valesse o primeiro caso,* Q *seria um A-loop comutativo, finito e unicamente 2-divisível, assim pela proposição 3.2.2,* Q *teria ordem ímpar, o que contradiz o fato*

de $|H|$ ser u a potência de 2. Logo, devemos ter $K_1(Q) = \{1\}$ e assim, $x^2 = 1$ para todo $x \in Q$, isto é, Q tem expoente 2.

Teorema 3.5.2. *Seja Q um A-loop comutativo de expoente 2. Então, $(Q, \divideontimes)$ é um 2-grupo abeliano elementar.*

Antes de demonstrarmos a proposição 3.5.2 façamos alguns resultados que serão necessários. Lembremos que $\divideontimes$ é definido por 3.15 e 3.16, ou seja,

$$x \divideontimes y = ((xy\backslash x)(yx\backslash y))^{-1} = L_{(y,x)}(y)L_{(x,y)}(x).$$

Como consequência imediata do teorema 3.5.2 temos que se Q for um A-loop comutativo finito e de expoente 2, então $|Q|$ será uma potência de 2.
Nessa seção Q será um A-loop comutativo de expoente 2. Vimos que

$$x \divideontimes y = x^2(x\backslash(xy\backslash x)^{-1}) \quad \text{e} \quad S_x = L_{x^2}L_x^{-1}D_xL_x,$$

mas, desde que Q tem expoente 2, obtemos

$$x \divideontimes y = x\backslash(xy\backslash x) \quad \text{e} \quad S_x = L_x^{-1}D_xL_x.$$

Lema 3.5.3. *Para todos $x, y \in Q$, $x \divideontimes (x \divideontimes y) = y$, isto é $S_x^2 = id_Q$.*

Demonstração. *De fato, como $S_x = L_x^{-1}D_xL_x$ e $D_x^2 = id_Q$, temos que*

$$S_x^2 = (L_x^{-1}D_xL_x)(L_x^{-1}D_xL_x) = L_x^{-1}D_x^2L_x = L_x^{-1}L_x = id_Q.$$

Lema 3.5.4. *Para todo $x \in Q$, $S_x = L_x^{-1}D_xL_x = L_xD_xL_x^{-1}$.*

Demonstração. *Como Q tem expoente 2, vale que $D_x = D_{L_x^2(x)}$ e $L_x^2 = L_{(x,x)} \in \mathcal{I}(L)$, ou seja, $D_xL_x^2 = D_{L_x^2(x)}L_x^2$. Temos que*

$$D_{L_x^2(x)}(L_x^2(y)) = [L_x^2(y)\backslash(L_x^2(x))] = L_x^2(y\backslash x) = L_x^2(D_x(y)),$$

para todo $y \in Q$, isto é $D_xL_x^2 = L_x^2D_x$ ou, equivalentemente, $L_x^{-1}D_xL_x = L_xD_xL_x^{-1}$.

Lema 3.5.5. *Para quaisquer $x, y, z \in Q$*

$$S_{zy}L_{(z\backslash(x(zy)),z)}(y) = L_x D_y L_x^{-1} L_y(z). \tag{3.27}$$

Demonstração. *Primeiramente, façamos*

$$\begin{aligned}
L_{zx}L_{zx\backslash zy}^{-1}S_{zy}L_{(x,z)}(y) &= (L_{zx}L_{zx\backslash zy}^{-1}L_{zy})L_{zy}^{-1}S_{zy}L_{(x,z)}(y) \\
&= (L_{(xz,yz)}L_{yz}^{-1})S_{zy}L_{(x,z)}(y) \\
&= L_{zy}^{-1}(L_{(zx,zy)}S_{zy})L_{(x,z)}(y) \\
&= L_{zy}^{-1}S_{zy}(L_{(zx,zy)}L_{(x,z)})(y) \qquad (3.28) \\
&= L_{zy}^{-1}S_{zy}L_{(zx)(zy)}^{-1}L_{zy}L_zL_x(y) \\
&= D_{zy}L_{zy}^{-1}L_{(zx)(zy)}^{-1}L_{zy}L_zL_y(x), \qquad (3.29)
\end{aligned}$$

onde usamos os lemas 3.3.5 e 3.5.4 para justificar as passagens 3.28 e 3.29, respectivamente.
Como Q tem expoente 2, temos que $L_{zy}L_zL_y(1) = 1$, ou seja, $L_{zy}L_zL_y \in \mathcal{I}(L)$, o que implica

$$L_{zy}L_zL_y(y\backslash x) = L_{zy}L_zL_y(y)\backslash L_{zy}L_zL_y(x).$$

Por outro lado, $L_{zy}L_zL_y(y\backslash x) = L_{zy}L_zL_yL_y^{-1}(x) = L_{zy}L_z(x) = (zx)(zy)$. Então

$$L_{zy}L_zL_y(x) = [(zx)(zy)]L_{zy}L_zL_y(y) = L_{(zx)(zy)}L_{zy}L_zL_y(y).$$

Desde que $y = L_{y\backslash x}^{-1}(x)$, a última equação ode ser reescrita como

$$L_{zy}L_zL_yL_{y\backslash x}^{-1}(x) = L_{(zx)(zy)}^{-1}L_{zy}L_zL_y(x).$$

Assim obtemos

$$\begin{aligned}
L_{zx}L_{zx\backslash zy}^{-1}S_{zy}L_{(x,z)}(y) &= D_{zy}L_{zy}^{-1}(L_{(zx)(zy)}^{-1}L_{zy}L_zL_y(x)) \\
&= D_{zy}L_zL_yL_{y\backslash x}^{-1}(x) \\
&= D_{zy}L_zL_y(y) = D_{zy}(z) = y.
\end{aligned}$$

Portanto, $S_{zy}L_{(x,z)}(y) = L_{zx\backslash zy}L_{zx}^{-1}(y) = L_{zx\backslash zy}L_{(zy\backslash zx)\backslash zy}^{-1}(y)$. *Agora, substitua* x *por* $L_z^{-1}L_{zy}(x) = z\backslash(x(zy))$ *para obter*

$$\begin{aligned} S_{zy}L_{(z\backslash(x(zy)),z)}(y) &= L_xL_{x\backslash(zy)}^{-1}(y) \\ &= L_x((x\backslash zy)\backslash y) \\ &= L_xD_y(x\backslash zy) \\ &= L_xD_yL_x^{-1}(zy) = L_xD_yL_x^{-1}L_y(z), \end{aligned}$$

como era desejado.

Lema 3.5.6. *Para todos* $u, v, w \in Q$,

$$L_{(v\backslash(w.uv),v)}(u) = L_wD_vL_w^{-1}L_v(u). \tag{3.30}$$

Demonstração. *De fato, para quaisquer* $u, v, w \in Q$, *temos*

$$\begin{aligned} L_{(v\backslash(w.uv),v)}(u) &= L_{w.uv}^{-1}L_v[L_{v\backslash(w.uv)}(u)] = L_{w.uv}^{-1}L_v[L_uL_v^{-1}L_{uv}](w) \\ &= L_{w.uv}^{-1}L_vL_{(u,uv)}(w) = L_{w.uv}^{-1}L_vL_{(v\backslash(uv),uv)}(w) \\ &= L_{w.uv}^{-1}[L_vL_{(uv\backslash v,uv)}](w) = L_{w.uv}^{-1}L_{uv}(L_{uv\backslash v}(w)) \\ &= L_{w.uv}^{-1}L_{uv}L_w(uv\backslash v) = L_{(w,uv)}L_{uv}^{-1}(v) \\ &= L_wL_{w\backslash uv}^{-1}(v) = L_wD_vL_w^{-1}L_v(u). \end{aligned}$$

Lema 3.5.7. *Para todos* $u, v, w \in Q$,

$$L_{(vw,u)}L_vL_{v\backslash w}^{-1}(u) = wu \tag{3.31}$$

Demonstração. *Novamente, para quaisquer* $u, v, w \in Q$, *temos*

$$\begin{aligned} L_{(vw,u)}[L_vL_{v\backslash w}^{-1}](u) &= L_{(vw,u)}L_w^{-1}L_{(v,w)}(u) = [L_{(vw,u)}L_{(v,w)}]L_w^{-1}(u) \\ &= L_{vw.u}^{-1}L_uL_wL_vL_w^{-1}(u) = L_{vw.u}^{-1}L_uL_wL_{w\backslash u}(v) \\ &= L_{vw.u}^{-1}L_{uw}[L_{(w,u)}L_{w\backslash u}](v) = L_{vw.u}^{-1}L_{wu}L_uL_w(v) \\ &= L_{wv.u}^{-1}((wv.u)wu) = wu \end{aligned}$$

Lema 3.5.8. *Para todos $u, v, w \in Q$,*

$$S_{uv}L_{(w,u)}(v) = L_v L_u^{-1} L_{(w,u)}(v). \tag{3.32}$$

Demonstração. *Vamos começar com*

$$S_{uv}L_{(u\backslash(w.uv),u)}(v) = L_w D_v L_w^{-1} L_v(u) = L_{(v\backslash(w.uv),v)}.$$

Substituindo w por $L_u L_{uv}^{-1}(w)$, obtemos

$$\begin{aligned} S_{uv}L_{(w,u)}(v) &= L_{(v\backslash wu,v)}(u) = L_{(wv\backslash v,v)}(u) \\ &= L_v L_{(wu)\backslash v} L^{-1}_{(wu\backslash v)\backslash v}(u) = L_v L_{wu\backslash v} L_{wu}^{-1}(u) \\ &= L_v L_{wu\backslash u} L_{wu}^{-1}(v) = L_v L_{u\backslash wu} L^{-1}_{(u\backslash uw)\backslash u}(v) \\ &= L_v L_w L_{wu}^{-1}(v) = L_v L_u^{-1} L_{(w,u)}(v). \end{aligned}$$

Lema 3.5.9. *Para todo $x, y \in Q$,*

$$L_x D_y L_x^{-1} = D_{xy} L_y D_x L_x^{-1}. \tag{3.33}$$

Demonstração. *Seja $z \in Q$. Temos*

$$\begin{aligned} L_x D_y L_x^{-1} L_y(z) &= S_{zy} L_{(z\backslash(x.yz),z)}(y) && (3.34) \\ &= S_{zy} L_x D_z L_x^{-1} L_z(y) && (3.35) \\ &= S_{zy} L_x D_z [L_x^{-1} L_z L_{z\backslash x}] L^{-1}_{z\backslash x}(y) \\ &= S_{zy} L_x D_z L_{(z\backslash x,z)} L^{-1}_{z\backslash x} \\ &= S_{zy} L_x L_{(z\backslash x,z)} D_z L^{-1}_{z\backslash x}(y) \\ &= S_{zy} L_z L_{z\backslash x} D_z L^{-1}_{z\backslash x}, && (3.36) \end{aligned}$$

onde nas passagens 3.34 e 3.35 foram usados as identidades 3.27 e 3.30, respectivamente.
Agora faça $u = L_{z\backslash x} D_z L^1_{z\backslash x}(y) = L_{z\backslash x} L_{(z\backslash x)\backslash y}(z)$ e observe que, pela equação 3.31,

$$L_{((z\backslash x)y,z)}(u) = L_{((z\backslash x)y,z)} L_{z\backslash x} L_{(z\backslash x)\backslash y}(z) = yz. \tag{3.37}$$

Usando que $\divideontimes$ é comutativa obtemos

$$\begin{aligned} L_x D_y L_x^{-1} L_y(z) &= S_{zy} L_z L_{z\backslash x} L^{-1}_{(z\ x)\backslash y}(z) \\ &= S_{zy} L_z(u) = S_{zy}(zu) \\ &= S_{zu}(zy) = S_{zu} L_{((z\backslash x)y,z)}(u) \\ &= L_u L_z^{-1} L_{((z\backslash x)y,z)}(u) = L_u L_z^{-1}(yz) \\ &= L_u(y) = L_y(z) \\ &= L_y L_{z\backslash x} L^{-1}_{(z\backslash x)\backslash y}(z) \\ &= L_{(z\backslash x,y)}(z) = L^{-1}_{(z\backslash x)y} L_y L_{z\backslash x}(z) \\ &= L^{-1}_{(z\backslash x)y}(yx) = D_{xy} L_y D_x(z), \end{aligned}$$

assim, $L_x D_y L_x^{-1} = D_{xy} L_y D_x L_y^{-1}$, como queríamos demonstrar.

Lema 3.5.10. *Para todos $x, y \in Q$, temos $L_x D_y L_x^{-1} = L_{xy} S_{(xy)\backslash x} L_{xy}^{-1}$.*

Demonstração. *De fato, temos que*

$$L_x D_y L_x^{-1} = L_x L_y S_y L_y^{-1} L_x^{-1} = L_{xy} L_{(y,x)} S_y L_y^{-1} L_x^{-1} =$$

$$= L_{xy} S_{L_(y,x)(y)} L_{(y,x)} L_y^{-1} L_x{-}1 = L_{xy} S_{(xy)\backslash x} L_{xy}^{-1},$$

onde, na última passagem, foi usado o lema 3.1.2.

Agora podemos demonstrar o teorema 3.5.2, que diz que se Q for um A-loop comutativo de expoente 2, então $(Q, \divideontimes)$ será um 2-grupo abeliano elementar.

Demonstração (Demonstração do Teorema 3.5.2)**.** *Já temos que $x \divideontimes x = x^2 = 1$, para todo $x \in Q$.Resta-nos provar que $\divideontimes$ é associativa.*
Pela equação 3.33 temos $L_x D_y L_x^{-1} = D_{xy} L_y D_x L_x^{-1}$. Aplicando o lema 3.5.10 nos dois lados dessa última equação, obtemos $L_{xy} S_{(xy)\backslash x} L_{xy}^{-1} = D_{xy} L_{yx} S_{(yx)\backslash y} L_{yx}^{-1}$, ou seja,

$$S_{(yx)\backslash x} = S_{(yx)\backslash y} L_{yx} D_{xy} L_{xy}^{-1} = S_{(yx)\backslash y} S_{xy}.$$

Agora, substituindo x por $y\backslash x$, temos $S_{x\backslash(y\backslash x)} = S_x S_{x\backslash y}$. Novamente, troque y por xy e, assim, temos $S_{x\backslash(xy\backslash x)} = S_x S_y$. Em outras palavras temos

$$S_{x \divideontimes y} = S_y S_x,$$

o que é equivalente a $\divideontimes$ ser associativa. Logo $(Q, \divideontimes)$ é um 2-grupo elementar.

3.6 p-Loops

Seja p um número primo. Um p-grupo é um grupo cuja ordem de qualquer um dos seus elementos é uma potência de p. Para grupos finitos essa definição é equivalente a dizer que a ordem do grupo é uma potência de p. Felizmente esse resultado também vale para A-loops comutativos finitos.

Teorema 3.6.1. *Seja Q um A-loop comutativo finito e seja p um número primo. Então $|Q|$ é uma potência de p se e somente se todo elemento de Q tem ordem potência de p.*

Demonstração. *Primeiramente, vamos supor p ímpar. Se $|Q|$ for uma potência de p, pela proposição 3.2.9 todo elemento de Q deve ter ordem potência de p. Reciprocamente de $|Q|$ for divisível por um outro primo ímpar q, então Q deve possuir um elemento de ordem q, então, $|Q|$ tem ordem potência de p. Agora analisemos o caso em que $p = 2$. Se $|Q|$ for uma potência de 2, pelo teorema 3.4.1 temos que $K(Q) = \{1\}$, e assim todo elemento de Q tem ordem potência de 2. Agora suponha que todo elemento de Q tenha ordem potência de 2. Assuma que Q seja o menor A-loop finito cujo expoente é uma potência de 2 tal que $|Q|$ não seja potência de 2. Pelo teorema 3.4.6, $H_1(Q) = \{x \in Q : x^2 = 1\} \lhd Q$. Como consequência do teorema 3.5.2, temos que $|H_1(Q)| = 2^n$ para algum n. Assim $H_1(Q) \neq Q$ e, pela minimalidade de $|Q|$, temos que $|Q/H_1(Q)|$ é uma potência de 2. Logo $|Q| = |H_1(Q)|.|Q/H_1(Q)|$ deve ser uma potência de 2, o que é uma contradição da escolha de Q.* □

Apresentemos aqui o teorema mais importante desse capítulo, que garante que propriedades importantes de grupos valem para A-loops comutativos finitos.

Teorema 3.6.2. *[Lagrange, Cauchy] Seja Q um A-loop comutativo finito. Então:*

(i) se $x \in A \leq Q$, então $|x|$ e $|A|$ dividem $|Q|$;

(ii) se um primo p divide $|Q|$, então Q possui um elemento de ordem p.

Demonstração. *Seja Q um A-loop comutativo finito. Então $Q = K(Q) \times H(Q)$ onde $K(Q)$ é o subloop formado pelos elementos de Q que têm ordem ímpar ($|K(Q)|$ é ímpar) e $H(Q)$ é o subloop formado pelos elementos de Q que têm ordem potência de 2 ($|H(Q)|$ é par). Se $|Q| = 2^k.m$ onde m é ímpar, então $|K(Q)| = m$ e $|H(Q)| = 2^k$.*

(i) Seja A um subloop de Q. Então, A é um A-loop comutativo finito. Então pelo teorema 3.4.1 temos que $A = K(A) \times H(A)$, onde $K(A)$ e $H(A)$ são como descrito acima. Se $y \in A$, então $y = y_1y_2$, onde $y_1 \in K(A)$ e $y_2 \in H(A)$. Como $K(A) \leq K(Q)$, pela proposição 3.2.9, temos que, $|y_1|$ divide $|K(A)|$ e $|K(A)|$ divide $|K(Q)|$. Do mesmo modo $H(A) \leq H(Q)$, assim $|y_2|$ divide $|H(A)|$ que, por sua vez, divide $|H(Q)|$. Logo $|y|$ divide $|A|$ que divide $|Q|$.

(ii) Seja p um número primo que divide $|Q|$. Se p é ímpar, temos que $K(Q) \neq \{1\}$ e, pela proposição 3.2.10, temos que Q possui um elemento de ordem p. Se $p = 2$, então $H(Q) \neq \{1\}$ e assim existe $x \in Q$, com $|x| = 2^n$, para algum n. Então $x^{2^n} = (x^{2^{n-1}})^2 = 1$, então $x^{2^{n-1}}$ é o elemento procurado.

Observação. *Se, para um A-loop comutativo finito de ordem ímpar, valer que existem subloops de Hall e Sylow, pelo Teorema da Decomposição, mostra-se que para todo A-loop comutativo finito existem subloops de Hall e Sylow.*

Capítulo 4

A-Loops Comutativos Finitos: Construções

4.1 Loops comutativos cujo núcleo intermediário tem índice 2

Para um conjunto X, denotaremos $\overline{X} = \{\overline{x} : x \in X\}$ uma cópia disjunta do conjunto X. Sejam G um grupo abeliano, com elemento neutro 1, e f um permutação de G. Considere no cojunto $G(f) = G \cup \overline{G}$ a seguinte operação binária:

$$x * y = xy, \quad x * \overline{y} = \overline{xy}, \quad \overline{x} * y = \overline{xy} \quad \text{e} \quad \overline{x} * \overline{y} = f(xy), \tag{4.1}$$

para quaisquer $x, y \in G$. Afirmamos que $(G(f), *) = G(f)$ é um loop com elemento neutro 1. De fato, sejam $a, b \in G$ temos que:

- $x = a^{-1}b$ é a única solução de $a * x = b$;
- $x = \overline{a^{-1}f^{-1}(b)}$ é a única solução de $\overline{a} * x = b$;
- $x = a^{-1}b$ é a única solução de $\overline{a} * x = \overline{b}$;
- $x = \overline{a^{-1}b}$ é a única solução de $a * x = \overline{b}$;

Temos que $G(f)$ é comutativo (lema 4.1.3) e assim, temos que $G(f)$ é um quase-grupo. Finalmente, vale que

$$a * 1 = a \quad \text{e} \quad \overline{a} * 1 = \overline{a}.$$

Portanto $G(f)$ é um loop com elemento neutro 1

Observação 4.1.1. *$Q = G(f)$ será um grupo se e somente se $\overline{1} \in \mathcal{N}_\mu(Q)$.*

Se Q for um grupo teremos $Q = \mathcal{N}_\mu(Q)$ e assim, é claro que, $\overline{1} \in \mathcal{N}_\mu(Q)$. Reciprocamente, vamos supor que $\overline{1} \in \mathcal{N}_\mu(Q)$. Sejam $x, y, z \in G$. Temos que $G \leq \mathcal{N}_\mu(Q)$ (lema 4.1.3), então vale que $\overline{x} * (y * \overline{z}) = (\overline{x} * y) * \overline{z}$, $\overline{x} * (y * \ z) = (\overline{x} * y) * z$, $x * (y * \overline{z}) = (x * y) * \overline{z}$ e $x * (y * z) = (x * y) * z$. Agora temos que

$$\begin{aligned} x * (\overline{y} * z) &= x * ((y * \overline{1}) * z) \\ &= x * (y * (\overline{1} * z)) \\ &= (x * y) * (\overline{1} * z) \\ &= ((x * y) * \overline{1}) * z) \\ &= (x * (y * \overline{1})) * z \\ &= x * (\overline{y} * z). \end{aligned}$$

Da mesma forma podemos mostrar que $\overline{x} * (\overline{y} * z) = (\overline{x} * \overline{y}) * z$, $x * (\overline{y} * \overline{z}) = (x * \overline{y}) * \overline{z}$ e $\overline{x} * (\overline{y} * \overline{z}) = (\overline{x} * \overline{y}) * \overline{z}$. Logo Q é um grupo. $\square$

Observação 4.1.2. *Se Q não for um grupo, então $G = \mathcal{N}_\mu(Q)$.*

Pelo lema 4.1.3 já temos que $G \subset \mathcal{N}_\mu(Q)$. Suponha $x \in G$ tal que $\overline{x} \in \mathcal{N}_\mu(Q)$. Então para quaisquer $a, b \in Q$ temos

$$a * (\overline{1} * b) = a * ((\overline{x} * x^{-1}) * b) = a * (\overline{x} * (x^{-1} * b)) = (a * \overline{x}) * (x^{-1} * b) =$$

$$= ((a * \overline{x}) * x^{-1}) * b = (a * (\overline{x} * x^{-1})) * b = (a * \overline{1}) * b,$$

assim, $\overline{1} \in \mathcal{N}_\mu(Q)$ o que contradiz o fato de Q não ser um grupo. Logo $\mathcal{N}_\mu(Q) \subset G$ e, então, $G = \mathcal{N}_\mu(Q)$.

Lema 4.1.3. *Sejam G um grupo abeliano e f uma permutação de G. Conidere o loop $Q = G(f)$ como definido em 4.1. Então.*

(i) Q *é comutativo;*

(ii) $x\backslash y = x^{-1}y$, $x\backslash\overline{y} = \overline{x^{-1}y}$, $\overline{x}\backslash y = \overline{x^{-1}f^{-1}(y)}$ *e* $\overline{x}\backslash\overline{y} = x^{-1}y$ *para todos* $x, y \in G$*;*

(iii) $G \leq \mathcal{N}_\mu(Q)$*;*

(iv) Q *será um grupo se e somente se* f *for uma translação de* G*;*

(v) Se Q *não for um grupo (isto é,* $G = \mathcal{N}_\mu(Q)$*) então* $\mathcal{N}_\lambda(Q) = \mathcal{N}_\rho(Q) = \mathcal{Z}(Q) = \{x \in G : f(x) = xf(1)\}$.

Demonstração. *Da definição 4.1 e do fato de* G *ser um grupo abeliano temos claramente que* Q *é comutativo. A demosntração do ítem (ii) segue do argumento usado para mostrar que* Q *é um loop. Para mostrar o ítem (iii), tome* $g, x, y \in G$*. Então*

$$x * (g * y) = (x * g) * y,$$

$$\overline{x} * (g * y) = \overline{x} * (gy) = \overline{xgy} = \overline{xg} * y = (\overline{x} * g) * y,$$

$$x * (g * \overline{y}) = x * \overline{gy} = \overline{xgy} = (xg) * \overline{y} = (x * g) * \overline{y} \quad e$$

$$\overline{x} * (g * \overline{y}) = \overline{x} * \overline{gy} = f(xgy) = \overline{xg} * \overline{y} = (\overline{x} * g) * \overline{y}.$$

Assim, $G \leq \mathcal{N}_\mu(Q)$*. Na demonstração do ítem (iv) vamos usar a observação 4.1.1. Desde que* $(x*\overline{1})*\overline{y} = x*(\overline{1}*\overline{y})$ *se e somente se* $f(xy) = xf(y)$, $(\overline{x}*\overline{1})*y = \overline{x}*(\overline{1}*y)$ *se e somente se* $f(xy) = f(x)y$ *e* $(\overline{x}*\overline{1})*\overline{y} = \overline{x}*(\overline{1}*\overline{y})$ *se e somente se* $f(x)y = xf(y)$*, temos que* $\overline{1} \in \mathcal{N}_\mu(Q)$ *se e somente se* $f(xy) = xf(y) = f(x)y$ *para todo* $x, y \in G$*. Fazendo* $y = 1$ *nessa última igualdade temos que* $f(x) = xf(1)$*, para todo* $x \in G$ *o que nos diz que* f *é uma translação de* G*. Reciprocamente, se* $f(x) = xf(1)$*, para todo* $x \in G$*,* $f(xy) = xyf(1) = xf(y)$ *e* $f(xy) = xyf(1) = yf(x)$*, donde temos que* $1 \in \mathcal{N}_\mu(Q)$*. Finalmente vamos mostrar que* $\mathcal{N}_\lambda(Q) = \mathcal{N}_\rho(Q) = \mathcal{Z}(Q) = \{x \in G : f(x) = xf(1)\}$ *sempre que* Q *não for um grupo. Para quaisquer* $x, y, z \in G$ *temos* $(x*y)*z = x*(y*z)$

$(x * \overline{y}) * z = \overline{xyz} = x * (\overline{y} * z)$ *e* $(x * y) * \overline{z} = \overline{xyz} = x * (y * \overline{z})$. *Então* $x \in \mathcal{N}_\lambda(Q)$ *se e somente se* $(x * \overline{y}) * \overline{z} = x * (\overline{y} * \overline{z})$ *o que é equivalente a* $xf(yz) = f(xyz)$ *para todo* $y, z \in G$. *Fazendo* $y = z = 1$ *temos* $f(x) = xf(1)$. *Reciprocamente* $f(x) = xf(1)$ *para todo* $x \in G$, *teremos que* $f(xyz) = x(yzf(1)) = xf(yz)$ *para todos* $y, z \in G$. *Como* Q *é comutativo temos que* $\mathcal{N}_\lambda(Q) = \mathcal{N}_\rho(Q)$ *e, por hipótese* $\mathcal{N}_\mu(Q) = G$, *donde segue o resultado.* □

Lema 4.1.4. *Seja* Q *um loop comutativo com um subloop* G *satisfazendo* $G \leq \mathcal{N}_\mu(Q)$ *e* $[Q : G] = 2$. *Então* G *é um grupo abeliano e existe* f *permutação de* G *tal que* Q *é isomorfo a* $G(f)$, *onde* $G(f)$ *é definido pela operação 4.1.*

Demonstração. *Como* $G \subset \mathcal{N}_\mu(Q)$, *é claro que* G *é um grupo abeliano. Por hipótese, temos que* $[Q : G] = 2$ *e então* $Q \backslash G \neq \emptyset$. *Escolha um elemento* $\overline{1} \in Q \backslash G$. *Para cada elemento* $x \in G$ *denote por* $\overline{x} = x\overline{1} = \overline{1}x$. *Se existisse* $y \in G \cap \overline{G}$, *onde* $\overline{G} = \{\overline{g} : g \in G\}$, *teríamos* $y = \overline{1}z$ *para algum* $z \in G$ *e, assim, como* G *é um subloop de* Q, *teríamos* $\overline{1} \in G$. *Então temos que* $G \cap \overline{G} = \emptyset$. *Se* $x_1, x_2 \in G$ *são tais que* $\overline{x_1} = \overline{x_2}$, *então de* $x_1\overline{1} = x_2\overline{1}$ *temos* $x_1 = x_2$. *Logo a aplicação* $\bar{\cdot} : G \longrightarrow Q \backslash G$ *é injetiva e desde que* $|G| = |Q \backslash G|$ *temos que* $\overline{G} = Q \backslash G$ *e assim* $Q = G \cup \overline{G}$ *e essa reunião é disjunta. Se* $x \in G$ *é tal que* $\overline{1}(x\overline{1}) = \overline{z} \in \overline{G}$, *então* $\overline{x} = z \in G \cap \overline{G}$. *Logo a aplicação* $f : G \longrightarrow G$ *dada por* $f(x) = \overline{1}(x\overline{1})$ *está bem definida. Além disso* f *é injetiva, pois* $\overline{1}(x\overline{1}) = \overline{1}(y\overline{1})$ *implica* $x\overline{1} = y\overline{1}$ *e assim* $x = y$. *Para cada* $g \in G$ *existe* $\alpha = \overline{z} \in \overline{G}$ *tal que* $\overline{1}\alpha = x$ *(pois* Q *é um loop), então* $f(z) = x$ *e então* f *é uma bijeção de* G. *Agora só nos resta mostrar que* Q *é isomorfo a* $G(f)$. *Para* $x, y \in G$, *vale que* $x\overline{y} = x(y\overline{1}) = \overline{xy}$ *e* $\overline{x}y = (\overline{1}x)y = \overline{xy}$, *e finalmete*

$$\overline{xy} = (\overline{1}x)(y\overline{1}) = \overline{1}((xy)\overline{1}) = f(xy).$$

Assim, a estrutura de loop Q *coincide com a estrutura de* $G(f)$.

Corolário 4.1.5. *Seja* Q *um loop comutativo. Então se* $[Q : \mathcal{N}_\mu(Q)] = 2$ *existe* G, *grupo abeliano, e* f, *permutação de* G, *tal que* $G(f)$ *é isomorfo a* Q. *Por outro lado, se existe* G *grupo abeliano e* f *permutação de* G *tal que* Q *é isomorfo a* $G(f)$ *então,* $[Q : \mathcal{N}_\mu(Q)] \leq 2$.

Agora trataremos das possíveis relações entre os loops $G(f_1) = G_1$ e $G(f_2) = G_2$, para distintas f_1, f_2 permutações de G. De fato, exibiremos um critério para determinar quando $G_1 \simeq G_2$.

Proposição 4.1.6. *Sejam G um grupo e f_1, f_2 permutações de G tais que G_1 e G_2 não sejam grupos. Então $G_1 \simeq G_2$ se e somente se existir $\psi \in Aut(G)$ tal que*

$$f_2^{-1}\psi f_1(x) = f_2^{-1}\psi f_1(1).\psi(x) \quad \textit{para todo} \quad x \in G \tag{4.2}$$

e ainda se $f_2^{-1}\psi f_1(1)$ for um quadrado em G.

Demonstração. *Denotaremos por $*$ a multiplicação em G_1 e por $\circ$ a multiplicação de G_2. Vamos assumir que existe $\phi : G_1 \longrightarrow G_2$ um isomorfismo. Como G_1 e G_2 não são grupos, temos que $\mathcal{N}_\mu(G_1) = G = \mathcal{N}_\mu(G_2)$ e, assim, $\psi = \phi|_G$ é uma permutação de G. Além disso*

$$\psi(xy) = \phi(xy) = \phi(x * y) = \phi(x) \circ \phi(y) = \phi(x)\phi(y) = \psi(x)\psi(y)$$

para todos $x, y \in G$. Logo ψ é um automorfismo de G. Agora, defina $\rho : G \longrightarrow G$ tal que $\overline{\rho(x)} = \phi(\overline{x})$. Temos que $\rho(x) = \psi(x)\rho(1)$ para todo $x \in G$, pois

$$\overline{\rho(x)} = \phi(\overline{x}) = \phi(x) \circ \phi(\overline{1}) = \psi(x) \circ \overline{\rho(1)} = \overline{\psi(x)\rho(1)}.$$

Portanto temos que,

$$\begin{aligned}
\psi(f_1(xy)) &= \phi(f_1(xy)) \\
&= \phi(\overline{x} * \overline{y}) \\
&= \phi(\overline{x}) \circ \phi(\overline{y}) \\
&= \overline{\rho(x)} \circ \overline{\rho(y)} \\
&= f_2(\rho(x)\rho(y)) \\
&= f_2(\rho(1)^2\psi(xy)).
\end{aligned}$$

Assim $f_2^{-1}\psi f_1(x) = \rho(1)^2\psi(x)$ para todo $x \in G$. Nessa última igualdade, basta fazer $x = 1$ para obter $f_2^{-1}\psi f_1(1) = \rho(1)^2$. Reciprocamente, suponha que valha a equação

4.2 para algum automorfismo ψ de G com $f_2^{-1}\psi f_1(1) = u^2$ para algum $u \in G$. Defina $\phi : G_1 \longrightarrow G_2$ por $\phi(x) = \psi(x)$ e $\phi(\overline{x}) = \overline{u\psi(x)}$. Vamos mostrar que ϕ é um isomorfismo. De fato,

$$\phi(x * y) = \phi(xy) = \psi(xy) = \psi(x)\psi(y) = \psi(x) \circ \psi(y) = \phi(x) \circ \phi(y),$$

$$\phi(\overline{x} * y) = \phi(\overline{xy}) = \overline{u\psi(xy)} = \overline{u\psi(x)\psi(y)} = \overline{u\psi(x)} \circ \psi(y) = \phi(\overline{x}) \circ \phi(y),$$

$$\phi(x * \overline{y}) = \phi(\overline{xy}) = \overline{u\psi(xy)} = \overline{u\psi(x)\psi(y)} = \psi(x) \circ \overline{u\psi(y)} = \phi(x) \circ \phi(\overline{y})$$

e, finalmente,

$$\phi(\overline{x} * \overline{y}) = \phi(f_1(xy)) = \psi(f_1(xy)) = f_2(u^2\psi(xy)) = \overline{u\psi(x)} \circ \overline{u\psi(y)} = \phi(\overline{x}) \circ \phi(\overline{x}).$$

Com isso mostramos que ϕ é um homomorfismo. O fato de ψ ser uma bijeção de G, faz com que ϕ seja bijetora. $\square$

Se existir um automorfismo ψ de G tal que $f_2 = \psi f_1 \psi^{-1}$, diremos que as aplicações f_1 e f_2 são conjugadas em $Aut(G)$.

Corolário 4.1.7. *Sejam G um grupo e f_1, f_2 permutações de G tais que G_1 e G_2 não sejam grupos. Vale que:*

1. *Se f_1 e f_2 são conjugadas em $Aut(G)$, então $G_1 \simeq G_2$.*
2. *Se $f_1(1) = f_2(1) = 1$, então $G_1 \simeq G_2$ se e somente se f_1 e f_2 forem conjugadas em $Aut(G)$.*
3. *Se $f_2 \in Aut(G)$, t for um quadrado em G e $f_1(x) = f_2(x)t$ para todo $x \in G$, então $G_1 \simeq G_2$.*

Demonstração. *1. Seja $\psi \in Aut(G)$ tal que $f_2 = \psi f_1 \psi^{-1}$. Então $f_2^{-1}\psi f_1 = \psi$ e como $f_2^{-1}\psi f_1(1) = 1$ é um quadrado em G, segue que $G_1 \simeq G_2$.*

2. *Vamos supor* $G_1 \simeq G_2$. *Pela proposição 4.1.6, existe* $\psi \in Aut(G)$ *tal que* $f_2^{-1}\psi f_1(x) = f_2^{-1}\psi f_1(1).\psi(x)$ *para todo* $x \in G$ *e que* $f_2^{-1}\psi f_1(1)$ *é um qquadrado em* G. *Como* $f_2^{-1}\psi f_1(1) = 1$, *temos que* $f_2^{-1}\psi f_1(x) = \psi(x)$ *para todo* $x \in G$ *e assim, temos* $f_2 = \psi f_1 \psi^{-1}$. *A recíproca segue do ítem 1.*

3. *Tomando* $\psi = id_G$, *a equação 4.2 se escreve como* $f_2^{-1}f_1(x) = f_2^{-1}f_1(1).x$. *Vamos mostrar que* $f_2^{-1}f_1(1)$ *é um quadrado em* G. *De fato*

$$f_2^{-1}f_1(1) = f_2^{-1}(f_2(1)t) = f_2^{-1}(t)$$

que, como t *é um quadrado em* G *e* $f_2 \in Aut(G)$, *é um quadrado em* G. □

O que foi feito até agora neste capítulo, independe de $G(f)$ ter ou não estrutura de A-loop. A próxima proposição será uma ferramenta para construção de A-loops comutativos com núcleo intermediário de índice 2.

Proposição 4.1.8. *As seguintes condições são equivalentes para um* A*-loop comutativo* Q *que possui um subgrupo de índice 2.*

1. Q *é um* A*-loop e* $[Q : \mathcal{N}_\mu(Q)] = 2$;

2. $Q = G(f)$ *onde* G *é um grupo abeliano,* $[Q : G] = 2$ *e* f *é uma permutação de* G *satisfazendo*

$$f(xy) = f(x)f(y)f(1)^{-1} \tag{4.3}$$

$$f(x^2) = x^2 f(1) \tag{4.4}$$

$$f^2(x^2)f(x)^{-2} = f^2(1) \tag{4.5}$$

para quaisquer $x, y \in G$.

3. $Q = G(f)$, *onde* G *é um grupo abeliano,* $[Q : G] = 2$ *e* f *é uma permutação de* G *que satisfaz 4.3, 4.4 e* $f^2(1) = f(1)^2$.

4. $Q = G(f)$, *onde* G *é um grupo abeliano,* $[Q : G] = 2$, $f(x) = g(x)t, g(x^2) = x^2$ *para todo* $x \in G$, *onde* $g \in Aut(G)$ *e* t *é um ponto fixo de* g.

Demonstração. *Vamos mostrar quue 1 é equivalente a 2, 2 é equivalente a 3 e 3 é equivalente a 4. Vamos mostrar o primeiro caso. Q é um A-loop e $[Q : \mathcal{N}_\mu(Q)] = 2$, se e somente se $Q = G(f)$ onde G é um grupo abeliano tal que $G \leq \mathcal{N}_\mu(Q)$ e f é uma permutação de G. Denote por $\alpha(a, b, c, d)$ a seguinte identidade*

$$[(a * b)\backslash(a * (b * c))] * [(a * b)\backslash(a * (b * d))] = [(a * b)\backslash(a * (b * (c * d)))],$$

com $a, b, c, d \in G \cup \overline{G}$. Temos que Q é um A-loop se e somente se $\alpha(a, b, c, d)$ for verdadeira para quaisquer $a, b, c, d \in Q$. Com excessão dos elementos a, b, c, d, os elementos sem barra estão em G e os elementos sem barra são elementos de $\overline{G}$. Sejam $x, y, u, v \in G$ temos que $\alpha(x, y, u, v)$, $\alpha(a, y, b, c)$ e $\alpha(x, \overline{y}, u, v)$ são sempre verdadeiras pois G é um grupo e $G \leq \mathcal{N}_\mu(Q)$. Por hipótese, Q é comutativo e então $\alpha(a, b, c, d)$ será verdadeira se e somente se $\alpha(a, b, d, c)$ for verdadeira. Segue da definição que:

$$\alpha(x, \overline{y}, u, \overline{v}) \quad \text{é equivalente a} \quad f^{-1}(xf(yuv)) = uf^{-1}(xf(yv)), \tag{4.6}$$

$$\alpha(x, \overline{y}, \overline{u}, \overline{v}) \quad \text{é o mesmo que} \quad f(uv) = f((xy)^{-2}f^{-1}(xf(yu))f^{-1}(xf(yv))), \tag{4.7}$$

$$\alpha(\overline{x}, \overline{y}, u, v) \quad \text{é equivalente a} \quad f(xyuv) = f(xy)^{-1}f(xyu)f(xyv), \tag{4.8}$$

$$\alpha(\overline{x}, \overline{y}, u, \overline{v}) \quad \text{vale se e só se} \quad xf(yuv) = f(xyu)f(xy)^{-1}xf(yv), \tag{4.9}$$

e finalmente temos que $\alpha(\overline{x}, \overline{y}, \overline{u}, \overline{v})$ se verifica se e somente se

$$f(xy)^{-1}f(xyf(uv)) = f(f(xy)^{-2}x^2f(yu)f(yv)). \tag{4.10}$$

Em 4.9, fazendo $x = y = 1$ temos que $f(uv) = f(u)f(v)f(1)^{-1}$ para quaisquer $u, v \in G$, ou seja 4.3 se verifica. Reciprocamente se vale 4.3 então

$$f(xyu)f(yv) = f(xy)(f(u)f(1)^{-1}f(yv)) = f(xy)f(yuv)$$

e, logo, $xf(yuv) = f(xy)^{-1}f(xyu)xf(yv)$, para quaisquer $x, y, u, v \in G$. Assim a identidade $\alpha(\overline{x}, \overline{y}, u, \overline{v})$ é equivalente a equação 4.3.

A partir de agora, vamos assumir 4.3 verdadeira e denotemos $t = f(1)$. *Como 4.3 é verdadeira temos que a equação 4.7 é equivalente a*

$$x^{-1}t^{-1} = f(x^{-2})f(y^{-2})f(y)^2xt^{-5}. \tag{4.11}$$

Como $t = f(1) = f(yy^{-1}) = f(y)f(y^{-1})f(1)^{-1}$, *segue que*

$$f(y^{-1}) = f(y)^{-1}t^2 \quad \textit{e ainda} \quad f(y^{-2}) = f(y)^{-2}t^3. \tag{4.12}$$

Voltando à equação 4.11 vem que

$$\begin{aligned} x^{-1}t^{-1} &= f(x^{-2})f(y^{-2})f(y)^2xt^{-5} \\ &= f(x^{-2})xt^{-2} \\ &= f(x^2)^{-1}x \\ &= (f(x)^2t^{-1})^{-1}x = f(x)^{-2}tx. \end{aligned}$$

Assim $f(x)^2 = x^2t$, *ou equivalentemente (usando 4.3),* $f(x^2) = x^2t$, *que é a identidade 4.4. Agora, usando 4.3 e 4.12 segue*

$$f^2(uv) = f(f(u)f(v)t^{-1}) = f^2(u)f^2(v)f(t^{-1})t^{-2} = f^2(u)f^2(v)f(t)^{-1}. \tag{4.13}$$

A partir das equações 4.3, 4.4 e 4.13, temos que $\alpha(\overline{x}, \overline{y}, \overline{u}, \overline{v})$ *é verdadeira se e só se*

$$f(t) = f(xy)^{-2}x^2f^2(y)^2. \tag{4.14}$$

Nessa última equação, faça $x = 1$, *donde segue 4.5.*
Agora, assumindo 4.5 vamos mostrar 4.14. De fato

$$f(t) = f^2(xy)f^2(xy)f(xy)^{-2} = f^(x)^2f^2(y)^2f(xy)^{-2}f(t)^{-2}.$$

Resta-nos mostrar que $x^2 = f^2(x)^2 f(t)^{-2}$. *Bem, usando 4.3 e 4.4*

$$\begin{aligned} f^2(x)^2 f(t)^{-2} &= f(f(x))f(f(x))f(t)^{-2} \\ &= f(f(x)^2)tf(t)^{-2} \\ &= f(f(x)^2)(f(t)f(t)t^{-1})^{-1} \\ &= f(f(x)^2)f(t^2)^{-1} \\ &= f(f(x)^2)(t^2t)^{-1} \\ &= f(x^2)t^{-2} = f(x^2)t^{-1} \\ &= x^2, \end{aligned}$$

e assim, 4.5 é equivalente a 4.14. Finalmente, as identidades $\alpha(x, \overline{y}, \overline{v}, u), \alpha(x, y, u, \overline{v}), \alpha(\overline{x}, \overline{y}, u, v)$ *seguem da identidade 4.3. Logo, 1 é equivalente a 2.*
Vamos agora assumir o ítem 2. Basta fazer $x = 1$ *em 4.5 para obter* $f(t) = t^2$, *o que demonstra o ítem 3. Agora se vale* $f(t) = t^2$, *temos*

$$f^2(x)^2 f(t)^{-1} = f(f(x))f(f(x))t^{-2} = f(f(x)^2)t^{-1} = f(x)^2,$$

donde temos 4.5. Assim 2 é equivalente a 3.
Assuma que valha o ítem 3. Defina $g : G \longrightarrow G$ *por* $g(x) = f(x)t^{-1}$, *onde* $t = f(1)$. *De 4.3, temos que*

$$g(xy) = f(xy)t^{-1} = f(x)f(y)t^{-2} = f(x)t^{-1}f(y)t^{-1} = g(x)g(y)$$

e de 4.4 temos $g(x^2) = f(x^2)t^{-1} = x^2$. *Ainda temos que* g *é uma bijeção de* G *(pois* f *o é) e* $g(t) = f(t)t^{-1}t^2t^{-1} = t$, *donde temos o ítem 4. Finalmente, supondo 4, defina* $f(x) = g(x)t$ *onde* t *é um ponto fixo de* g. *Temos que* $f(1) = g(1)t = t$. *De*

$$f(xy) = g(xy)t = g(x)tg(y)tt^{-1} = f(x)f(y)t^{-1},$$

temos 4.3. De $f(x^2) = g(x^2)t = x^2t$, *que é 4.4 e, por fim,* $f^2(1) = f(t) = g(t)t = t^2$, *provando o ítem 3.* □

4.2 Construções de A-Loops Comutativos com Núcleo Intermediário de Índice 2

O principal objetivo dessa seção é aplicar a proposição 4.1.8 para classificar os A-loops comutativos de ordem 8 e apresentar uma classe de A-loops comutativos de expoente 2 com centro trivial e núcleo intermediário de índice 2.

4.2.1 A-loops comutativos de ordem 8

Através de cálculos feitos computacionalmente, sabemos que existem 4 A-loops não-associativos de ordem 8, e todos esses têm núcleo intermediário de índice 2. Vamos classificar os A-loops comutativos de ordem 8.

Lema 4.2.1. *Sejam G um grupo abeliano, $g \in Aut(G)$ e $t \in G$. Seja f a permutação de G definida por $f(x) = g(x)t$. Então $\mathcal{Z}(G(f)) = \mathcal{Z}(G(g))$ como conjuntos.*

Demonstração. *Se $g = id_G$ então tanto g quanto f são translações de G e assim $G(g)$ e $G(g)$ são grupos abelianos. Portanto $\mathcal{Z}(G(f)) = G \cup \overline{G} = \mathcal{Z}(G(g))$. Agora, se $g \neq id_G$, nem f nem g são translações de G. Assim, pelo lema 4.1.3 tanto $G(f)$ como $G(g)$ são não-associativos e, além disso,*

$$\mathcal{Z}(G(f))\{x \in G : f(x) = xf(1)\} = \{x \in G : g(x)t = xt\} =$$

$$= \{x \in G : g(x) = xg(1)\} = \mathcal{Z}(G(g)). \quad \square$$

Suponha Q um A-loop comutativo de ordem 8 com $[Q : \mathcal{N}_\mu(Q)] = 2$. Temos que, pela proposição 4.1.8, $Q = G(f)$ onde G é um grupo abeliano de ordem 4 e $f(x) = g(x)t$ para algum $g \in Aut(G)$ tal que $g(x^2) = x^2$ e $g(t) = t$. No que se segue, denotaremos os automorfismos do grupo G com a notação cíclica, isto é, o automorfismo (a, b) está definido por $a \mapsto b$. Vamos analisar os casos possíveis:

1. Suponha $G = \mathbb{Z}_4 = \langle a \rangle$. O grupo G possui apenas os automorfismos (a, a) e (a, a^3) e ambos fixam os quadrados de G.

- Se $g = (a, a)$ temos que $f(x) = g(x)t$ é uma trasnlação e então $G(f)$ é um grupo abeliano.
- Se $g = (a, a^3)$ então $G(f)$ é um A-loop comutativo não-associativo de oredem 8. Como o único elemnto não trivial de G que é fixado por g é a^2, se $f(x) = g(x)a^2$ teremos que $G(f) \simeq G(g)$.

2. Suponha $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle a \rangle \times \langle b \rangle$. Temos que

$$Aut(G) = \{id_G, (a, b), (a, ab), (b, ab), (a, b, ab), (b, a, ab)\} \simeq S_3.$$

O elemento neutro 1 é o único quadrado de G e é fixo por todo elemento de $Aut(G)$.

- Se $g = id_G$ e $f(x) = g(x)t$ para algum $t \in G$, então $G(f)$ é um grupo abeliano.
- Assuma $g_1 = (a, b)$. A duas possíveis escolhas para $t \in G$ tal que $g(t) = t$, a saber, $t = 1$ e $t = ab$. Seja $f_1(x) = g_1(x)ab$. Então $G(f_1)$ e $G(g_1)$ são A-loops comutativos não associativos. Afirmamos que $G(f_1) \nsim G(g_1)$. De fato, como $g_1(xx) = g_1(1) = 1$, te,os que $G(g_1)$ tem expoente 2, por outro lado $f_1(xx) = f_1(1) = ab$.
- Considere $g_2 = (a, ab)$. Se $t \in G$ é tal que $g(t) = t$, então ou $t = 1$ ou $t = b$. Seja $f_2(x) = g_2(x)b$. Visto que $Aut(G) \simeq S_3$ temos que g_1 e g_2 são conjugados em $Aut(G)$, logo pelo corolário 4.1.7 temos $G(g_1) \simeq G(g_2)$. Como consequência do fato de g_1 e g_2 srem conjugados em $Aut(G)$ temos que f_1 e f_2 são conjugadas em $Aut(G)$, donde segue $G(f_1) \simeq G(f_2)$.
- Se $g_3 = (b, ab)$ temos que g_3 e g_2 saõ conjugadas e assim $G(g_3)$ já foi listado anteriormente.
- Considere $g_4 = (a, b, ab)$. Observe que o automorfismo g_4 não possui nenhum ponto fixo, exceto 1. Como g_4 não é uma translação de G, então

$G(g_4)$ é um A-loop comutativo não associativo. Pelo lema 4.1.3, segue

$$\mathcal{Z}(G(g_4)) = \{x \in G : g_4(x) = xg_4(1)\} = \{1\}$$

e

$$\mathcal{Z}(G(g_1))\{x \in G : g_1(x) = xg_1(1)\} = \{1, ab\}$$

. Donde temos que $G(g_4)$ é um A-loop não-associativo que ainda não havia sido listado.

- Finalmente, se $g_5 = (b, a, ab)$ então g_4 e g_5 são conjugados em $Aut(G)$ donde temos que $G(g_4) \simeq G(g_5)$.

4.2.2 Uma classe de A-loops comutativos de expoente 2 com centro trivial e núcleo intermediário de índice 2

Considere $\mathbb{F}_2$ o corpo com dois elementos, V um $\mathbb{F}_2$-espaço veotorial de dimensão n, $n \geq 2$ e $G = (V, +)$ o 2-grupo abeliano elementar correspondente. Para uma base $\mathcal{B} = \{e_1, e_2, ..., e_n\}$ defina um automorfismo g de G fazendo

$$g(e_i) = e_{i+1} \quad \text{para} \quad i = 1, ..., n-1 \quad \text{e} \quad g(e_n) = e_1 + e_n.$$

Temos que $g(x + x) = g(0) = 0 = x + x$, então fazendo $f = g$, pela proposição 4.1.8, temos que $Q_n = G(f)$ é um A-loop comutativo de ordem 2^{n+1} cujo núcleo intermediário tem índice, no máximo, 2. Se

$$g(a_1e_1 + a_2e_2 + ... + a_ne_n) = a_1e_1 + a_2e_2 + .. + a_ne_n$$

então $a_1 = a_2 = ... = a_n = 0$ o que, pelo lema 4.1.3, nos garante que $G(f)$ tem centro trivial. Segue que $[Q_n : \mathcal{N}_\mu(Q_n)] = 2$ pois f não é uma translação e como $x * x = x + x = 0$ e $\overline{x} * \overline{x} = g(x + x) = 0$, Q_n tem expoente 2.

4.3 Extensões Centrais Baseadas em Formas Trilineares

Nessa seção, faleremos de construções de A-loops comutativos através de extensões centrais de um grupo abeliano por um A-loop comutativo. Tais extensões serão dadas por cociclos de loops. Determinaremos condições para quando tais cociclos geram A-loops comutativos e grupos abelianos. Estudaremos também, cociclos definidos por formas trilineares.

Definição 4.3.1. *Dizemos que o loop Q é uma extensão do loop Z pelo loop K se $Z \lhd Q$ e se $Q/Z \simeq K$. No caso de $Z \leq \mathcal{Z}(Q)$, tal extensão é chamada de extensão central.*

É sabido que (vide [BP]) extensões centrais de um grupo abeliano Z por um loop K são loops da forma $K \ltimes_\theta Z = (Z, K, \theta(x, y))$ definidos em $K \times Z$ com

$$(x, a)(y, b) = (xy, ab\theta(x, y))$$

onde $\theta : K \times K \longrightarrow Z$ é uma aplicação que satisfaz $\theta(1, x) = \theta(x, 1) = 1$, para todo $x \in K$. Tal aplicação θ é chamada de *cociclo de loops*. No teorema 2.5.3 é exibido condições para θ para que $K \ltimes_\theta Z$ seja um A-loop, onde Z é um grupo abeliano e K já tem estrutura de A-loop. Apresentaremos aqui uma versão desse teorema cuja demontração será omitida por se tratar de um caso particular da realizada no capítulo 2.

Teorema 4.3.2. *Sejam Z um grupo abeliano e K um A-loop comutativo. Considere $\theta : K \times K \longrightarrow Z$ satisfazendo $\theta(x, y) = \theta(y, x)$ para todo $x, y \in K$ e*

$$F(x, y, z)F(x', y, z)\theta(R_{(y,z)}(x), R_{(y,z)}(x')) = F(xx', y, z)\theta(x, x')$$

para quaisquer $x, x', y, z \in K$ onde a função F é definida por
$F(x, y, z) = \theta(R_{(y,z)}(x), yz)^{-1}\theta(y, z)^{-1}\theta(xy, z)\theta(x, y)$. Então $K \ltimes_\theta Z$ é um A-loop comutativo.

Observação 4.3.3. *O teorema 4.3.2 é um caso particular do teorema 2.5.3 pois para loops comutativos L, o grupo das aplicações internas é gerado por $\{R_{(a,b)} : a, b \in L\}$.*

Teorema 4.3.4. *Sejam Z um 2-grupo abeliano elementar e K um A-loop comutativo de expoente 2. Considere o cociclo de loop θ tal que $\theta(x,y) = \theta(y,x)$ e $\theta(x,x) = 1$ para todos $x, y \in K$ e*

$$\theta(x,y)\theta(x^{'},y)\theta(xx^{'},y)\theta(x,x^{'})\theta(xy,z)\theta(x^{'}y,z)\theta(y,z)\theta((xx^{'})y,z) =$$

$$= \theta(R_{(y,z)}(x),yz)\theta(R_{(y,z,)}(x^{'}),yz)\theta(R_{(y,z,)}(xx^{'}),yz)\theta(R_{(y,z,)}(x),R_{(y,z)}(x^{'})),$$

para todos $x, x^{'}, y, z \in K$. Então $K \ltimes_\theta Z$ é um A-loop comutativo de expoente 2.

Demonstração. *Visto que $(x,a)(x,a) = (xx, aa\theta(x,x))$, temos que $Q = K \ltimes_\theta Z$ é um loop comutativo de expoente 2. Resta mostrar que Q é um A-loop. Sejam $(x,a),(x^{'},a^{'}),(y,b),(z,c) \in Q$. Fazendo $R_{((y,b),(z,c))}(x,a) = (u,v)$, obtemos $u = R_{(y,z)}(x)$ e $v = \theta(R_{(y,z)}(x),yz)\theta(y,z)\theta(xy,z)\theta(x,y)a$. Assim temos*

$$R_{((y,b),(z,c))}(x,a) = (R_{(y,z)}(x), \theta(R_{(y,z)}(x),yz)\theta(y,z)\theta(xy,z)\theta(x,y)a), \tag{4.15}$$

$$R_{((y,b),(z,c))}(x^{'},a^{'}) = (R_{(y,z)}(x^{'}), \theta(R_{(y,z)}(x^{'}),yz)\theta(y,z)\theta(x^{'}y,z)\theta(x^{'},y)a^{'}) \tag{4.16}$$

e também,

$$R_{((y,b),(z,c))}((x,a)(x^{'},a^{'})) = (R_{(y,z)}(xx^{'}),$$

$$\theta(R_{(y,z)}(xx^{'}),yz)\theta(y,z)\theta((xx^{'})y,z)\theta((xx^{'}),y)aa^{'}).$$

Multiplicando as expressões 4.15 e 4.16 e comparando com $R_{((y,b),(z,c))}((x,a)(x^{'},a^{'}))$ temso que Q é um A-loop. □

Se tivéssimos K um 2-grupo elementar a identidade do teorema 4.3.4 poderia ser escrita da forma

$$[\theta(x,y)\theta(x^{'},y)\theta(xx^{'},y)][\theta(xy,z)\theta(x^{'}y,z)\theta(xx^{'},z)]$$

$$[\theta(x,yz)\theta(x^{'},yz)\theta(xx^{'},yz)][\theta(y,z)\theta(xx^{'},z)\theta((xx^{'})y,z)] = 1.$$

Por essa identidade, da vontade de impor que θ satisfaça $\theta(u,w)\theta(v,w)\theta(uv,w)=1$ para todo $u,v,w \in K$ para que o loop $Z \ltimes_\theta K$ se "encaixe"nas hipótese do teorema 4.3.4. Entretanto $\theta(u,w)\theta(v,w)\theta(uv,w)=1$ para todo $u,v,w \in K$ implica associatividade para $Z \ltimes_\theta K$, pois

$$[(u,a)(v,b)](w,c) = (u,a)[(v,b)(w,c)]$$

se e somente se $\theta(uv,w)\theta(uv) = \theta(u,vw)\theta(v,w)$.

Proposição 4.3.5. *Seja $Z = \mathbb{F}_2$ e seja K um 2-grupo abeliano elementar. Seja $g : K^3 \longrightarrow \mathbb{F}_2$ uma forma trilinear tal que $g(x,xy,y) = g(y,xy,x)$ para todo $x,y \in K$. Defina $\theta : K^2 \longrightarrow \mathbb{F}_2$ por $\theta(x,y) = g(x,xy,y)$. Então $Q = K \ltimes_\theta Z$ é um A-loop comutativo de expoente 2. Além disso, $(y,b) \in \mathcal{N}_\mu(Q)$ se e somente se*

$$g(y,x,z) = g(x,z,y).$$

Demonstração. *Desde que $g(x,xy,y) = g(y,xy,x)$ para todos $x,y \in K$ temos $\theta(x,y) = \theta(y,x)$ para todos $x,y \in K$ e como K é um 2-grupo elementar temos que $\theta(x,x) = g(x,e,x) = 0$. Pela tri-linearidade de g, temos que*

$$\theta(u,w)\theta(v,w)\theta(uv,w) = g(u,uw,w)g(v,vw,w)g(uv,uvw,w) = g(u,v,w)g(v,u,w),$$

donde segue que

$$[\theta(x,y)\theta(x',y)\theta(xx',y)][\theta(xy,z)\theta(x'y,z)\theta(xx',z)]$$

$$[\theta(x,yz)\theta(x',yz)\theta(xx',yz)][\theta(y,z)\theta(xx',z)\theta(xx'y,z)] = 1.$$

Assim, pelo teorema 4.3.4, $K \ltimes_\theta Z$ é um A-loop comutativo de expoente 2. Finalmente, tome $(y,b) \in Q$. Por definição $(y,b) \in \mathcal{N}_\mu(Q)$ se e somente se

$$[(x,a)(y,b)](z,c) = (x,a)[(y,b)(z,c)]$$

para quaisquer $(x,a),(y,b) \in Q$ o que é equivalene a

$$\theta(xy,z)\theta(x,y) = \theta(x,yz)\theta(y,z)$$

para todos $x, z \in Q$ que, usando a definição de θ e a tri-linearidade de g, é o mesmo que $g(y, x, z) = g(x, z, y)$ para todo $x, z \in K$.

Definição 4.3.6. *Seja $V = (\mathbb{F}_2)^n$. Uma forma trilinear $g : V^3 \longrightarrow \mathbb{F}_2$ é chamada de* ***(1,3)-simétrica*** *se $g(x, y, z) = g(z, y, x)$ quaisquer que sejam $x, y, z \in V$.*

Portanto uma forma trilinear (1,3)-simétrica define um cociclo de loops que gera um A-loop comutativo de expoente 2. Além disso $(y, b) \in \mathcal{N}_\mu(Q)$ se e somente se $g(y, x, z) = g(x, z, y) = g(y, z, x)$ para todos $x, z \in K$, ou seja, se a aplicação bilinear $g(y, \cdot, \cdot) : V^2 \longrightarrow \mathbb{F}_2$ for simétrica. Jedlicka, Kinyon, Vojtechovsky mostraram em [JKV-02] que para $n \geq 3$, e $V = (\mathbb{F}_2)^n$ sempre existe uma forma trilinear (1,3)-simétrica $g : V^3 \longrightarrow \mathbb{F}_2$ tal que para todo $x \in V \backslash \{0\}$, a forma $g(x, \cdot, \cdot) : V^2 \longrightarrow \mathbb{F}_2$ não é simétrica. Além disso, se $n < 3$ para qualquer forma trilinear (1,3)-simétrica $f : V^3 \longrightarrow \mathbb{F}_2$ existe $y \in V, y \neq 0$ tal que $f(y, \cdot, \cdot) : V^2 \longrightarrow \mathbb{F}_2$ é simétrica.

Exemplo 4.3.7. *Para todo $n \geq 3$, existe um A-loop Q de expoente 2, de ordem 2^{n+1} com $\mathcal{N}_\mu(Q) = \mathcal{Z}(Q)$ e $|\mathcal{Z}(Q)| = 2$. De fato, pela proposição 4.3.5 e pelo fato de que existe $g : V^3 \longrightarrow \mathbb{F}_2$ trilinear (1,3)-simétrica, onde $V = (\mathbb{F}_2)^n$, tal que se $g(x, \cdot, \cdot) : V^2 \longrightarrow \mathbb{F}_2$ for simétrica, então $x = 0$, temos que $Q = V \ltimes_\theta \mathbb{F}_2$, onde $\theta(x, y) = g(x, xy, y)$ é um A-loop. Sabemos que $(0, \mathbb{F}_2)$ é um subloop normal de Q contido em $\mathcal{Z}(Q)$. Por outro lado, se $(x, a) \in \mathcal{Z}(Q)$, em particular, $(x, a) \in \mathcal{N}_\mu(Q)$ e então, $g(x, \cdot, \cdot) : V^2 \longrightarrow \mathbb{F}_2$ é simétrica, e assim $x = 0$. Logo $\mathcal{N}_\mu(Q) = \mathcal{Z}(Q) = (0, \mathbb{F}_2)$ e $|\mathcal{Z}(Q)| = 2$.*

Vimos que se Q for um A-loop comutativo finito de expoente 2, $|Q| = 2^k$ e $|\mathcal{N}_\mu(Q)| = 2^l$ onde $l \leq k$. Queremos determinar todos os possíveis pares (k, l) com $l > 0$.

Lema 4.3.8. *Seja $k \geq l > 0$. Então existe um A-loop comutativo não associativo de ordem 2^k com núcleo intermediário de ordem 2^l se ou $d = k - l \geq 3$ ou $d \geq 1$ e $l \geq 2$.*

Demonstração. *Suponha $d \geq 3$.*
Considere o A-loop Q de ordem 2^{d+1} com $|\mathcal{N}_\mu(Q)| = 2$. Se $k - d = l = 1$, Q é o loop

procurado. Caso $k-d=l>1$*, tome* $L=Q\times(\mathbb{Z}_2)^{k-d-1}$*. Claramente* L *é um A-loop não associativo de ordem* 2^k *e como* $\mathcal{N}_\mu(L)=\mathcal{N}_\mu(Q)\times(\mathbb{Z}_2)^{k-d-1}$*, temos que* $|\mathcal{N}_\mu(L)|=2^l$*. Agora assuma* $d=2$*. Se* $l=1$*, temos o parâmetro* $(3,1)$*. Pela seção anterior, todo A-loop comutativo não associativo de ordem* 8*, possui núcleo intermediário de índice* 2*, portanto de ordem* 4*. Jedlicka, Kinyon e Vojtechovsky, citam em [JKV-02], que, computacionalmente, é possível encontrar um A-loop comutativo* L*, de ordem* 16 *com* $|\mathcal{N}_\mu(L)|=4$*. Finalmente para um par de parâmetros* (k,l) *com* $l>2$ *e* $k-l=2$ *faça* $Q=L\times(\mathbb{Z}_2)^{k-4}$*. O caso* $d=1$ *está feito na seção, 4.2.2, onde, para* Q *ser não associativo, devemos ter* $l>1$*.* □

4.3.1 Somando Cociclos de Grupos

Dizemos que o cociclo de loops $\theta : K\times K\longrightarrow Z$, onde K é um loop e Z é um grupo abeliano é um ***cociclo de grupos*** se θ satisfizer a identidade

$$\theta(x,y)\theta(xy,z)=\theta(y,z)\theta(x,yz)$$

para todos $x,y,z\in K$. O nome cociclo de grupos é justificado pelo fato de que se K for um grupo e θ um cociclo de grupos, então $K\ltimes_\theta Z$ também será um grupo.

Lema 4.3.9. *Sejam* Z *um grupo abeliano,* K *um grupo e* $\theta,\mu : K\times K\longrightarrow Z$ *cociclos de loops tais que* $\nu=\theta\mu^{-1}:(x,y)\mapsto\theta(x,y)\mu(x,y)^{-1}$ *seja um cociclo de grupo. Então as aplicações internas à esquerda* $(L_{(\alpha,\beta)})$ *em* $K\ltimes_\theta Z$ *coincidem com as em* $K\ltimes_\mu Z$*.*

Demonstração. *Em* $K\ltimes_\theta Z$ *vale que*

$$(x,a)(y,b)=(xy,\theta(x,y)ab)\quad e\quad (x,a)\backslash(y,b)=(x\backslash y,a^{-1}b\theta(x,x\backslash y)^{-1}). \tag{4.17}$$

Assim, temos que

$$[(x,a)(y,b)]\backslash(x,a)[(y,b)(z,c)]=(z,\theta(x,y)^{-1}\theta(x,yz)\theta(y,z)\theta(xy,z)^{-1}c).$$

Então as aplicações internas à esquerda de $K\ltimes_\theta Z$ *e* $K\ltimes_\mu Z$ *coincidem se e somente se*

$$\theta(x,y)^{-1}\theta(x,yz)\theta(y,z)\theta(xy,z)^{-1}=\mu(x,y)^{-1}\mu(x,yz)\mu(y,z)\mu(xy,z)^{-1}$$

para todo $x, y, z \in K$, ou seja se ν for um cociclo de grupos. $\square$

Lema 4.3.10. *Sejam Z um grupo abeliano, K um grupo e θ um cociclo de loops tal que $K \ltimes_\theta Z$ seja um A-loop comutativo. Seja $\mu : K \times K \longrightarrow Z$ um cociclo de grupos satisfazendo $\mu(x, y) = \mu(y, x)$ para todos $x, y \in K$. Então $K \ltimes_{\mu\theta} Z$ é um A-loop comutativo com as mesmas aplicações internas à esquerda de $K \ltimes_\theta Z$*

Demonstração. *Denotemos $Q_\theta = K \ltimes_\theta Z$ e $Q_{\mu\theta} = K \ltimes_{\mu\theta} Z$. Visto que Q_θ é comutativo e $\mu(x, y) = \mu(y, x)$, temos que $Q_{\mu\theta}$ também é comutativo. Como $\mu = (\mu\theta)\theta^{-1}$ é um cociclo de grupo, pelo lema 4.17 as aplicações internas à esquerda de Q_θ e $Q_{\mu\theta}$ coincidem. Resta mostrar que $\mathcal{I}(Q_{\mu\theta}) \leq Aut(Q_{\mu\theta})$. Antes disso, obeserve que, se cdot denota a multiplicação de Q_θ e $*$ a de $Q_{\mu\theta}$, temos*

$$(x, a) * (y, b) = (xy, \mu(x, y)\theta(x, y)ab) = (xy, \theta(x, y)ab) \cdot (1, \mu(x, y)) =$$

$$= (x, a) \cdot (y, b) \cdot (1, \mu(x, y)).$$

Seja φ uma aplicação interna à esquerda de $Q_{\mu\theta}$, então

$$\begin{aligned} \varphi((x, a) * (y, b)) &= \varphi((x, a) \cdot (y, b) \cdot (1, \mu(x, y)) \\ &= \varphi(x, a) \cdot \varphi(y, x) \cdot (1, \mu(x, y)) \qquad (4.18) \\ &= (x, a') \cdot (y, b') \cdot (1, \mu(x, y)) \qquad (4.19) \\ &= (x, a') * (y, b') \\ &= \varphi(x, a) * \varphi(y, b), \end{aligned}$$

onde 4.18 é veradeira pois $(1, \mu(x, y)) \in \mathcal{Z}(Q_\theta)$ e 4.19 vale porque Q_θ é um A-loop. Logo, $\varphi \in Aut(Q_{\mu\theta})$. $\square$

4.4 Uma Classe de A-Loops Comutativos de Ordem p^3

Encerramos esse trabalho construindo um classe de A-loops comutativos finitos de ordem p^3.

Seja Q um A-loop comutativo finito de ordem ímpar. Consideremos (vide capítulo 3) o loop $(Q, \circ)$ onde

$$x \circ y = (x^{-1} \backslash x y^2)^{\frac{1}{2}} \quad \text{para} \quad x, y \in Q.$$

Sabemos que o loop $(Q, \circ)$ é um loop de Bruck e além disso sabemos que $(Q, \circ)$ será comutativo se e somente se for isomorfo a Q.

Proposição 4.4.1. *Seja p um primo ímpar e seja Q um A-loop comutativo de ordem $p, 2p, 4p, p^2, 2p^2$ e $4p^2$. Então, Q é um grupo abeliano.*

Demonstração. *Como A-loops de ordem menor que ou igual a 5 são grupos abelianos, se mostrarmos o resultado para A-loops de ordem p e p^2, do Teorema da Decomposição obteremos os outros casos. Caso $|Q| = p$, temos que Q é o grupo cíclico de ordem p pois vale o Teorema de Lagrange em Q e Q associa potências. Caso $|Q| = p^2$, Q é um grupo pois Burn em* Finite Bol Loops, Math. Proc. Cambriage Philos. Soc., vol 84 (1978) n.03 $377 - 385$ *mostrou que todo loop de Bol de ordem p^2 é um grupo. Assim $(Q, \circ)$ é um grupo de ordem p^2, portanto abeliano. Logo $(Q, \circ)$ é isomorfo a Qe assim Q é um grupo abeliano.*

A partir de agora, estudaremos alguns A-loops de ordem p^3 para p um primo ímpar (Tratamos de A-loops de ordem 8, no início desse capítulo).

Lema 4.4.2. *Não existe A-loop comutativo cujo centro tem índice p.*

Demonstração. *Vamos supor que Q seja um A-loop comutativo tal que $|Q/\mathcal{Z}(Q)| = p$, para algum primo p. Então, pelo Teorema de Lagrange e porque A-loops associam potências, temos que $Q/\mathcal{Z}(Q)$ é o grupo cíclico de ordem p. Se $x\mathcal{Z}(Q) \in Q/\mathcal{Z}(Q)\backslash\{1\}$, todo elemento de Q pode ser escrito da forma $x^i z$ com $i = 1, .., p-1$ e $z \in \mathcal{Z}(Q)$. Suponha $0 \leq i, j, k < p$ e $z_1, z_2, z_3 \in \mathcal{Z}(Q)$, então*

$$(x^i z_1 . x^j z_2) x^k z_3 = (x^i x^j) x^k . z_1 z_2 z_3 = x^i z_1 (x^j z_2 . x^k z_3).$$

Assim Q é um grupo abeliano cujo centro tem índice p, o que é uma contradição.

Como corolário desse lema temos que A-loops finitos, comutativos, não associativos e de ordem p^3, têm centro de ordem 1 ou p. Se p for ímpar, o centro de Q tem ordem p.

Definição 4.4.3. *Seja $n \geq 1$. definimos o "overflow indicator"pela função $(\cdot,\cdot)_n : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \{0,1\}$ dada por*

$$(x,y)_n = \begin{cases} 1, & x+y \geq n \\ 0, & x+y < n \end{cases} \tag{4.20}$$

Denotando por $\oplus$ a soma em $\mathbb{Z}_n$ e $+$ a em $\mathbb{Z}$ temos que para quaisquer $x, y \in \mathbb{Z}_n$, vale $x \oplus y = x + y - n(x,y)_n$ e assim

$$(x,y)_n = \frac{x+y-(x\oplus y)}{n}. \tag{4.21}$$

Note que da eqaução 4.21 segue

$$(x,y)_n + (x\oplus y, z)_n = (y,z)_n + (x, y\oplus z)_n \quad \text{para quaisquer} \quad x,y,z \in \mathbb{Z}_n. \tag{4.22}$$

A partir de agora, não vamos mais fazer diferença entre os sinais de soma de $\mathbb{Z}$ e $\mathbb{Z}_n$.

Definição 4.4.4. *Para $n \geq 1$ e $a, b \in \mathbb{Z}_n$, defina $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$, em $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ por*

$$xy = (x_1 + y_1 + (x_2+y_2)x_3y_3 + a(x_2,y_2)_n + b(x_3+y_3)_n, x_2+y_2, x_3+y_3). \tag{4.23}$$

onde $x = (x_1,x_2,x_3)$ e $y = (y_1,y_2,y_3) \in \mathcal{Q}_{a,b}(\mathbb{Z}_n)$.

Temos que $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ é um loop comutativo com elemnto neutro $(0,0,0)$ de ordem n^3, pois este pode ser visto como extensão de $\mathbb{Z}_n$ por $\mathbb{Z}_n \times \mathbb{Z}_n$ via o cociclo de loops

$$\theta((x_2,x_3),(y_2,y_3)) = (x_2+y_2)x_3y_3 + a(x_2,y_2)_n + b(x_3,y_3)_n.$$

Podemos escrever o cociclo θ como a soma de cociclos $\theta = \mu + \nu$, onde $\mu((x_2,x_3),(y_2,y_3)) = (x_2+y_2)x_3y_3$ e $\nu((x_2,x_3),(y_2,y_3)) = a(x_2,y_2)_n + b(x_3,y_3)_n$, e note que, da equação 4.22, temos que ν é um cociclo de grupos.

O objetivo é estudar exemplos de A-loops comutativos de ordem p^3, para p, um primo ímpar, dado por $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$. Temos em [JKV-02], a seguinte proposição, que explicita algumas identidades de $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$ e será útil na demonstração dos próximos resultados.

Proposição 4.4.5. *Sejam $n \geq 2$ e $a, b \in \mathbb{Z}_n$. Para $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$ e $z = (z_1, z_2, z_3) \in Q = \mathcal{Q}_{a,b}(\mathbb{Z}_n)$, valem:*

1. $x \backslash y = (y_1 - x_1 - (y_3 - x_3)x_3y_2 - a(x_2, x_2 - y_2)_n - b(x_3, y_3 - x_3)_n, y_2 - x_2, y_3 - x_3)$;
2. $(xy)\backslash x(yz) = (z_1 + y_3(x_3z_2 - x_2z_3), z_2, z_3)$;
3. *Q é um A-loop não associativo, comutativo de ordem n^3;*
4. $\mathcal{N}_\lambda(Q) = \mathcal{Z}(Q) = \mathbb{Z}_n \times 0 \times 0$ *e* $\mathcal{N}_\mu(Q) = \mathbb{Z}_n \times \mathbb{Z}_n \times 0$, *como subconjuntos de Q;*
5. $Q/\mathcal{Z}(Q) \simeq \mathcal{I}(Q)$ *e* $\mathcal{I}(Q) = \{L_{(v,v)} : u, v \in Q\}$;
6. *Para todo $m \geq 0$,*

$$x^m = \left(mx_1 + 2\binom{m+1}{3}x_2x_3^2 + at_2 + bt_3, mx_2, mx_3\right),$$

onde $t_i = \sum_{k=1}^{m-1}(x_i, kx_i)_n$.

As somas são consideradas vazias e o coeficiente binomial nulo se $m < 2$.

Lema 4.4.6. *Sejam p um número primo $a, b \in \mathbb{Z}_p$ e $Q = \mathcal{Q}_{a,b}(\mathbb{Z}_p)$. Então:*

1. *se $(a, b) = (0, 0)$ e $p \neq 3$, então Q tem expoente p;*
2. *$(a, b) \neq (0, 0)$ ou $p = 3$, então Q tem expoente p^2;*
3. *Se $a = 0$ então $\mathcal{N}_\mu(Q) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$;*
4. *Se $a \neq 0$ então $\mathcal{N}_\mu(Q) \simeq \mathbb{Z}_{p^2}$.*

Demonstração. *Como $|Q| = p^3$ todo elemento de Q têm ordem potência de p, então expoente de Q é p, p^2 ou p^3. Visto que Q não é associativo, então Q não pode ter expoente p^3, pois caso contrário, Q seria o grupo cíclico de ordem p^3.*

1. *Assuma $a = b = 0$. Pela proposição 4.4.5 temos que $(x_1, x_2, x_3)^p = (2\binom{p+1}{3} x_2 {x_3}^2, 0, 0)$. Mas o inteiro $2\binom{p+1}{3}$ é divisível por p se e somente se $p \neq 3$. Assim, Q tem expoente 2.*

2. *É suficinte mostrar que Q tem expoente p^2 se $(a, b) \neq (0, 0)$. Primeiro, assuma $a \neq 0$. Então $(0, 1, 0)^p = (a, 0, 0) \neq 0$ pois $\sum_{k=1}^{p-1}(1, k)_p = 1$. Da mesma forma se $b \neq 0$, então $(0, 0, 1)^p = (b, 0, 0) \neq 0$ e isso mostra que Q não pode ter expoente p.*

3. *Se $a = 0$, temos $(x_1, x_2, 0)^p = (0, 0, 0) \neq 0$, o que mostra que $\mathcal{N}_\mu(Q) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.*

4. *Se $a \neq 0$, temos que $(0, 1, 0)^p = (a, 0, 0) \neq 0$, ou seja $\mathcal{N}_\mu(Q)$ é um grupo abeliano em um loop de expoente p^2, com um elemento não nulo que não possui ordem p. Logo, $\mathcal{N}_\mu(Q) \simeq \mathbb{Z}_2$.*

No próximo lema, mostraremos que uma condição suficiente para $a_1, a_2 \in \mathbb{Z}_p$, onde p é ímpar, para que os loops $\mathcal{Q}_{a_1,0}$ e $\mathcal{Q}_{a_2,0}$ sejam isomorfos. Na verdade é suficiente que $a_1 a_2^{-1}$ seja um resíduo quadrático de p. Usando os símbolos de Legendre, basta que a_1 e a_2 sejam, simultaneamente resíduos quadráticos de p ou simultaneamente resíduos não quadráticos. Lembrando que $a \in \mathbb{Z}_p$ é um resíduo quadrático de p se a equação $x^2 \equiv a(mod p)$ tem solução.

Lema 4.4.7. *Sejam p um primo ímpar e $a_1, a_2 \in \mathbb{Z}_p^*$. Se a_1 e a_2 são ambos resíduos quadráticos ou ambos resíduos não quadáticos, então $\mathcal{Q}_{a_1,0} \simeq \mathcal{Q}_{a_2,0}$.*

Demonstração. *Sendo $a_1 a_2^{-1}$ resíduo quadrático de p, existe $u \in \mathbb{Z}_p^*$ tal que $a_2 = a_1 u^2$. Definindo $\varphi : \mathcal{Q}_{a_1,0} \longrightarrow \mathcal{Q}_{a_2,0}$ por $\varphi(x_1, x_2, x_3) = (u^2 x_1, x_2, u x_3)$. Desde que $u \in \mathbb{Z}_p^*$ temos que φ é uma bijeção. Vamos mostrar que φ é um isomorfismo. Temos*

que

$$\varphi((x_1,x_2,x_3)(y_1,y_2,y_3)) = \varphi(x_1+y_1+(x_2+y_2)x_3y_3+a_1(x_2,y_2)_p, x_2+y_2, x_3+y_3) =$$

$$= (u^2(x_1+y_1)+u^2(x_2+y_2)x_3y_3+a_1u^2(x_2,y_2)_p, x_2+y_2, u(x_3+y_3)).$$

Por outro lado,

$$\varphi(x_1,x_2,x_3)\varphi(y_1,y_2,y_3) = (u^2x_1,x_2,ux_3)(u^2y_1,y_2,uy_3) =$$

$$= (u^2(x_1+y_1)+u^2(x_2+y_2)x_3y_3+a_2(x_2,y_2)_p, x_2+y_2, u(x_3+y_3)).$$

Donde segue que φ é um homomorfismo.

Apresentamos aqui uma forma de construir A-loops comutativos de ordem p^3. Jedlicka, Kinyon, Vojtechovsky cojecturam em [JKV-02], uma "versão dual"para o lema 4.4.7 que diz que, se $p>3$, $a_1 \in \mathbb{Z}_p^*$ for resíduo quadrático de p e $a_2 \in \mathbb{Z}_p^*$ não o for, então $\mathcal{Q}_{a_1,0}$ não é isomorfo a $\mathcal{Q}_{a_2,0}$.

Capítulo 5

Apêndice: A-Loops Comutativos Nilpotentes de Grau 2

Grichkov e Vojtechovsky estão estudando A-loops comutativos nilpotentes de grau 2. Tais loops têm a propriedade de qualquer associador se um elemento central. Em outras palavras o A-loop comutativo L é tal que

$$A(L) = \{(x, y, z) : x, y, z \in L\} \subset \mathcal{Z}(L),$$

onde (x, y, z) é o único elemento de L que satisfaz a equação $(xy)z = [x(yz)](x, y, z)$. Um dos principais objetivos do estudo deles é demonstrar o seguinte teorema:

Teorema 5.0.8. *Sejam $X = \{x_1, x_2, ...\}$ um conjunto enumerável, $Y = \{(x_i, x_j, x_k) : x_i, x_j, x_k \in X, i < k\}$ e A e B grupos abelianos livres gerados por X e Y, respectivamente. Então $F = A \times B$ admite uma estrutura de A-loop comutativo nilpotente de grau 2, tal que*

$$\mathcal{N}_\mu(F) = \mathcal{N}_\rho(L) = \mathcal{N}_\lambda(L) = B.$$

Mais ainda $(x_i, x_j, x_k) = (x_i, x_j, x_k) \in Y$ se $i < k$.

Nesse apêndice, estudaremos um caso particular, onde X possui dois elementos. Para simplificar a notação, vamos escrever $xy.z$ para indicar $(xy)z$. Seja L um

A-loop comutativo. Em [BP] vemos que $L = G \ltimes_\theta Z$, onde $Z \subset \mathcal{Z}(L)$, $L/Z = G$ é um grupo abeliano e $\theta : G \times G \to Z$ é um cociclo de loops. Sejam $g_1, g_2 \in G$ e $k_1, k_2 \in Z$. Notemos que

$$(g_1, k_1)(g_2, k_2) = (g_1 g_2, k_1 k_2 \theta(g_1, g_2)). \tag{5.1}$$

Vamos denotar por g o elemento $(g, 1) \in L$. De $g_1 g_2 . g_3 = (g_1 . g_2 g_3)(g_1, g_2, g_3)$ tiramos que

$$(g_1, g_2, g_3) = (1, \theta(g_1, g_2)\theta(g_1 g_2, g_3)\theta(g_2, g_3)^{-1}\theta(g_1, g_2 g_3)^{-1}),$$

que escreveremos apenas como

$$(g_1, g_2, g_3) = \theta(g_1, g_2)\theta(g_1 g_2, g_3)\theta(g_2, g_3)^{-1}\theta(g_1, g_2 g_3)^{-1}. \tag{5.2}$$

Para $g_1, g_2, g_3, g_4 \in G$ vale que

$$\begin{aligned} g_1 g_2 . g_3 g_4 &= g_1(g_2 . g_3 g_4)(g_1, g_2, g_3 g_4) \\ &= g_1(g_3 . g_2 g_4)(g_3, g_4, g_2)(g_1, g_2, g_3 g_4) \\ &= (g_2 g_4 . g_3) g_1 (g_3, g_4, g_2)(g_1, g_2, g_3 g_4) \\ &= (g_1 g_3 . g_2 g_4)(g_2 g_4, g_3, g_1)(g_3, g_4, g_2)(g_1, g_2, g_3 g_4), \end{aligned}$$

e assim, por 5.1, temos

$$\theta(g_1 g_2, g_3 g_4) = \theta(g_1 g_3, g_2 g_4)(g_4 g_2, g_3, g_1)(g_3, g_4, g_2)(g_1, g_2, g_3 g_4). \tag{5.3}$$

Da mesma forma obtemos

$$\theta(g_1 g_2, g_3 g_4) = \theta(g_1 g_3, g_2 g_4)(g_1 g_3, g_2, g_4)(g_2, g_1, g_3)(g_4, g_3, g_1 g_2) \quad \text{e} \tag{5.4}$$

$$\theta(g_1 g_2, g_3 g_4) = \theta(g_1 g_3, g_2 g_4)(g_1 g_3, g_4, g_2)(g_4, g_3, g_1)(g_2, g_1, g_3 g_4). \tag{5.5}$$

Note que, para quaisquer elementos a, b, x, y no A-loop comutativo L, $(ab.x)y = (ab.xy)(ab, x, y)$ e, visto que, $R_{(x,y)}(a)R_{(x,y)}(b) = R_{(x,y)}(ab)$, temos que $(ab, x, y) = (a, x, y)(b, x, y)$. Ainda

$$ax.b = (a.xb)(a, x, b) = (bx.a)(a, x, b) = (b.xa)(b, x, a)(a, x, b) = (ax.b)(b, x, a)(a, x, b),$$

que implica que $(a,x,b) = (b,x,a)^{-1}$, e também

$$ax.a = (a.xa)(a,x,a) = (a.xa)(a,x,a).$$

Resumindo, para quaisquer $a,b,x,y \in L$, temos

$$(ab,x,y) = (a,x,y)(b,x,y), \quad (a,x,b) = (b,x,a)^{-1} \quad \text{e} \quad (a,x,a) = 1. \tag{5.6}$$

Como dito antes, vamos supor

$$X = \{x_1, x_2\} \quad \text{e} \quad Y = \{z_1 = (x_1,x_1,x_2), z_2 = (x_1,x_2,x_2)\}.$$

Sejam $g_1 = x_1^i, g_2 = x_2^s, g_3 = x_1^j, g_4 = x_1^t \in L$. Como L associa potências, segue que $\theta(x_k^l, x_k^m) = 1$ com $k = 1,2$ e $l,m \in \mathbb{Z}$. Das equações 5.3, 5.4 e 5.5, temos que

$$\begin{aligned}(x_2^{s+t}, x_1^j, x_1^i)(x_1^j, x_2^t, x_2^s)(x_1^i, x_2^s, x_1^j x_2^t) &= (x_1^{i+j}, x_2^s, x_2^t)(x_2^t, x_1^j, x_1^i x_2^s)(x_2^s, x_1^i, x_1^j) \\ &= (x_1^{i+j}, x_2^t, x_2^s)(x_2^s, x_1^i, x_1^j x_2^t)(x_2^t, x_1^j, x_1^i)\end{aligned}$$

Agora, por 5.6, temos

$$(x_1, x_2^s, x_2)^{t(i+j)} = (x_1, x_2^t, x_2)^{s(i+j)},$$

ou seja

$$(x_1, x_2^s, x_2)^t = (x_1, x_2^t, x_2)^s. \tag{5.7}$$

Fazendo $t = 1$ temos

$$(x_1, x_2^s, x_2) = (x_1, x_2, x_2)^s. \tag{5.8}$$

Sejam $g_1, g_2, g_3, g_4, g_5, g_6 \in G$. Da equação 5.2 segue que

$$(g_1g_2, g_3g_4, g_5g_6) = \theta(g_1g_2, g_3g_4)\theta(g_3g_4, g_5g_6)^{-1}\theta(g_1g_3.g_2g_4, g_5g_6)\theta(g_1g_2, g_3g_5.g_4g_6)^{-1}$$

e assim, por 5.3 e 5.6 temos

$$(g_1g_2, g_3g_4, g_5g_6) = \theta(g_1g_3, g_2g_4)(g_2g_4, g_3, g_1)(g_3, g_4, g_2)(g_1, g_2, g_3)(g_1, g_2, g_4)$$

$$\theta(g_3g_5, g_4g_6)^{-1}(g_4g_6, g_5, g_3)^{-1}(g_5, g_6, g_4)^{-1}(g_3, g_4, g_5)^{-1}(g_3, g_4, g_6)^{-1}$$

$$\theta(g_1g_3g_5, g_2g_4g_6)(g_2g_4g_6, g_5, g_1g_3)(g_5, g_6, g_2g_4)(g_1g_3, g_2g_4, g_5)(g_1g_3, g_2g_4, g_6)$$

$$\theta(g_1g_3g_5, g_2g_4g_6)^{-1}(g_2g_4g_6, g_3g_5, g_1)^{-1}(g_3g_5, g_4g_6, g_2)^{-1}(g_1, g_2, g_3g_5)^{-1}(g_1, g_2, g_4g_6)^{-1}.$$

Note que para $(x_1^m, w_1), (x_2^l, w_2) \in L = G \ltimes_\theta Z$,

$$(x_1^m, w_1)(x_2^s, w_2) = (x_1^m x_2^l, w_1 w_2 \theta(x_1^m, x_2^l)).$$

Nessa última igualdade, fazendo $w_1 = w_2 = 1$, temos $\theta(x_1^m, x_2^l) = 1$.

Agora, substituindo $g_1 = x_1^i, g_2 = x_2^s, g_3 = x_1^j, g_4 = x_1^t, g_5 = x_1^k, g_6 = x_2^r$ temos

$$(g_1g_2, g_3g_4, g_5g_6) = (x_1^i x_2^s, x_1^j x_2^t, x_1^k x_2^r) = (x_2^{s+t}, x_1^j, x_1^i)(x_1^j, x_2^t, x_2^2)(x_1^i, x_2^s, x_2^t)(x_2^{t+r}, x_1^k, x_1^j)^{-1}$$

$$(x_1^k, x_2^r, x_2^t)^{-1}(x_1^j, x_2^t, x_2^r)^{-1}(x_2^{s+r+t}, x_1^k, x_1^{i+j})(x_1^k, x_2^r, x_2^{s+t})(x_1^{i+j}, x_2^{s+t}, x_2^r)(x_2^{s+t+r}, x_1^{j+k}, x_1^i)^{-1}$$
$$(x_1^{j+k}, x_2^{t+r}, x_2^s)^{-1}(x_1^i, x_2^s, x_2^{t+r})^{-1} = z_1^{j(ir-ks)} z_2^{t(ir-ks)}.$$

Então, o que mostramos foi

$$(x_1^i x_2^s, x_1^j x_2^t, x_1^k x_2^r) = z_1^{j(ir-ks)} z_2^{t(ir-ks)}. \tag{5.9}$$

Da equação 5.3, temos

$$\theta(x_1^i x_2^s, x_1^j x_2^t) = \theta(x_1^{i+j}, x_2^{s+t})(x_2^{s+t}, x_1^j, x_1^i)(x_1^j, x_2^t, x_2^s)(x_1^i, x_2^s, x_1^j)(x_1^i, x_2^s, x_2^t),$$

ou seja,

$$\theta(x_1^i x_2^s, x_1^j x_2^t) = z_1^{-ij(s+t)} z_2^{ts(i+j)}. \tag{5.10}$$

Com tudo isso mostramos um caso particular do teorema 5.0.8. Para $X\{x_1, x_2\}$ e $Y = \{z_1, z_2\}$ temos que $\mathbf{F} = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ admite a seguinte estrutura de A-loop comutativo livre, $\mathbf{F} = \mathbb{Z} \times \mathbb{Z} \ltimes_\theta \mathbb{Z} \times \mathbb{Z}$ onde

$$\theta((a_1, a_2), (b_1, b_2)) = (-a_1b_1(a_2 + b_2), a_2b_2(a_1 + b_1)).$$

Sejam $\alpha = (a, x), \beta = (b, y)$ e $\gamma = (c, z)$ com $a = (a_1, a_2), b = (b_1, b_2)$ e $c = (c_1, c_2)$. Temos que

$$(a, x)[(b, y)(c, z)] = [(a, x)(b, y)](c, z) \tag{5.11}$$

se e somente se

$$a_1 b_1 c_2 = a_2 b_1 c_1 \quad \text{e} \quad a_2 b_2 c_1 = a_1 b_2 c_2. \tag{5.12}$$

Donde obtemos $\mathcal{N}_\mu(L) = \mathcal{N}_\lambda(L) = \mathcal{N}_\rho(L) = 0 \times 0 \times \mathbb{Z} \times \mathbb{Z}$ e assim $\mathcal{Z}(L) = \mathcal{N}(L) = 0 \times 0 \times \mathbb{Z} \times \mathbb{Z}$.

Além disso, desde que $(\alpha\beta)\gamma = (abc, \theta(ab, c)\theta(a, b)xyz)$, $\alpha(\beta\gamma) = (abc, \theta(a, bc)\theta(b, c)xyz)$ e (α, β, γ) é o único elemento de L tal que $(\alpha\beta)\gamma = [\alpha(\beta\gamma)](\alpha, \beta, \gamma)$ temos

$$(\alpha, \beta, \gamma) = (0, \theta(ab, c)\theta(a, b)\theta(a, bc)^{-1}\theta(b, c)^{-1}), \tag{5.13}$$

e, portanto, o associador $(\mathbf{F}, \mathbf{F}, \mathbf{F})$ está contido em $0 \times 0 \times \mathbb{Z} \times \mathbb{Z}$. Segue da definição do cociclo θ que $0 \times 0 \times \mathbb{Z} \times \mathbb{Z} \subset (\mathbf{F}, \mathbf{F}, \mathbf{F})$. Logo $(\mathbf{F}, \mathbf{F}, \mathbf{F}) = 0 \times 0 \times \mathbb{Z} \times \mathbb{Z}$.

Referências Bibliográficas

[GJM] GOODAIRE, E.G., JESPERS, E., MILIES, C.P., *Alternative loop Rings*, Mathematics Studies, 184, North Holland.

[Br] BRUCK, R. H., *Contributions to the Theory of Loops*, Transactions of American Mathematical Society, Vol. 60, No. 02, 1946, pp.245-354.

[BP] BRUCK, R. H., PAIGE, L. J., *Loops Whose Inner Mappings Are Automorphisms*, Annals of Mathematics, vol. 63, No. 2, 1956, pp.308-323.

[Gl-01] GLAUBERMAN, G., *On Loops of Odd Oreder*, Journal of Algebra, vol. 1, 1964 pp.374-396.

[Gl-02] GLAUBERMAN, G., *On Loops of Odd Oreder II*, Journal of Algebra, vol. 8, 1968 pp.393-414.

[JKV-01] JEDLICKA, P., KINYON, M., VOJTECHOVSKY, P. *The Structure of Commutative Automorphic Loops* to appear in Transactions of American Mathematical Society.

[JKV-02] JEDLICKA, P., KINYON, M., VOJTECHOVSKY, P. *Constructions of Commutative Automorphic Loops* to appear in Communications in Algebra.