Trabalho de Conclusão de Curso - Bacharelado em Matemática

Loops e o Teorema de Moufang

Lucas Guimarães Miranda

Universidade Federal do ABC

Título: Loops e o Teorema de Moufang

Autor: Lucas Guimarães Miranda
Orientador: Profa. Dra. Maria de Lourdes Merlini Giuliani

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção do título de Bacharel em Matemática pela Universidade Federal do ABC.

Banca Examinadora:

Prof. Dr. Alcindo Teles Galvão
Universidade Federal de Alagoas

Profa. Dra. Dylene Agda Souza de Barros
Universidade Federal de Uberlândia

Santo André, Novembro de 2020.

Sumário

1 Introdução **6**

2 Quasigrupos e loops **7**

2.1 Quasigrupos 7
2.2 Loops 10
2.3 Subloops 11
2.4 Classes laterais e loops tipo-Lagrange 13
2.5 Núcleos e Centro de um loop 16
2.6 Propriedade de inversão 21
2.7 Grupo das multiplicações e grupo de aplicações internas 23
2.8 Homomorfismos de loops 26
2.9 Normalidade 27

3 Loops de Moufang **33**

3.1 Definição e propriedades 33
3.2 Ferramentas para demonstrar o teorema de Moufang 36
3.3 O teorema de Moufang 40
3.4 Uma outra demonstração 44

Agradecimento

Agradeço a Deus pelos dons que me foram concedidos para realização desse trabalho.

Sou grato a minha orientadora Profa. Maria de Lourdes Merlini Giuliani por aceitar me orientar e auxiliar não só nesse trabalho, mas também na minha formação.

A todos os docentes do Bacharelado em Matemática da UFABC pela grandiosa qualidade de seus trabalhos.

E aos meus pais João e Zuleide Miranda que sempre foram de heroico suporte para mim.

Resumo

O objetivo deste trabalho é investigar o teorema de Moufang. Este famoso teorema que representa um ponto crucial no estudo dos loops de Moufang. Faremos um estudo comparativo das duas versões da sua demonstração.

Palavras Chaves: Quasigrupos, loops, loops de Moufang, teorema de Moufang.

Abstract

The goal of this work is to investigate Moufang's theorem. This famous theorem represents a crucial point in the study of Moufang loops. We will do a comparative study of the two versions of its proof.

Keywords: Quasigroups, loops, Moufang loops, Moufang's theorem.

1 Introdução

Um loop é um conjunto L, não vazio, equipado com uma operação de multiplicação denotada por $\cdot : L \times L \to L$ tal que $(x, y) \to x \cdot y$, satisfazendo as seguintes propriedades:

(i) dados $a, b \in L$, as equações $a \cdot x = b$ e $y \cdot a = b$ têm soluções únicas para quaisquer $x, y \in L$;

(ii) existe um elemento identidade $1 \in L$ satisfazendo $1 \cdot x = x \cdot 1 = x$; para todo $x \in L$

Deixaremos de indicar a operação do loop, escrevendo simplesmente L para denotar o loop $(L, \cdot)$. Também, escreveremos xy no lugar de $x \cdot y$.

L é um *loop de Moufang* se L satisfaz qualquer uma das três equivalentes *identidades de Moufang*:

$$((xy)x)z = x(y(xz)); \quad ((xy)z)y = x(y(zy)); \quad (xy)(zx) = (x(yz))x.$$

Estes loops foram introduzidos por *Ruth Moufang* em 1934, [5] e são discutidos em detalhes nos textos de *Bruck* [1] e *Pflugfelder* [6]. Qualquer elemento x de um loop de Moufang tem inverso bilateral x^{-1}, isto é, um elemento que satisfaz $xx^{-1} = x^{-1}x = 1$. Para $x \in L$ definimos *translações à direita e à esquerda* por $yR_x = yx$ e $yL_x = xy$, respectivamente. O grupo das multiplicações de L é o grupo de permutações $Mult(L) = \langle R_x, L_x; x \in L \rangle$, gerado por translações à direita e à esquerda. Definimos o *grupo de aplicações internas*, $I(L)$, como sendo o subgrupo de $Mult(L)$ que fixa 1. Se L é um grupo, então $I(L)$ é o grupo dos automorfismos internos.

O teorema de Moufang estabelece que em um loop de Moufang L se três elementos $x, y, z \in L$ se associam, isto é, $x(yz) = (xy)z$ então eles geram um subgrupo de L. Como corolário deste teorema (levando em conta que loops de Moufang satisfazem as identidade alternativas às quais apresentarei no texto) obtemos que quaisquer dois elementos de um loop de Moufang geram um subgrupo (ou um subloop associativo). A primeira prova deste teorema data de 1956 e sua prova, bastante engenhosa, é devida à Bruck [5]. Recentemente Aleš Drápal [3] forneceu uma prova mais simplificada e elegante. O estudo deste teorema é um ponto alto dentro dos conceitos iniciais de loops e é o objetivo principal deste trabalho.

2 Quasigrupos e loops

2.1 Quasigrupos

Um quasigrupo é um conjunto Q não vazio munido de uma operação binária fechada onde para todo $a, b \in Q$ as equações $ax = b$ e $ya = b$ têm soluções únicas em Q. Essa definição algébrica é bastante útil ao trabalharmos com quasigrupo.

Para efeito de compreensão deixo aqui algumas abreviações e notações que usarei quando conveniente daqui para frente.

Primeiramente, quando estiver aplicando uma função em algum argumento, escreverei o argumento à esquerda e depois a função que estou aplicando, por exemplo escreverei $(x)f$, além disso, escreverei $xy \cdot w$ para dizer $(xy)w$. Assim também denotaremos a composição de funções simplesmente pela justaposição delas, isto é, tomando funções com domínios e contradomínios apropriados f e g, denotarei sua composta por gf.

Definição 2.1 (Funções de translação) Seja $(Q, \cdot)$, onde Q é um quasigrupo e $a \in Q$, então a translação à esquerda por a é definida por:

$$\begin{aligned} L_a \colon Q &\to Q \\ x &\mapsto ax \end{aligned}$$

e a translação à direita por a é definida por:

$$\begin{aligned} R_a \colon Q &\to Q \\ x &\mapsto xa \end{aligned}$$

Podemos usar as translações para definirmos as propriedades de comutatividade e de associatividade da seguinte forma:

Definição 2.2 No contexto acima, Q é dito comutativo se, e somente se, temos a identidade $L_a = R_a \ \forall a \in Q$, isto é, $ab = ba \ \forall a, b \in Q$.

Definição 2.3 No contexto acima, Q é dito associativo se, e somente se, temos que vale $R_{a \cdot b} = R_a R_b \ \forall a, b \in Q$,isto é, $c \cdot ab = ca \cdot b \ \forall a, b, c \in Q$.

Definição 2.4 (Quasigrupo) No contexto acima, Q é dito um quasigrupo se, e somente se, L_a e R_a são bijeções para todo $a \in Q$.

Teorema 2.5 *Seja $(Q,\cdot)$, são equivalentes:*

(i) *L_a e R_a são bijetoras para todo $a \in Q$ (isto é, Q é um quasigrupo).*

(ii) *$\forall a,b \in Q$, existe um único par $(x,y) \in Q \times Q$, tal que $xa = b$ e $ay = b$;*

Demonstração: ((ii) $\Rightarrow$ (i)) Sejam a e b elementos arbitrários de Q por hipótese existem $x,y \in Q$, tais que, $xa = b$ e $ay = b$, isto é, $xa = xR_a = b$ e $ay = yL_a = b$, concluindo então que L_a e R_a são sobrejetoras para todo a em Q.

Agora suponha que $x_1R_a = x_2R_a = c \in Q$, logo obtemos $x_1a = x_2a = c$, e pela unicidade da solução para w em Q na equação $wa = c$ temos que $x_1 = x_2$, concluindo que R_a é injetora para todo a em Q. Analogamente concluímos que L_a é injetora para todo a em Q.

((i) $\Rightarrow$ (ii)) Sejam a e b elementos arbitrários de Q, a existência de um elemento $(x,y) \in Q \times Q$ tal que $xR_a = xa = b$ e $yL_a = ay = b$ é garantida pela sobrejeção das funções R_a e L_a.

Agora suponha que existam elementos $(x_1,y_1),(x_2,y_2) \in Q \times Q$, tais que, $x_1a = b$, $ay_1 = b$, $x_2a =$ e $ay_2 = b$, temos então que $x_1a = x_1R_a = b = x_2a = x_2R_a$ e pela bijeção de R_a, segue que $x_1 = x_2$, similarmente provamos que $y_1 = y_2$, concluimos então que $(x_1,y_1) = (x_2,y_2)$ daí a unicidade. □

Exemplo 2.6 O conjunto $Q = \{1,2,3,4,5\}$ é um quasigrupo $(Q,\cdot)$, onde a multiplicação de seus elementos é dada pela tabela:

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

Corolário 2.7 ***(Leis de cancelamento)*** *Seja Q um quasigrupo. Valem que:*

(i) *$\forall a,x,y \in Q$, $ax = ay \Rightarrow x = y$*

(ii) *$\forall a,x,y \in Q$, $xa = ya \Rightarrow x = y$*

Demonstração: Basta seguir a parte $((i) \Rightarrow (ii))$ do **Teorema 2.5**, onde mostramos a injetividade das translações. □

Algo importante a ser notado no **corolário 2.7**, é o fato de que mesmo sem uma noção de inversos temos que em quasigrupos valem as leis de cancelamento, que seguem diretamente do fato das translações serem bijetoras.

Analisaremos agora a relação entre quasigrupos e grupos, isto é, o quanto um quasigrupo está próximo de ser grupo, para isso definirei a ideia de elemento identidade através das transalações.

Definição 2.8 Seja Q um quasigrupo e $e \in Q$. Então e é um elemento identidade à esquerda (analogamente, à direita) para Q se, e somente se, L_e (analogamente, R_e) é a função identidade de Q, isto é, $ex = x \ \forall x \in Q$ (analogamente, $xe = x \ \forall x \in Q$).

Definição 2.9 Um elemento e em um quasigrupo Q é dito um elemento identidade se, e somente se, e é um elemento identidade à esquerda e também um elemento identidade à direita.

Definição 2.10 Seja Q um quasigrupo com elemento identidade, denote por e o elemento identidade de Q e considere x um elemento de Q. Denotamos por x^λ e x^ρ os elementos unicamente determinados por:

$$x^\lambda \cdot x = e = x \cdot x^\rho.$$

Observação: Nos casos que $x^\lambda = x^\rho$ escreverei $x^\lambda = x^\rho = x^{-1}$, neste caso pela unicidade de $x^\lambda = x^\rho$, segue que x^{-1} é único, e chamarei x^{-1} por inverso bilateral de x, ou ainda, simplesmente por inverso de x.

Teorema 2.11 *Seja Q um quasigrupo associativo, então Q necessariamente têm um único elemento identidade.*

Demonstração: Existência: Seja $a, b \in Q$ e $e, y \in Q$ tais que $ae = a$ e $ya = b$ (tais elementos têm exitência garantida por Q ser quasigrupo). Temos:

$$bR_e = be = ya \cdot e = y \cdot ae = ya = b$$

$\therefore R_e = Id_Q$ (isto é,, e é elemento identidade à direita), considere agora:

$$bb = be \cdot b = b \cdot eb$$

Pelo cancelamento à esquerda $b = eb$.

$\therefore L_e = Id_Q$ (isto é,, e é elemento identidade à esquerda), logo e é elemento identidade.

Unicidade: Suponha que e e e' são dois elementos identidades de um quasigrupo então temos:

$$eR_{e'} = e;$$
$$e'L_e = e';$$
$$e' = e'L_e = ee' = eR_{e'} = e.$$

Concluimos que o elemento identidade é único. □

Observação: Note como que para provar a unicidade do elemento identidade no **Teorema 2.11** não foi usado a hipótese do quasigrupo ser associativo, isto é, essa propriedade de unicidade do elemento identidade vale para qualquer quasigrupo com elemento identidade (o qual chamaremos de loop).

Teorema 2.12 *Seja Q um quasigrupo associativo com elemento identidade e, então para qualquer x em Q temos que $x^\lambda = x^\rho$.*

Demonstração: Seja $z = x^\rho x$, então $zz = x^\rho(xx^\rho)x = z$. Agora existe $w \in Q$ de forma que $zw = e$. Como $zz = z$, temos $z(zw) = zw$, e pelo cancelamento, $x^\rho x = z = e$, pela unicidade da definição de $x^\lambda = x^\rho = x^{-1}$ □

Observação: Este teorema nos garante que em um quasigrupo associativo todo elemento têm inverso bilateral.

2.2 Loops

Nesta seção introduzimos o conceito de loops que é o objeto deste trabalho, segue a definição:

Definição 2.13 Um quasigrupo Q é dito *loop* se, e somente se, Q possui um elemento identidade.

Exemplo 2.14 O conjunto $L = \{1, 2, 3, 4, 5\}$, é um loop $(L, \cdot)$ quando a multiplicação de seus elementos é dada pela seguinte tabela:

$\cdot$	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

Claramente $1 \in L$ é elemento identidade, além disso, tal quasigrupo não é associativo pois $3 \cdot (3 \cdot 4) = 5 \neq 4 = (3 \cdot 3) \cdot 4$. Logo L é um quasigrupo com elemento identidade, isto é, loop, mas não é associativo.

Corolário 2.15 *Seja L um loop, então o elemento identidade de L é único.*

Demonstração: A demonstração deste fato é garantida pelo **Teorema 2.11**. □

Podemos definir outras operações me um loop, que correspondem de certa forma à divisões.

Seja L um loop definimos as operaçõe / e \ da seguinte forma:

$$x\backslash y = yL_x^{-1}, \text{ i.e } x\backslash y = z \Leftrightarrow xz = y;$$
$$x/y = xR_y^{-1}, \text{ i.e } x/y = z \Leftrightarrow zy = x.$$

E isso nos dá a possibilidade de estabelecer uma definição equivalente de loops.

Definição 2.16 Um loop é um conjunto não vazio L munido de três operações binárias $(.)$, $(/)$ e $(\backslash)$ satisfazendo a:

i) $a \cdot (a\backslash b) = b, \quad (b/a) \cdot a = b;$

ii) $a\backslash(a \cdot b) = b, \quad (b \cdot a)/a = b;$

iii) $a\backslash a = b/b.$

2.3 Subloops

Definição 2.17 Um subconjunto não vazio H de um conjunto L é chamado de subloop de um loop L se, e somente se, $(H, \cdot_H)$ é um loop, onde $\cdot_H$ é a restrição de $\cdot$ ao conjunto $H \times H$.

Observação: Analogamente se define o conceito de subquasigrupo.

Daqui para frente omitirei a restrição da operação para economizar notação, isso é escreverei sempre $\cdot$ ao invés de $\cdot_H$.

Teorema 2.18 *Seja L um loop. Então $\emptyset \neq H \subseteq L$ é um subloop de L se, e somente se, $(H, \cdot)$, $(H, /)$ e $(H, \backslash)$ são fechados para suas respectivas operações.*

Omitiremos a sua prova e deixamos aqui a referência.[6]

Usaremos a notação $H \leq L$ para indicar que H é subloop de L.

Esse teorema se torna bem familiar na presença de associatividade, ou seja em um grupo G dizer que $(H, /)$ ou $(H, \backslash)$ são fechados é o mesmo que dizer que xy^{-1} ou $x^{-1}y$ pertencem à H para quaisquer $x, y \in H$. Na verdade é resultado conhecido na teoria de grupos que basta que $xy^{-1} \in H$ para todo $x, y \in H$, para concluir que $H \leq G$, portanto na presença de associatividade as hipóteses do teorema podem ser enfraquecidas, isto é, $H \leq L$ se, e somente se, $(H, \backslash)$ ou $(H, /)$ são fechados.

Teorema 2.19 *Seja L um loop, e $\emptyset \neq S \subseteq L$, e seja T qualquer conjunto de subloops de L com $S \subseteq H$, $\forall H \in T$. Então $\bigcap_{H\in T} H$ é um subloop de L valendo também $\emptyset \neq S \subseteq \bigcap_{H\in T} H$.*

Demonstração: Tome $D = \bigcap_{H\in T} H$ é evidente que $S \subseteq D \subseteq L$, com $S \neq \emptyset$, logo $\emptyset \subsetneq D \subseteq L$.

Sejam $a, b \in H$, $\forall H \in T$, como $(H, \cdot)$ é subloop de $(Q, \cdot)$ $\forall H \in T$, logo temos $(H, \cdot)$, $(H, \backslash)$ e $(H, /)$ são fechados para suas operações $\forall H \in T$.

Portanto os elemento $a \cdot b$, $a\backslash b$, $a/b \in H$ $\forall H \in T$.

E temos por definição de D que $a \cdot b$, $a\backslash b$, $a/b \in D$.

Concluindo que $(D, \cdot)$, $(D, \backslash)$ e $(D, /)$ são fechados para suas operações, então pelo **Teorema 2.18** $(D, \cdot)$ é subloop de $(L, \cdot)$.

□

Agora seja L um loop, considere $\emptyset \neq S \subseteq Q$ e também T o conjunto de todos subloops de Q tais que têm S como subconjunto. Claramente $T \neq \emptyset$ já que $L \in T$. Portanto, invocamos o teorema acima e deduzimos que $\bigcap_{H\in T} H$ é um subloop de L com $S \subseteq \bigcap_{H\in T} H$. É de costume denotar o a interseção $\bigcap_{H\in T} H$ por $\langle S \rangle$ e formular a seguinte definição.

Definição 2.20 Seja L um loop, e $\emptyset \neq S \subseteq L$ e seja $T = \{H \leq L \mid S \subseteq H\}$. Então o subloop $(\langle S \rangle = \bigcap_{H\in T} H, \cdot)$ é chamado de subloop gerado por S.

É fato que $\langle S \rangle$ é o menor subloop do loop Q que contêm S como subconjunto. Quando acontece que $\langle S \rangle = L$ dizemos que S gera L ou que S é um conjunto gerador para L.

Para loops segue o resultado que qualquer interseção de subloops é novamente um subloop, já que todos subloops de um loop necessáriamente compartilham o elemento identidade entre si, logo as interseções nunca são vazias, e isto garante que são subloops (no contexto acima, tomando $S = \{e\}$, nos garante que a interseção de famílias de subloops é um subloop).

Algumas classificações de quasigrupos e loops

Definição 2.21 Um loop L é dito associativo por potências se, e somente se, $\langle a \rangle$ é associativo $\forall a \in L$.

Definição 2.22 Um loop L é dito diassociativo se, e somente se, $\langle a, b \rangle$ é associativo $\forall a, b \in L$.

Teorema 2.23 *Seja L quasigrupo diassociativo, então L associativo por potências.*

Demonstração: Seja L diassociativo e $a \in L$, então $\langle a \rangle = \langle a, a \rangle$ é associativo pois L é diassociativo.

Concluindo que L é associativo por potências. □

2.4 Classes laterais e loops tipo-Lagrange

Algumas das propriedades conhecidas sobre subloops são meramente uma generalização de certos resultados estabelecidos na teoria de grupos, darei aqui uma dessas generalizações. Sobre casses laterais, decomposição em classes laterais, e resutados tipo-Lagrange (isto é, resultados semelhantes ao teorema de Lagrange na teoria de grupos). Outra generalização importante seria subloops normais, que serão tratadas mais a frente.

Definição 2.24 Seja L um loop e $H \leq L$. Se $a \in L$, então aH e Ha são definidos por:

$$aH = \{ah \mid h \in H\} \text{ e } Ha = \{ha \mid h \in H\}.$$

Claramente aH e Ha são subconjuntos de L. Qualquer subconjunto de L construido desta maneira é chamando de classe lateral módulo H. Conjuntos da forma aH são chamados de classes laterais à esquerda módulo H, e analogamente, conjuntos da forma Ha são chamados classes laterais à direita módulo H.

Definição 2.25 Seja L um loop e $H \leq L$. Então L têm uma decomposição em classes laterais à esquerda modulo H (analogamente, à direita) se, e somente se, o conjunto P de todas as classes laterais à esquerda (analogamente, à direita) de H é uma partição de L.

Diferente do que ocorre na teoria de grupos, as classes laterais de um subloop H de L podem não formar um partição do loop.

Exemplo 2.26 Seja $L = \{1, 2, 3, 4, 5\}$, então $(L, \cdot)$ é um loop onde a multiplicação de seus elementos é dada pela seguinte tabela:

$\cdot$	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

Temos que $H = \{1, 2\}$ é subloop de L, e suas classes laterais à esquerda são $1H = 2H = \{1, 2\}$, $3H = \{3, 5\}$, $4H = \{3, 4\}$ e $5H = \{4, 5\}$. Por inspeção é fácil ver que o conjunto P de todas as classes laterais à esquerda módulo H não forma uma partição de L (note que $3H \cap 4H \neq \emptyset$ mas $3H \neq 4H$).

Exemplo 2.27 Seja $L = \{1, 2, 3, 4, 5, 6, 7, 8\}$, então $(L, \cdot)$ é um loop onde a multiplicação de seus elementos é dada pela seguinte tabela:

·	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	8	7	5	6
4	4	3	2	1	7	8	6	5
5	5	6	7	8	1	2	3	4
6	6	5	8	7	2	1	4	3
7	7	8	5	6	4	3	1	2
8	8	7	6	5	3	4	2	1

Seja $H = \{1,2\}$, claramente $H \leq L$. Note que $1H = 2H = \{1,2\}$, $3H = 4Hh\{3,4\}$, $5H = 6H = \{5,6\}$ e $7H = 8H = \{7,8\}$. O conjunto de todas as classes laterais à esquerda módulo H forma uma partição do conjunto L. Logo L se decompõe em classes laterais módulo H.

O seguinte resultado fornece uma condição para que as classes laterais de um subloop particionem o loop.

Teorema 2.28 *Seja L um loop e $H \leq L$. Então L têm uma decomposição em classes laterais à esquerda (à direita) módulo H se , e somente se, $ah \cdot H = aH$ ($H \cdot ha = H \cdot a$) $\forall a \in L \; \forall h \in H$.*

Demonstração: Seja e o elemento identidade de L e P o conjunto de todas as classe laterais à esquerda módulo H.

($\Rightarrow$) Por hipótese P é uma partição de L. E temos, para qualquer elemento $a \in L$ e para qualquer $h \in H$, $ah = ah \cdot e$.

Como $e \in H$ temos, $ah \in a \cdot H \cap (a \cdot h) \cdot H$, como P é partição concluímos que $aH = ah \cdot H$.

($\Leftarrow$) Claramente $P \subseteq 2^L$ e $\forall g \in L$, $g = ge \in g \cdot H$, então $L = \bigcup_{X \in P} X$.

Além disso, $X \in P$ garante a existência de um elemento $g \in L$ tal que $X = gH$ e $g = ge \in g \cdot H = X$, portanto $X \neq \emptyset$.

Finalmente sejam $a, b \in L$ tais que $aH \cap bH \neq \emptyset$, segue que existe um elemento $g \in aH \cap bH$ e logo $g = ax = by$ para certos $x, y \in H$. E por hipótese:

$$aH = ax \cdot H = by \cdot H = bH.$$

Concluindo que P é partição, isto é, L é decomposto em classes laterais à esquerda de H.

Analogamente provamos o resultado para classes laterais à direita. □

Definição 2.29 Seja L um loop finito. Definimos a ordem do loop L, e denotamos por $|L|$, como sendo a sua cardinalidade, isto é, a quantidade de elementos no conjunto L.

Definição 2.30 Seja L um loop finito e $H \leq L$. Então H é dito *tipo-Lagrange* se $|H| \,||L|$.

Definição 2.31 Seja L um loop finito e $H \leq L$. Então L satisfaz a *condição fraca de Lagrange* se, e somente se, todo subloop de L é tipo-Lagrange.

Definição 2.32 Seja L um loop finito. Então L safisfaz a *condição forte de Lagrange* se, e somente se, para qualquer $H \leq L$ temos que H satisfaz a condição fraca de Lagrange.

Para um loop finito L satisfazer a condição forte de Lagrange deve acontercer que $|H| \,|\, |K|$ sempre que $H \leq K \leq L$. Podemos encontrar loops que satisfaçam a propriedade fraca de Langrange sem satisfazer a propriedade forte de Lagrange. Considere a seguinte ilustração:

Exemplo 2.33 Seja L um loop de ordem 10 com elemento identidade e, onde $\langle e \rangle$, H e K são seus únicos subloops. Suponha ainda que $\langle e \rangle \leq H \leq K \leq L$, com ordem de H igual a 2 e order de K igual a 5. Como $1, 2$ e 5 são divisores de 10, temos que L têm a propriedade fraca de Lagrange. Porém K não têm a propriedade fraca de Lagrange, segue então que L não têm a propriedade forte de Lagrange.

Por agora, verifiquemos a óbvia conexão entre decomposições em classes laterais e propriedades tipo-Lagrange.

Teorema 2.34 *Seja L um loop finito e $H \leq L$. Se L têm uma decomposição em classes à esquerda (analogamente, à direita) módulo H, então H é tipo-Lagrange.*

Demonstração: Seja P o conjunto de todas as classe laterais à esquerda módulo H, por definições anteriores P é uma partição de L, portanto, $|L| = \sum_{X \in P} |X|$.

Conside $X \in P$, então temos que $X = a \cdot H$ para algum $a \in L$, como $L(a) : H \to aH = X$ é bijetora (pois H é loop, em particular H é quasigrupo) temos que $|H| = |a \cdot H| = |X|$,logo segue que:

$$|L| = \sum_{X \in P} |X| = |P||H|$$

Concluindo que $|H| \,|\, |L|$, isto é, H é tipo-Lagrange.

Observação: Analogamente provamos o resultado para classes laterais à direita. □

Teorema 2.35 *Seja L um loop finito e $H \leq L$. Se $ah \cdot H = aH$ (analogamente, $H \cdot ha = Ha$) para quaisquer $a \in L$ e $h \in H$, então H é tipo-Lagrange.*

Demonstração: Pelo **Teorema 2.28** L se decompõe em classes laterais módulo H. Pelo **Teorema 2.34** L é tipo-Lagrange. □

Definição 2.36 Seja L um loop e $N \leq L$. Então N é chamado de subloop normal se, e somente se:

$$xN = Nx,\ xN \cdot y = x \cdot Ny \text{ e } x \cdot yN = xy \cdot N,\ \forall x, y \in L$$

Sempre que N for um subloop normal de um loop L irei denotar este fato por $N \trianglelefteq L$.

Teorema 2.37 *Seja L um loop e $N \trianglelefteq L$, então L se decompõe em classes laterais à esquerda (analogamente, à direita) módulo N.*

Demonstração: De fato, pois sendo N um subloop de L temos que $N = nN$ para qualquer n em N, esse fato segue já que a função $L_n : N \to N$ é bijetora.

Portanto temos para quaisquer a e n, elementos de L e N respectivamente.

$$\begin{aligned} aN &= a \cdot nN \\ &= an \cdot N. \end{aligned}$$

O que conclui, pelo **Teorema 2.28**, que L se decompõe em classes laterais à esquerda módulo N.

Observação: Analogamente provamos o resultado para classes laterais à direita. □

Corolário 2.38 *Seja L um loop e $N \trianglelefteq L$, então N é um subloop tipo-Lagrange.*

Demonstração: Basta seguir os resultados dos **Teoremas 2.37** e **2.35**. □

Outra definição equivalente de subloop normal será dada ainda neste capítulo.

2.5 Núcleos e Centro de um loop

Seja Q um quasigrupo. Algumas vezes a importância que um elemento a têm como membro de Q pode ser descrita ou caracterizada pelo comportamento das translações L_a e R_a, que já foram introduzidas anteriormente.

Definição 2.39 Seja Q um quasigrupo, $a \in Q$, a é dito nuclear à esquerda (analogamente, nuclear à direita e nuclear central) se, e somente se:

$$L_{ax} = L_x L_a \ \forall x \in Q.$$
$$\text{(Analogamente, } R_{xa} = R_x R_a \ \forall x \in Q \text{ e } L_{xa} = L_a L_x \ \forall x \in Q).$$

isto é:

$$a \cdot xy = ax \cdot y \ \forall x, y \in Q.$$
$$\text{(Analogamente, } xy \cdot a = x \cdot ya \ \forall x, y \in Q \text{ e } xa \cdot y = x \cdot ay \ \forall x, y \in Q).$$

Definição 2.40 Seja Q um quasigrupo. O núcleo à esquerda de Q (denotado N_λ), o núcleo ao centro de Q (denotado N_μ) e o núcleo à direita de Q (denotado N_ρ) são definidos da seguinte forma:

$$N_\lambda = \{a \in Q \mid a \cdot xy = ax \cdot y \ \forall x, y \in Q\}.$$
$$N_\rho = \{a \in Q \mid xy \cdot a = x \cdot ya \ \forall x, y \in Q\}$$
$$N_\mu = \{a \in Q \mid xa \cdot y = x \cdot ay \ \forall x, y \in Q\}$$

Mais ainda, $N = N_\lambda \cap N_\mu \cap N_\rho$, é chamado de núcleo de Q.

Não podemos garantir que existam elementos nucleares à esquerda, centrais ou à direita, cada um dos N_λ, N_μ e N_ρ podem muito bem ser vazios.

Porém, caso sejam não vazios temos alguns resultados interessantes.

Teorema 2.41 *Seja Q um quasigrupo. Se N_λ (analogamente, N_μ, N_ρ) for não vazio então N_λ (analogamente, N_μ, N_ρ) é fechado para a operação do quasigrupo. Mais ainda, é associativo.*

Demonstração: Suponha que $N_\lambda \neq \emptyset$, e seja $a, b \in N_\lambda$ e $x \in Q$. Então temos:

$$L_{ab\cdot x} = L_{a\cdot bx} = L_{bx}L_a = L_xL_bL_a = L_xL_{ab}.$$

O que conclui que $ab \in N_\lambda$, concluindo que N_λ fechado para operação do do quasigrupo.

Provemos agora que N_λ é associativo, sejam $a, b, c \in N_\lambda$, então como $a \in N_\lambda$, segue que $a \cdot bc = ab \cdot c$, concluindo que N_λ é associativo.

Observação: Similarmente concluímos os resultados análogos para N_μ e N_ρ.

□

Teorema 2.42 *Seja Q um quasigrupo, valem:*

(i) Se $N_\mu \neq \emptyset$, então N_μ é um subgrupo de Q e o elemento identidade e de N_μ é o elemento identidade de Q.

(ii) Se $N_\lambda \neq \emptyset$, então N_λ é um subgrupo de Q e o elemento identidade e de N_λ é o elemento identidade à esquerda de Q.

(iii) Se $N_\rho \neq \emptyset$, então N_ρ é um subgrupo de Q e o elemento identidade e de N_ρ é o elemento identidade à direita de Q.

Demonstração: (i) Suponha que $N_\mu \neq \emptyset$, seja $a \in N_\mu$ e $y \in Q$, como Q é quasigrupo existe um único $x \in Q$ tal que $y = xa$ e existe um único $w \in Q$ tal que $y = aw$, também existe um único $e \in Q$ tal que $a\ e = a$, usando do fato de $a \in N_\mu$, temos:

$$y \cdot e = xa \cdot e = x \cdot ae = x \cdot a = y.$$

Concluindo que e é elemento identidade à direita de Q.

Além disso, temos:

$$a \cdot a^{\rho} = e = e \cdot e = e \cdot aa^{\rho} = ea \cdot a^{\rho}$$

Como valem as leis do cancelamento em Q concluímos que $a = ea$, logo:

$$y = a \cdot w = ea \cdot w = e \cdot aw = e \cdot y$$

Concluindo que e é elemento identidade à esquerda de Q, juntando com a informação obtida anteriormente e é elemento identidade de Q.

É fácil ver que $e \in N_{\mu}$, já que para arbitrários x e y em Q, temos:

$$xe \cdot y = x \cdot y = x \cdot ey.$$

E temos os seguintes resultados para qualquer $b \in N_{\mu}$:

$$b^{\lambda} \cdot bb^{\lambda} = b^{\lambda}b \cdot b^{\lambda} = e \cdot b^{\lambda} = b^{\lambda} \cdot e = b^{\lambda} \cdot bb^{\rho}$$

Pelo cancelamento $bb^{\lambda} = bb^{\rho}$, e usando do cancelamento mais uma vez, $b^{\lambda} = b^{\rho} = b^{-1}$.

Além disso, como para qualquer $y \in L$ existe $u \in Q$ tal que $ub = y$ temos:

$$yb^{-1} \cdot b = (ub \cdot b^{-1})b = (u \cdot bb^{-1})b = ue \cdot b = ub = y$$

Logo $yb^{-1} \cdot b = y \ \forall y \in Q$, isto é $R_b^{-1} = R_{b^{-1}} \ \forall b \in N_{\mu}$, analisando a expressão espelhada $b \cdot b^{-1}y$ concluímos analogamente que $L_b^{-1} = L_{b^{-1}}$.

Outro resultado é que $b^{-1} \in N^{\mu}$, pelo seguinte, seja a e c elementos arbitrários em Q, e considere o único elemento $t \in Q$ tal que $a = tb$, então segue:

$$\begin{gathered} ab^{-1} \cdot c = (tb \cdot t^{-1})c = (tR_bR_{b^{-1}})c = (tR_bR_b^{-1})c = tc; \\ a \cdot b^{-1}c = (tb)(t^{-1}c) = t(b \cdot b^{-1}c) = t(cL_{b^{-1}}L_b) = t(cL_b^{-1}L_b) = tc; \end{gathered}$$

Concluindo que $ab^{-1} \cdot c = a \cdot b^{-1}c$ para quaisquer $a, c \in L$, isto é $b^{-1} \in N_{\mu}$.

Lembrando que N_{μ} é fechado para operação do quasigrupo pelo **Teorema 2.41**, tomando $b, c \in N_{\mu}$ notamos que:

$$\begin{gathered} c \backslash b = cR(b)^{-1} = cR(b^{-1}) = c \cdot b^{-1} \in N_{\mu}; \\ b/c = cL(b)^{-1} = cL(b^{-1}) = b^{-1} \cdot c \in N_{\mu}. \end{gathered}$$

Concluímos que $(N_{\mu}, \cdot)$, $(N_{\mu}, /)$ e $(N_{\mu}, \backslash)$ são fechados para suas respectivas operações pelo resultado do **Teorema 2.18** temos que N_{μ} é subquasigrupo de Q.

Logo já sabemos que N_{μ} é quasigrupo associativo com elemento identidade e, portanto N_{μ} é grupo com elemento identidade e, finalmente concluímos que N_{μ} é subgrupo de Q com e sendo elemento identidade de N_{μ} e de Q.

(ii) Suponha que $N_{\lambda} \neq \emptyset$, e seja $a \in N_{\lambda}$, sabemos que existe um único $e \in Q$, tal que $a = a \cdot e$, segue que, para quaisquer x e y em Q:

$$a(ex \cdot y) = (a \cdot ex)y = (ae \cdot x)y = ax \cdot y = a \cdot xy = ae \cdot xy = a(e \cdot xy);$$

Usando do cancelamento à esquerda segue que $ex \cdot y = e \cdot xy$, isto é, $e \in N_\lambda$.

Agora tomando $x \in Q$ arbitrário, temos:

$$a \cdot ex = ae \cdot x = a \cdot x$$

E pelo cancelamento $e \cdot x = x$ para qualquer $x \in Q$, isto é, e é elemento identidade à esquerda para Q, e também para qualquer $b \in N_\lambda$ segue:

$$be \cdot a = b \cdot ea = ba;$$

Cancelando à direita concluimos $e \cdot b = b$, $\forall b \in N_\lambda$, ficando claro que se concluirmos que N_λ for subgrupo, então e será elemento identidade de N_λ.

Também observamos para qualquer $b \in N_\lambda$ que:

$$e \cdot b = b = b \cdot e = b \cdot b^\lambda b = bb^\lambda \cdot b;$$

Portanto cancelando à esquerda $b \cdot b^\lambda = e$, logo segue da unicidade da definição de b^ρ que $b^\lambda = b^\rho = b^{-1}$.

Ainda se $x, y \in Q$ temos:

$$b(b^{-1} \cdot xy) = bb^{-1} \cdot xy = e \cdot xy = xy = ex \cdot y = (bb^{-1} \cdot x)y = (b \cdot b^{-1}x)y = b(b^{-1}x \cdot y);$$

Logo $b(b^{-1} \cdot xy) = b(b^{-1}x \cdot y)$ e cancelando à esquerda, obtemos $b^{-1} \cdot xy = b^{-1}x \cdot y$, portanto $b^{-1} \in N_\lambda$.

Agora considerando $b, c \in N_\lambda$ arbitrários, temos:

$$c/b \cdot b = c = c \cdot e = c \cdot b^{-1}b = cb^{-1} \cdot b;$$
$$b \cdot b\backslash c = c = e \cdot c = bb^{-1} \cdot c = b \cdot b^{-1}c.$$

Usando dos cancelamentos e do fato de N_λ ser fechado para operação do quasigruop, temos que $c/b = c \cdot b^{-1} \in N_\lambda$ e $b\backslash c = b^{-1} \cdot c \in N_\lambda$, concluindo que $(N_\lambda, \cdot)$, $(N_\lambda, /)$ e $(N_\lambda, \backslash)$ são fechados para suas operações, analogamente encerrando como no caso (i) concluindo que N_λ é subgrupo de Q, com e sendo elemento identidade à esquerda de Q, e também, e sendo elemento identidade de N_λ.

(iii) Poderíamos espelhar a prova de (ii) para concluir (iii). (ii) e (iii) são duais no seguinte sentido:

Para $x, y \in Q$ defina $x \star y = y \cdot x$ e note que $(Q, \star)$ também é um quasigrupo. E também N_ρ que é o núcleo à direita de $(Q, \cdot)$ é claramente o núcleo à esquerda de $(Q, \star)$. Simplemente aplique (ii) para $(Q, \star)$, e traduza o resultado para $(Q, \cdot)$, concluindo (iii), terminando a demonstração do teorema. □

Sobre loops, segue o seguinte resultado aprimorado do teorema acima.

Teorema 2.43 *Seja L um loop, então os núcleos N_λ, N_μ e N_ρ, e também N são subgrupos de L.*

Demonstração: Seja e o elemento identidade do loop L. É claro que $e \in N_\lambda \cap N_\mu \cap N_\rho$, portanto $N_\lambda \neq \emptyset$, $N_\mu \neq \emptyset$ e $N_\rho \neq \emptyset$, daqui basta aplicar o **Teorema 2.42**, e notar que N é interseção de subgrupos para concluir o enunciado. □

Definição 2.44 Seja Q um quasigrupo. O centro Z de Q é dado pelo seguinte conjunto $Z = \{a \in N \mid L(a) = R(a)\}$. Também se $a \in Z$ dizemos que a é um elemento central.

Fica claro que um elemento $a \in Q$ é um elemento do centro Z de $(Q, \cdot)$ se, e somente se, $a \cdot xy = ax \cdot y$, $xa \cdot y = x \cdot y$, $xy \cdot a = x \cdot ya$ e $xa = ax$ $\forall x, y \in Q$, isto é a sempre se associa e comuta com quaisquer elementos de Q.

Temos então os seguintes resultados:

Teorema 2.45 *Seja Q um quasigrupo com núcleo N e centro Z. Se N e Z são não vazios, então ambos são fechados para a operação do quasigrupo com Z sendo comutativo.*

Demonstração: Como N é não vazio e é interseção de conjuntos fechados para operação do quasigrupo, então N é fechado para a operação do quasigrupo.

Agora sejam $a, b \in Z$, provemos que $ab \in Z$, conhecemos que $Z \subseteq N$ por definição, logo sabemos que $a, b \in N$, além disso, se $x \in Q$ temos:

$$x \cdot ab = xa \cdot b = ax \cdot b = a \cdot xb = a \cdot bx = ab \cdot x.$$

Concluindo que $ab \in Z$, logo Z é fechado para operação do quasigrupo, como por definição $\forall a \in Z$, $L_a = R_a$ segue que Z é comutativo. □

Teorema 2.46 *Seja Q um quasigrupo com núcleo N e centro Z. Se N é não vazio, então Z é não vazio e N e Z são subgrupos de Q com Z sendo um subgrupo comutativo de N.*

Demonstração: Por hipótese N é não vazio, logo N_μ é não vazio, aplicando o **Teorema 2.42** concluimos que Q têm elemento identidade (isto é, Q é loop). Tal elemento é denotado por e. É facil ver que $e \in Z$, isto é $Z \neq \emptyset$.

Como $N = N_\lambda \cap N_\mu \cap N_\rho$ e N é não vazio, segue disso que N_λ, N_μ e N_ρ são todos não vazios, e aplicando de novo o **Teorema 2.42**, concluimos que N_λ, N_μ e N_ρ são todos subgrupos de Q, logo N é interseção de subgrupos de Q e, portanto, também é subgrupo de Q.

Do resultado do teorema acima, Z é fechado para a operação e como já visto Z têm elemento identidade e, portanto, para concluirmos que Z é grupo basta mostra que Z é fechado para inversos. Lembrando que a existência dos inversos é garantida por resultado desenvolvido no **Teorema 2.42**, e que este inverso está em N.

Seja agora $z \in Z$, sabemos que $\forall g \in Q$, temos $g \cdot z = z \cdot g$, logo:

$$z^{-1}(gz)z^{-1} = z^{-1}(zg)z^{-1};$$
$$z^{-1}g(zz^{-1}) = (z^{-1}z)gz^{-1};$$
$$z^{-1}(ge) = (eg)z^{-1};$$
$$z^{-1}g = gz^{-1};$$

Concluindo que $z^{-1} \in Z$, como por definição Z é comutativo, segue que Z é subgrupo comutativo de N. □

Teorema 2.47 *Seja L um loop com núcleo N e centro Z. Então N e Z são subgrupos de L com Z sendo um subgrupo comutativo de L.*

Demonstração: L sendo loop, significa que L é quasigrupo com elemento identidade e. É evidente que $e \in N$ e, portanto, $N \neq \emptyset$, bastando agora aplicar o teorema acima para concluir o resultado. □

Teorema 2.48 *O centro Z de um loop L é um subloop normal de L.*

Demonstração: Como para qualquer $a \in Z$ temos que $a \cdot xy = ax \cdot y$, $xa \cdot y = x \cdot y$, $xy \cdot a = x \cdot ya$ e $x \cdot a = a \cdot x$ para quaisquer $x, y \in L$, segue disso que:

$$xZ = Zx,\ (xZ) \cdot y = x \cdot (Zy) \text{ e } x \cdot (yZ) = (xy) \cdot Z, \forall x, y \in L.$$

O que conclui que Z é subloop normal de L. □

2.6 Propriedade de inversão

O conceito de inverso de um elemento só têm significado se um sistema possui um elemento identidade, lembremos que na teoria de grupos, $aa^{-1} = a^{-1}a = e$. Porém, na teoria de quasigrupos, o conceito de inverso pode ser generalizado, e pode ser definido com significado de inversão mesmo na ausência de um elemento identidade.

Definição 2.49 Um quasigrupo Q é dito ter a propriedade de inversão à esquerda (e é chamado de L.I.P. quasigrupo) se, e somente se, existe uma bijeção $J_\lambda : Q \to Q$ tal que $aJ_\lambda \cdot ax = x\ \forall x \in Q$.

Similarmente, um quasigrupo Q é dito ter a propriedade de inversão à direita (e é chamado de R.I.P. quasigrupo) se, e somente se, existe uma bijeção $J_\rho : Q \to Q$ tal que $xa \cdot aJ_\rho = x\ \forall x \in Q$. Se um quasigrupo (ou loop) Q é ambos um R.I.P. quasigrupo (ou loop) e um L.I.P quasigrupo (ou loop), então Q é dito ter a propriedade de inversão e será chamado de I.P quasigrupo (ou loop) daqui para frente.

Definição 2.50 A função J_λ em um L.I.P quasigrupo é chamada de função de inversão à esquerda, analogamente a função J_ρ em um R.I.P quasigrupo é chamada de função de inversão à direita.

Mais ainda, quando $J_\lambda = J_\rho = J$ em um I.P quasigrupo, J é dito função de inversão.

Exemplo 2.51 Qualquer grupo G é um I.P. quasigrupo com $aJ_\lambda = aJ_\rho = a^{-1}$ para qualquer a elemento de G.

A classe de I.P. quasigrupos é extremamente importante e evidenciarei algumas propriedades importantes de tais quasigrupos.

No caso em que L é um loop com elemento identidade e, todo elemento $a \in L$ têm únicos inversos laterais a^λ e a^ρ. Porêm, a existência de tais elementos não valida as identidades $a^\lambda \cdot ax = x$ e $xa \cdot a^\rho = x$. Portanto nem todo loop é um I.P. loop.

Exemplo 2.52 Considere o loop $(L, \cdot)$ dado pela seguinte tabela de Cayley:

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

Neste loop $xx = 1$, $\forall x \in L$, portanto $x^\lambda = x^\rho = x$ para qualquer $x \in L$. Mas já que $(3 \cdot 4) \cdot 4 = 2 \neq 3$ e $3 \cdot (3 \cdot 4) = 2 \neq 4$, L não é um I.P. loop.

Teorema 2.53 *Seja L um L.I.P loop, para qualquer elemento a de L temos que* $aJ_\lambda = a^\lambda$.

Demonstração: Seja $a \in L$, o resultado segue já que $e = aJ_\lambda \cdot ae = aJ_\lambda a$, por outro lado $e = a^\lambda a$ e pelo cancelamento à esquerda $aJ_\lambda = a^\lambda$. □

Teorema 2.54 *Seja L um R.I.P. loop, para qualquer elemento a de L temos que* $aJ_\rho = a^\rho$.

Demonstração: Basta fazer um espelhamento da demonstração do **Teorema 2.53**. □

Teorema 2.55 *Seja L um L.I.P. ou um R.I.P. loop com elemento identidade e, temos* $J_\lambda = J_\rho = J$ *(isto é,* $a^\lambda = a^\rho = a^{-1}$*).*

Demonstração: Em um L.I.P. loop, temos $a^\lambda = a^\lambda e = a^\lambda \cdot aa^\rho = a^\rho$.

Já em um R.I.P. loop, temos $a^\rho = ea^\rho = a^\lambda a \cdot a^\rho = a^\lambda$. □

Teorema 2.56 *Os núcleos de um I.P. loop coincidem, isto é* $N_\lambda = N_\rho = N_\mu = N$.

Demonstração: Sejam N_λ,N_μ e N_ρ os núcleos de um I.P. loop L.

Seja $l \in N_\lambda$ e $r \in N_\rho$, provemos que $r \in N_\lambda$ e $l \in N_\rho$, para concluir que N_λ coincide com N_ρ.

Se $l \in N_\lambda$, então $l^{-1} \in N_\lambda$ (já que N_λ é subgrupo de L), logo como em I.P. loops inversos bilaterais existem, temos $l^{-1} \cdot b^{-1}a^{-1} = l^{-1}b^{-1} \cdot a^{-1}$, $\forall a, b \in L$. Tomando o inverso em ambos os lados obtemos, $a \cdot bl = ab \cdot l$, portanto $l \in N_\rho$.

De forma análoga provamos que $r \in N_\lambda$, concluindo que $N_\lambda = N_\rho$.

Provemos agora que $N_\lambda = N_\rho = N_\mu$, considere $c \in N_\mu$ e $l \in N_\lambda = N_\rho$.

Primeiramente mostremos que $c \in N_\lambda = N_\rho$, considere $a, b \in L$ arbitrários, usando a bijeção das funções de translação e da função de inversão, existe um elemento d em L tal que $b = a^{-1} \cdot cd$, como $c \in N_\mu$, temos $b = a^{-1}c \cdot d$, levando em $d = c^{-1}a \cdot b$ (multiplicando por $(a^{-1}c)^{-1} = c^{-1}a$ pela esquerda em ambos os lados da igualadade), por outro lado obtemos:

$$c^{-1} \cdot ab = c^{-1} \cdot (a(a^{-1} \cdot cd)) = c^{-1} \cdot cd = d.$$

Portanto, $c^{-1}a \cdot b = c^{-1} \cdot ab$, isto é, $c^{-1} \in N_\lambda = N_\rho$, já que $N_\lambda = N_\rho$ é grupo, concluímos que $c \in N_\lambda = N_\rho$.

Considere novamente $a, b \in L$ arbitrários, usando da bijeção das funções de translação e da função inversa, existe um elemento g em L tal que $b = l \cdot a^{-1}g$, como $l \in N_\lambda$, temos $b = la^{-1} \cdot g$, levando em $g = al^{-1} \cdot b$ (multiplicando por $(la^{-1})^{-1} = al^{-1}$ pela esquerda em ambos os lados da igualdade), por outro lado obtemos:

$$a \cdot l^{-1}b = a(l^{-1}(l \cdot a^{-1}g)) = a \cdot a^{-1}g = g.$$

Portanto, $al^{-1} \cdot b = a \cdot l^{-1}b$, isto é, $l^{-1} \in N_\mu$, já que N_μ é grupo, concluímos que $l \in N_\mu$.

Terminando em $N_\lambda = N_\rho = N_\mu$. □

Existem classes de loops que não são I.P. loops mas possuem propriedades que podem ser consideradas como variações de I.P. loops.

2.7 Grupo das multiplicações e grupo de aplicações internas

Seja Q um quasigrupo. Foi mencionado na seção 2 deste capítulo que para todo elemento $a \in Q$ temos associadas duas funções (chamadas de translações à direita e à esquerda) L_a e R_a de Q para Q, tais que $xL_a = ax$ e $xR_a = xa$ para qualquer x em Q, e definimos tais funções como bijetoras no caso de Q ser quasigrupo. Logo, L_a e R_a são permutações de Q e podem ser consideradas como elementos do grupo simétrico $S(Q)$ de todas as permutações do conjunto Q.

Definição 2.57 O conjunto de todas L_x e suas inversas L_x^{-1}, $x \in Q$, geram um subgrupo $LMult(Q) \leq S(Q)$ chamado de grupo das multiplicações à esquerda de Q.

Similarmente, $\langle \{R_x \mid x \in Q\} \rangle = RMult(Q)$ é chamado de grupo das multiplicações à direita de Q. E finalmente, o grupo gerado por todas as multiplicações de Q é chamado de grupo das multiplicações e denotamos por $Mult(Q)$.

É importante enfatizar que o conjunto de multiplicações à esquerda ou à direita não necessariamente formam um grupo, pois o produto de duas multiplicações podem não ser uma multiplicação. Para grupos, $xR_aR_b = xa \cdot b = x \cdot ab = xR_{ab}$, ou seja, $R_aR_b = R_{ab}$. Este não é sempre o caso para quasigrupos devido a possível ausência de associatividade.

Para alguns quasigrupos as multiplicações à direita (ou esquerda) podem formar um grupo, mas isso seria um caso excepcional.

A importância dos grupo das multiplicações é devido a sua conexão com a estrutura do quasigrupo. Algumas vezes é mais facíl obter informações sobre um quasigrupo ou loop estudadando o seu grupo das multiplicações, darei um exemplo para fazer ilustração deste fato no final desta seção.

Teorema 2.58 *O centro Z de um loop L é isomorfo ao centro $Z_{Mult(L)}$ de $Mult(L)$.*

Demonstração: Para qualquer $z \in Z$, as seguintes relações $x \cdot yz = xy \cdot z$, $zy \cdot x = z \cdot yx$ e $zy = yz$ para todos $x, y \in L$ podem ser reescritas em termos de multiplicações à direita e à esquerda: $R_zL_x = L_xR_z$, $L_zR_x = R_xL_z$ e $R_z = L_z$ para todo $x \in L$, o que significa que as multiplicações por z comutam com todas outras multiplicações de $Mult(L)$, e portanto com todos os elementos de $Mult(L)$. Logo $L_z = R_z \in Z_Mult(L)$ para qualquer $z \in Z$. Trabalhando na direção oposta e traduzindo as relações $R_zL_x = L_xR_Z$, $L_zR_x = R_xL_z$ e $R_z = L_z$ para qualquer $x \in L$, se escrevem como as relações $x \cdot yz = xy \cdot z$, $zy \cdot x = z \cdot yx$ e $zy = yz$ para todos $x, y \in L$, e observamos que cada multiplicação que pertence à $Z_{Mult(L)}$ corresponde à um elemento no centro Z de L.

Da discussão acima concluímos que a função $\phi : z \mapsto R_z$ é bijetora, mais do que isso é isomorfismo, já que $z_1z_2\phi = R_{z_1z_2} = R_{z_1}R_{z_2} = z_1\phi \cdot z_2\phi$. □

Definição 2.59 Seja L um loop com elemento identidade e. Considere um elemento $\alpha \in Mult(L)$ tal que $e\alpha = e$. Tal função α é chamada de aplicação interna de L. O conjunto de todas as aplicações internas é um subgrupo de $Mult(L)$ que é chamado de grupo de aplicações internas de L denotado por $I(L)$.

Vejamos que de fato $I(L)$ é sempre subgrupo de $Mult(L)$.

Teorema 2.60 *Seja L um loop com elemento identidade e, então o conjunto $I(L)$ de suas aplicações internas é um subgrupo de $Mult(L)$.*

Demonstração: Por definição $I(L) \subseteq Mult(L)$.

Seja $\alpha \in I(L)$, então $e\alpha = e$, e então claramento $e\alpha^{-1} = e$, portanto $\alpha^{-1} \in I(L)$. Agora considere $\alpha, \beta \in I(L)$, temos então, $e(\alpha\beta) = (e\alpha)\beta = e\beta = e$, portanto $\alpha\beta \in I(L)$, concluindo que $I(L) \leq Mult(L)$ □

Teorema 2.61 *O grupo de aplicações internas $I(L)$ de um loop L é gerado por todas as funções $R(x,y), L(x,y)$ e $T(x)$ com $x,y \in L$, onde:*

$$R(x,y) = R_x R_y R_{xy}^{-1},\ L(x,y) = L_x L_y L_{yx}^{-1} \text{ e } T(x) = R_x L_x^{-1}\ \forall x,y \in L.$$

Demonstração: Considere e o elemento identidade de L. Seja F o conjunto de todas as funções do tipo $R(x,y)$, $L(x,y)$ e $T(x)$ a seja $\langle F \rangle$ o grupo gerado pelo conjunto F. $\langle F \rangle$ é então um subgrupo do grupo das multiplicações $Mult(L)$. Devemos mostrar que $\langle F \rangle = I(L)$. A primeira parte, $\langle F \rangle \subseteq I(L)$, é fácil de ver, já que todo gerador de F pertence à $I(L)$, pois temos para quaisquer $x,y \in L$:

$$eR(x,y) = eR_xR_yR_{xy}^{-1} = (ex)yR_{xy}^{-1} = eR_{xy}R_{xy}^{-1} = e, \text{ isto é } R(x,y) \in I(L);$$
$$eL(x,y) = eL_xL_yL_{yx}^{-1} = y(xe)L_{yx}^{-1} = eL_{yx}L_{yx}^{-1} = e, \text{ isto é } L(x,y) \in I(L);$$
$$eT(x) = eR_xL_x^{-1} = exL_x^{-1} = eL_xL_x^{-1} = e, \text{ isto é } T(x) \in I(L).$$

Para provar a segunda parte, isto é, $I(L) \subseteq \langle F \rangle$, denote K o conjunto de todos os elementos $\beta \in Mult(L)$ tais que $\beta \in \langle F \rangle R_{e\beta}$:

$$K = \{\beta \in Mult(L) \mid \beta \in \langle F \rangle R_{e\beta}\}$$

Pela definição de K segue que para qualquer $\beta \in K$ existe um $\phi \in \langle F \rangle$ tal que, sendo $e\beta = t$:

$$\beta = \phi R_{e\beta} = \phi R_t.$$

E temos:

$$\begin{aligned}\beta R_x &= \phi R_t R_x \\ &= \phi R(t,x) R_{tx} \\ &= \phi R(t,x) R_{e\beta R_x}.\end{aligned}$$

Como ϕ e $R(t,x)$ pertencem à $\langle F \rangle$, $\beta R_x \in \langle F \rangle R_{e\beta R_x}$, o que significa que $\beta R_x \in K$

Temos $\beta L_x \in K$, pois:

$$\begin{aligned}\beta L_x &= \phi R_t L_x \\ &= \phi T(t) L_t L_x \\ &= \phi T(t) L(t,x) L_{xt} \\ &= \phi T(t) L(t,x) L_{e\beta L_x} \in K.\end{aligned}$$

Temos $\beta R_x^{-1} \in K$ já que vale o seguinte, seja $s \in L$ tal que $t = sx$, temos $e\beta R_x^{-1} = s$, e

ainda:

$$\begin{aligned}\beta R_x^{-1} &= \phi R_t R_x^{-1} \\ &= \phi R_{sx} R_x^{-1} R_s^{-1} R_s \\ &= \phi R(s,x)^{-1} R_s \\ &= \phi R(s,x)^{-1} R_{e\beta R_x^{-1}} \in K.\end{aligned}$$

Temos $\beta L_x^{-1} \in K$ já que vale o seguinte, seja $u \in L$ tal que $t = xu$, temos $e\beta L_x^{-1} = u$, e ainda:

$$\begin{aligned}\beta L_x^{-1} &= \phi R_t L_x^{-1} \\ &= \phi T(t) L_t L_x^{-1} L_u^{-1} L_u \\ &= \phi T(t) L_{xu} L_x^{-1} L_u^{-1} L_u \\ &= \phi T(t) L(u,x)^{-1} L_u \\ &= \phi T(t) L(u,x)^{-1} L_{e\beta L_x^{-1}} \in K\end{aligned}$$

O fato de βR_x, βR_x^{-1}, βL_x, $\beta L_x^{-1} \in K$, implica que, $KMult(L) \subseteq K \subseteq Mult(L) \subseteq KMult(L)$ e $K = Mult(L)$. Em outras palavras, todo elemento $\alpha \in Mult(L)$ pertence ao conjunto $\langle F \rangle R_{e\alpha}$. Então para $\alpha \in I(L)$ nós temos $\alpha \in \langle F \rangle R_e = \langle F \rangle$, ou $I(L) \subseteq \langle F \rangle$. □

2.8 Homomorfismos de loops

Definição 2.62 Seja $(L_1, \cdot)$ e $(L_2, \circ)$ loops, e seja ϕ uma função de L_1 para L_2 tais que $(xy)\phi = x\phi \circ y\phi$, então ϕ é chamado de homomorfismo de L_1 para L_2 e o conjunto $\phi(L_1) = \{x\phi \mid x \in L_1\}$ é chamada de imagem homomórfica de L_1 sobre L_2.

Ainda, quando a função ϕ for bijetora, chamamos ϕ de isomorfismo e dizemos que L_1 é isomorfo à L_2. Isso é, quando existir um isomorfismo entre L_1 e L_2 dizemos que tais loops são isomorfos e denotamos tal fato por $L_1 \cong L_2$, além disso, quando $L_1 = L_2$ um isomorfismo será chamado de automorfismo.

A definição acima pode ser estabelecida para quasigrupos.

Todas essas definições tem o mesmo significado que a suas homônimas em teoria de grupos, com tudo isso definido podemos agora concluir resultados novos referentes à seção anterior.

Definição 2.63 Seja L um loop e considere $I(L)$. Um elemento $\alpha \in I(L)$ é dito automorfismo interno se a função α é um automorfismo. O conjunto de todos os automorfismo internos de L é denotado por $\mathcal{I}(L)$.

É fácil ver que $\mathcal{I}(L)$ é um grupo.

Um resultado enunciado na introdução é estabelecido pelo seguinte teorema.

Teorema 2.64 *O grupo de todos os automorfismos de um quasigrupo Q é isomorfo a um subgrupo do grupo de automorfismo de $LMult(Q)$, $RMult(Q)$ e $Mult(Q)$.*

Demonstração: Seja σ um automorfismo de um quasigrupo Q. Considere $x, y \in Q$, logo $xR_y\sigma = (xy)\sigma = x\sigma \cdot y\sigma = x\sigma R_{y\sigma}$ ou $R_y\sigma = \sigma R_{y\sigma}$. Daqui $R_{y\sigma} = \sigma^{-1}R_y\sigma$. O que significa que para qualquer $y \in Q$, $\sigma^{-1}R_y\sigma$ é um elemento de $RMult(Q)$, e já que o conjunto de todas as R_y é um gerador do conjunto $RMult(Q)$ podemos dizer que qualquer automorfismo σ de Q determina um único automorfismo $\sigma_\rho : T \mapsto \sigma^{-1}T\sigma$ do grupo $RMult(Q)$. É fácil ver que a função que leva $\sigma \mapsto \sigma_\rho$ é injetora, e logo tal função é um isomorfismo sobre a sua imagem.

Analogamente, podemos mostrar que $L_{y\sigma} = \sigma^{-1}L_y\sigma$ para qualquer $y \in Q$, e podemos construir um isomorfismo da mesma forma como fizemos acima, já que L_y com $y \in Q$ é um gerador do grupo $LMult(Q)$.

Juntando os dois resultados e usando do fato que os elementos da forma R_x e L_y são geradores do grupo $Mult(Q)$, construímos um isomorfismo análogo aos anteriores.

□

Em teoria de grupos o conceito de homomorfismo está intimamente relacionado com o de subgrupo normal. A situação é bastante similar para loops. Entretanto, é diferente para quasigrupos. O conceito de kernel não têm significado para quasigrupos, também talvez não exista um subquasigrupo normal associado com um dado homomorfismo. Por essa razão é preferível introduzir o conceito de relação de equivalência normal associada com um homomorfismo.

2.9 Normalidade

Definição 2.65 Uma relação de equivalência θ em um quasigrupo Q é chamada de normal se satisfaz as seguintes condições para elementos $a, b, c, d \in Q$:

(i) Se $ca\theta cb$, então $a\theta b$;

(ii) Se $ac\theta bc$, então $a\theta b$;

(iii) Se $a\theta b$ e $c\theta d$, então $ac\theta bd$.

Uma relação de equivalência normal também pode ser chamada de congruência normal.

Denotarei o conjunto de todas as classes de equivalência de Q sobre a relação θ por Q/θ, chamado de quasigrupo quociente de Q com respeito à relação de equivalência normal θ, isto é, $Q/\theta = \{K_a \mid a \in Q\}$, onde para cada $a \in Q$ temos $K_a = \{x \in Q \mid x\theta a\}$.

Teorema 2.66 *Seja α um homomorfismo entre o quasigrupo Q_1 e o quasigrupo Q_2. Então α define uma relação de equivalência normal θ*

Demonstração: De fato considere θ dado pela seguinte relação para quaisquer $a, b \in Q_1$ temos $a\theta b$ se, e somente se, $a\alpha = b\alpha$, então para quaisquer elementos $a, b, c, d \in Q_1$:

(i) $a\theta a$, pois $a\alpha = a\alpha$;

(ii) Se $a\theta b$, então $a\alpha = b\alpha$, e também $b\alpha = a\alpha$, isto é $b\theta a$;

(iii) Se $a\theta b$ e $b\theta c$, então $a\alpha = b\alpha = c\alpha$, e logo $a\theta c$;

Daqui garantimos que θ é relação de equivalência, provemos que θ é normal.

(iv) Se $ca\theta cb$, então $(ca)\alpha = (cb)\alpha$, e logo $c\alpha \cdot a\alpha = c\alpha \cdot b\alpha$, cancelando à esquerda obtemos, $a\alpha = b\alpha$, isto é $a\theta b$;

(v) Espelhando (iv) obtemos (v).

(vi) Se $a\theta b$ e $c\theta d$, então $a\alpha = b\alpha$ e $c\alpha = d\alpha$, portanto $a\alpha \cdot c\alpha = b\alpha \cdot d\alpha$, e logo $(ac)\alpha = (bd)\alpha$, isto é $ac\theta bd$.

Concluindo que θ é relação de equivalência normal sobre Q_2. □

Vejamos que munido de alguma operação relacionada com a operação de Q, temos que Q/θ é quasigrupo.

Para isso temos de notar que para quaisquer $a, b \in Q$, temos $bK_a = \{ba_i \mid a_i \in K_a\} = K_{ba}$, isso segue pois para qualquer $a_i \in K_a$ temos $b\theta b$ e $a_i\theta a$ implica que $ba_i\theta ba$, isto é $ba_i \in K_b a$, concluindo $bK_a \subseteq K_{ba}$. Para a inclusão inversa, se $c \in K_{ba}$, então existe $x \in Q$, tal que, $bx = c$, portanto $bx\theta ba$, que leva em $x\theta a$, ou seja, $x \in K_a$, isto é, $c = bx \in bK_a$, analogamente provamos que $K_a b = K_{ab}$.

Com isso é facil ver que se $b_i, b_j \in K_b$ temos $b_i K_a = K_{b_i a} = K_{b_j a} = b_j K_a$ e que $K_a b_i = K_{ab_i} = K_{ab_j} = K_a b_j$.

Deste fato podemos definir a operação $\circ$ em Q/θ da seguinte forma, $K_a \circ K_b = K_{ab}$, tal operação constrói um quaisigrupo pois as equações $K_x \circ K_a = K_b$ e $K_a \circ K_y = K_b$ têm soluções únicas determinadas pelas soluções únicas das equações $xa = b$ e $ay = b$ em Q.

Teorema 2.67 *Seja θ uma relação de equivalência normal sobre Q, então θ induz um homomorfismo de Q sobre Q/θ.*

Demonstração: Seja σ a função sobrejetora de Q para Q/θ dada por $a\sigma = K_a$ para qualquer $a \in Q$. Então para quaisquer a e b elementos de Q, temos:

$$(ab)\sigma = K_{ab} = K_a \circ K_b = a\sigma \circ b\sigma.$$

Portanto σ é um homomorfismo de Q para Q/θ. □

Essa relação de reciprocidade dada pelos dois teoremas anteriores, sugerem a seguinte definição de subquasigrupo normal.

Definição 2.68 Um subquasigrupo N de $(Q,\cdot)$ é dito normal se, e somente se, N é uma classe de equivalência com respeito à alguma relação de equivalência normal θ sobre Q.

Se N é um subquasigrupo normal de um quasigrupo Q denotarei por $N \trianglelefteq Q$.

É importante lembrar que já tinhamos dado uma definição de subloop normal, vejamos que ambas são equivalentes.

Teorema 2.69 *Seja L um loop e $N \leq L$. São equivalentes:*

(i) N é classe de congruência de alguma relação de congruência normal;

(ii) $xN = Nx$, $xN \cdot y = x \cdot Ny$ e $x \cdot yN = xy \cdot N$, $\forall x, y \in L$.

Demonstração: Seja L um loop com elemento identidade e.

((i)⇒(ii)) Considere $N \trianglelefteq L$ no sentido da **Definição 2.68**, temos que mostrar que para quaisquer $x, y \in L$ valem (1) $xN = Nx$, (2) $xy \cdot N = x \cdot yN$ e (3) $xN \cdot y = x \cdot Ny$.

Seja σ o homomorfismo definido por N.

(1) Seja $x \in L$ e $n \in N$, então existe um único elemento g em L tal que $xn = gx$. Aplicando σ temos $g\sigma \circ x\sigma = x\sigma \circ n\sigma = x\sigma = K_e \circ x\sigma$, cancelando à direita, $g\sigma = K_e$, isto é, $g \in N$. Então de $xn = gx$, concluímos $xN = Nx$.

(2) Sejam $x, y \in L$ e $n \in N$, considere g o único elemento de L tal que $xy \cdot n = x \cdot yg$. Aplicando σ obtemos $x\sigma \circ (y\sigma \circ g\sigma) = x\sigma \circ y\sigma$, cancelando à esquerda, $y\sigma \circ g\sigma = y\sigma = y\sigma \circ K_e$, cancelando à esquerda novamente, $g\sigma = K - e$, isto é $g\sigma \in N$. Então de $xy \cdot n = x \cdot yg$, concluímos $xy \cdot N = x \cdot yN$.

(3) Sejam $x, y \in L$ e $n \in N$, considere g o único elemento de L tal que $xn \cdot y = x \cdot gy$. Aplicando σ obtemos $x\sigma \circ (gy)\sigma = x\sigma \circ y\sigma$, cancelando à esquerda, $g\sigma \circ y\sigma = y\sigma = K_e \circ y\sigma$, cancelando desta vez à esquerda, $g\sigma = K_e$, isto é $g \in N$. Então de $xn \cdot y = x \cdot gy$, concluímos $xN \cdot y = y \cdot Ny$.

((ii)⇐(i)) Considere $N \trianglelefteq L$ no sentido da **Definição 2.36**. Seja θ a relação $a\theta b$ se, e somente se $aN = bN$, $a, b \in L$. Como N é normal sabemos também que N é tipo-Lagrange, e logo θ é relação de equivalência. Resta mostrar que θ é ralação de equivalência normal, isto é, para elementos $a, b, c, d \in L$ (1) se $ca\theta cb$, então $a\theta b$, (2) se $ac\theta bc$, então $a\theta b$ e (3) se $a\theta b$ e $c\theta d$, então $ac\theta bd$.

(1) Sejam $a, b, c \in L$, tais que $ca\theta cb$, isso significa que $ca \cdot N = cb \cdot N$, Mas como para N vale a propriedade $xy \cdot N = x \cdot yN$, nós temos $c \cdot aN = c \cdot bN$, cancelando à esquerda, $aN = bN$, isto é $a\theta b$.

(2) Sejam $a,b,c \in L$, tais que $ac\theta bc$, isso significa que $ac \cdot N = bc \cdot N$, mas $ac \cdot N = a \cdot cN = a \cdot Nc = aN \cdot c$, e analogamente $bc \cdot N = bN \cdot c$, e logo obtemos $aN \cdot c = bN \cdot c$, e cancelando à direita, $aN = bN$, isto é $a\theta b$.

(3) Sejam $a,b,c,d \in L$, tais que $a\theta b$ e $c\theta d$, isso significa que $aN = bN$ e $cN = dN$, então temos:

$$\begin{aligned}(aN)(cN) &= (bN)(dN)\\ (aN)(Nc) &= (bN)(Nd)\\ a(N \cdot Nc) &= b(N \cdot Nd)\\ a(NN \cdot c) &= b(NN \cdot d)\\ a \cdot Nc &= b \cdot Nd\\ a \cdot cN &= b \cdot dN\\ ac \cdot N &= bd \cdot N\end{aligned}$$

concluindo que $ac\theta bd$. □

Em certo sentido, o papel de elemento identidade em um quasigrupo é assumido pelos elementos chamados idempotentes.

Definição 2.70 Um elemento i em um quasigrupo Q é chamado idempotente se, e somente se, $ii = i^2 = i$.

O papel de um elemento idempotente é ilustrado pelo fato que uma classe de equivalência K_h que contém um elemento idempotente é um subquasigrupo. Este enunciado é uma consequência do seguinte.

Teorema 2.71 *Seja Q um quasigrupo. Uma classe de equivalência $H = K_h$ com respeito a uma relação de equivalência normal θ é um subquasigrupo se, e somente se, $h\theta h^2$.*

Demonstração: **(⇒)** Seja $H = K_h$ um subquasigrupo e também $a,b \in H$. Então de $a\theta h$ e $b\theta h$ segue que $ab\theta h^2$. Mas já que H é subquasigrupo, $ab \in H$ ou $ab\theta h$, de $ab\theta h$ e $ab\theta h^2$ obtemos $h\theta h^2$.

(⇐) Agora seja K_h uma classe de equivalência tal que $h\theta h^2$. Seja $a,b \in K_h$, então $a\theta h$ e $b\theta h$, logo $ab\theta h^2$, mas por sua vez $h\theta h^2$, logo $ab\theta h$, isto é $ab \in K_h$, concluindo que K_h é fechado para operação no quociente.

Agora temos de mostrar a existência de soluções para $ax = b$ e $ya = b$ em K_h. Sendo $a,b \in K_h$, sendo $b = ax$, como $a \in K_h$, segue que $ax\theta hx$, mas $ax = b$, logo $b\theta hx$, do fato de $b\theta h\theta h^2$ temos $hx\theta h^2$, e logo $x\theta h$, isso é $x \in K_h$.

Considerando agora $ya = b$, como $a\theta h$ temos $(b = ya)\theta yh$, portanto de $b\theta h\theta h^2$ segue $yh\theta h^2$, e logo $y\theta h$, isto é $y \in K_h$.

A unicidade dessas soluções é evidente já que K_h é um subconjunto de um quasigrupo. □

Exemplo 2.72 Um dos exemplos mais simples de quasigrupo com elementos idempotentes é dado pela seguinte tabela de Cayley:

·	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

Neste quasigrupo todo elemento é idempotente, e toda classe de equivalência $K_x = \{x\}$ da relação de igualdade é um subquasigrupo normal.

Em vista dos resultados acima, podemos dizer que, em um loop, para toda congruência normal θ existe exatamente um subloop normal N, tal N é dado pela classe de equivalência que contêm o elemento identidade (pois o elemento identidade é idempotente, além disso, todo subloop deve conter a identidade) do loop.

Isso não ocorre para quasigrupos sem elemento identidade! Para tais quasigrupos, dada um relação de equivalência normal θ podem existir diversos subquasigrupos normais diferentes, ou até mesmo não existir nenhum quasigrupo normal.

De maneira análoga o que ocorre em grupos, o subloop normal N de um loop L consiste de todas as pré-imagens de elemento identidade K_e de L/θ. Assim, podemos estabelecer um resultado muito importante:

Corolário 2.73 *Em um loop L, todo subloop normal é núcleo de algum homomorfismo e todo núcleo de homomorfismo é subloop normal.*

Demonstração: Seja L um loop com elemento identidade e e seja N um subloop normal de L. Sendo um subloop normal, N é uma classe de equivalência com respeito a alguma relação de equivalência normal θ, que por sua vez define um homomorfismo σ de L para L/θ tal que $x\sigma = K_x$ para qualquer $x \in L$, é evidente que L/θ é loop com elemento identidade K_e. Como N é subloop, N contêm o elemento identidade e de L, logo $N = K_e$, portanto para qualquer $n \in N$, temos $n\sigma = K_e$, logo $N = \{x \in L \mid x\sigma = K_e\}$, concluindo que N é o conjunto de todos os lementos de L tais que suas imagens homomórficas sobre σ são o elemento identidade K_e, tal conjunto é chamado de kernel de σ e denotado $ker(\sigma)$.

E também dado um homomorfismo ϕ entre dois loops, defina a congruência normal θ como no **Teorema 2.66**, e obteremos que $K_e = ker(\phi)$, como e é idempotente, K_e é subloop normal do domínio, concluindo então o corolário. □

Já definimos anteriormente o grupo de aplicações internas $I(L)$ de um loop L. Sendo L um loop, N um subloop de L, no próximo teorema usaremos a seguinte notação $NI(L) = N$ se, e somente se, $N\alpha = N$ (dizemos N invariante sobre α) para qualquer $\alpha \in I(L)$ e chamamos N invariante sobre $I(L)$. Então vale o seguinte resultado:

Teorema 2.74 *Seja L um loop e $N \leq L$, então N é normal em L se, e somente se, $NI(L) = N$.*

Demonstração: $(\Rightarrow)$ Seja $N \trianglelefteq L$. Mostremos que $NI(L) = N$.

Sabemos que $I(L)$ é gerado por elementos da forma $R(x,y)$, $L(x,y)$ e $T(x)$, como $x, y \in L$. Primeiro considere para $x, y \in L$ o conjunto $NL(x,y) = \{nL(x,y) \mid n \in N\}$, considerando a normalidade de N, temos $NL(x,y) = (y \cdot xN)L_{xy}^{-1} = (yx \cdot N)L_{xy}^{-1} = NL_{xy}L_{xy}^{-1} = N$.

Agora considere para $x \in L$ o conjunto $NT(x)$, considerando a normalidade de N, temos $NT(x) = (Nx)L_x^{-1} = (xN)L_x^{-1} = NL_xL_x^{-1} = N$.

Agora observando que para $x, y \in L$ vale $Nx \cdot y = xN \cdot y = x \cdot Ny = x \cdot yN = xy \cdot N = N \cdot xy$, temos que para qualquer $x, y \in L$ o seguinte, $NR(x,y) = (Nx \cdot y)R_{xy}^{-1} = (N \cdot xy)N_{xy}^{-1} = NR_{xy}R_{xy}^{-1} = N$.

Sendo invariante sobre todos os geradores do grupo $I(L)$, N é invariante sobre $I(L)$, isto é, $NI(L) = N$.

$(\Leftarrow)$ Assumindo que $NI(L) = N$, e sendo x e y elementos abitrários de L.

Então de $NT(x) = N$, segue que $NR_xL_x^{-1} = N$ se, e somente se $NR_x = NL_x$, isto é, $Nx = xN$.

De $NR(x,y) = N$, temos $NR_xR_yR_{xy}^{-1} = N$ se, e somente se, $NR_xR_y = NR_{xy}$, isto é, $Nx \cdot y = N \cdot xy$.

Também de $NL(y,x) = N$, temos $NL_yL_xL_{xy}^{-1} = N$ se, e somente se $NL_yL_x = NL_{xy}$, isto é, $x \cdot yN = xy \cdot N$.

Juntando as três informações obtidas acima $xN \cdot y = Nx \cdot y = N \cdot xy = x \cdot yN = xy \cdot N$, como em x e y são arbitrários segue que N é subloop normal de L. $\square$

3 Loops de Moufang

Loops de Moufang foram introduzidos por Ruth Moufang em seu artigo "Zur Struktur von Alternativ-Körpern" [5] e é a categoria de loops de mais conhecida.

3.1 Definição e propriedades

Um loop de Moufang é um loop que satisfaz três identidades, conhecidas como identidades de Moufang. Estas são uma versão fraca da propriedade associativa. E mesmo na ausência da associatividade, esses loops capturam muitas propriedades que são válidas para grupos.

Definição 3.1 Um loop L é dito um *loop de Moufang* se ele satisfaz as seguintes identidades:

$$(xy \cdot x)z = x(y \cdot xz), \text{ a identidade de Mounfag à esquerda (IME);}$$
$$(xy \cdot z)y = x(y \cdot zy), \text{ a identidade de Moufang à direita (IMD);}$$
$$(xy)(zx) = (x \cdot yz)x, \text{ a identidade de Moufang central (IMC).}$$

Dizer que um loop satisfaz uma certa identidade, significa que este loop satisfaz a identidade referida para todos os seus elementos. Por exemplo, dizer que um loop L satisfaz a identidade central de Moufang, significa que para quaisquer x, y e z em L temos $(xy)(zx) = (x \cdot yz)x$.

O teorema a seguir estabelece que um loop de Moufang pode ser definido com apenas uma das identidades de Moufang.

Teorema 3.2 *Em um loop L, as três identidades de Moufang são equivalentes. Além disso, se alguma das identidades de Moufang é satisfeita, então valem as seguintes identidades:*

(i) $yx \cdot x = yx^2$, *conhecida como identidade alternativa à direita (IAD);*

(ii) $x \cdot xy = x^2y$, *conhecida como identidade alternativa à esquerda (IAE);*

(iii) $xy \cdot x = x \cdot yx$, *conhecida como indentidade flexivel (IF).*

Passos da demonstração:

(i) Primeiro mostremos que se L satisfaz a IME, então L satisfaz a IAD, IAE, IF, IMD e a IMC

(ii) Mostremos que se L satisfaz a IMC, então L satisfaz IMD.

(iii) Finalmente, mostremos que se L satisfaz a IMD, então L satisfaz a IME.

Demonstração: Considere e o elemento identidade de L.

(i) Assuma que L satisfaz a IME, tomando $z = e$ na IME, obtemos $xy \cdot x = x \cdot yx$, que é a IF. Usando da IF tomando $y = x^\lambda$, temos:

$$xx^\lambda \cdot x = x \cdot x^\lambda x = xe$$

Cancelando à esquerda obtemos que $x^\lambda x = e$, ou seja, $x^\lambda = x^\rho = x^{-1}$, isto é, todo elemento em L têm inverso bilateral.

Agora tomando $x = y^{-1}$ na IME, temos $y^{-1}z = y^{-1}(y \cdot y^{-1}z)$, cancelando à esquerda obtemos $z = y \cdot y^{-1}z$, já conhecida como propriedade de inversão à esquerda. Desta vez, tomando $z = x^{-1}$ na IME, temos $(xy \cdot x)x^{-1} = xy$, como a equação $xy = w$ sempre têm solução única para qualquer x e w, temos $wx \cdot x^{-1} = w$, já conhecida como propriedade de inversão à direita. Concluindo que L é um I.P. loop.

Tomando $y = e$ na IME, temos $x^2z = x \cdot xz$ que é a IAE, aplicando a inversão em ambos os lados temos $z^{-1}(x^{-1})^2 = z^{-1}x^{-1} \cdot x^{-1}$, que é equivalente a IAD.

Aplicando a função inversão nos dois lados da IME, obtemos a seguinte nova identidade $z^{-1}(x^{-1} \cdot y^{-1}x^{-1}) = (z^{-1}x^{-1} \cdot y^{-1})x^{-1}$, que é equivalente a IMD.

Trocando z por $x^{-1}z$ na IME, obtemos $(xy \cdot x)(x^{-1}z) = x \cdot yz$, multiplicando por x à direita:

$$\begin{aligned}(x \cdot yz)x &= [(xy \cdot x)(x^{-1})z]x \\ &= (xy)[x(x^{-1}z \cdot x))] \quad (IMD) \\ &= (xy)[(x \cdot x^{-1}z)x] \quad (IF) \\ &= (xy)(zx).\end{aligned}$$

Obtendo exatamente a IMC, concluindo a primeira parte.

(ii) Suponha que L satisfaz a IMC, tomando $y = e$ na IMC, temos $x \cdot zx = xz \cdot x$, isso é a IF. Logo por raciocínio análogo ao da parte (i), todo elemendo de L têm inverso bilateral.

Como $y = x^{-1}$ na IMC, temos $zx = (x \cdot x^{-1}z)x$, cancelando à direita, $z = x \cdot x^{-1}z$, obtendo a propriedade de inversão à esquerda, dessa vez tomando $z = x^{-1}$ na IMC temos $xy = (x \cdot yx^{-1})x = x(yx^{-1} \cdot x)$ pela flexibilidade, agora cancelando à esquerda,

$yx^{-1} \cdot x = y$, obtendo a propriedade de inversão à direita. Concluindo que L é um I.P. loop.

De IMC $(xy)(zx) = (x \cdot yz)x$, implica que $(zx) = (y^{-1}x^{-1})[(x \cdot yz)x]$. Trocando y por y^{-1}:

$$(zx) = (yx^{-1})[(x \cdot y^{-1}z)x]$$

Agora trocando z por yz, temos:

$$yz \cdot x = (yx^{-1})(xz \cdot x)$$

Finalmente trocando y por yx, temos:

$$(yx \cdot z)x = y(xz \cdot x) = y(x \cdot zx)$$

Que é exatamente a IMD, concluindo a segunda parte.

(iii) Suponha que L satisfaz a IMD, tomando $x = e$ na IMD, temos $yz \cdot y = y \cdot zy$, isso é a IF, como visto anteriormente no item (i), todo elememto em L têm inverso bilateral.

Trocando z por y^{-1} na IMD, temos $(xy \cdot y^{-1})y = xy$, e cancelando à direita, $x = xy \cdot y^{-1}$, isso é a propriedade de inversão à direita. Agora trocando x por y^{-1}, obtemos $zy = y^{-1}(y \cdot zy)$, como a equação $zy = w$ têm solução única em z para qualquer w e y em L, segue $w = y^{-1} \cdot yw$, que é a propriedade de inversão à esquerda. Concluindo que L é um I.P. loop.

Com isso aplicando a função inversão em ambos os lados da IMD, obtemos a seguinte identidade $y^{-1}(z^{-1} \cdot y^{-1}x^{-1}) = (y^{-1}z^{-1} \cdot y^{-1})x^{-1}$, que é equivalente a IME, terminando a demonstração. □

Corolário 3.3 *Todo loop de Moufang M é I.P. loop.*

Demonstração: Basta seguir o passo (i) da demonstração anterior. □

Deixamos como observação que o menor loop de Moufang tem ordem 12. Segue abaixo o exemplo de um loop de Moufang muito especial.

Exemplo 3.4 Seja $M = \{\pm 1, \pm i, \pm j, \pm k, \pm e, \pm ei, \pm ej, \pm ek\}$ com a operação $(\cdot)$ dada pela seguinte tabela.

·	1	i	j	k	e	ei	ej	ek
1	1	i	j	k	e	ei	ej	ek
i	i	-1	k	-j	-ei	e	-ek	ej
j	j	-k	-1	i	-ej	ek	e	-ei
k	k	j	-i	-1	-ek	-ej	ei	e
e	e	ei	ej	ek	-1	-i	-j	-k
ei	ei	-e	-ek	ej	i	-1	-k	j
ej	ej	ek	-e	-ei	j	k	-1	-i
ek	ek	-ej	ei	-e	k	-j	i	-1

$(M,\cdot)$ é um loop de Moufang não-associativo, não-comutativo. Alguém com familiaridade em álgebras não associativas poderá reconhecer os elementos de M como sendo os elementos da base de uma álgebra de Cayley-Dickson, tomando os sinais positivos e negativos. Este loop é conhecido como *loop dos octônios*.

3.2 Ferramentas para demonstrar o teorema de Moufang

Como já dito, o principal objetivo desse trabalho é o teorema de Moufang. O teorema de Moufang estabelece que em um loop de Moufang M se três elementos $x,y,z \in M$ se associam, isto é, $x \cdot yz = xy \cdot z$, então eles geram um subrgrupo de M.

Essa seção tem por objetivo desenvolver ferramentas necessárias para a demonstração do teorema de Moufang.

Definição 3.5 Seja L um loop. Para elementos arbitrário $x,y,z \in L$, o comutador, denotado por (x,y), e o associador, denotado por (x,y,z), são definidos como os únicos elementos que satisfazem:

$$xy = yx \cdot (x,y);$$
$$xy \cdot z = (x \cdot yz)(x,y,z).$$

Para subconjunto arbitrários $A,B,C \subseteq L$, o comutador, denotado por (A,B), e o associador, denotado por (A,B,C), são definidos do seguinte modo:

$$(A,B) = \{(a,b) \mid a \in A, b \in B\};$$
$$(A,B,C) = \{(a,b,c) \mid a \in A, b \in B, c \in C\}.$$

Agora vamos definir isotopismo, pela brevidade do trabalho não vamos nos aprofundar no assunto, embora seja um tema bastante importante.

Definição 3.6 Uma tripla (α,β,γ) de bijeções de um conjunto L_1 em um conjundo L_2 é chamada de isotopismo de um loop $(L_1,\cdot)$ em um loop $(L_2,\circ)$ se, e somente se, vale a seguinte expressão $x\alpha \circ y\beta = (x \cdot y)\gamma$, para todo $x,y \in L_1$.

Quando $(L_1,\cdot) = (L_2,\circ)$, a tripla (α,β,γ) é chamada de autotopismo.

Não é dificil ver que o conjunto de todos os autotopismos de um loop forma um grupo com a operação de composição, onde a operação de composição é dada entrada por entrada, isto é, $(A,B,C)(A',B',C') = (AA',BB',CC')$. O elemento identidade é (Id,Id,Id) e o inverso é dado por $(A,B,C)^{-1} = (A^{-1},B^{-1},C^{-1})$.

Daqui para frente denotarei por J a função inversão. Ou seja, $xJ = x^{-1}$.

Teorema 3.7 *Se $A = (U,V,W)$ é um autotopismo de um I.P. loop L, então $A_\mu = (W,JVJ,U)$ e $A_\lambda = (JUJ,W,V)$ também são autotopismos de L.*

Demonstração: Do autotopismo (U, V, W) temos $xU \cdot yV = (xy)W$. Pela propriedade de inversão à direita $xU = (xy)W \cdot yVJ$.

Tome $xy = a$, $y = b^{-1} = bJ$, consequentemente $x = ab$. Substituindo a e b na relação anterior, temos $aW \cdot bJVJ = abU$ para quaisquer $a, b \in L$. Logo $A_\mu = (W, JVJ, U)$ é autotopismo.

Para A_λ, $xU \cdot yV = (xy)W$ implica pela inversão à esquerda que $yV = xUJ \cdot (xy)W$.

Tomando $y = ab$, $x = a^{-1} = aJ$, consequentemente $xy = b$. Substituindo a e b na relação anterior, temos $(ab)V = xJUJ \cdot bW$ para quaisquer $a, b \in L$. Logo $A_\lambda = (JUJ, W, V)$ é autotopismo. □

Definição 3.8 Seja Q um quasigrupo. Uma bijeção U em Q é chamada de pseudoautomorfismo à direita de Q se, e somente se, existe ao menos um elemento $c \in Q$ tal que:

$$xU \cdot (yU \cdot c) = (xy)U \cdot c \text{ para todo } x, y \in Q. \text{ Ou ainda, pode ser visto como}$$
$$xU \cdot [y(UR_c)] = (xy)[UR_c]$$

O elemento c é chamado de companheiro de U.

Note que um pseudoautomorfismo à direita pode ser visto com um autotopismo da seguinte maneira. U é um pseudoautomorfismo à direita com companheiro c se, e somente se, (U, UR_c, UR_c) é um autotopismo.

Teorema 3.9 *Se (U, V, W) é um autotopismo de um loop L com elemento identidade e, e se $eU = e$, então U é um pseudoautomorfismo à direita com companheiro $c = eV$.*

Demonstração: Aplicando (U, V, W) ao produto $ex = x$, temos $(eU)(xV) = xW$, ou ainda, $xV = xW$ para todo $x \in L$, e logo $V = W$.

Denote $eV = c$. Então aplicando (U, V, W) ao produto $xe = x$, temos $xU \cdot c = xW = xV$ para todo $x \in L$, ou seja, $UR_c = V = W$.

E portanto, o autotopismo (U, V, W) pode ser reescrito como (U, UR_c, UR_c). Concluindo que U é um pseudoautomorfismo à direita com companheiro $c = eV$.

□

Teorema 3.10 *Se L é um I.P. loop com elemento identidade e S é um pseudoautomorfismo à direita, então $JSJ = S$.*

Demonstração: Denotando por e o elemento identidade de L. Da identidade $(xS)(yS \cdot c) = (xy)S \cdot c$, Colocando $y = e$ em $(xy)S \cdot c = xS(yS \cdot c)$, temos $xS \cdot c = xS(eS \cdot c)$, cancelando à esquerda e em seguida à direita, temos $eS = e$.

Tomando $y = x^{-1} = xJ$, temos $xS(xJS \cdot c) = eS \cdot c = c$, e logo $xJS \cdot c = xSJ \cdot c$, cancelando à direita $xJS = xSJ$ para qualquer $x \in L$, e logo $JS = SJ$, ou ainda $S = JSJ$.

□

Teorema 3.11 *Se L é um I.P. loop, então* $R(x,y) = JL(x^{-1},y^{-1})J$ *e* $L(x,y) = JR(x^{-1},y^{-1})J$

Demonstração: Por calculo direto temos:

$$\begin{aligned} JR(x^{-1},y^{-1})J &= JR_{x^{-1}}R_{y^{-1}}R_{(x^{-1}y^{-1})^{-1}}J \\ &= JR_{x^{-1}}JJR_{y^{-1}}JJR_{yx}J \\ &= L_xL_yL_{yx}^{-1} \\ &= L(x,y) \end{aligned}$$

Concluindo que $L(x,y) = JR(x^{-1},y^{-1})J$, trocando x por x^{-1} e trocando y por y^{-1}, temos $L(x^{-1},y^{-1}) = JR(x,y)J$, ou ainda $R(x,y) = JL(x^{-1},y^{-1})J$. □

Teorema 3.12 *Toda aplicação interna de um loop de Moufang M é um pseudoautomorfismo à direita. Aplicações internas* $R(x,y)$, $L(x,y)$ *e* $T(x)$ *têm* (x,y), (x^{-1},y^{-1}) *e* x^{-3} *como seus respectivos companheiros à direita.*

Demonstração: Para concluir o teorema basta mostrar que os geradores do grupo de aplicações internas, $R(x,y)$, $L(x,y)$ e $T(x)$, são pseudoautomorfismos e determinar seus companheiros.

Da IMC temos $(xy)(zx) = (x \cdot yz)x$, pode ser traduzida como $yL_x \cdot zR_x = yzL_xR_x$, concluindo que $A(x) = (L_x, R_x, L_xR_x)$ é autotopismo para todo $x \in M$.

Já que o conjunto de autotopismos de M formam um grupo, tomando $x, i \in M$, temos quer $A(x^{-1})A(y^{-1})(A(y^{-1}x^{-1}))^{-1} = (S,T,X)$ é um autotopismo, onde em particular:

$$\begin{aligned} S = L_{x^{-1}}L_{y^{-1}}(L_{y^{-1}x^{-1}})^{-1} = L(y^{-1},x^{-1}); \\ T = R_{x^{-1}}R_{y^{-1}}(R_{y^{-1}x^{-1}})^{-1} \end{aligned}$$

Como $eS = e$, do **Teorema 3.9**, temos $T = X = SR_c$ onde $c = eT = (x^{-1}y^{-1})(xy)$. Já que $(yx)c = xy$, então $c = (x,y)$. Então S é um pseudoautomorfismo à direita com companheiro (x,y). Além disso, pelos **Teorema 3.10** e **Teorema 3.11** $S = JSJ = JL(x^{-1},y^{-1})J = R(x,y)$. Concluindo que $R(x,y)$ é um pseudoautomorfismo à direita com companheiro (x,y).

Para $L(x,y)$, note que $L(x,y) = JR(x^{-1},y^{-1})J$ do **Teorema 3.11**, e já que $R(x^{-1},y^{-1})$ é pseudoautomorfismo como concluido acima, do **Teorema 3.10** $L(x,y) = JR(x^{-1},y{-}1)J = R(x^{-1},y^{-1})$, e combinando com o resultado acima, $L(x,y)$ é pseudoautomorfismo à direita com companheiro (x^{-1},y^{-1}).

Para $T(x) = R_xL_{x^{-1}}$, usando do **Teorema 3.7**, $C(x)$ definido da seguinte forma é um autotopismo.

$$\begin{aligned} C(x) = A_{\lambda\mu} &= (R_x, JL_xR_xJ, JL_xJ) \\ &= (R_x, R_{x^{-1}}L_{x^{-1}}, R_{x^{-1}}) \end{aligned}$$

Denote (U, V, W), pelo seguinte autotopismo:

$$(U, V, W) = C(x)A(x^{-1}) = (R_x L_{x^{-1}}, R_{x^{-1}} L_{x^{-1}} R_{x^{-1}}, R_{x^{-1}} L_{x^{-1}} R_{x^{-1}})$$

Então $U = T(x)$ e $eU = eT(x) = e$.

Pelo **Teorema 3.9**, $U = T(x)$ é um pseudoautomorfismo à direita com companheiro $c = eV = eR_{x^{-1}} L_{x^{-1}} R_{x^{-1}} = x^{-3}$, concluindo o teorema. □

Definição 3.13 Uma função θ em um loop de Moufang $(M, \cdot)$ nele mesmo é chamado de semiendomorfismo de M se, somente se, vale para todo $x, y \in M$:

$$(xyx)\theta = (x\theta)(y\theta)(x\theta) \text{ e } e\theta = e.$$

Onde e é o elemento identidade de M. Se θ é uma bijeção então θ é dito um semiautomorfismo.

Note que pela IF, temos $x \cdot yx = xy \cdot x$ por isso omitimos a ambiguidade e simplesmente podemos escrever xyx como acima. Daqui para frente, considere M um loop de Moufang com elemento identidade e.

Teorema 3.14 *Se θ é um semiendomorfismo de M, então $(x^{-1})\theta = (x\theta)^{-1}$ para qualquer elemento $x \in M$.*

Demonstração: Da definição de semiendomorfismo, temos que $(xyx)\theta = (x\theta)(y\theta)(x\theta)$ para quaisquer $x, y \in M$. Tomando $y = x^{-1}$, obtemos:

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

E cancelando à esquerda, $e = (x^{-1}\theta)(x\theta)$, concluindo que $(x^{-1}\theta) = (x\theta)^{-1}$. □

Teorema 3.15 *Todo pseudoautomorfismo de M é um semiautomorfismo de M.*

Demonstração: Seja S um pseudoautomorfismo com companheiro c, logo S é bijetora por definição.

Tomando $x, y \in M$, aplicando S ao produto $x \cdot yx$, temos:

$$\begin{aligned}(x \cdot yx)S \cdot c &= (xS)[(yx)S \cdot c] \\ &= (xS)[(yS)(xS \cdot c)] \\ &= [(xS \cdot yS)xS] \cdot c \quad (IME)\end{aligned}$$

Cancelando à direita, $(xyx)S = xS \cdot yS \cdot xS$. Já vimos no **Teorema 3.10** que $eS = e$, concluimos que S é um semiautomorfismo.

□

Corolário 3.16 *Toda aplicação interna de M é um semiautomorfismo de M.*

Demonstração: Obtemos esse resultado juntando o já conhecido no **Teorema 3.12** e no **Teorema 3.15**. □

3.3 O teorema de Moufang

Finalmente chegamos ao objetivo desse trabalho, a finalidade dessa seção é provar um dos teoremas fundamentais para a teoria de loops de Moufang, o teorema de Moufang.

Teorema 3.17 ***(Teorema de Moufang)*** *Seja M um loop de Moufang e e seu elemento identidade. Se $(a,b,c) = e$ para certos $a,b,c \in M$, então a,b,c geram um subgrupo de M.*

Utilizaremos alguns resultados preliminares a demonstração do teorema.

Teorema 3.18 *Seja M um loop de Moufang com elemento identidade e, E um conjunto não vazio de semiendomorfismo de M, F o conjunto de todos os elementos $f \in M$ que se mantêm fixado para todos os elementos de E e, finalmente, seja H o conjunto de todos os elementos $h \in M$ tal que $hF \subseteq F$. Então:*

(i) $H \subseteq F$;

(ii) $F^{-1} = F$ *e* $fFf = f$ *para qualquer* $f \in F$;

(iii) H *é subloop de* M.

Demonstração: Definindo F e H em notação de conjuntos:

$$F = \{f \in M \mid f\theta = f \ \forall \theta \in E\} \text{ e } H = \{h \in M \mid hF \subseteq F\}$$

(i) seja $h \in H$, já que $hF \subseteq F$, $(hf)\theta = hf$ para todo $h \in H$, $f \in F$ e $\theta \in E$, de $e\theta = e$ para todo $\theta \in E$, segue que $e \in F$. Então $h\theta = (he)\theta = he = h$, logo $h \in F$, ou $H \subseteq F$.

(ii) Do **Teorema 3.14**, se $x = f^{-1}$ com $f \in F$, temos $x\theta = f^{-1}\theta = (f\theta)^{-1} = f^{-1} = x$, ou seja $F^{-1} \subseteq F$, se $f \in F$ então $f^{-1} \in F$ e $(f^{-1})^{-1} = f \in F^{-1}$, logo $F^{-1} = F$.

E também temos para todo $f \in F$ e $f' \in F$:

$$(ff'f)\theta = (f\theta)(f'\theta)(f\theta) = ff'f, \text{ ou } fFf \subseteq F.$$

Reciprocamente, para todo $f \in F$, $f = efe \in fFf$, concluindo $fFf = F$.

(iii) É claro que $e \in H$, já que $eF = F$.

Também de (i) e (ii), segue que F contêm a expressão $h_1[h_2(h_1 f)^{-1}]h_1 \ \forall f \in F$ e $\forall h_1, h_2 \in H$, a qual que pela IMC e propriedade alternativa é igual a $(h_1h_2)f^{-1} \in F$. Logo por **(ii)** $(h_1h_2)f' \in F \ \forall f' \in F$, e temos $h_1h_2 \in H$.

Para mostrar que $h^{-1} \in H$ para todo $h \in H$, considere o elemento $f(hf)^{-1}f$ de F: $f(hf)^{-1}f = f(f^{-1}h^{-1})f = (ff^{-1})h^{-1}f = h^{-1}f \in F$, para qualquer $f \in F$. Portanto $h^{-1} \in H$. O que completa a prova para H ser subloop de M. □

Teorema 3.19 *Em um loop de Moufang com elemento identidade e, a equação* $(a,b,c) = e$ *implica qualquer equação obtida por permutar* a,b,c *ou substituir qualquer elemento por seu inverso.*

Demonstração: De $ab \cdot c = a \cdot bc$, segue que $[ab \cdot c](bc)^{-1} = a$, ou ainda, $aR_bR_cR_{bc}^{-1} = aR(b,c) = a$. Como $R(b,c)$ é uma aplicação interna, e como tal, é um semiendomorfismo, então $a^{-1}R(b,c) = (aR^(b,c))^{-1}$, ou $a^{-1}R_bR_cR_{bc}^{-1} = a^{-1}$, e $a^{-1}b \cdot c = a^{-1} \cdot bc$. Logo $(a,b,c) = e$ implica $(a^{-1},b,c) = e$.

De $ab \cdot c = a \cdot bc$, segue que $cL_bL_aL_{ab}^{-1} = c = L(b,a)$. Sendo $L(b,a)$ um semiendomorfismo, $c^{-1}L(b,a) = (cL(b,a))^{-1} = c^{-1}$, ou $ab \cdot c^{-1} = a \cdot bc^{-1}$. Logo $(a,b,c) = e$ implica $(a,b,c^{-1}) = e$.

De $ab \cdot c = a \cdot bc, segueque [a^{-1}(ab \cdot c)]c^{-1} = b$, em outras palavras $bL_aR_cL_{a^{-1}}R_{c^{-1}} = b$, seja $\theta = L_aR_cL_{a^{-1}}R_{c^{-1}}$, então $e\theta = [a^{-1}(ae \cdot c)]c^{-1} = (a^{-1} \cdot ac)c^{-1} = cc^{-1} = e$, logo θ é uma aplicacão interna, mais ainda é semi-endormofismo, e temos $b^{-1}\theta = (b\theta)^{-1} = b^{-1}$, ou ainda $ab^{-1} \cdot c = a \cdot b^{-1}c$. Logo $(a,b,c) = e$ implica $(a,b^{-1},c) = e$.

Como consequência, temos $(a^{-1},b^{-1},c^{-1}) = e$, ou ainda, $a^{-1}b^{-1} \cdot c^{-1} = a^{-1} \cdot b^{-1}c^{-1}$. Tomando o inverso em ambos os lados da equação, temos $c \cdot ba = cb \cdot a$, ou $(c,b,a) = e$.

De $a \cdot bc = ab \cdot c$, temos:

$$\begin{aligned} bc \cdot a^{-1} &= [a^{-1}(ab \cdot c)]a^{-1} \\ &= (a^{-1} \cdot ab)(ca^{-1}) \quad (IMC) \\ &= b(ca^{-1}) \end{aligned}$$

Ou ainda, $(b,c,a^{-1}) = e$, e também $(b,c,a) = e$.

Já que as permutações (em notação de ciclos) (ac) e (abc) geram o grupo de permutações do conjunto $\{a,b,c\}$, segue que $(a,b,c) = e$ implica que $(f(a),f(b),f(c)) = e$, onde f é uma permutação de $\{a,b,c\}$. □

Teorema 3.20 *Se* a,b,c,d *são quatro elementos de um loop de Moufang M com elemento identidade e, tais que quisquer três deles satisfazem a equação* $(x,y,z) = e$*, então as seguintes equações são equivalentes:*

(i) $(ab,c,d) = e$;

(ii) $((ab)^2,c,d) = e$;

(iii) $((a,b),c,d) = e$;

(iv) $(cd,a,b) = e$;

(v) $(bc,d,a) = e$.

Demonstração: $(i) \Rightarrow (ii)$ A equação (i) pode ser reescrita na forma $(ab \cdot c) = (ab)(cd)$ ou $ab = (ab)R_c R_d R_{cd}^{-1} = (ab)R(c,d)$. Seja $\theta = R(c,d)$, θ é semiautomorfismo tal que $ab\theta = ab$, como no **Teorema 3.18** com $\theta = R(c,d)$ e $E = \{\theta\}$, então $ab \in F$. E também $(ab)^2\theta = [(ab)e(ab)]\theta = (ab\theta)(ab\theta) = (ab)^2$, ou $(ab)^2 \in F$. Logo $(ab)^2 R(c,d) = (ab)^2$, em outras palavras $((ab)^2, c, d) = e$.

$(ii) \Rightarrow (iii)$ Tome $p = (a,b) = (a^{-1}b^{-1})(ab)$. Então $ab = ba \cdot p$, ou $ab \cdot a = (ba \cdot p)a$. Aplicando a IMD na igualdade anterior, temos $ab \cdot a = b(a \cdot pa)$. Multiplicando ambos os lados por b à direita nos dá $(ab \cdot a)b = b(a \cdot pa)b$. Porêm:

$$\begin{aligned}(ab \cdot a)b &= (ab \cdot a)(a^{-1} \cdot ab) \\ &= (ab)(aa^{-1})(ab) \quad (IMC) \\ &= (ab)^2\end{aligned}$$

Logo $(ab)^2 = b(apa)b$. Aplicando $\theta = R(c,d)$ em ambos os lados, temos $(ab)^2\theta = b\theta \cdot (apa)\theta \cdot b\theta$, se **(ii)** vale então $(ab)^2\theta = (ab)^2 = b(apa)b$, ou $b\theta \cdot (apa)\theta \cdot b\theta = b(apa)b$. Como por hipótese do lema $b\theta = b$, $(apa)\theta = apa$, mas denovo, por hipótese $a\theta = a$, segue que $p\theta = p$, ou ainda $((a,b),c,d) = e$.

$(iii) \Rightarrow (iv)$ Considere o pseudoautomorfismo $V = R(a,b)$ com companheiro à direita $p = (a^{-1}b^{-1})(ab)$. Aplicando V ao produto cd, temos $(cd)V \cdot p = cV(dV \cdot p)$.

Como $(c,a,b) = (d,a,b) = e$, então $cV = c$ e $dV = d$. Agora temos $(cd)V \cdot p = c \cdot dp$. Se **(iii)** vale então $(c,d,p) = e$ ou $c \cdot dp = cd \cdot p$, e logo $(cd)V \cdot p = cd \cdot p$, cancelando à direita, $(cd)V = cd$, ou ainda, $(cd,a,b) = e$.

$(iv) \Rightarrow (v)$ De $(a,b,c) = e$ e (iv) temos $(a \cdot bc)d = (ab \cdot c)d = (ab)(cd)$. De $(b,c,d) = e$ e (iv) temos $(ab)(cd) = a(b \cdot cd) = a(bc \cdot d)$. Então $(a \cdot bc)d = a(bc \cdot d)$, ou ainda, $(bc,d,a) = e$.

$(v) \Rightarrow (i)$ (i) pode ser obtida de (v) simplesmente trocando b,c,d,a por a,b,c,d nesta exata ordem. □

Agora introduziremos dois novos conceitos que serão necessários para a prova do teorema de Moufang.

Definição 3.21 Seja M um loop de Moufang com elemento identidade e.

Seja A um subconjunto de M e H um subloops de M que contenha A. Seja A' o subconjunto de H que consiste de todos os elementos $a' \in H$ tais que $(A,a',H) = e$. Então A' é chamado de adjunto de A com respeito a H. O subconjunto $A^* = (A')'$ é chamado de fechamento de A com respeito a H.

No caso de $H = M$, A e A' são simplesmente chamados de adjunto e fechamento, respectivamente.

Note que, já que $(a,a',h) = e$ implica que $(a',a,h) = e$, logo $A \subseteq A^*$.

Teorema 3.22 *Seja M um loop de Moufang com elemento identidade e. O adjunto e o fechamento de um conjunto não vazio A com relação a um subloop H são subloops de M. Além disso, se $(A,A,H) = e$ então $(A^*,A^*,H) = e$.*

Demonstração: Denote A' por B, então $(A,B,H) = e$. Pelo **Teorema 3.19**, $B^{-1} \subseteq B$. Também é claro que $e \in B$. Para mostrar que $B = A'$ é um subloop, só temos que mostrar que $b_1 b_2 \in B$ para quaisquer $b_1, b_2 \in B$. Considere a expressão $[(a \cdot b_1 b_2)x]b_2$ com quaisquer $x \in H$ e $a \in A$.

Usando $(A,B,H) = e$, as identidades de Moufang e o **Teorema 3.19**, temos:

$$\begin{aligned}
[(a \cdot b_1 b_2)x]b_2 &= [(ab_1 \cdot b_2)x]b_2 \quad (A,B,H) = e \\
&= (ab_1)(b_2 x b_2) \quad (IMD) \\
&= a[b_1(b_2 \cdot x b_2)] \quad (A,B,H) = e \\
&= a[(b_1 b_2 \cdot x)b_2] \quad (IMD) \\
&= [a(b_1 b_2 \cdot x)]b_2 \quad (A,H,B) = e
\end{aligned}$$

Cancelando à direita, $(a \cdot b_1 b_2)x = a(b_1 b_2 \cdot x)$, ou $b_1 b_2 \in B$, concluindo $B = A'$ é um subloop de M. Como A^* é o adjunto de B, A^* também é um subloop de M.

Agora seja $(A,A,H) = e$, isso significa que $A \subseteq A'$, e de $(A,A^*,H) = e$ segue que $(A,A^*,H) = e$ ou $A^* \subseteq A'$, logo $(A^*,A^*,H) = e$. □

Corolário 3.23 *Se $(A,A,H) = e$ então A^* é associativo.*

Demonstração: Como $A^* \subseteq H$, $(A^*,A^*,H) = e$ implica que $(A^*,A^*,A^*) = e$, ou A^* é um grupo. □

Agora podemos finalmente completar a demonstração do teorema de Moufang

Demonstração: (Teorema de Moufang) Seja $(a,b,c) = e$, $a,b,c \in M$. Considere os seguintes subconjuntos de M.

$D = \{a,b,c\}$, $F = \{x \in M \mid (D,D,x) = e, (ab,c,x) = e\}$, $H = \{h \in M \mid hF \subseteq F\}$.

No seguinte, usaremos repetidamente as identidades alternativas e o **Teorema 3.20** aplicando a quadruplas de elementos de M:

De $(ab,c,c) = e$ segue que $c \in F$.

Usando c,a,b,b, em $(b,b,ca) = e$, temos $(ab,c,a) = e$. Logo $b \in F$.

Usando a,a,b,c, em $(a,a,bc) = e$, temos $(ab,c,a) = e$. Logo $a \in F$.

E portanto $D \subseteq F$. Podemos também mostrar que $(ab,c,f) = e$ implica um resultado mais geral $(DD,D,F) = e$. Isso pode ser feito mostrando que qualquer a,b,c pode ser substituído por qualquer elemento de D. Por exemplo, usando elementos a,a,b,f em $(a,a,bf) = e$, temos $(ab,a,f) = e$ o que significa que c pode ser substituído por a, e assim por diante.

Como $D \subseteq F$, $(DD, D, F) = e$ implica $(DD, D, D) = e$. Agora aplicamos o **Teorema 3.20** para D, D, D, F. Então $(DD, D, F) = e$ implica que $(D, D, DF) = e$. A seguir considerando $d \in D$ arbitrário, usando D, FD, d, d, de $(D \cdot DF, d, d) = e$, temos $(FD, d, dD) = e$, que implica em $(dD, D, dF) = e$, em particular $(ab, c, aF) = e$, isto é, $a \in H$. Usando d, d, FD, D, de $(d, d, FD \cdot D) = e$, temos $(FD, Dd, d) = e$, que implica em $(Dd, D, dF) = e$, em particular $(ab, c, bF) = e$, isto é, $b \in H$. Usando d, F, DD, d, de $(d, d, F \cdot DD) = e$, temos $(DD, d, dF) = e$, em particular, significa que $(ab, c, cF) = e$. Logo $cF \subseteq F$, ou $c \in H$. Concluindo que $D \subseteq H$.

Consideremos agora o conjunto $E = E_1 \cup E_2$ de semiendomorfismos de M, onde $E_1 = \{R(d_i, d_j) \mid d_i, d_j \in D\}$, e $E_2 = \{R(d_i d_j, d_k) \mid d_i, d_j, d_k \in D\}$.

Então os conjuntos F e H satisfazem as condições do **Teorema 3.18** com respeito ao conjunto E. Assim, $H \subseteq F$, e H é um subloop de M. De $(D, D, F) = e$ e $H \subseteq F$, segue que $(D, D, H) = e$. Agora pelo **Teorema 3.22**. Então $(D, D, H) = e$ implica $(D^*, D^*, H) = e$, onde D^* é o fechamento do conjunto D em respeito a H. Pelo **Teorema 3.22** D^* é subloop de M. Como $D \subseteq D^*$, é claro que o subloop gerado por D está contido em D^*. Pelo **corolário 3.23** D^* é associativo, e assim também é o subloop gerado por D. Finalizando a prova do teorema. □

Corolário 3.24 *Qualquer loop de Moufang M é diassociativo, isto é, quaisquer dois elementos $a, b \in M$ gera um grupor denotado por $\langle a, b \rangle$.*

Demonstração: A demonstração é consequência direta do teorema de Moufang e do fato de valer, por exemplo, a identidade alternativa à direita em loops de Moufang (isto é, $(a, b, b) = e$), bastando tomar $D = \{a, b, b\} = \{a, b\}$ no teorema de Moufang. □

Corolário 3.25 *Qualquer loop de Moufang M é associativo por potência, isto é, qualquer elemento $a \in M$ gera um grupo denotado por $\langle a \rangle$.*

Demonstração: Novamente, a demonstração é consequência direta do teorema de Moufang e do fato de valer, por exemplo, a identidade alternativa à direita em loops de Moufang (particularmente, $(a, a, a) = e$), bastando tomar $D = \{a, a, a\} = \{a\}$ no teorema de Moufang. □

3.4 Uma outra demonstração

Em seu "A simplified proof of Moufangs theorem" [3] Aleš Drápal forneceu uma demonstração mais direta, segue a sua demonstração em nível detalhado.

Primeiro obteremos resultados auxiliares para a demonstração.

Teorema 3.26 *Seja (α, β, γ) um autotopismo de um I.P. loop L com elemento identidade e. Suponha que $e\alpha = e$ e que $x\alpha = x$ para algum $x \in L$. Então $(x^{-1})\alpha = x^{-1}$.*

Demonstração: Tome $b = e\beta$, temos a seguinte identidade $x\alpha \cdot (x^{-1})\beta = e\gamma = x \cdot (x^{-1})\beta$, ou ainda , $(x^{-1})\beta = x^{-1} \cdot e\gamma = x^{-1}(e\alpha \cdot e\beta) = x^{-1}b$, denote a identidade $(x^{-1})\beta = x^{-1}b$ por (I).

E ainda:

$$\begin{aligned} b &= x \cdot x^{-1}b \\ &= x(e \cdot (x^{-1})\beta) \quad (I) \\ &= x \cdot (x^{-1})\gamma \\ &= x \cdot ((x^{-1})\alpha \cdot b) \end{aligned}$$

Ou ainda, $x^{-1}b = (x^{-1}\alpha) \cdot b$, cancelando à direita $x^{-1} = (x^{-1})\alpha$. □

Teorema 3.27 *Seja M um loop de Moufang com elemento identidade e, e seja (α, β, γ) um autotopismo de M tal que $e\alpha = e$. Se $x, y \in M$ tais quer $x\alpha = x$ e $y\alpha = y$, então $(xyx)\alpha = xyx$.*

Demonstração: Tome $e\beta = b$. Note que para $w, z \in M$, temos:

$$\begin{aligned} (wz)\alpha &= (wz)\alpha b \cdot b^{-1} \\ &= (wz)\gamma \cdot b^{-1} \\ &= (w\alpha \cdot z\beta)b^{-1} \\ &= (w\alpha \cdot z\gamma)b^{-1} \\ &= [w\alpha \cdot (z\alpha \cdot b)]b^{-1} \end{aligned}$$

Denote a identidade $(wz)\alpha = (w\alpha \cdot (z\alpha \cdot b))b^{-1}$, por (I), agora calculando $(xyx)\alpha$:

$$\begin{aligned} (xy \cdot x)\alpha &= ((xy)\alpha \cdot xb)b^{-1} \quad (I) \\ &= ((xy)\alpha \cdot xb)b^{-1} \\ &= \{[(x \cdot yb)b^{-1}]xb\}b^{-1} \quad (I) \\ &= (x \cdot yb)(b^{-1} \cdot xb \cdot b^{-1}) \quad (IMD) \\ &= (x \cdot yb)(b^{-1}x) \\ &= x(yb \cdot b^{-1})x \quad (IMC) \\ &= xyx. \end{aligned}$$

O que conclui a demonstração. □

Definição 3.28 Seja M um loop de Moufang e $\emptyset \subsetneq X \subseteq M$, definimos $X^{\pm}$ pelo seguinte conjunto $X^{\pm} := \{x, x^{-1} \mid x \in X\}$.

O seguinte resultado têm um correspondente conhecido na teoria de grupos e para I.P. loops têm prova análoga, o resulado é o seguinte: Em um I.P. loop L se $\emptyset \subsetneq X \subseteq L$

então $\langle X\rangle$ é o conjunto de todas as multiplicações de termos sobre $X^{\pm}$, e segue de corolário que $\langle X\rangle = L$ se, e somente se, cada elemento de $u \in L$ pode ser escrito como multiplicação de termos sobre $X^{\pm}$.

Demos então notação para alguns desses termos multiplicativos, considerando e o elemento identidade do I.P. loop, definimos o termo $s = l(u_1,...,u_k)$ de tal forma que $s = e$ se $k = 0$, e $s = u_1 l(u_2,...,u_k)$ se $k \geq 1$, similarmente, $r(u_1,...,u_k) = e$ se $k = 0$ e $r(u_1,..,u_{k-1})u_k$ se $k \geq 1$.

Definição 3.29 $(G,\cdot)$ é dito um semigrupo se, e somente se, a operação de $(G,\cdot)$ é associativa.

Teorema 3.30 *Seja M um loop de Moufang gerado por um conjunto X tal que $l(x_1,..,x_k) = r(x_1,...,x_k)$ para todas as sequências finitas $x_1,...,x_k$ em $X^{\pm}$. Então M é um grupo.*

Demonstração: Primeiramento mostremos por indução em n, que vale a igualdade $l(u_1,...,u_n)\cdot l(v_1,...,v_m) = l(u_1,...,u_n,v_1,...,v_m)$ para todo $u_1,..,u_n,v_1,...,v_m \in X^{\pm}$. Os casos $n \leq 1$ é claramente válido. Assuma que $n \geq 2$, e tome $x = u_1$, $s = l(u_2,...,u_n)$ e também $t = (v_1,...,v_m)$.

Expresse $xs\cdot t$ por $xs\cdot(tx^{-1}\cdot x) = x(s\cdot tx^{-1})x$. Porém obtemos a seguinte igualdade $tx^{-1} = r(v_1,...,v_m)x^{-1} = r(v_1,...,v_m,x^{-1}) = l(v_1,...,v_m,x^{-1})$, e então, pela hipótese de indução:

$$\begin{aligned} xs\cdot t &= x(sl(v_1,...,v_m,x^{-1}))x \\ &= xl(u_2,...,u_n,v_1,...,v_m,x^{-1})x \\ &= x(r(u_2,...,u_n,v_1,...,v_m)x^{-1})x \\ &= xl(u_2,...,u_n,v_1,...,v_m) \\ &= l(u_1,u_2,...,u_n,v_1,...,v_m). \end{aligned}$$

Tome $a = l(u_1,...,u_n)$, $b = l(v_1,...,v_m)$ e $c = l(w_1,...,w_p)$. A igualdade provada deixa claro que $ab\cdot c$ e $a\cdot bc$ são iguais a $l(u_1,...,u_n,v_1,...,v_m,w_1,...,w_p)$.

Logo $S = \{l(u_1,...,u_n) \mid u_1,...,u_n \in X^{\pm}\}$ é um subsemigrupo de M que é gerado por $X^{\pm}$. O semigrupo S é um grupo já que todos os elementos geradores possuem inverso. Como $X \subseteq X^{\pm}$, segue quer $X \subseteq S$, e logo $M = \langle X\rangle \subseteq M$, concluindo $S = M$ e terminado a prova. □

Uma notação que usarei adiante é a seguinte: dado um conjunto A com α e β bijeções de A, denotarei $[\alpha,\beta] = \beta\alpha\beta^{-1}\alpha^{-1}$.

Teorema 3.31 *Sejam x e y elementos de um loop de Moufang M. Então $L_yL_xL_{xy}^{-1} = [R_x^{-1},L_y]$ e $R_yR_xR_{yx}^{-1} = [L_x^{-1},R_y]$.*

Demonstração: Primeiro observamos que $R_{yx}^{-1}R_xR_y = [L_x^{-1}, R_y]$ é equivalente a igualdade $L_xR_xL_y = L_{xy}R_x$, que é uma expressão da (IMC) $x(yz\cdot x) = xy\cdot zx$.

Agora observe que $R_yR_xR_{yx}^{-1} = [L_x^{-1}, R_y]$ é equivalente a $R_yL_xR_x = L_xR_{yx}$, que é uma expressão da (IMC) $(x\cdot yz)x = xz\cdot yx$. □

Teorema 3.32 *Seja M loop de Moufang. Suponha que $\alpha = [R_x, L_y]^{\pm}$ onde $x, y \in M$ ou que $\alpha = L_{x_1}^{\epsilon_1}...L_{x_n}^{\epsilon_n}$ onde $x_1, ..., x_n \in M$ e $\epsilon_1, ..., \epsilon_n \in \{-1, 1\}$. Então existem β e γ tais quer (α, β, γ) é um autotopismo de M.*

Demonstração: Temos $R_x = R_{x^{-1}}^{-1}$, então do **Teorema 3.31** é suficiente mostrar o enunciado somente para o caso $\alpha = L_{x_1}^{\epsilon_1}...L_{x_n}^{\epsilon_n}$. A identidade de Moufang $xy\cdot zx = x(yz\cdot x)$ nos diz que (L_x, R_x, L_xR_x) é um autotopismo para todo $x \in M$. O autotopismo procurado (α, β, γ) pode então ser obtido pela composição dos autotopismos $(L_{x_i}, R_{x_i}, L_{x_i}R_{x_i})^{\epsilon_i}$ com $1 \leq i \leq n$. □

Teorema 3.33 *Seja M um loop de Moufang com elemento identidade e gerado por $\{x, y, z\}$. Se $x\cdot yz = xy\cdot z$, então $u_0\cdot l(u_1, ..., u_k)u_{k+1} = u_0l(u_1, ..., u_k)\cdot u_{k+1}$ e $l(u_0, ..., u_{k+1}) = r(u_0, ..., u_{k+1})$ para qualquer sequência $u_0, ..., u_{k+1}$ de elementos de $X^{\pm}$, $k \geq 1$.*

Demonstração: Existem duas igualdades a serem provadas. Procederemos com uma indução em k. O caso $k = 1$ segue da hipótese e do **Teorema 3.19**. No passo de indução consideremos as igualdade:

$$u_0 \cdot l(u_1, ..., u_k)u_{k+1} = u_0l(u_1, ..., u_k) \cdot u_{k+1}$$

O caso $u_0 = u_{k+1}^{\pm}$ segue do **Teorema 3.19** e da identidade flexivel. Podemos então dizer quer $u_0 = x$ e $u_{k+1} = y$.

Tome $s = l(u_2, ..., u_k)$. Queremos mostrar que $x(u_1s\cdot y) = (x\cdot u_1s)y$. Se $u_1 = x^{-1}$, então é equivalente a $x^{-1}s\cdot y = x^{-1}\cdot sy$, que segue por hipótese de indução. Trocando x por x^{-1} temos $x^{-1}(xs\cdot y) = (x^{-1}\cdot xs)y$, logo pelo **Teorema 3.19** $x(xs\cdot y) = (x\cdot xs)y$, resolvendo o caso $u_1 = x^{\pm}$.

Por hipótese de indução, $xs\cdot y = x\cdot sy$. Portanto $xy\cdot s = x\cdot sy$ pelo **Teorema 3.19** e $(x\cdot ys)y = (xy\cdot s)y = x(ys\cdot y)$ pela (IMD), oque nos da o caso $u_1 = y$. Pelo **Teorema 3.19**, $(x\cdot ys)y^{-1} = x(ys\cdot y^{-1})$, trocando y por y^{-1}, temos $(x\cdot y^{-1}s)y = x(y^{-1}s\cdot y)$. O que nos da o caso $u_1 = y^{\pm}$.

Tome $r = r(u_1, ..., u_{k-1})$. Queremos mostrar quer $x(ru_k\cdot y) = (x\cdot ru_k)y$. Se $u_k = y^{-1}$, então é equivalente a $xr\cdot y^{-1} = x\cdot ry^{-1}$, que segue por hipótese de indução. Trocando y por y^{-1} temos $x(ry\cdot y^{-1}) = (x\cdot ry)y^{-1}$, logo pelo **Teorema 3.19** $x(yr\cdot y) = (x\cdot yr)y$, resolvendo o caso $u_k = y^{\pm}$.

Por hipótese de indução, $xr\cdot y = x\cdot ry$. Portanto $rx\cdot y = r\cdot xy$ pelo **Teorema 3.19** e $x(rx\cdot y) = x(r\cdot xy) = (x\cdot yr)y$ pela (IME), oque nos da o caso $u_k = x$. Pelo **Teorema 3.19**,

$x^{-1}(rx \cdot y) = (x^{-1} \cdot rx)y$, trocando x por x^{-1}, temos $x(rx^{-1} \cdot y) = (x \cdot rx^{-1})y$. O que nos da o caso $u_k = x^{\pm}$.

Restam os casos $u_1 = z^{\pm}$ e $u_k = z^{\pm}$, tome $w = l(u_2, ..., u_{k-1})$.

Para o caso $u_1 = z = u_k$, precisamos mostrar que $x(zwz) \cdot y = x \cdot (zwz)y$, isto é, que $(zwz)[L_x, R_y] = zwz$. A hipótese de indução nos dá $w[L_x, R_y] = w$, temos $e[L_x, R_y] = e$ e $z[L_x, R_y] = z$,então pelo **Teorema 3.27** e o **Teorema 3.32** segue que $(zwz)[L_x, R_y] = zwz$ (Note que $[L_x, R_y] = [R_y, L_x]^{-1}$).

O caso $u_1 = z^{-1} = u_2$ é análogo ao anterior já que $z^{-1}[L_x, R_y] = z^{-1}$, então segue do **Teorema 3.27** e do **Teorema 3.32** que $(z^{-1}wz^{-1})[L_x, R_y] = z^{-1}wz^{-1}$.

Para o caso $u_1 = z$ e $u_k = z^{-1}$, precisamos mostrar que $x(zwz^{-1}) \cdot y = x \cdot (zwz^{-1})y$, isto é, que $(z^{-1})\alpha_1 = z^{-1}$ onde $\alpha_1 = L_w L_z [R_y, L_x] L_z^{-1} L_w^{-1}$. Pela hipótese de indução $x(zw \cdot y) = (x \cdot zw)y$, logo $e\alpha_1 = e$. A igualdade já provado $x(zwz \cdot y) = (x \cdot zwz)y$ pode ser expressa por $z\alpha_1 = z$. Pelo **Teorema 3.32** existem β_1 e γ_1 tais que $(\alpha_1, \beta_1, \gamma_1)$ é um autotopismo de M. Então $(z^{-1})\alpha_1 = z^{-1}$ segue já que $z\alpha_1 = z$ e $e\alpha_1 = e$ através do **Teorema 3.26**.

Para o caso $u_1 = z^{-1}$ e $u_k = z$, precisamos mostrar que $x(z^{-1}wz) \cdot y = x \cdot (z^{-1}wz)y$, isto é, que $(z)\alpha_2 = z$ onde $\alpha_2 = L_w L_z^{-1} [R_y, L_x] L_z L_w^{-1}$. Pela hipótese de indução $x(z^{-1}w \cdot y) = (x \cdot z^{-1}w)y$, logo $e\alpha_2 = e$. A igualdade já provado $x(z^{-1}wz^{-1} \cdot y) = (x \cdot z^{-1}wz^{-1})y$ pode ser expressa por $z^{-1}\alpha_2 = z^{-1}$. Pelo **Teorema 3.32** existem β_2 e γ_2 tais que $(\alpha_2, \beta_2, \gamma_2)$ é um autotopismo de M. Então $z\alpha_2 = z$ segue já que $(z^{-1})\alpha_2 = z^{-1}$ e $e\alpha_2 = e$ através do **Teorema 3.26**.

Para terminar o passo indutivo observe que:

$$\begin{aligned} l(u_0, ..., u_{k+1}) &= u_0 l(u_1, ..., u_{k+1}) \\ &= u_0 \cdot r(u_1, ..., u_k)u_{k+1} \\ &= u_0 \cdot l(u_1, ..., u_k)u_{k+1} \\ &= u_0 l(u_1, ..., u_k) \cdot u_{k+1} \\ &= l(u_0, ..., u_k)u_{k+1} \\ &= r(u_0, ..., u_k)u_{k+1} \\ &= r(u_0, ..., u_{k+1}). \end{aligned}$$

□

Demonstração: (Teorema de Moufang) É consequência direta do **Teorema 3.30** junto com o **Teorema 3.33**. □

Referências Bibliográficas

[1] R. H. Bruck; *Survey of Binary Systems*, Terceira Edição, Springer, 1971.

[2] R.H.Bruck, *Contributions to the theory of loops*, Trans.Amer.Math.Soc.,**60** (1946) 245-354.

[3] A. Drápal; *A simplified proof of Moufang's theorem*, Proc. Amer. Math. Soc., 139 : 93 – 98, 2010

[4] E. G. Goodaire, E. Jespers, C. P. Milies; *Alternative Loops Rings*, Elsevier Science B.V., 1996.

[5] R. Moufang; *Zur Structur Von Alternativ Korpern*, Math Ann., 110 : 416 – 430, 1935.

[6] H. O. Pflugfelder , *Quasigroups and loops: Introduction*, Sigma Series in Pure Math. **7**, Heldermann Verlag, Berlin,1990.

[7] H. O. Pflugfelder, *Historical notes on loop theory*, Comment. Math. Univ. Carolinae, **41**-**2** 359 – 370, 2000.

[8] W. R. Scott; *Half-homomorphisms of Groups*, Proc. Amer. Math. Soc., 8 : 1141 – 1144, 1957.

[9] R. Artzy; *On loops with a special property*, Proc. Amer. Math. Soc. 6(1955), 480 – 492. MR. 16 (1955), p. 1083.