TEOREMAS DE SYLOW PARA LOOPS DE MOUFANG

Pedro Paulo Abel Balbo

DISSERTAÇÃO APRESENTADA À UNIVERSIDADE FEDERAL DO ABC PARA A DEFESA DE DISSERTAÇÃO DO MESTRADO EM MATEMÁTICA APLICADA

Programa: Mestrado em matemática aplicada
Orientadora: Profª Drª Maria de Lourdes Merlini Giuliani

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro do CNPq

Santo André, maio de 2016

Pedro Paulo Abel Balbo

TEOREMAS DE SYLOW PARA LOOPS DE MOUFANG

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do ABC, como requisito parcial à obtenção do título de Mestre em Matemática. Linha de pesquisa: Álgebra.

Orientadora: Profª Drª Maria de Lourdes Merlini Giuliani.

Santo André – SP

2016

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

Balbo, Pedro Paulo Abel
Teoremas de Sylow para loops de Moufang / Pedro Paulo Abel Balbo. — 2016.

47 fls.

Orientadora: Maria de Lourdes Merlini Giuliani

Dissertação (Mestrado) — Universidade Federal do ABC, Programa de Pós-Graduação em Matemática, Santo André, 2016.

1. Teoremas de Sylow. 2. Loops de Moufang. 3. Loops de Chein. 4. Loops de Paige. 5. Estruturas Hexagonais. I. Giuliani, Maria de Lourdes Merlini. II. Programa de Pós-Graduação em Matemática, 2016. III. Título.

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

Santo André, 26 **de** MAIO **de 20**16**.**

Assinatura do autor: _____

Assinatura do orientador: _____

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Programa de Pós-Graduação em Matemática
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017
ppg.matematica@ufabc.edu.br

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Pedro Paulo Abel Balbo, realizada em 28 de abril de 2016:

Prof.(a) Dr.(a) **Maria de Lourdes Merlini Giuliani** (UFABC) – Presidente

Prof.(a) Dr.(a) **Francisco Cesar Polcino Milies** (UFABC) – Membro Titular

Prof.(a) Dr.(a) **Raul Antonio Ferraz** (USP) – Membro Titular

Prof.(a) Dr.(a) **Nazar Arakelian** (UFABC) – Membro Suplente

Prof.(a) Dr.(a) **Alegria Gladys Chalom** (USP) – Membro Suplente

Resumo

Neste trabalho foram abordados os Teoremas de Sylow para loops de Moufang finitos. A validade destes teoremas no contexto não associativo não ocorre de maneira direta uma vez que o menor loop de Moufang finito simples tem ordem 120 e não possui subloop de ordem 5. Foi analisada a aplicação destes teoremas para duas categorias de loops de Moufang de ordem par: os loops de Chein e os loops de Paige. Para os loops de Chein vemos que dois subloops de Sylow são conjugados. Para os loops de Paige $P(q)$ verificamos a existência e o número de p-subloops de Sylow.

Palavras-chave: Teoremas de Sylow, loops de Moufang, loops de Chein, loops de Paige, linhas hexagonais, estruturas hexagonais

Abstract

In this work Sylow's theorems for finite Moufang loops were investigated. The validity of these theorems in a non-associative context does not occur directly as the smallest simple finite Moufang loop has order 120 and contains no subloop of order 5. We analyzed the application of these theorems for two categories of Moufang loops of even order: Chein loops and Paige loops. For Chein loops we can see that any two Sylow's subloops are always conjugated. For Paige loops $P(q)$ we verified the existence of p-Sylow subloops and studied their number.

Keywords: Sylow's theorems, Moufang loops, Chein loops, Paige loops, hexagon lines, hexagon structures.

Lista de Símbolos

$\|G\|$	Número de elementos do conjunto G.
$o(x)$	Ordem do elemento x.
$H \leq G$	H é subgrupo (ou subloop) de G.
$H < G$	H é subgrupo (ou subloop) próprio de G.
$Syl_p(G)$	Conjunto de todos os p-subgrupos de Sylow de G.
$(G : H)$	Número de classes laterais de H em G.
$\langle x \rangle$	Grupo gerado pelo elemento x.
G/H	Quociente de G por H.
$M_{2n}(G, 2)$	Loops de Chein obtido a partir do grupo G.
$\mathbb{O}(F)$	Álgebra de Zorn sobre o corpo F.
$G \times H$	Produto cartesiano do conjunto G pelo conjunto H.
F^n	Produto cartesiano do conjunto F por ele mesmo (n vezes).
$u \times v$	Produto escalar entre os vetores u e v.
$det(x)$	Determinante do elemento x.
G^*	Conjunto de todos os elementos inversíveis de G.
$SLL(F)$	Loop linear geral sobre o corpo F.
$Z(G)$	Centro do grupo (ou loop) G.
$PSLL(F)$	Loop projetivo linear sobre o corpo F.
F_q	Corpo F com q elementos.
$a \mid b$	a divide b.
$a \nmid b$	a não divide b.
$P(q)$	Loop de Paige sobre um corpo com q elementos.
$U^\perp$	Subespaço ortogonal a U.
$stab(U)$	Estabilizador do subespaço U.
$(x \mid y)$	Forma bilinear entre x e y.

Conteúdo

Introdução

Os teoremas de Sylow representam um dos pontos altos da teoria dos grupos finitos, unindo ideias simples para provar resultados complexos e surpreendentes. O primeiro deles dá uma recíproca parcial do teorema de Lagrange, ou seja se G é um grupo finito de ordem n e m é a maior potência de um número primo p que divide n então G possui um subgrupo H cuja ordem é m. Estes são chamados p-subgrupos de Sylow. Além disso eles nos permitem calcular quantos são os tais subgrupos e em alguns casos se G possui subgrupo normal não trivial.

A teoria de loops é relativamente jovem em comparação com outros ramos da matemática. Um loop pode ser entendido como um "grupo não associativo". Mas a teoria de loops não é exatamente uma generalização da teoria de grupos. Ela é usada basicamente em quatro áreas: álgebra, geometria, topologia e combinatória. Um loop é um conjunto não vazio L com uma operação binária $(\cdot)$, que possui elemento identidade 1, e tal que a equação $x \cdot y = z$ possui uma única solução sempre que dois dos três elementos são conhecidos.

Um *loop de Moufang* é um loop que satisfaz a identidade de Moufang

$$x((yz)x) = (xy)(zx).$$

Os loops de Moufang são diassociativos, ou seja, um subloop gerado por dois elementos é um grupo.

Como o teorema de Lagrange vale para loops de Moufang finitos faz sentido falar em p-subloops de Sylow para essa categoria de loops. No entanto temos um obstáculo imediato para o análogo ao 1º teorema de Sylow para loops de Moufang, desde que o menor loop de Moufang simples tem ordem 120 e não possui um subloop de ordem 5. Para loops de Moufang de ordem ímpar, Glaubermann [13] mostrou que este resultado é válido (teorema 1.20).

Posteriormente Fenyves [3] mostrou que, para p um primo ímpar, os teoremas de Sylow são válidos para a categoria de Extra loops finitos. Sua prova se baseou no seguinte fato: "se L é um extra loop então para todo $x \in L$, x^2 está no núcleo de L".

Grishkov e Zavarnitsine [15] estabeleceram que se K é um loop de Moufang finito, a existência de um p-subloop de K está relacionada a existência de um S-subgrupo invariante de um corresponde grupo G com trialidade. Infelizmente não é possivel garantir a existência de um p-subloop de Sylow S invariante de G.

Neste trabalho investigamos os teoremas de Sylow para loops de Moufang sob a luz dos trabalhos de Stephen Gagola III. Nossa escolha deste autor se baseou no fato de que este apresenta, de forma clara, o mais amplo e completo estudo deste tema na categoria dos loops de Moufang, fazendo uso de ferramentas não tradicionais, como por exemplo as estrutura hexagonais.

O trabalho foi dividido em 3 capítulos. No primeiro apresentamos os teoremas de Sylow para grupos finitos, os conceitos básicos da teoria de loops e seus principais resultados.

No segundo capítulo foi apresentado duas categorias de loops de Moufang de ordem par: os loops de Chein e os loops de Paige. A classe dos loops de Chein representa uma porção significativa dos loops de Moufang não associativos e foram definidos por Orin Chein em 1974 [1]. A construção desses loops tem como ponto de partida um grupo não abeliano em um processo similar à obtenção dos grupos diedrais à partir de um grupo cíclico. Na análise dos loops de Chein, investigamos o 2^o teorema de Sylow. Constatamos que no caso $p \neq 2$, qualquer p-subloop de Sylow de um loop de Chein, é também um p-subgrupo de Sylow e com isso, todos os teoremas de Sylow são satisfeitos. Além disso, desenvolvemos uma ferramenta para mostrar que todos os p-subloops de Sylow de loops de Chein são conjugados entre si no caso $p = 2$.

Outra categoria dos loops de Moufang relevantes são os loops de Paige. Estes surgem naturalmente como o loop multiplicativo dos elementos inversíveis da álgebra dos octônios, conhecida como álgebra de Cayley-Dickson split. Em 1956, Paige mostrou que esses são loops simples. Bannai e Song denotaram esses loops por "Paige loops". Posteriormente Liebeck provou que qualquer loop de Moufang não associativo finito simples é isomorfo ao loop de Paige.

No terceiro capítulo introduzimos o conceito de estruturas hexagonais, com ênfase em linhas hexagonais. Conceito este necessário para analisarmos a existência de p-subloops de Sylow em $P(q)$ quando $p \equiv 1\,(mod\,4)$ e também a quantidade de p-subloops de Sylow em $P(q)$ quando $p \equiv 3\,(mod\,4)$.

1 Conceitos Básicos

Assumimos que o leitor está familiarizado com conceitos básicos de teoria elementar de grupos. Assim, neste primeiro capítulo explicitaremos apenas as principais definições e resultados para fixar a notação.

1.1 Teoremas de Sylow

Definição 1.1. *Dado G um grupo finito, dizemos que P é um p-subgrupo de G, com p primo, se $|P| = p^n$ para algum $n \in \mathbb{N}$.*

O 1º Teorema de Sylow nos garante a existência de p-subgrupos em G:

Teorema 1.2. *(1º Sylow) Seja G um grupo finito cuja ordem é $|G| = p^m b$, com p primo e $mdc(b, p) = 1$. Então existe um subgrupo P de G tal que $|P| = p^n$, para qualquer $n \leq m$.*

Em particular, se a ordem de P é a maior potência possível de p em G, isto é, $|P| = p^m$, dizemos que P é um *p-subgrupo de Sylow de G*. Denotaremos o conjunto de todos os p-subgrupo de Sylow de G por $Syl_p(G)$. O 2º Teorema de Sylow mostra que os p-subgrupos de Sylow são conjugados.

Teorema 1.3. *(2º Sylow) Sejam G um grupo finito cuja ordem é $|G| = p^m b$, com p primo e $mdc(b, p) = 1$ e P um p-subgrupo de G. Então são válidos:*

1. *Existe $S \in Syl_p(G)$ tal que $P \subset S$.*
2. *Todos os p-subgrupo de Sylow de G são conjugados entre si.*

Corolário 1.4. *Seja $S \in Syl_p(G)$ e n_p o número de p-subgrupos de Sylow de G, então $n_p = (G : N(S))$.*

Uma consequência deste teorema é que S é o único p-subgrupo de Sylow de G se e somente se S é um subgrupo normal em G. Além disso, se $P \subset S$, então P é um

subgrupo de S. Finalmente, sabemos que os p-subgrupo de Sylow existem e que são únicos, a menos de conjugação. O 3º Teorema de Sylow propõe uma contagem para estes subgrupos.

Teorema 1.5. *(3º Sylow) Sejam G um grupo finito tal que $|G| = p^m b$, com p primo e $mdc(p, b) = 1$ e n_p o número de p-subgrupo de Sylow de G então:*

1. *n_p divide b*
2. *$n_p \equiv 1 (mod\, p)$*

1.2 Loops de Moufang

Definição 1.6. *Um conjunto não vazio L junto com uma operação binária $\cdot$ é chamado de quasigrupo se as equações*

$$a \cdot x = b$$

$$y \cdot a = b$$

têm solução única para quaisquer $a, b \in L$.

A partir daqui omitiremos $\cdot$, como de costume, e escreveremos apenas $ax = b$ ou $ya = b$.

O menor quasigrupo não associativo tem ordem 3 e sua tabela de multiplicação é dada por:

$\cdot$	1	2	3
1	2	1	3
2	1	3	2
3	3	2	1

Note que este quasigrupo não possui elemento neutro 1 e não é associativo.

Definição 1.7. *Um quasigrupo L recebe o nome de Loop se possui elemento neutro 1 tal que $x1 = 1x = x$, para qualquer $x \in L$.*

Definição 1.8. *Seja L_1 um subconjunto não vazio de um loop L. Dizemos que L_1 é um subloop de L se L_1 é um loop com a operação induzida por L.*

Considere L um loop e $x \in L$, o *inverso à esquerda de x* é o único elemento x^λ que satisfaz $x^\lambda x = 1$. Similarmente, o *inverso à direita de x* é o único elemento x^ρ tal que

$xx^\rho = 1$. Em geral, x^λ e x^ρ não são iguais, porém, quando isso acontece, denotamos $x^\lambda = x^\rho = x^{-1}$ e chamamos x^{-1} de *inverso bilateral de* x, ou apenas inverso de x.

Definição 1.9. *Um loop L possui a propriedade inversa, ou PI, se todo elemento $x \in L$ possui inverso bilateral x^{-1}, e satisfaz:*

$$x^{-1}(xy) = y \tag{1.1}$$

$$(yx)x^{-1} = y \tag{1.2}$$

Definição 1.10. *Um loop L é chamado de alternativo se satisfaz as leis alternativas, ou seja, para quaisquer $x, y \in L$, são válidas as propriedades:*

$$x(xy) = x^2y \tag{1.3}$$

$$(yx)x = yx^2 \tag{1.4}$$

Definição 1.11. *Um loop L é chamado de flexível se satisfaz a lei flexível, isto é, para quaisquer $x, y \in L$, é válida a propriedade:*

$$(xy)x = x(yx) \tag{1.5}$$

Definição 1.12. *Dizemos que L é um loop de Moufang se satisfaz as identidades de Moufang:*

$$(xy)(zx) = (x(yz))x \tag{1.6}$$

$$((xy)x)z = x(y(xz)) \tag{1.7}$$

$$((xy)z)y = x(y(zy)) \tag{1.8}$$

Lema 1.13. *Em um loop de Moufang L, qualquer elemento $x \in L$ possui inverso bilateral x^{-1}.*

Demonstração. Sejam y^λ, y^ρ os inversos de $y \in L$ à esquerda e à direita, respectivamente. Mostremos que $y^\lambda = y^\rho$. Substituindo x por y^λ e z por y^ρ na equação 1.6, ficamos com $(y^\lambda y)(y^\rho y^\lambda) = (y^\lambda(yy^\rho))y^\lambda$. Por outro lado, $(y^\lambda y)(y^\rho y^\lambda) = (y^\rho y^\lambda)$ e portanto $y^\rho = y^\lambda(yy^\rho)$. Daí:

$$y^\lambda = y^\lambda 1 = y^\lambda(yy^\rho) = y^\rho$$

□

Teorema 1.14. *As Identidades de Moufang (1.6, 1.7 e 1.8) são equivalentes.*

Demonstração. (1.8 $\Rightarrow$ 1.7) Já vimos que todo elemento de um loop de Moufang possui inverso bilateral, então substituindo em 1.8 cada elemento pelo seu inverso:

$$\begin{aligned}((xy)z)y = x(y(zy)) \longrightarrow &((x^{-1}y^{-1})z^{-1})y^{-1} = x^{-1}(y^{-1}(z^{-1}y^{-1}))\\ &((yx)^{-1}z^{-1})y^{-1} = x^{-1}(y^{-1}(yz)^{-1})\\ &(z(yx))^{-1}y^{-1} = x^{-1}((yz)y)^{-1}\\ &(y(z(yx)))^{-1} = (((yz)y)x)^{-1}\\ &y(z(yx)) = ((yz)y)x\end{aligned}$$

Agora substitua nesta última equação $z \longrightarrow y \longrightarrow x \longrightarrow z$ e teremos

$$x(y(xz)) = ((xy)x)z$$

que é precisamente a equação 1.7. Se repetirmos o mesmo processo, encontraremos também 1.7 $\Leftrightarrow$ 1.8, ou seja, 1.7 e 1.8 são equivalentes.
(1.7 $\Rightarrow$ 1.6) Substituindo $z \longrightarrow x^{-1}z$ na equação 1.7, encontramos

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

Multiplicando a última igualdade por x à direita:

$$\begin{aligned}(x(yz))x &= (((xy)x)(x^{-1}z))x\\ &\overset{1.8}{=} (xy)(x((x^{-1}z)x))\\ &= (xy)((x(x^{-1}z))x)\\ &= (xy)(zx)\end{aligned}$$

(1.6 $\Rightarrow$ 1.8) Finalmente, considere válida a propriedade 1.6. Ou seja,

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

Substituindo o elemento y pelo seu inverso:

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

Agora $z \longrightarrow yz$:

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

Por fim, considere $y \longrightarrow yx$:

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

Ou seja, $((yx)z)x = y(x(zx))$ e portanto 1.8 é válida. □

Lema 1.15. *Todo loop de Moufang L é um PI-loop.*

Demonstração. Seja $x = y^{-1}z \in L$, então:

$$x = y^{-1}z = ((y^{-1}y)y^{-1})z \overset{1.7}{=} y^{-1}(y(y^{-1}z)) = y^{-1}(yx)$$

Portanto vale a propriedade 1.1. Analogamente, considere $z = xy$, então:

$$z = xy = x(y(xx^{-1})) \overset{1.7}{=} ((xy)x)x^{-1} = (zx)x^{-1}$$

Logo, vale 1.2. □

Lema 1.16. *Todo loop de Moufang L é um loop alternativo.*

Demonstração. Sejam $x, y, z \in L$. Temos

$$x(xz) = x(1(xz)) \overset{1.7}{=} ((x1)x)z = x^2z$$

Por outro lado,

$$(xy)y = ((xy)1)y \overset{1.8}{=} x(y(1y)) = xy^2$$

Portanto valem 1.4 e 1.3 □

Lema 1.17. *Todo loop de Moufang L é um loop flexível.*

Demonstração. Considere $x, y \in L$. Temos

$$(xy)x = ((xy)x)1 \overset{1.7}{=} x(y(x1)) = x(yx)$$

□

As identidades de Moufang são uma aproximação da propriedade associativa e com isso, muitas das propriedades válidas para grupo também são válidas para loops de

Moufang, como por exemplo o Teorema de Lagrange [5] e [15]. Isto é, dado um loop L e um subloop L_1 de L, então $|L_1|$ divide $|L|$.

Definição 1.18. *Dado um loop de Moufang L, dizemos que P é um p-subloop de L se $|P| = p^n$ para algum $n \in \mathbb{N}$. Além disso, se n é a maior potência de p em L, então P é chamado de p-subloop de Sylow de L.*

Lema 1.19. *Um loop de Moufang L é um p-loop se, e somente se, a ordem de cada elemento de L é potência de p.*

Demonstração. ($\Longrightarrow$) Sejam $|L| = p^n$, $x \in L$ e considere o subloop $H = \langle x \rangle$. Então $|H| = |\langle x \rangle| = |x|$. Pelo teorema de Lagrange, temos que $|x| = |H|$ divide $|L| = p^n$, ou seja, $|x|$ divide p^n. Portanto $|x| = p^k$, com $k \leq n$.
($\Longleftarrow$) Suponha que exista um loop de Moufang finito que não é um p-loop mas que todos os seus elementos têm ordem potência de p. Seja L um tal loop de menor ordem. Como todo loop de Moufang finito simples é um loop de Paige $P(q)$ cuja ordem é $\frac{q^3(q^4-1)}{mdc(q+1,2)}$ [17], onde q é a ordem do corpo F_q (ver seção 2.2), temos que L não é simples uma vez que todos seus elementos tem ordem potência de p. Assim L possui um subloop normal não trivial N. Pela minimalidade da ordem de L, ambos $|N|$ e $|L/N|$ possui ordem potência de p.
Mas $|L| = |N|.|L/N|$ o que implica que L tem ordem potência de p contradizendo nossa hipótese. □

Em um loop de Moufang L, podemos definir duas funções bijetoras, chamadas de *translações*, à esquerda e à direita de $x \in L$, e são dadas por:

$$xL(y) = yx$$

$$xR(y) = xy$$

para qualquer elemento $y \in L$. Com essas duas translações, definimos por *conjugação de x por y* a composição

$$T(y) = R(y)L(y^{-1})$$

Ou seja, $xT(y) = y^{-1}xy$. Assim, dizemos que dois subloops, L_1 e L_2 são *conjugados em* L se existem elementos $y_1, ..., y_n \in L$ tais que

$$L_1 = L_2T(y_1)...T(y_n)$$

Encerramos enunciando um teorema de Glauberman, cuja demonstração pode ser encontrada em [13]:

Teorema 1.20. *[13] Sejam L um loop de Moufang de ordem ímpar e K um p-subloop de L. Então K está contido em algum p-subloop de Sylow de L.*

Este teorema nos garante que o primeiro item do 2º teorema de Sylow é válido para loops de Moufang de ordem ímpar. No próximo capítulo estudaremos dois exemplos importantes de loops de Moufang: os loops de Chein e de Paige, cuja ordem, em ambos os casos, é sempre par.

2 Dois importantes loops de Moufang

2.1 Loops de Chein

Considere um grupo finito G, um elemento $u \notin G$ de ordem 2 e defina o conjunto L por

$$L = G \cup Gu$$

Neste conjunto, definimos a operação induzida por G da seguinte forma:

$$g_1(g_2u) = (g_2g_1)u \tag{2.1}$$

$$(g_1u)g_2 = (g_1g_2^{-1})u \tag{2.2}$$

$$(g_1u)(g_2u) = g_2^{-1}g_1 \tag{2.3}$$

para quaisquer elementos $g_1, g_2 \in G$.

Lema 2.1. *O conjunto $L = G \cup Gu$ com a operação definida acima é um loop de Moufang.*

Demonstração. Provaremos que a propriedade 1.6 está satisfeita para quaisquer $x, y, z \in L$. Para isso, dividiremos em 8 casos:

1. Se $x, y, z \in G$, é trivial.

2. Se $x, y \in G$ e $z \in Gu$:

$$(xy)((zu)x) = (xy)((zx^{-1})u) = (zx^{-1}xy)u = (zy)u = (zyxx^{-1})u = ((zyx)u)x = (x((zy)u))x = (x(y(zu)))x$$

3. Se $x, z \in G$ e $y \in Gu$:

$$(x(yu))(zx) = ((yx)u)(zx) = ((yx)(zx)^{-1})u = (yz^{-1})u = (yz^{-1}xx^{-1})u = ((yz^{-1}x)u)x = (x((yz^{-1})u))x = (x((yu)z))x$$

4. Se $y, z \in G$ e $x \in Gu$:

$$((xu)y)(z(xu)) = ((xy^{-1})u)((xz)u) = (xz)^{-1}(xy^{-1}) = z^{-1}y^{-1} = x^{-1}xz^{-1}y^{-1} = ((x(yz)^{-1})u)(xu) = ((xu)(yz))(xu)$$

5. Se $x \in G$ e $y, z \in Gu$:

$$(x(yu))((zu)x) = ((yx)u)((zx^{-1})u) = (zx^{-1})^{-1}(yx) = xz^{-1}yx = (x(z^{-1}y))x = (x((yu)(zu)))x$$

6. Se $y \in G$ e $x, z \in Gu$:

$$((xu)y)((zu)(xu)) = ((xy^{-1})u)(x^{-1}z) = ((xy^{-1})(x^{-1}z)^{-1})u = (xy^{-1}z^{-1}x)u = ((zy)^{-1}x)(xu) = ((xu)((zy)u))(xu) = ((xu)(y(zu)))(xu)$$

7. Se $z \in G$ e $x, y \in Gu$:

$$((xu)(yu))(z(xu)) = (y^{-1}x)((xz)u) = (xzy^{-1}x)u = ((yz^{-1})^{-1}x)(xu) = ((xu)((yz^{-1})u))(xu) = ((xu)((yu)z))(xu)$$

8. Se $x, y, z \in Gu$:

$$((xu)(yu))((zu)(xu)) = (y^{-1}x)(x^{-1}z) = y^{-1}z = x^{-1}xy^{-1}z = ((x(z^{-1}y)^{-1})u)(xu) = ((xu)(z^{-1}y))(xu) = ((xu)((yu)(zu)))(xu)$$

□

Definição 2.2. *O loop $L = G \cup Gu$ é chamado loop de Chein e será denotado por $M_{2n}(G, 2)$.*

É fácil ver que $|L| = 2|G|$.

Exemplo 2.3. *Considere $G = S_3 = \{1, a, a^2, b, ba, ba^2\}$. O loop de Chein é:*

$$M_{12}(S_3, 2) = \{1, a, a^2, b, ba, ba^2, u, au, a^2u, bu, (ba)u, (ba^2)u\}$$

cuja tabela de multiplicação pode ser encontrada no apêndice deste trabalho. O. Chein e H. Pflugfelder provaram em seu artigo "The smallest Moufang loop" que $M_{12}(S_3, 2)$ é o menor (no sentido de menor ordem) loop de Moufang não associativo.

Vamos explorar este loop quanto aos teoremas de Sylow. Existem 9 2-subloop de Sylow de $M_{12}(S_3, 2)$, são eles:

$$S_1 = \{1, b, u, bu\}$$

$$S_2 = \{1, b, au, (ba^2)u\}$$

$$S_3 = \{1, b, a^2u, (ba)u\}$$

$$S_4 = \{1, ba^2, au, (ba)u\}$$

$$S_5 = \{1, ba^2, a^2u, bu\}$$

$$S_6 = \{1, ba^2, u, (ba^2)u\}$$

$$S_7 = \{1, ba, a^2u, (ba^2)u\}$$

$$S_8 = \{1, ba, u, (ba)u\}$$

$$S_9 = \{1, ba, au, bu\}$$

Observe que o número de 2-subloop de Sylow é congruente a 1 módulo 2 embora este número não divide 3. No entanto esses subloops satisfazem a propriedade de conjugação, ou seja todos são conjugados entre si. Mostremos que S_1 e S_4 são conjugados pelo elemento a:

$$1T(a) = a^{-1}1a = 1$$

$$bT(a) = a^{-1}ba = ba^2$$

$$uT(a) = (a^{-1}u)a = au$$

$$(bu)T(a) = a^{-1}(bu)a = (ba)u$$

Lema 2.4. *Seja $L = M_{2n}(G, 2)$ com G finito e p um primo ímpar. Então $S \in Syl_p(G)$ se e somente se $S \in Syl_p(L)$.*

Demonstração. ($\Longrightarrow$) Sejam $S \in Syl_p(G)$ onde $|G| = p^m b$, com $p \neq 2$ e $mdc(b, p) = 1$. Então $|L| = 2|G| = 2p^m b$ e $|S| = p^m$. Logo, $|S|$ é a maior potência possível de p em L, isto é, $S \in Syl_p(L)$.
($\Longleftarrow$) Agora considere $S \in Syl_p(L)$ e suponha que exista $x = gu \in S \backslash G$, então $x^2 = (gu)^2 = g^{-1}g = 1$ e pelo lema 1.19, $x = gu$ pertence a um 2-subloop. Absurdo pois

$p \neq 2$, logo cada p-subloop S possui elementos de ordem diferente de potências de 2, isto é, $x = gu \notin S$. Portanto $S \subseteq G$ e como $|S| = p^m$, temos $S \in Syl_p(G)$. □

Exemplo 2.5. *Seja* $|G| = 36 = 2^2.3^2$ *e* $L = M_{2n}(G, 2)$ *e considere* H, K *subgrupos de* G *tais que*

$$|H| = 3^2 \text{ e } |K| = 2^2$$

Portanto H *é um 3-subgrupo de Sylow de* G *e* K *é um 2-subgrupo de Sylow de* G. *Mas* $|L| = 2|G| = 2^3.3^2$. *Logo* H *é um 3-subloop de Sylow de* L, *mas* K *não é um 2-subloop de Sylow de* L.

Para $p \neq 2$, se escolhermos qualquer S p-subloop de Sylow de L, então S será um p-subgrupo de Sylow de G, e portanto os teoremas de Sylow estão satisfeitos. Em outras palavras, $M_{2n}(G, 2)$ satisfaz os teoremas de Sylow para $p \neq 2$.

Nosso objetivo agora é mostrar que se $L = M_{2n}(G, 2)$ para algum grupo finito G, dados $S_1, S_2 \in Syl_2(L)$, então S_1 e S_2 são conjugados em L. Que nada mais é do que mostrar que a segunda parte do 2º teorema de Sylow vale para loops de Chein.

Observe que, se H é um subgrupo de um grupo G, então $M(H, 2) = H \cup Hu$ é um subloop de $M(G, 2) = G \cup Gu$. Em particular, $M(S, 2) = S \cup Su$ é um 2-subloop de Sylow de $M(G, 2) = G \cup Gu$ se S é um 2-subgrupo de Sylow de G.

Lema 2.6. *Seja* $L = M_{2n}(G, 2)$ *para algum grupo finito* G. *Então* $L_1 \in Syl_2(L)$ *se, e somente se,* $L_1 = S \cup (gS)u$, *para algum* $S \in Syl_2(G)$ *e* $g \in G$.

Demonstração. ($\Longleftarrow$) Seja $|G| = 2^m.b$ com $mdc(2, b) = 1$. Daí $|L| = 2|G| = 2^{m+1}.b$. Quero mostrar então que $|L_1| = 2^{m+1}$. Como $|S| = 2^m$ e gS é uma classe lateral de S, temos também $|gS| = 2^m$, o que segue:

$$|L_1| = |S \cup (gS)u| = |S| + |gS| = 2^m + 2^m = 2^{m+1}$$

Logo $L_1 \in Syl_2(L)$.
($\Longrightarrow$) Seja L_1 um 2−subloop de L. Então:

1. Se $L_1 \cap G = L_1$ então $L_1 \subseteq G$ e portanto L_1 é um subgrupo de G. Pelo 2º teorema de Sylow, existe $S \in Syl_2(G)$ tal que $L_1 \subseteq S$ e portanto L_1 também é subgrupo (e subloop) de S e sabemos que S é subgrupo (e subloop) de $S \cup Su$, portanto

$$L_1 \leq S \cup Su$$

2. Se $L_1 \cap G \neq L_1$, existe $(gu) \in L_1 - G$ para algum $g \in G$. Seja $(hu) \in L_1 - G$, então $(gu)(hu) \in L_1$ e pela regra 2.3, $(gu)(hu) = h^{-1}g \in G$. Logo,

$$(gu)(hu) \in L_1 \cap G$$

Mas $L_1 \cap G$ é subgrupo (e subloop) de G. Usando novamente o 2º teorema de Sylow, existe $S \in Syl_2(G)$ tal que $L_1 \cap G$ é subgrupo de S. Como $(gu) \in L_1 - G$, segue que

$$L_1 \leq S \cup S(gu) \overset{2.1}{=} S \cup (gS)u$$

□

Lema 2.7. *Sejam $S \in Syl_2(G)$ e g um elemento de algum 2-subgrupo de Sylow de G. Então $S \cup Su$ e $S \cup (gS)u$ são conjugados em L.*

Demonstração. Como dois 2-subgrupos de Sylow são conjugados e g pertence a um 2-subgrupo de Sylow de G, existe um elemento $h \in G$ tal que $h^{-1}gh = x \in S$ (ou $g = hxh^{-1}$). Assim:

$$\begin{aligned}
(gS)u &= (hxh^{-1}S)u \\
&= ((hx)h^{-1}Sx)u \\
&= ((hx)h^{-1}Sh^{-1}(hx))u \\
&= (hxh^{-1}Sx)u \\
&\overset{2.1}{=} (hSx)((hx)u) \\
&= (h^{-1}Sh^{-1}hx)((hx)u) \\
&= ((hSh)^{-1}(hx))((hx)u) \\
&\overset{2.3}{=} ((hx)u)((hSh)u)((hx)u) \\
&= ((hx)u)^{-1}((hSh)u)((hx)u) \\
&= ((hSh)u)T((hx)u) \\
&\overset{2.1}{=} ((Sh)(hu))T((hx)u) \\
&\overset{2.3}{=} ((hu)(Su)(hu))T((hx)u) \\
&= ((hu)^{-1}(Su)(hu))T((hx)u) \\
&= (Su)T(hu)T((hx)u)
\end{aligned}$$

Portanto existem $y_1, y_2 \in L\backslash G$ tais que $(gS)u = (Su)T(y_1)T(y_2)$. Além disso,

$$\begin{aligned} S &= (hx)^{-1}(hx)S \\ &\overset{2.3}{=} ((hxS)u)((hx)u) \\ &\overset{2.2}{=} ((hx)u)S((hx)u) \\ &= ((hx)u)^{-1}S((hx)u) \\ &= (h^{-1}hS)T((hx)u) \\ &\overset{2.3}{=} ((hS)u)(hu)T((hx)u) \\ &\overset{2.2}{=} (hu)S(hu)T((hx)u) \\ &= (hu)^{-1}S(hu)T((hx)u) \\ &= ST(hu)T((hx)u) \end{aligned}$$

Ou seja, os mesmos $y_1, y_2 \in L\backslash G$ vistos anteriormente, também são tais que $S = ST(y_1)T(y_2)$. Com isso, temos que:

$$S \cup (gS)u = ST(y_1)T(y_2) \cup (Su)T(y_1)T(y_2) = (S \cup (Su))T(y_1)T(y_2)$$

Então $S \cup (gS)u$ e $S \cup (Su)$ são conjugados em L. □

Corolário 2.8. *Sejam $S \in Syl_2(G)$ e $g \in \langle x \in S_i : S_i \in Syl_2(G)\rangle$. Então $S \cup Su$ e $S \cup (gS)u$ são conjugados em L.*

Lema 2.9. *Sejam $S \in Syl_2(G)$ e $g \in N(S)$. Então $S \cup Su$ e $S \cup (gS)u$ são conjugados em L.*

Demonstração. Inicialmente, observe que se $g \in N(S)$ então $gS = Sg$. Daí $g^2S = g(gS) = g(Sg) = (gS)g = (Sg)g = Sg^2$. Podemos provar por indução em n que $g^nS = Sg^n$ para qualquer $n \in \mathbb{N}$. Seja $|S| = 2^m$ e $k = mdc(2^m, o(g)) = 2^t$ para algum $t \leq m, r$, então existe $k' \in \mathbb{Z}$ tal que $o(g) = k'k$. Considere também $k'' = \frac{k'+1}{2}$. Nessas condições temos $e = g^{o(g)} = g^{k'k} = (g^{k'})^k$, então $|g^{k'}| = k = 2^t$. Como $|g^{k'}|$ é uma

potência de 2, segue que $g^{k'} \in S$ e portanto $g^{k'}S = S$. Agora considere $z = \frac{k'+1}{2}$

$$\begin{aligned}(Su)T(g^z u) &= (g^z u)^{-1}(Su)(g^z u)\\ &= (g^z u)(Su)(g^z u)\\ &\overset{2.3}{=} (Sg^z)(g^z u)\\ &\overset{2.1}{=} (g^z(Sg^z))u\\ &= (g^z(g^z S))u\\ &= (g^{2z}S)u\\ &= (g^{2\frac{k'+1}{2}}S)\\ &= (g^{k'+1}S)u\\ &= (gg^{k'}S)u\\ &= (gS)u\end{aligned}$$

Isto é, existe $y = g^z u \in L\backslash G$ tal que $(gS)u = (Su)T(y)$. E também:

$$\begin{aligned}ST(g^z u) &= (g^z u)^{-1}S(g^z u)\\ &= (g^z u)S(g^z u)\\ &\overset{2.2}{=} ((g^z S)u)(g^z u)\\ &= (g^z)^{-1}g^z S\\ &= S\end{aligned}$$

Portanto, o mesmo $y = g^z u \in L\backslash G$ também é tal que $S = ST(y)$. Logo,

$$S \cup (gS)u = ST(y) \cup (Su)T(y) = (S \cup Su)T(y)$$

Ou seja, $S \cup Su$ e $S \cup (gS)u$ são conjugados em L. □

Proposição 2.10. *Sejam $S \in Syl_2(G)$ e $g \in G$. Então $S \cup Su$ e $S \cup (gS)u$ são conjugados.*

Demonstração. Seja $S' = gSg^{-1} \in Syl_2(G)$. Pelo corolário 1, existe um elemento $c \in \langle x \in S_i : S_i \in Syl_2(G)\rangle$ tal que $S' = c^{-1}Sc$. Então $gSg^{-1} = c^{-1}Sc$, ou seja, $S = x^{-1}Sx$ com $x = cg$. Logo $x \in N(S)$. Assim, $g = c^{-1}x = a_1...a_k x$ onde cada a_i pertence a um 2-subgrupo de Sylow de G, para qualquer $1 \leq i \leq k$. Portanto, pelo lema anterior temos

que existe um elemento $x' \in N(S)$ tal que

$$\begin{aligned}
(gS)u &= (a_1...a_k xS)u \\
&= (a_1...a_k x'Sx')u \\
&= (x'b_1...b_k Sx')u \\
&\overset{2.1}{=} (b_1...b_k Sx')(x'u) \\
&= (S(b_1...b_k)^{-1})^{-1}(x')(x'u) \\
&\overset{2.3}{=} (x'u)((S(b_1...b_k)^{-1})u)(x'u) \\
&= (x'u)^{-1}((S(b_1...b_k)^{-1})u)(x'u) \\
&= ((S(b_1...b_k)^{-1})u)T(x'u) \\
&= ((b_1...b_k S)^{-1}u)T(x'u) \\
&\overset{2.3}{=} u((b_1...b_k S)u)uT(x'u) \\
&= u^{-1}((b_1...b_k S)u)T(x'u) \\
&= ((b_1...b_k S)u)T(u)T(x'u)
\end{aligned}$$

para alguns elementos b_i que estão contidos em algum 2-subgrupo de Sylow de G. Agora, usando novamente o corolário 1, existem elementos $y_1, y_{2k} \in L$ tais que

$$(b_1...b_k S)u = (Su)T(y_1)...T(y_{2k})$$

logo, $(gS)u = ((b_1...b_k S)u)T(u)T(x'u) = (Su)T(y_1)...T(y_{2k})T(u)T(x'u)$. De maneira análoga, concluímos que $S = ST(y_1)...T(y_{2k})T(u)T(x'u)$ e então

$$S \cup (gS)u = ST(y_1)...T(y_{2k})T(u)T(x'u) \cup (Su)T(y_1)...T(y_{2k})T(u)T(x'u) = (S \cup Su)T(y_1)...T(y_{2k})T(u)T(x'u)$$

Portanto $S \cup Su$ é conjugado de $S \cup (gS)u$ em L.

□

Teorema 2.11. *Sejam $S_1, S_2 \in Syl_2(M_{2n}(G, 2))$. Então S_1 e S_2 são conjugados.*

Demonstração. Pelo lema 2.6, temos

$$L_1 = S_1 \cup (g_1 S_1)u \text{ e } L_2 = S_2 \cup (g_2 S_2)u$$

Para algum $S_1, S_2 \in Syl_2(G)$ e $g_1, g_2 \in G$. Como S_1 e S_2 são conjugados em G, existe

$h \in G$ tal que $S_2 = h^{-1}S_1h$, então:

$$\begin{aligned}
(S_1u)T(h)T(hu) &= (h^{-1}(S_1u)h)T(hu) \\
&\overset{2.1}{=} (((S_1h^{-1})u)h)T(hu) \\
&\overset{2.2}{=} ((S_1h^{-1}h^{-1})u)T(hu) \\
&= ((S_1h^{-2})u)T(hu) \\
&= (hu)^{-1}((S_1h^{-2})u)(hu) \\
&= (hu)((S_1h^{-2})u)(hu) \\
&\overset{2.3}{=} (h^2S_1h)(hu) \\
&\overset{2.1}{=} (hh^2S_1h)u \\
&= (h^3S_1h)u \\
&= (h^4h^{-1}S_1h)u \\
&= (h^4S_2)u
\end{aligned}$$

E também,

$$\begin{aligned}
S_1T(h)T(hu) &= (h^{-1}S_1h)T(hu) \\
&= S_2T(hu) \\
&= (hu)S_2(hu) \\
&\overset{2.2}{=} ((hS_2)u)(hu) \\
&\overset{2.3}{=} h^{-1}hS_2 \\
&= S_2
\end{aligned}$$

Assim temos que S_1 é conjugado de S_2 em G pelos elementos h e hu e que S_1u é conjugado de $(h^4S_2)u$ pelos mesmos h e hu. Logo $S_1 \cup S_1u$ é conjugado de $S_2 \cup (h^4S_2)u$. Mas pela proposição, $L_1 = S_1 \cup (g_1S_1)u$ é conjugado de $S_1 \cup (S_1)u$, que acabamos de ver que é conjugado de $S_2 \cup (h^4S_2)u$ e este, usando novamente a proposição, é conjugado de $S_2 \cup (g_2S_2)u = L_2$. Portanto L_1 é conjugado de L_2 em L. □

Com este último teorema, concluímos também que a segunda parte do 2º teorema de Sylow é válido para loops de Chein para todo p um número primo.

2.2 Loops de Paige

Seja F um corpo e considere o conjunto de matrizes 2×2 dado por:

$$\mathbb{O}(F) = \left\{ \begin{pmatrix} a & u \\ v & b \end{pmatrix} : a, b \in F, u, v \in F^3 \right\}$$

E sobre este conjunto defina as operações:

$$\begin{pmatrix} a & u \\ v & b \end{pmatrix} + \begin{pmatrix} c & w \\ z & d \end{pmatrix} = \begin{pmatrix} a+c & u+w \\ v+z & b+d \end{pmatrix}$$

$$\begin{pmatrix} a & u \\ v & b \end{pmatrix} \begin{pmatrix} c & w \\ z & d \end{pmatrix} = \begin{pmatrix} ac + u \cdot z & aw + du - (v \times z) \\ cv + bz + (u \times w) & v \cdot w + bd \end{pmatrix}$$

onde $\cdot$ e $\times$ denotam o produto escalar e o produto vetorial em F^3, respectivamente.

Dessa maneira obtemos uma álgebra alternativa conhecida por *Álgebra de Zorn sobre* F, que também é chamada de *Álgebra de Cayley-Dickson split sobre* F.

Sabemos que a álgebra de Zorn $\mathbb{O}(F)$ é simples [14, p.18], isto é, não possui ideais bilaterais próprios. Além disso, pelo teorema de Kleinfeld [14, p.38], qualquer álgebra simples alternativa (e não associativa) sobre F que não é um anel de divisão, é isomorfa a $\mathbb{O}(F)$.

Definimos o *determinante* de um elemento $\alpha \in \mathbb{O}(F)$ por

$$\alpha = \begin{pmatrix} a & u \\ v & b \end{pmatrix} \mapsto det(\alpha) = ab - u \cdot v$$

Não é difícil mostrar que a função determinante é uma função multiplicativa. Dizemos que o elemento $A \in \mathbb{O}(F)$ é inversível se e somente se $det(A) \neq 0$ e, nesse caso, seu inverso é dado por

$$\alpha^{-1} = \frac{1}{det(\alpha)} \begin{pmatrix} b & -u \\ -v & a \end{pmatrix}$$

De fato,

$$\begin{aligned}
\alpha\alpha^{-1} &= \begin{pmatrix} a & u \\ v & b \end{pmatrix} \frac{1}{det\,\alpha} \begin{pmatrix} b & -u \\ -v & a \end{pmatrix} \\
&= \frac{1}{ab - u\cdot v} \begin{pmatrix} ab - u\cdot v & -au + au - (v \times (-v)) \\ bv - bv + (u \times (-u)) & ab - u\cdot v \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

E também,

$$\begin{aligned}
\alpha^{-1}\alpha &= \frac{1}{det\,\alpha} \begin{pmatrix} b & -u \\ -v & a \end{pmatrix} \begin{pmatrix} a & u \\ v & b \end{pmatrix} \\
&= \frac{1}{ab - u\cdot v} \begin{pmatrix} ab - u\cdot v & bu - bu - (-v \times v) \\ -av + av + (-u \times u) & ab - u\cdot v \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

Denotaremos por $\mathbb{O}(F)^*$ o conjunto de todos os elementos inversíveis em $\mathbb{O}(F)$.

Lema 2.12. *O conjunto $\mathbb{O}(F)^*$ com a multiplicação é um loop.*

Demonstração. Inicialmente observe que:

$$\begin{pmatrix} a & u \\ v & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & u \\ v & b \end{pmatrix} = \begin{pmatrix} a & u \\ v & b \end{pmatrix}$$

Logo, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é o elemento neutro de $\mathbb{O}(F)^*$. Além disso, em $\mathbb{O}(F)^*$ todos os elementos são inversíveis, então é claro que, dados $\alpha, \beta \in \mathbb{O}(F)^*$, existem α^{-1}, β^{-1} tais que $\alpha\alpha^{-1} = \alpha^{-1}\alpha = I$ e $\beta\beta^{-1} = \beta^{-1}\beta = I$. Sabemos que toda álgebra alternativa satisfaz as propriedades de Moufang [14], e já vimos no lema 1.15 que as propriedades de Moufang implicam na propriedade inversa (PI). Com isso temos que as equações:

$$\alpha x = \beta$$

$$y\alpha = \beta$$

possuem soluções $x = \alpha^{-1}\beta$ e $y = \beta\alpha^{-1}$, respectivamente, e são únicas pois α^{-1} e β^{-1} são únicos. □

Como $\mathbb{O}(F)$ é uma álgebra alternativa [14, p.17], segue que $\mathbb{O}(F)$ satisfaz as identidades de Moufang [14, p.9], logo $\mathbb{O}(F)^*$ é um loop de Moufang.

O conjunto $SLL(F) = \{\alpha \in \mathbb{O}(F)^* : det(\alpha) = 1\}$ é um subloop normal de $\mathbb{O}(F)^*$ uma vez que $SLL(F)$ é o núcleo do homomorfismo $det : \mathbb{O}(F)^* \to F$. Análogo ao caso associativo este loop será chamado de *Loop Linear Especial*. Não é difícil mostrar que o centro de $SLL(F)$ é $Z(SLL(F)) = \{\pm I\}$, onde I é a matriz identidade.

Definição 2.13. *Definimos o Loop Projetivo Linear sobre F como sendo o loop-quociente denotado por $PSLL(F)$:*

$$PSLL(F) = \frac{SLL(F)}{Z(SLL(F))}$$

Paige [19] mostrou que $PSLL(F)$ é simples, para um corpo finito F. Assim, esses loops são chamados de *loops de Paige* e serão denotados por $P(F)$, ou $P(q)$ onde $|F_q| = q$.

Se F_2 é o corpo com 2 elementos, então $\mathbb{O}(F_2)^* = SLL(F_2) = P(F_2)$. Assim $P(F_2)$ é o *menor loop de Moufang simples* e o denotaremos apenas por $P(2)$.

De agora em diante, analisaremos os teoremas de Sylow para o menor loop de Moufang Simples, $P(2)$.

Todos os resultados a seguir, e suas respectivas demonstrações, podem ser encontrados em [11], mas optamos por exibir as demonstrações feitas pelo autor.

Lema 2.14. *Dados $u, v \in (F_2)^3$, temos 28 possibilidades para $u \cdot v = 1$ e 36 possibilidades para $u \cdot v = 0$.*

Demonstração. Suponha $u \cdot v = 0$, então:

1. Se $u = (0,0,0)$, então $v = (v_1, v_2, v_3)$ para quaisquer $v_1, v_2, v_3 \in (F_2)^3$. ($2^3 = 8$ possibilidades).

2. Se $u = (1,0,0)$, então $v = (0, v_2, v_3)$ para quaisquer $v_2, v_3 \in (F_2)^3$. ($2^2 = 4$ possibilidades).

3. Se $u = (0,1,0)$, então $v = (v_1, 0, v_3)$ para quaisquer $v_1, v_3 \in (F_2)^3$. ($2^2 = 4$ possibilidades).

4. Se $u = (0,0,1)$, então $v = (v_1, v_2, 0)$ para quaisquer $v_1, v_2 \in (F_2)^3$. ($2^2 = 4$ possibilidades).

5. Se $u = (1, 1, 0)$, então $v = (0, 0, v_3)$ para qualquer $v_3 \in (F_2)^3$. ($2^1 = 2$ possibilidades).

6. Se $u = (1, 0, 1)$, então $v = (0, v_2, 0)$ para qualquer $v_2 \in (F_2)^3$. ($2^1 = 2$ possibilidades).

7. Se $u = (0, 1, 1)$, então $v = (v_1, 0, 0)$ para qualquer $v_1 \in (F_2)^3$. ($2^1 = 2$ possibilidades).

8. Se $u = (1, 1, 1)$, então $v = (0, 0, 0)$ (1 possibilidades).

Mas, em F_2, temos $2 \equiv 0$. Suponha então $u \cdot v = 2$, dai:

1. Se $u = (1, 1, 0)$, então $v = (1, 1, v_3)$ para qualquer $v_3 \in (F_2)^3$. ($2^1 = 2$ possibilidades).

2. Se $u = (1, 0, 1)$, então $v = (1, v_2, 1)$ para qualquer $v_2 \in (F_2)^3$. ($2^1 = 2$ possibilidades).

3. Se $u = (0, 1, 1)$, então $v = (v_1, 1, 1)$ para qualquer $v_1 \in (F_2)^3$. ($2^1 = 2$ possibilidades).

4. Se $u = (1, 1, 1)$, então $v = (1, 1, 0)$ ou $v = (1, 0, 1)$ ou $v = (0, 1, 1)$ (3 possibilidades).

Até aqui explicitamos todas as possibilidades para $u \cdot v = 0$ em F_2. Somando-as, temos 36 possibilidades.

Como $u, v \in (F_2)^3$, temos um total $2^3.2^3 = 64$ possibilidades para $u \cdot v$. Então para $u \cdot v = 1$ basta fazer $64 - 36 = 28$. □

Lema 2.15. $|P(2)| = 120$

Demonstração. Um elemento $\alpha \in P(2)$ é de uma das formas

$$\begin{pmatrix} 0 & u \\ v & 0 \end{pmatrix}, \begin{pmatrix} 1 & u \\ v & 0 \end{pmatrix}, \begin{pmatrix} 0 & u \\ v & 1 \end{pmatrix}, \begin{pmatrix} 1 & u \\ v & 1 \end{pmatrix}$$

com $det\alpha = 1$ e $u, v \in (\mathbb{F}_2)^3$. Então vamos analisar cada um dos casos:

1. Se $\alpha = \begin{pmatrix} 0 & u \\ v & 0 \end{pmatrix}, \begin{pmatrix} 1 & u \\ v & 0 \end{pmatrix}$ ou $\begin{pmatrix} 0 & u \\ v & 1 \end{pmatrix}$, então $1 = det\alpha = 0 - u \cdot v$. Logo $u \cdot v = 1$. Pelo lema anterior, temos 28 possibilidades para este caso.

2. Se $\alpha = \begin{pmatrix} 1 & u \\ v & 1 \end{pmatrix}$, ficamos com $1 = det\alpha = 1 - u \cdot v$, ou $u \cdot v = 0$, que pelo lema anterior possiu 36 possibilidades.

No primeiro caso temos $3.28 = 84$ elementos, que somado com 36 elementos do segundo caso, concluímos que $|P(2)| = 84 + 36 = 120$. □

O lema anterior nos mostra que o loop de Paige sobre o corpo com dois elementos tem ordem 120. Mais geralmente, Liebeck [17] mostrou que a ordem de um loop de Paige sobre um corpo com q elementos é dada pela expressão:

$$|P(q)| = \frac{q^3(q^4 - 1)}{mdc(q+1, 2)}$$

Lema 2.16. *Sejam $\alpha \in P(2)$, então $o(\alpha) = 2$ ou 3.*

Demonstração. Novamente dividiremos em casos.

1. Se $\alpha = \begin{pmatrix} 0 & u \\ v & 0 \end{pmatrix}$, temos $\alpha^2 = \begin{pmatrix} u \cdot v & 0 \\ 0 & u \cdot v \end{pmatrix}$. Mas $\alpha^2 \in P(2)$, logo $1 = det\, \alpha^2 = (u \cdot v)(u \cdot v)$. Portanto $u \cdot v = 1$ e $\alpha^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, isto é, $o(\alpha) = 2$.

2. Se $\alpha = \begin{pmatrix} 1 & u \\ v & 0 \end{pmatrix}$, temos $\alpha^2 = \begin{pmatrix} 1 + (u \cdot v) & u \\ v & (u \cdot v) \end{pmatrix}$, então $1 = det\, \alpha^2 = (u \cdot v) + (u \cdot v)(u \cdot v) - (u \cdot v)$, logo $(u \cdot v) = 1$ e $\alpha^2 = \begin{pmatrix} 0 & u \\ v & 1 \end{pmatrix}$. Assim descobrimos $\alpha^3 = \begin{pmatrix} u \cdot v & 0 \\ 0 & u \cdot v \end{pmatrix}$ e $1 = det\alpha^3 = (u \cdot v)(u \cdot v)$, portanto $(u \cdot v) = 1$ e $\alpha^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Daí $o(\alpha) = 3$.

3. Se $\alpha = \begin{pmatrix} 0 & u \\ v & 1 \end{pmatrix}$, temos $\alpha^2 = \begin{pmatrix} (u \cdot v) & u \\ v & (u \cdot v) + 1 \end{pmatrix}$, então $1 = det\, \alpha^2 = (u \cdot v) + (u \cdot v)(u \cdot v) - (u \cdot v)$, logo $(u \cdot v) = 1$ e $\alpha^2 = \begin{pmatrix} 1 & u \\ v & o \end{pmatrix}$. Assim descobrimos $\alpha^3 = \begin{pmatrix} u \cdot v & 0 \\ 0 & u \cdot v \end{pmatrix}$ e $1 = det\alpha^3 = (u \cdot v)(u \cdot v)$, portanto $(u \cdot v) = 1$ e $\alpha^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Daí $o(\alpha) = 3$.

4. Se $\alpha = \begin{pmatrix} 1 & u \\ v & 1 \end{pmatrix}$, temos $\alpha^2 = \begin{pmatrix} 1+(u\cdot v) & 0 \\ 0 & (u\cdot v)+1 \end{pmatrix}$. Mas $\alpha^2 \in P(2)$, logo $1 = det\,\alpha^2 = 1 + 2(u\cdot v) + (u\cdot v)(u\cdot v)$. Portanto $1 + (u\cdot v)(u\cdot v) = 1$, ou seja, $u\cdot v = 0$ e $\alpha^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $o(\alpha) = 2$.

□

Podemos observar por este último lema que os elementos $\alpha \in P(2)$ cuja ordem é 3 são aqueles que possuem traço igual a 1. Ou seja têm uma das seguintes formas:

$$\alpha = \begin{pmatrix} 1 & u \\ v & 0 \end{pmatrix} \text{ ou } \beta = \begin{pmatrix} 0 & u \\ v & 1 \end{pmatrix}$$

Logo existem $2.28 = 56$ elementos de ordem 3 em $P(2)$ e, consequentemente, 63 elementos de ordem 2. Como qualquer elemento e seu inverso possuem a mesma ordem, se A é um elemento de ordem 3, podemos formar subloops do tipo $\{1, A, A^{-1}\}$. Ou seja existem $56/2 = 28$ subloops de ordem 3. Isso nos revela um fato importante sobre os teoremas de Sylow para este loop: existem 28 3-subloops de Sylow em $P(2)$.

Por outro lado, denotando por n_p o número de p-subloops de Sylow de $P(2)$, e aplicando o primeiro item do 3º teorema de Sylow, para $p = 3$, deveríamos ter

$$n_3 \mid 2^3.5 = 40$$

Assim os possíveis valores de n_3 seriam $1, 2, 4, 5, 8, 10, 20, 40$, mas acabamos de ver que $n_3 = 28$. Com isso, concluímos que o primeiro item do 3º teorema de Sylow não vale para $P(2)$ no caso $p = 3$.

Agora se $p = 2$, em [16] é mostrado que existem 63 2-subloops de Sylow em $P(2)$, isto é $n_2 = 63$, mas aplicando novamente o primeiro item do 3º teorema de Sylow, temos

$$n_2 \mid 3.5 = 15$$

Isso por sua vez implica que $1, 3, 5, 15$ são os possíveis valores de n_2, e assim o primeiro item do 3º teorema de Sylow também não é válido no caso $p = 2$.

Além disso, $|P(2)| = 120 = 2^3.3.5$ e, pelo lema anterior, concluimos que $P(2)$ não possui nenhum elemento de ordem 5 e portanto o 1º teorema de Sylow não é válido para $P(2)$ quando $p = 5$.

Até o momento analisamos o loop de Paige sobre o corpo F_2. No próximo capítulo abordaremos os p-subloops no caso geral $P(q)$, onde $q = |F_q|$.

3 Estruturas Hexagonais

Neste capítulo vamos introduzir o conceito de *estruturas hexagonais*, que se mostrou uma ferramenta muito útil ao trabalharmos com a álgebra de Zorn sobre corpos finitos. Inicialmente as estruturas hexagonais foram utilizadas para investigar a estrutura dos subgrupos de um p-subgrupo de Sylow, P, de um grupo G, mais especificamente, para determinar a estrutura dos estabilizadores de P.

Uma estrutura hexagonal é uma estrutura incidente contendo vértices e linhas onde quaisquer dois elementos podem ser unidos por um caminho contendo no máximo sete destes elementos e não existe qualquer n-ágono para $n < 6$. Um hexágono generalizado de ortem (s, t) é um hexágono onde cada vértice incide em $t+1$ linhas e cada linha incide em $s + 1$ vértices. Os únicos exemplos de hexágono generalizado finito de ordem (q, q) são aqueles associados com o grupo $G_2(q)$, grupo de Chavelley sobre F_q [2]. Destacamos aqui dois motivos para se utilizar essas estruturas:

1. o estabilizador de uma linha hexagonal é um bom exemplo onde podemos obter um subloop maximal de $\mathbb{O}(F_q)$ que não gera o espaço todo;

2. existe uma correspondencia biunívoca entre o conjunto dos p-subloops de Sylow de $SLL(F_q)$ e os vértices de um hexágono generalizado.

Segue abaixo uma sequência de definições e resultados.

Considere a álgebra de Zorn sobre um corpo finito F_q, $\mathbb{O}(F_q)$. Sabemos que a função determinante *det* é uma forma quadrática, assim definimos a *forma bilinear* $(\cdot \mid \cdot)$, associada à função determinante, como sendo a aplicação:

$$\begin{aligned} (\cdot \mid \cdot): \quad \mathbb{O}(F_q) \times \mathbb{O}(F_q) &\longrightarrow F_q \\ (x \mid y) &\longmapsto det(x+y) - det(x) - det(y) \end{aligned}$$

Dizemos que x é *ortogonal* a y se $(x \mid y) = 0$. Um exemplo de elementos ortogonais são

$x = \begin{pmatrix} 1 & (1,0,0) \\ (1,0,0) & 3 \end{pmatrix}$ e $y = \begin{pmatrix} 1 & (3,0,0) \\ (2,0,0) & 2 \end{pmatrix}$ pois $det(x) = 2$, $det(y) = -4$ e $det(x+y) = -2$.

Observe que existem elementos cujos determinantes são nulos mas que não são ortogonais entre si. Tome por exemplo $\begin{pmatrix} 1 & (1,0,0) \\ (2,0,0) & 2 \end{pmatrix}$ e $\begin{pmatrix} 0 & (1,0,0) \\ (0,0,0) & 1 \end{pmatrix}$, cujos determinantes são iguais a 0, mas

$$det\left[\begin{pmatrix} 1 & (1,0,0) \\ (2,0,0) & 2 \end{pmatrix} + \begin{pmatrix} 0 & (1,0,0) \\ (0,0,0) & 1 \end{pmatrix}\right] = det\left[\begin{pmatrix} 1 & (2,0,0) \\ (2,0,0) & 3 \end{pmatrix}\right] = -1 \neq 0$$

Definição 3.1. *Seja U um subespaço vetorial de $\mathbb{O}(F_q)$. O subespaço ortogonal a U é dado por:*

$$U^{\perp} = \{x \in \mathbb{O}(F_q) : (x \mid y) = 0, \forall y \in U\}$$

Considere a identidade I de $\mathbb{O}(F_q)$. Dizemos que um elemento $x \in \mathbb{O}(F_q)$ é ortogonal a I se $(x \mid I) = 0$, em outras palavras, se $x = \begin{pmatrix} a & u \\ v & b \end{pmatrix} \in \mathbb{O}(F_q)$ então:

$$\begin{aligned} 0 &= det(x+I) - det(x) - det(I) \\ &= (a+1)(b+1) - u \cdot v - ab + u \cdot v - 1 \\ &= a + b \end{aligned}$$

e portanto temos o seguinte conjunto:

$$I^{\perp} = \left\{ \begin{pmatrix} a & u \\ v & -a \end{pmatrix} : a \in F_q, u, v \in (F_q)^3 \right\}$$

Definição 3.2. *Seja U um subespaço de $\mathbb{O}(F_q)$. O estabilizador de U é dado por:*

$$stab(U) = \{x \in \mathbb{O}(F_q) : xy \in U, \forall y \in U\}$$

Definição 3.3. *Dizemos que um subespaço vetorial U é totalmente singular se todos seus elementos tem determinante nulo e todos são ortogonais entre si, ou seja, $det(x) = 0$ e $(x \mid y) = 0$ para quaisquer $x, y \in U$.*

Definição 3.4. *Uma linha hexagonal é um subespaço vetorial $S \subset \mathbb{O}(F_q)$ totalmente singular de dimensão 2, que está contido em $I^{\perp}$ e tal que o produto entre dois de seus elementos é sempre nulo.*

Um exemplo de linha hexagonal é o subespaço:

$$S = \left\{ \begin{pmatrix} 0 & (u,0,0) \\ (0,v,0) & 0 \end{pmatrix} : u, v \in F_q \right\}$$

pois para quaisquer $s, r \in S$ temos que $det(s) = 0$, $(s \mid r)$=0, $(s \mid I) = 0$, $sr = 0$ e além disso $(u,0,0)$ e $(0,v,0)$ são linearmente independentes (e portanto S é um subespaço bidimensional).

De maneira análoga, definimos *vértice* como sendo um subespaço vetorial $P \subset \mathbb{O}(F_q)$ totalmente singular de dimensão 1, que está contido em $I^{\perp}$ e tal que o produto entre dois de seus elementos é sempre nulo.

Em [21] foi demonstrado que o número de vértices e linha hexagonais em $\mathbb{O}(F_q)$ é $\frac{q^6-1}{q-1}$.

Agora considere um subgrupo multiplicativo abeliano H de $\mathbb{O}(F_q)$ de forma que $\{h-I : h \in H\}$ seja uma linha hexagonal. Um exemplo deste subgrupo é

$$H = \left\{ \begin{pmatrix} 1 & (u,0,0) \\ (0,v,0) & 1 \end{pmatrix} : u, v \in F_q \right\}$$

Note que o subgrupo H foi obtido do subespaço S trocando apenas os elementos da diagonal principal por 1.

É um fato conhecido que o grupo dos automorfismos de $P(q)$ é o grupo de Chevalley $G_2(q)$, [7]. Desde que $G_2(q)$ age transitivamente sobre $P(q)$ podemos considerar os subespaços S, H como dos exemplos anteriores. Seja $r \in \mathbb{O}(F_q)$ um elemento de $stab(\{h-I : h \in H\}) = stab(S)$. Então $rs \in S$, onde

$$\begin{aligned} rs &= \begin{pmatrix} a & (x_1,x_2,x_3) \\ (y_1,y_2,y_3) & b \end{pmatrix} \begin{pmatrix} 0 & (u,0,0) \\ (0,v,0) & 0 \end{pmatrix} \\ &= \begin{pmatrix} x_2 v & (au,0,0) - (y_1,y_2,y_3) \times (0,v,0) \\ (0,bv,0) + (x_1,x_2,x_3) \times (u,0,0) & y_1 u \end{pmatrix} \\ &= \begin{pmatrix} x_2 v & (au + vy_3, 0, vy_1) \\ (0, bv + ux_3, -ux_2) & y_1 u \end{pmatrix} \end{aligned}$$

e portanto devemos ter $x_2v = y_1u = 0$, ou seja, $x_2 = y_1 = 0$. Assim temos que r é da forma:

$$r = \begin{pmatrix} a & (b,0,c) \\ (0,d,e) & f \end{pmatrix} \text{ onde } a,b,c,d,e,f \in F_q$$

Ou seja, o estabilizador de uma linha hexagonal é uma subálgebra de dimensão 6. Sendo assim, considere uma subalgebra Q de $\mathbb{O}(F_q)$ de forma que $Q \subseteq stab(S)$, onde S é uma linha hexagonal.

Definição 3.5. *Sejam H e Q o subgrupo e a subálgebra definidos anteriormente. Então o produto $Q \bullet H$ é o conjunto $\{(x,h) : x \in Q, h \in H\}$ onde a operação entre seus elementos é dada por:*

$$(x,g) \odot (y,h) = (xy, I + x(h-I) + (g-I)y)$$

Lema 3.6. *Seja S uma linha hexagonal de $\mathbb{O}(F_q)$. Então $stab(S) \cong M_2(F_q) \bullet (F_q)^2$*

Demonstração. Suponha que $S = \left\{ \begin{pmatrix} 0 & (u,0,0) \\ (0,v,0) & 0 \end{pmatrix} : u,v \in F_q \right\}$. Já vimos que $stab(S) = \left\{ \begin{pmatrix} a & (b,0,c) \\ (0,d,e) & f \end{pmatrix} : a,b,c,d,e,f \in F_q \right\}$.

É fácil ver que:

$$M_2(F_q) \cong \left\{ \begin{pmatrix} a & (0,0,c) \\ (0,0,e) & f \end{pmatrix} : a,c,e,f \in F_q \right\}$$
$$(F_q)^2 \cong \left\{ \begin{pmatrix} 1 & (b,0,0) \\ (0,d,0) & 1 \end{pmatrix} : b,d \in F_q \right\}$$

Considere $\phi : M_2(F_q) \bullet (F_q)^2 \longrightarrow stab(S)$, definida da seguinte forma:

$$\phi\left(\begin{pmatrix} a & (0,0,c) \\ (0,0,e) & f \end{pmatrix}, \begin{pmatrix} 1 & (b,0,0) \\ (0,d,0) & 1 \end{pmatrix} \right) = \begin{pmatrix} a & (b,0,c) \\ (0,d,e) & f \end{pmatrix}$$

Pela própria construção de ϕ, podemos afirmar que esta função é injetora e sobrejetora. Vamos provar que ϕ é um homomorfismo. Para isso, suponha $x,y \in M_2(F_q) \bullet (F_q)^2$, e tomemos:

$$x = \left(\begin{pmatrix} a & (0,0,c) \\ (0,0,e) & f \end{pmatrix}, \begin{pmatrix} 1 & (b,0,0) \\ (0,d,0) & 1 \end{pmatrix} \right)$$
$$y = \left(\begin{pmatrix} g & (0,0,i) \\ (0,0,k) & l \end{pmatrix}, \begin{pmatrix} 1 & (h,0,0) \\ (0,j,0) & 1 \end{pmatrix} \right)$$

Dessa forma:

$$\phi(x \odot y) = \begin{pmatrix} ag + ck & (ah + ej + bl - dk, 0, ai + cl) \\ (0, fj + ch + dg - bi, ge + fk) & ei + fl \end{pmatrix}$$

Por outro lado:

$$\begin{aligned} \phi(x)\phi(y) &= \begin{pmatrix} a & (b,0,c) \\ (0,d,e) & f \end{pmatrix} \begin{pmatrix} g & (h,0,i) \\ (0,j,k) & l \end{pmatrix} \\ &= \begin{pmatrix} ag + ck & (ah,0,ai) + (bl,0,cl) - (dk - ej,0,0) \\ (0,dg,eg) + (0,fj,fk) + (0,ch - bi,0) & ei + fl \end{pmatrix} \\ &= \begin{pmatrix} ag + ck & (ah + ej + bl - dk, 0, ai + cl) \\ (0, fj + ch + dg - bi, ge + fk) & ei + fl \end{pmatrix} \end{aligned}$$

Assim $\phi(x \odot y) = \phi(x)\phi(y)$, logo ϕ é um homomorfismo bijetor, ou seja, ϕ é um isomorfismo. □

3.1 A existência de p-subloops em P(q)

Nesta seção abordaremos a existência de p-subloops de $P(q)$, onde p um primo ímpar e $q = |F_q|$ é potência de outro primo.

Iniciamos com dois lemas de teoria dos números. O primeiro é conhecido como Teorema de Dirichlet:

Lema 3.7. *(Teorema de Dirichlet) [18] Sejam $a, b \in \mathbb{Z}$ tais que $mdc(a,b) = 1$. Então existem infinitos números primos q_i que satisfazem $q_i \equiv a \,(mod\, b)$.*

Lema 3.8. *Seja p um primo ímpar e q um inteiro. Se $p \mid (q^2 + 1)$ então $p \equiv 1 \,(mod\, 4)$. Reciprocamente, se $p \equiv 1 \,(mod\, 4)$, então existe um primo q tal que $p \mid (q^2 + 1)$*

Demonstração. Suponha que $p \mid (q^2 + 1)$, então $q^2 + 1 \equiv 0 \,(mod\, p)$ e portanto $q^2 \equiv -1 \,(mod\, p)$. Assim temos que $q^4 \equiv 1 \,(mod\, p)$, ou seja, existe um elemento $q \in \mathbb{Z}_p^*$ de

ordem 4. Pelo teorema de Lagrange, 4 divide $|\mathbb{Z}_p^*| = p-1$, logo $p \equiv 1\,(mod\,4)$.
Agora suponha que $p \equiv 1\,(mod\,4)$, ou seja, 4 divide $p-1$. Como $|\mathbb{Z}_p^*| = p-1$, temos pelo teorema de Lagrange que existe um subgrupo H de $\mathbb{Z}_p^*$ cuja ordem é 4. Além disso, $\mathbb{Z}_p^*$ é cíclico e portanto H também é cíclico. Então existe em $H \leq \mathbb{Z}_p^*$ um elemento gerador de ordem 4. Seja a tal elemento, então $a^4 \equiv 1\,(mod\,p)$. Desta forma temos duas possibilidades, $a^2 \equiv 1\,(mod\,p)$ ou $a^2 \equiv -1\,(mod\,p)$, mas a primeira nos leva a um absurdo, já que $o(a) = 4$. Só nos resta $a^2 \equiv -1\,(mod\,p)$, o que significa que $mdc(a^2, p) = 1$ e portanto $mdc(a, p) = 1$. Pelo lema 3.7, existe um primo q tal que $q \equiv a\,(mod\,p)$. Então $q^2 \equiv a^2 \equiv -1\,(mod\,p)$, isto é, $p \mid (q^2+1)$. □

Dizemos que um subgrupo H de G é maximal em G se $H \leq K \leq G$ implica que $K = H$ ou $K = G$. Esse conceito pode ser estendido a subloops. Formalmente temos:

Definição 3.9. *Seja L um loop e M um subloop próprio de L. Dizemos que M é um subloop maximal de L se $M \leq N \leq L$ implica que $N = M$ ou $N = L$.*

É bem conhecido o fato que um subgrupo maximal é sempre isomorfo ao estabilizador de um subgrupo. Da mesma forma, um subloop maximal é isomorfo ao estabilizador de um subloop. O próximo teorema é fundamental na identificação dos subloops maximais de $P(q)$.

Teorema 3.10. *[7] Seja p um número primo e M um subloop maximal de $P(q)$. Então M é de um dos tipos a seguir:*

1. *$M \cong PSL_2(q) \bullet (F_q)^2$ onde*

$$|M| = \frac{q^3(q^2-1)}{mdc(q+1,2)}$$

2. *$M = H \cup xH$ onde $H \cong PSL_2(q)$, $x \in H^{\perp}$, $det(x) = 1$ e*

$$|M| = \frac{2q(q^2-1)}{mdc(q+1,2)}$$

3. *$M \cong SLL(q_0)/\{\pm I\} = P(q_0)$ onde F_{q_0} é um subcorpo de F_q e*

$$|M| = \frac{q_0^3(q_0^4-1)}{mdc(q+1,2)}$$

4. $M \cong SLL(q_0)2/\{\pm I\} = P(q_0) \times C_2$ *onde* F_{q_0} *é um subcorpo de* F_q *de característica ímpar e*

$$|M| = \frac{2q_0^3(q_0^4 - 1)}{2}$$

5. $M \cong 2SLL(F_2)/\{\pm I\} = P(2)$ *onde* F_q *é de característica ímpar e*

$$|M| = \frac{2 \cdot 120}{2} = 120$$

Observe que os subloops descritos no teorema acima já foram definidos neste trabalho. São eles:

- $PSL_2(q) \cup x(PSL_2(q))$ é o loop de Chein $M_{2k}(PSL_2(q), 2)$ com $k = |PSL_2(q)|$.
- $SLL(q_0)/\{\pm I\} = P(q_0)$ é um loop de Paige sobre um subcorpo F_{q_0} do corpo F_q.
- $SLL(q_0)2/\{\pm I\}$ é o produto direto entre $P(q_0)$ e o grupo cíclico de ordem 2, C_2.
- $2SLL(F_2)/\{\pm I\} = P(2)$ é exatamente o loop de Paige sobre o corpo F_2.

Teorema 3.11. *Seja* p *um primo ímpar,* T *um* p*-subloop de* $P(q)$ *sobre* F_q*. Então* T *está contido em um subloop maximal,* M*, de* $P(q)$ *que é isomorfo a* $PSL_2(q) \bullet (F_q)^2$*.*

Demonstração. Já vimos que a ordem de $P(q)$ é $\frac{q^3(q^4-1)}{mdc(q+1,2)}$. Como p é ímpar, temos que q é ímpar, portanto q^3 é ímpar, q^4-1 é par e $mdc(q+1,2) = 2$, ou seja, a ordem de $P(q)$ é sempre par e portanto $P(q)$ não pode ser um p-loop. Então o p-subloop T é próprio e portanto deve estar contido em um subloop maximal próprio M de $P(q)$, que é uma das 5 possibilidades do teorema anterior.

Note que se M está no caso 1, então o teorema está provado.

Agora suponha que M está no caso 3 ou 4. Como p é ímpar e C_2 tem ordem 2, podemos ver que T não está no caso 4 e portanto é isomorfo ao subloop $SLL(F')/\{\pm I\} = P(F')$ para algum subcorpo F' de F_q. Se F' for o menor subcorpo de F_q que preserva este isomorfismo, então T será isomorfo a um subloop de M', onde M' é um subloops maximal de $P(F')$. Pela minimalidade de $|F'|$, ou $M' \cong PSL_2(F') \bullet F'^2$, $M' \cong P(2)$, ou $M' = H \cup xH$ onde $H \cong PSL_2(q)$, $x \in H^\perp$ e $det(x) = 1$. Então T está contido em um subloop maximal, M, de $P(q)$, o que nos leva aos casos 1, 2 ou 5.

Se $M \cong P(2)$, como T é um p-loop com p ímpar, então pelo teorema de Lagrange para loops de Moufang, temos que $p = 3$ ou 5 (pois $|P(2)| = 120 = 2^3 \cdot 3 \cdot 5$) e portanto T é

cíclico. Seja $T = \langle x \rangle$. Pela proposição 2.1 e pelo teorema 2.2 de [7], qualquer elemento inversível em uma álgebra split dos octônios está contido em uma subálgebra isomorfa a $M_2(F)$. Então x está contido em um subloop de $P(q)$ que é isomorfo a $PSL_2(q)$. Portanto $T = \langle x \rangle$ está contido em um subloop de $P(q)$ que é isomorfo a $PSL_2(q) \bullet F^2$. Se $M = H \cup xH$ onde $H \cong PSL_2(q)$, $x \in H^{\perp}$ e $det(x) = 1$, em outras palavras, se M é o loop de Chein $M(PSL_2(q), 2)$, então $|M|$ é par e, como p é ímpar, temos que T é um subloop de H. Então T está contido em um subloop $H \bullet (F_q)^2$, que é isomorfo a $PSL_2(q) \bullet (F_q)^2$. □

Corolário 3.12. *Se $p \mid (q^2 + 1)$, então $P(q)$ não contém nenhum p-subloop, exceto o subloop trivial.*

Demonstração. Seja T um p-subloop de $P(q)$ tal que $p \mid (q^2+1)$. Pelo teorema anterior, temos que T está contido em um subloop, M, de $P(q)$, que é isomorfo a $PSL_2(q) \bullet (F_q)^2$. Então, pelo teorema de Lagrange para loops de Moufang

$$|T| \mid |M| = \frac{q^3(q^2-1)}{2}$$

Mas $p \mid (q^2 + 1)$, logo $p \nmid q^2$ e portanto $p \nmid (q^2 - 1)$ (pois $p \neq 2$) e $p \nmid q^3$. Com isso temos que p não divide $|M|$. Como $|T| = p^n$, só podemos ter $n = 0$ e portanto $|T| = 1$. Então $T = \{I\}$. □

Corolário 3.13. *Se $p \mid (q^2 + 1)$, então $P(q)$ não contém nenhum p-subloop de Sylow.*

Demonstração. Seja p um primo que divide $(q^2 + 1)$. Pelo corolário anterior, $T = \{I\}$ é o único p-subloop do loop de Paige $P(q)$. Já vimos que

$$|P(q)| = \frac{q^3(q^4-1)}{mdc(q+1,2)} = \frac{q^3(q^2-1)(q^2+1)}{mdc(q+1,2)}$$

e como p divide $(q^2 + 1)$ temos que p divide $|P(q)|$, mas p não divide $|T| = 1$. Logo, o único p-subloop de $P(q)$, T, não é um p-subloops de Sylow. Então $P(q)$ não possui nenhum. □

Em particular, se não existe nenhum p-subloop, então é claro que não existe nenhum p-subloop de Sylow. Com essas informações temos condições de enunciar o principal teorema desta seção:

Teorema 3.14. *Seja p um número primo da forma $p = 4k + 1$, então o loop de Paige $P(q)$ não possui nenhum p-subloop.*

Demonstração. Como p é da forma $p = 4k + 1$, temos $p \equiv 1\,(mod\,4)$. Pelo lema 3.8, existe um primo q tal que $p \mid (q^2 + 1)$. Assim, pelo corolário anterior concluímos que o loop de Paige $P(q)$ não contém nenhum p-subloop. □

Teorema 3.15. *Existem 2-subloops de Sylow em $P(q)$.*

Demonstração. De fato, observe que $|P(q)| = \frac{q^3(q^4-1)}{mdc(q+1,2)}$.
Se q é ímpar, então $P(q)$ contém um 2-subloop P onde $P = H \cup xH$, com $H \cong S \in Syl_2(PSL_2(q))$, $x \in H^{\perp}$ e $det(x) = 1$. Portanto, pela consideração da ordem, temos que $P \in Syl_2(P(q))$.
Se q é par, então $P(q)$ contém um 2-subloop P onde $P \cong S \bullet F^2$, com $S \in Syl_2(PSL_2(q))$. Como 2 não divide $[P(q) : P]$, temos que $P \in Syl_2(P(q))$. □

3.2 O número de p-subloops de Sylow em *P(q)*

Nosso objetivo nesta seção é mostrar que o número de p-subloops de Sylow em $P(q)$ é congruente a 1 módulo p, onde q é potência de um primo e p é um número primo, $p \neq 2$, tal que $p \nmid (q^2 + 1)$. Números primos nessas condições serão chamados daqui para frente de *primos de Sylow*. E, nesse caso, pelo lema 3.8, temos que $p \equiv 3\,(mod\,4)$, ou seja, p é da forma $p = 4k - 1$.

Iniciamos com alguns resultados que dizem respeito à contagem de linhas hexagonais.

Lema 3.16. *Seja F_q um corpo com q elementos e Q uma subálgebra isomorfa a $M_2(F_q)$. Então:*

1. *O número de linhas hexagonais contidas em $\mathbb{O}(F_q)$ é $\frac{q^6-1}{q-1}$.*
2. *O número de linhas hexagonais contidas em $\mathbb{O}(F_q)$ que uma determinada subálgebra isomorfa a $M_2(F_q)$ estabiliza é $q + 1$.*
3. *O número de subálgebras isomorfas a $M_2(F_q)$ contidas em $\mathbb{O}(F_q)$ que estabiliza uma dada linha hexagonal é q^2.*
4. *O número de subálgebra isomorfas a $M_2(F_q)$ contidas em $\mathbb{O}(F_q)$ é $q^2(q^4 + q^2 + 1)$.*

Demonstração. O primeiro item foi mostrado em [21] e não será apresentado neste trabalho. Para o item 2, seja Q uma subálgebra isomorfa a $M_2(F_q)$, digamos:

$$Q = \begin{pmatrix} a & \langle b,0,0\rangle \\ \langle c,0,0\rangle & d \end{pmatrix}$$

Se Q estabiliza uma linha hexagonal h, então h é ortogonal a Q. Logo h é da forma $\begin{pmatrix} 0 & v \\ u & 0 \end{pmatrix}$, onde $u_1 = v_1 = 0$. Assim temos $\frac{q^2-1}{q-1}$ escolhas para v e, fixado v, temos $\frac{q-1}{q-1}$ escolhas para u. Ou seja, temos $\frac{q^2-1}{q-1}\frac{q-1}{q-1}$.
Na demonstração do item 3 procedemos de maneira análoga ao item 2. O item 4 é consequência dos itens 1,2 e 3. Sua demonstração também pode ser encontrada em [16]. □

No próximo lema usaremos o fato de que o conjunto das ordens dos elementos de $P(q)$ (analogamente $SLL(q)$) é igual ao conjunto das ordens de $PSL_2(q)$ (analogamente $SL_2(q)$) e consiste de todos os divisores de $\frac{q-1}{d}$, $\frac{q+1}{d}$ e p, onde $d = mdc(q+1,2)$. [16]

Lema 3.17. *Sejam Q uma subálgebra isomorfa a $M_2(F_q)$ em $\mathbb{O}(F)$ e p um primo ímpar que divide $|Q^*|$. Então um p-subgrupo de Sylow de Q^* gera uma subálgebra de Q bidimensional.*

Demonstração. Se T é um p-subgrupo de Sylow de Q^*, então ou T é cíclico (quando $p \mid (q+1)$), ou é produto direto de dois grupos cíclicos (quando $p \mid (q-1)^2$), ou é isomorfo a um grupo abeliano de F_q (quando p é a característica de F). Em todos os casos temos que T é abeliano e necessariamente gera uma subálgebra comutativa de Q. Como não existe subálgebra comutativa de Q tridimensional, então a dimensão dessa subálgebra é menor do que 3. Assim temos que Q é uma subálgebra bidimensional. □

Lema 3.18. *Seja p um primo ímpar, então o número de p-subloops de Sylow de $P(q)$ é igual ao número de p-subloops de Sylow de $SLL(q)$, isto é, $|Syl_p(P(q))| = |Syl_p(SLL(q))|$.*

Lema 3.19. *Seja T um subloop de $SLL(q)$ que gera $S = \left\{ \begin{pmatrix} a & (0,0,0) \\ (0,0,0) & b \end{pmatrix} : a,b \in F \right\}$. Então as 3 igualdades a seguir são equivalentes:*

1. $$|Syl_p(SLL(q)| = \frac{\left(\begin{array}{c} \textit{número de linhas} \\ \textit{hexagonais em } \mathbb{O}(F) \end{array}\right)^{\cdot |Syl_p(SL_2(q))|}}{\left(\begin{array}{c} \textit{número de linhas hexagonais que um dado} \\ \textit{p-subloop de Sylow de } SLL(q) \textit{ stabiliza} \end{array}\right)}$$

2. $$|Syl_p(SLL(q)| = \frac{\left(\begin{array}{c} \textit{número de subálgebras} \\ \textit{isomorfas a } M_2(F_q) \textit{ em } \mathbb{O}(F) \end{array}\right)^{\cdot |Syl_p(SL_2(q))|}}{\left(\begin{array}{c} \textit{número de subálgebras} \\ \textit{isomorfas a } M_2(F_q) \textit{ que contém } T \end{array}\right)}$$

3. $$|Syl_p(SLL(q)| = \left(\begin{array}{c} \textit{número de subálgebras} \\ \textit{isomorfas a } M_2(F_q) \textit{ que contém } S \end{array}\right) \cdot |Syl_p(SL_2(q))|$$

Lema 3.20. *Se p é um primo ímpar tal que p divide q, então $|Syl_p(P(q))| \equiv 1 (mod\, p)$.*

Demonstração.

$$\begin{aligned}
|Syl_p(P(q))| &\overset{3.18}{=} |Syl_p(SLL(q)| \\
&\overset{3.19}{=} \frac{\left(\begin{array}{c} \text{número de linhas} \\ \text{hexagonais em } \mathbb{O}(F) \end{array}\right) \cdot |Syl_p(SL_2(q)|}{\left(\begin{array}{c} \text{número de linhas hexagonais que um dado} \\ p\text{-subloop de Sylow de } SLL(q) \text{ stabiliza} \end{array}\right)} \\
&\overset{3.16}{=} \frac{(q^5+q^4+q^3+q^2+q+1) \cdot |Syl_p(SL_2(q)|}{q+1} \\
&= \frac{(q+1)(q^4+q^2+1) \cdot |Syl_p(SL_2(q))|}{q+1} \\
&= (q^4+q^2+1) \cdot |Syl_p(SL_2(q))| \\
&\equiv 1 \, (mod\, p).
\end{aligned}$$

□

Lema 3.21. *Se p é um primo ímpar tal que p divide $q-1$, então $|Syl_p(P(q))| \equiv 1 (mod\, p)$.*

Demonstração. Note que existe um p-subloop de Sylow de $SLL(q)$, T, que está contido

e gera a álgebra $\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right\}$. Então

$$\begin{aligned}\begin{pmatrix} \text{número de subálgebras} \\ \text{isomorfas a } M_2(F_q) \text{ que contém T} \end{pmatrix} &= \frac{\begin{pmatrix} \text{número de elementos} \\ \text{inversíveis em } T^{\perp} \end{pmatrix}}{(q-1)^2} \\ &= \frac{(q^3-1)(q-1)q^2}{(q-1)^2} \\ &= q^2(q^2+q+1)\end{aligned}$$

Com isso temos que

$$\begin{aligned}|Syl_p(P(q))| &\overset{3.18}{=} |Syl_p(SLL(q))| \\ &\overset{3.19}{=} \frac{\begin{pmatrix} \text{número de subálgebras} \\ \text{isomorfas a } M_2(F_q) \text{ em } \mathbb{O}(F) \end{pmatrix} \cdot |Syl_p(SL_2(q))|}{\begin{pmatrix} \text{número de subálgebras} \\ \text{isomorfas a } M_2(F_q) \text{ que contém T} \end{pmatrix}} \\ &\overset{3.16}{=} \frac{q^2(q^2+q+1)(q^2-q+1)\cdot|Syl_p(SL_2(q))|}{q^2(q^2+q+1)} \\ &= (q^2-q+1)\cdot|Syl_p(SL_2(q))| \\ &\equiv 1\,(mod\,p)\end{aligned}$$

□

Lema 3.22. *Se p é um primo ímpar tal que p divide $q+1$, então $|Syl_p(P(q))| \equiv 1(mod\,p)$.*

Demonstração. Seja P um p-subgrupo de Sylow de $SLL(q)$. Pelo lema 3.17, temos que P gera uma subálgebra isomorfas a $M_2(F_q)$ de $\mathbb{O}(F)$ bidimensional. Como P não está contido em uma subálgebra isomorfa ao conjunto das matrizes triangulares superiores, $\left\{\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\right\}$, segue que P está contido em uma, e apenas uma, subálgebra isomorfa a

$M_2(F_q)$ que também contém $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right\}$. Portanto,

$$\begin{aligned}
|Syl_p(P(q))| &\overset{3.18}{=} |Syl_p(SLL(q))| \\
&\overset{3.19}{=} \begin{pmatrix} \text{número de subálgebras} \\ \text{isomorfas a } M_2(F_q) \text{ que contém S} \end{pmatrix} \cdot |Syl_p(SL_2(q))| \\
&\overset{3.16}{=} q^2(q^2+q+1) \cdot |Syl_p(SL_2(q))| \\
&= (q^4+q^3+q^2) \cdot |Syl_p(SL_2(q))| \\
&= ((-1)^4+(-1)^3+(-1)^2)(1) \\
&\equiv 1\,(mod\,p)
\end{aligned}$$

□

Teorema 3.23. *Se p é um primo de Sylow, então $|Syl_p(P(q))| \equiv 1(mod\,p)$.*

Demonstração. Seja p um primo de Sylow e lembre que

$$|P(q)| = \frac{q^3(q^4-1)}{2} = \frac{q^3(q^2+1)(q^2-1)}{2} = \frac{q^3(q^2+1)(q+1)(q-1)}{2}$$

Como p é um primo (de Sylow, portanto $p \nmid (q^2-1)$) que divide $|P(q)|$, temos 3 possibilidades:

1. $p \mid (q-1)$
2. $p \mid (q+1)$
3. $p \mid q$

Dos lemas 3.21 e 3.22, temos que $|Syl_p(P(q))| \equiv 1(mod\,p)$ nos casos 1 e 2 respectivamente. Se $p \mid q$ então, pelo lema 3.20, temos que $|Syl_p(P(q))| \equiv 1(mod\,p)$ também é válido para o caso 3. □

4 Apêndice

Neste apêndice é apresentada a tabela de multiplicação do loop $M_{12}(S_3, 2)$.

.	1	a	a^2	b	ba	ba^2	u	au	a^2u	bu	$(ba)u$	$(ba^2)u$
1	1	a	a^2	b	ba	ba^2	u	au	a^2u	bu	$(ba)u$	$(ba^2)u$
a	a	a^2	1	ba^2	b	ba	au	a^2u	u	$(ba)u$	$(ba^2)u$	bu
a^2	a^2	1	a	ba	ba^2	b	a^2u	u	au	$(ba^2)u$	bu	$(ba)u$
b	b	ba	ba^2	1	a	a^2	bu	$(ba^2)u$	$(ba)u$	u	a^2u	au
ba	ba	ba^2	b	a^2	1	a	$(ba)u$	bu	$(ba^2)u$	au	u	a^2u
ba^2	ba^2	b	ba	a	a^2	1	$(ba^2)u$	$(ba)u$	bu	a^2u	au	u
u	u	a^2u	au	bu	$(ba)u$	$(ba^2)u$	1	a^2	a	b	ba	ba^2
au	au	u	a^2u	$(ba^2)u$	bu	$(ba)u$	a	1	a^2	ba	ba^2	b
a^2u	a^2u	au	u	$(ba)u$	$(ba^2)u$	bu	a^2	a	1	ba^2	b	ba
bu	bu	$(ba^2)u$	$(ba)u$	u	au	a^2u	b	ba	ba^2	1	a^2	a
$(ba)u$	$(ba)u$	bu	$(ba^2)u$	a^2u	u	au	ba	ba^2	b	a	1	a^2
$(ba^2)u$	$(ba^2)u$	$(ba)u$	bu	au	a^2u	u	ba^2	b	ba	a^2	a	1

Bibliografia

[1] O. Chein, Moufang loops of small order, *Mem. Amer. Math. Soc.* **197** (1978), no.13.

[2] A.M. Cohen, J. Tits, On generalized hexagons and a near octagon whose lines have three points. *Eur. J. Comb.* **6** (1985), 13-27.

[3] F. Fenyves, Extra loops I, *Publ. Math. Debrecen* **15** (1968), 235-238.

[4] F. Fenyves, Extra loops II, *Publ. Math. Debrecen* **16** (1969), 187-192.

[5] S. Gagola III and J. Hall, Lagrange's theorem for Moufang loops, *Acta. Sci. Math.* **71** (2005), 45-64.

[6] S. Gagola III, Conjugacy of Sylow 2-subloops of the Chein loops $M_{2n}(G, 2)$, Communications in Algebra **37(8)** (2009), 2084-2810.

[7] S. Gagola III, Subloops of the unit octonions, *Acta. Sci. Math.* **23** (2005), 255-270.

[8] S. Gagola III, The development of Sylow p-subloops in finite Moufang loops, *Journal of Algebra* **322** (2009), no. 5, 1565-1574.

[9] S. Gagola III, The existence of Sylow 2-subloops in finite Moufang loops, *Journal of Algebra* **322** (2009), no. 4, 1029-1037.

[10] S. Gagola III, The number of Sylow p-subloops in finite Moufang loops, *Communications in Algebra* **38** (2010), no. 4, 1436-1448.

[11] M.L. Giuliani, C.P. Milies, On the structure of the simple Moufang loop $GLL(F_2)$, *Lecture notes in pure and applied mathematics* **211** (2000), 313-319.

[12] M.L. Giuliani, C.P. Milies, The smallest simple Moufang loop, *Journal of Algebra* **320** (2008), no. 3, 961-979.

[13] G. Glauberman, On loops of odd order I,II, *Journal of Algebra* **8** (1968), 393-414.

[14] E. Goodaire, E. Jespers, C. Polcino Milies, *Alternative Loop Rings*, North-Holland, Mathematics Studies, **184**, 1996.

[15] A. Grishkov, A. Zavarnitsini, Lagrange's theorem for Moufang loops, Math. Proc. Cambrigde Philos. Soc. **139** (2005), 41-57.

[16] A. Grishkov, M.L. Giuliani, A. Zavarnitsine, Classification of subalgebras of the Cayley algebra over a finite field, *Journal of Algebra* **9** (2010), no. 5, 791-808.

[17] M.W. Liebeck, The classification of finite simple Moufang loops, *Math. Proc. Cambrigde Philos. Soc.* **102** (1987), 33-47.

[18] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An introduction to the Theory of Numbers*, fifth edição, John Wiley and Sons Inc. New York, 1991.

[19] L. Paige, A class of simple Moufang loops, *Proc. Amer. Math. Soc.* **7** (1956), 471-482.

[20] G.J. Schellekens, On a hexagonic structure I, II, *Nedrl. Akad. Wetensch. Proc. A65=Indag. Math.* **24** (1962), 201-234.

[21] A. Yanushka, Generalized Hexagon of order (t, t), *Israel Journal of Mathematics* **23** (1976), nos. 3-4, 309-324.