Zorn vector matrices over commutative rings and the loops arising from their construction

by

Andrew Thomas Wells

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Mathematics

Program of Study Committee:
Jonathan D. H. Smith, Major Professor
Elgin Johnston
Richard Ng
Sung Song
Steve Willson

Iowa State University

Ames, Iowa

2010

DEDICATION

I would like to dedicate this thesis to the memories of Janet Andersen, Jason Begue, John Quinn, and Barbara Wells. Their lives changed my life and they will be forever missed. Rest in peace.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my thanks to those who helped me with various aspects of conducting research and the writing of this thesis. First and foremost, Dr. Jonathan Smith for his guidance, patience and support throughout this research and the writing of this thesis. I would also like to thank my committee members for their efforts and contributions to this work and my studies in general: Dr. Richard Ng, Dr. Stephen Willson, Dr. Sung-Yell Song, and Dr. Elgin Johnston. Their support in the classroom, in my research, and in my life has been most welcome. I would additionally like to thank Melanie Erickson who is an outstanding graduate secretary and without whose hard work, no one would graduate.

ABSTRACT

This thesis shows that the Zorn vector matrix construction which Paige used to construct simple nonassociative Moufang loops over finite fields can, in fact, be done over any commutative ring with the proper adjustments. The resulting loops are still Moufang, but no longer simple in general. Given a commutative ring and an ideal of that ring, the loop constructed over that ring can be decomposed into two pieces. In this way, it is shown that the loop constructed over $\mathbb{Z}/4\mathbb{Z}$ shares some structure with the Paige loop constructed over the finite field $\mathbb{Z}/2\mathbb{Z}$. An in depth study of the loop constructed over $\mathbb{Z}/4\mathbb{Z}$ follows including significant portions of the subloop lattice and a variety of structural results.

CHAPTER 1. OVERVIEW

The first encounter that students have with algebra is traditionally, although not always, group theory. This is not without good reason, since group theory has been a major topic in algebra since the beginning and provides a deep and rich experience with basic algebraic ideas and techniques. This has the unintended side effect of cementing associativity, one of the main attributes of a group's binary operation, as a starting point for algebraic discussions. Associativity is far from an innocent assumption, indeed it is very powerful and imposes a lot of structure on the resulting algebraic object. This is difficult to see, however, without a dedicated study of nonassociative objects. The study of nonassociative algebras and the study of associative algebras are not opposed to one another, but instead inform and illuminate each other. One of the most basic nonassociative structures is the loop, which forms the basis for this work.

1.1 Introduction

The opening chapter of this work provides a number of definitions and relevant pieces of background information about loops and quasigroups, which are the nonassociative objects with which this work is concerned. The theory of loops and quasigroups is very large, and since this work focuses on such objects with a binary operation satisfying the Moufang identities, most of the treatment is limited to Moufang loop theory. Certainly not every aspect of this theory is included, in fact a concerted effort has been made to include only information which is of use in understanding the rest of the work. The proofs of these results are generally not reproduced here, but references are provided for those who wish to investigate further. Some standardization of the notation used throughout this work is also established in this opening

chapter.

The second chapter reexamines Paige's influential paper (16), with a new perspective. Paige's construction over finite fields can actually be extended to a construction over any commutative ring. This chapter follows the structure of Paige's original work, but reworks the proofs and results to apply in a broader context. It is shown that loops constructed from Zorn vector matrices over any commutative ring with unity are Moufang, though not necessarily simple. Some time is devoted to describing the structure of the resulting loops based on the underlying ring. In particular, the loops constructed over rings which have a nilpotent ideal of class 2 lend themselves to a useful loop extension style description.

The third chapter examines some results about the smallest Paige loop, which is constructed using the methods of chapter 2 over the finite field of two elements. This provides a base for the investigation of the loop constructed using the methods of Chapter 2 over the ring $\mathbb{Z}/4\mathbb{Z}$ which occurs in Chapters 4 and 5. The structure of this Paige loop has been well studied in (14) and elsewhere, therefore, this loop is somewhat more accessible than others and is a natural place to start. In this section, it is also shown that $GLL(\mathbb{Z}/pq\mathbb{Z}) \cong GLL(\mathbb{Z}/p\mathbb{Z}) \times GLL(\mathbb{Z}/q\mathbb{Z})$ when p and q are relatively prime. This suggests the importance of examining loops of the form $GLL(\mathbb{Z}/p^e\mathbb{Z})$ for p prime and the smallest such loop is the focus of the rest of the work.

The fourth chapter begins in earnest the study of the loop constructed over the ring $\mathbb{Z}/4\mathbb{Z}$. This chapter presents many calculational results which provide the basis for the work in Chapter 4, and which stand on their own as interesting and sometimes unexpected quirks of this loop. In particular, it is shown that all elements of this loop have order of 1, 2, 3, 4,, or 6. Each element's order can be predicted from the form of the vector matrix representing it, and this analysis is also presented here. Also, the chapter includes proofs about what elements of the loop commute with one another and uses this to conclude that if a subloop, L contains a copy of C_2^2, then the projection of L into the smallest Paige loop can not be isomorphic to L. The Sylow subloops are also listed here and some comments about associative subloops are also made. If the projective image of a subloop is cyclic, then that loop must be associative, for instance.

The fifth chapter studies portions of the subloop lattice of the loop over $\mathbb{Z}/4\mathbb{Z}$. Due to the large size of the loop in question, the focus remains on the possible orders of subloops although some structural information is provided where available. Particular attention is paid to subloops whose projective image in $GLL(\mathbb{Z}/2\mathbb{Z})$ is associative. The chapter organizes the subloops into sets based on how they project down to the smallest Paige loop. Particular attention is paid to subloops whose projective image in $GLL(\mathbb{Z}/2\mathbb{Z})$ is associative. This projective structure is very useful in understanding the larger loop and this is very evident throughout these sections. In addition, the height of the subloop lattice of $GLL(\mathbb{Z}/4\mathbb{Z})$ is determined to be 14.

The final chapter presents some open questions and future directions of study.

The first appendix contains specific examples of the loops mentioned in Chapter 4. They are constructed using the results and techniques expressed in earlier chapters, and are included as illustrations of these principles. It also provides a concrete starting place for anyone who wants to do calculations or further investigation of this loop.

The second appendix includes MATLAB® code that was used during this research. Many of these codes were simply used to conduct the everyday calculations of vector matrices quicker and more accurately than I could do by hand. They were also of considerable assistance in creating and verifying the examples in the first appendix. None of the proofs require the use of these codes, but if anyone wants to duplicate my results or examples, they would be served by having access to the codes I used. They are mostly self explanatory, but I comment on how they work and what they were used for during my research as each is displayed.

1.2 Quasigroups and loops

This section serves to review some of the basic definitions and properties of quasigroups and loops.

Definition 1.2.1. A *binar* is a set, Q together with a binary operation $\cdot : Q \times Q \to Q$.

A binar is also often called a *groupoid* or *magma* and is written $(Q, \cdot)$ or simply Q if the binary operation is known. In the sense of universal algebra it is an algebra of type $\{2\}$.

Definition 1.2.2. A *quasigroup* is a binar which satisfies the property that $xy = z$ has a unique solution if any two of the three variables are specified.

This is equivalent to saying that the multiplication table of a (finite) quasigroup is a Latin square. That is, each symbol appears exactly once in each column and once in each row. Another way to look at this is through the right and left multiplication maps, R_x and L_x, also often called translation maps. If these functions are defined as $R_x : Q \to Q; y \mapsto yx$ and $L_x : Q \to Q; y \mapsto xy$, then a binar is a quasigroup if and only if R_x and L_x are bijections for every element x.

Another common way of looking at quasigroups which is useful from a universal algebra perspective, is as an algebra $(Q, \cdot, /, \backslash)$ where the equations

$$x \cdot (x \backslash y) = y, \qquad (y/x) \cdot x = y, \qquad x \backslash (x \cdot y) = y, \qquad (y \cdot x)/x = y$$

hold for all $x, y \in Q$. This definition is equivalent to Definition 1.2.2, but has the advantage that it guarantees closure under homomorphic images and thus that quasigroups form a variety in the universal algebra sense.

Definition 1.2.3. A *neutral element* of a quasigroup, Q, is an element $e \in Q$ such that $ex = xe = x$ for all $x \in Q$.

If such a neutral element exists, it must be unique. If e_1 and e_2 are both neutral elements, then $e_1e_2 = e_1e_1$ and so $e_2L_{e_1} = e_1L_{e_1}$ and since the left multiplication map is a bijection, $e_1 = e_2$. This is, of course, the same argument used to show that the identity element of a group is unique. For this reason, the neutral element of a quasigroup is sometimes referred to as the identity element.

Definition 1.2.4. A *loop* is a quasigroup with a neutral element.

Since a loop is a quasigroup, for any element, x, there exist elements y and z such that $xy = zx = e$. It is convenient to refer to y in this case as the right inverse of x and z as the left inverse of x. In a group, the left and right inverses of an element are identical, but this is

not the case for loops in general. The following is the multiplication table of a loop in which the right and left inverses of every non neutral element are distinct.

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

Because neither loops nor quasigroups are generally associative, many equations can quickly become overburdened with parentheses. In order to reduce the number of necessary parentheses, this paper will adopt the following convention: that $xy \cdot z = (x \cdot y) \cdot z$ and $x \cdot yz = x \cdot (y \cdot z)$. So in general, the operation which is denoted by juxtaposition is to be done first and then the operation denoted by the actual symbol. Similarly, $xy \cdot yz = (x \cdot y) \cdot (y \cdot z)$ and so on.

Definition 1.2.5. Let P be a subloop of a loop, L. Then the *left coset* of P by x be $\{xp | p \in P\}$ denoted xP. Similarly, the right coset would be denoted Px.

Since multiplication on the left, or right, is bijective, all cosets of a given subloop, P, have the same cardinality.

Because loops are not associative, the definition of a normal subloop is slightly more complicated than that of a normal subgroup. Still, obvious similarities exist between the two.

Definition 1.2.6. Let P be a subloop of a loop, L. Then P is normal in L if

$$xP = Px, \qquad (xP)y = x(Py), \qquad x(yP) = (xy)P$$

holds for every x and y in L.

For a normal subloop, P, it is easy to show that the set of left cosets of P, denoted L/P,

has a well defined coset multiplication.

$$xP \cdot yP = x(P \cdot yP) = x(Py \cdot P) = x(yP \cdot P) = x(y \cdot PP) = x \cdot yP = xy \cdot P$$

Of course, a similar statement can be made about right cosets.

1.3 Moufang Loops

Loops are such a general structure, that it is daunting to classify them all without restricting in some way which ones should be considered. The common way to do this is to look at sets of loops that fulfill some property, which is usually a weakened form of associativity. Bol and Moufang loops are both examples of this. It is instructive to see, in some sense, how much associativity is needed for various theorems to hold. The loops examined in this thesis are all Moufang loops and so this section is devoted to providing some background on them.

Definition 1.3.1. A *Moufang loop* is a loop which further satisfies any of the (equivalent) Moufang identities:

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

Moufang loops also satisfy the alternative and flexible laws, so that

$$x(xy) = (xx)y, \quad (xy)y = x(yy), \quad (xy)x = x(yx).$$

This can easily be shown by setting y or z to the identity element in the Moufang identities.

The main result on Moufang loops that is used in this paper is Moufang's Theorem (15) which is stated below:

Theorem 1.3.2. *If x, y, and z are elements of a Moufang loop and associate in any order, then x, y, and z generate an associative subloop.*

Combining Moufang's theorem and the previous identities, it is easy to see that Moufang

loops are diassociative, that is, any two elements generate an associative subloop. This fact is used repeatedly throughout this paper and often without specific mention.

Proposition 1.3.3. *In a Moufang loop, the right and left inverses of any element must be equal. That is for any x in a Moufang loop, L, there exists an element $x^{-1} \in L$ such that $xx^{-1} = e$ and $x^{-1}x = e$.*

Proof. Let z be the right inverse of x, so that $xz = e$. Since L is diassociative, $x \cdot zx = xz \cdot x = x = xe$. Since L_x is a bijection, $zx = e$. □

All groups are Moufang loops since the associative law implies the Moufang identities. Indeed, any Moufang loop of order less than 12 is actually a group as proved by Chein and Pflugfelder in (5). The smallest nonassociative Moufang loop is order 12 and can be constructed from S_3 in a manner detailed in (4) and discussed in section 1.4.

A number of familiar theorems involving groups still hold in some form in the Moufang loop case. Some of the more important are listed here with reference.

Theorem 1.3.4. *If L is a finite Moufang loop and $P \leq L$, then $|P|$ divides $|L|$.*

This result was proved independently and in different ways in (11) and (10). Obviously, this theorem has value in classifying subloops in the finite case which is a large portion of this paper's work.

Sylow's Theorem also has a Moufang loop analogue, however, there is some restriction on the primes that are allowed. In order to understand this restriction, it is necessary to talk about the class of finite nonassociative simple loops.

Simple groups are the building blocks of group theory and it is no surprise that the search for finite simple Moufang loops was an early priority for loop theory. Obviously, any finite simple group is also a finite simple Moufang loop, but finding nonassociative examples was difficult. The first to find such a family of loops was Paige in (16). Each loop is constructed over a finite field of prime power order. For now, the Paige loop constructed over F_p will be referred to as $M(p)$. The construction used in that paper involves vector matrices and will be detailed later so no further remarks will be made here except to note that the smallest

simple nonassociative Moufang loop is order 120 and contains elements of order 2 and 3. The immediate consequence is that the existence portion of Sylow's theorem need not hold in every case, since 120 is divisible by 5 and yet there is clearly no subloop of order 5 in this case. Indeed all of the Paige loops provide some counterexample of this sort.

In (13), Liebeck proves that all finite simple nonassociative Moufang loops are isomorphic to the loops which Paige constructed. This family of loops is now commonly referred to as the Paige loops. Liebeck's proof relies heavily on the work of Doro in (7) which connects simple Moufang loops to simple groups with triality. Grishkov and Zavarnitsine noted in (12) that every Moufang loop has a unique normal sequence and that the presence of $M(q)$ in these sequences determines which primes satisfy Sylow's Theorem.

Definition 1.3.5. Let L be a Moufang loop. A prime p is called a *Sylow prime for* L if for every composition factor of L which is isomorphic to $M(q)$ for some q, then $p \nmid \frac{q^2+1}{(2,q-1)}$.

Theorem 1.3.6. *Let L be a finite Moufang loop and let p be a prime. Then L has a Sylow p-subloop if and only if p is a Sylow prime for L.*

This existence theorem is proven in (12). In (9), Gagola proves that any p-subloop in a Moufang loop, L, where p is a Sylow prime for L, is contained in a Sylow p-subloop of L. This familiar result provides some tools for describing the subloop structure of Moufang loops.

This is far from an exhaustive treatment of Moufang loop theory and readers interested in more information would do well to read Bruck's survey (2) which contains extensive information on Moufang loops and other quasigroups. Other books on quasigroups and loops that can provide a good background are Pflugfelder's (17) and the related book edited by Chein, Plugfelder and Smith (6).

1.4 Chein's construction

In a number of places throughout this work, there will be a need to refer to specific loops. If a loop is associative, then it will be referred to by its usual group name. All the nonassociative loops that appear will be defined as needed, but there is a class of such loops with an established notation which will be noted here.

In (4), Chein details a method of constructing a non-associative Moufang loop of order $2n$ from a non-abelian group of order n. A loop formed in this way is written $M_{2n}(G, 2)$ and such loops appear in the subloop lattice of the smallest Paige loop so it is necessary to provide some information about them up front.

In Chein's construction the underlying set of the loop is all elements of the form gh^a where $g \in G$ and h is an abstract element of order two. The multiplication is given by

$$g_1 h^\delta \cdot g_2 h^\epsilon = (g_1^\nu g_2^\mu)^\nu h^{\delta+\epsilon}$$

where $\nu = (-1)^\epsilon$ and $\mu = (-1)^{\delta+\epsilon}$ (4). This could also be summarized as

$$\begin{aligned} g_1 h \cdot g_2 h &= (g_1^{-1} g_2)^{-1} = g_2^{-1} g_1 \\ g_1 h \cdot g_2 &= g_1 g_2^{-1} h \\ g_1 \cdot g_2 h &= (g_1^{-1} g_2^{-1})^{-1} x = g_2 g_1 h \\ g_1 \cdot g_2 &= g_1 g_2. \end{aligned}$$

In (4), it is proven that such loops are nonassociative if G is nonabelian to start with. This is a convenient way to classify a number of finite loops of relatively small order. For instance, the smallest nonassociative Moufang loop is $M_{12}(S_3, 2)$.

CHAPTER 2. CONSTRUCTION OVER COMMUTATIVE RINGS

Paige constructed an important class of finite simple nonassociative Moufang loops in his famous paper (16). This class of loops is now traditional referred to as Paige loops. They are constructed using vector matrices over finite fields. Paige credits this construction to Zorn, but this construction has appeared a number of times. What follows is the same construction, except that the entries of the vector matrices come from a commutative unital ring as opposed to a finite field. The result is also a class of Moufang loops, which are not simple in general, of course, but which share some properties with Paige loops. In particular, it is possible to define a norm on these loops which is multiplicative. The first section follows the approach of Paige in (16) very closely with the appropriate adjustments made for the presence of zero divisors in the base ring. The next section explores the structure of these loops by examining a decomposition based on projecting vector matrix entries from the base ring to that ring modulo some ideal. Particular interest is shown to the case where said ideal is maximal.

2.1 The Construction

Let R be a commutative ring with identity. The set $\mathrm{Zorn}(R)$ is a non-associative ring constructed in the following way. The elements of $\mathrm{Zorn}(R)$ are matrices of the form $\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix}$ where a and b are elements of R, and $\mathbf{u}$ and $\mathbf{v}$ are elements of R^3. Addition is carried out componentwise. The multiplication is given by

$$\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} c & \mathbf{w} \\ \mathbf{x} & d \end{bmatrix} = \begin{bmatrix} ac + \mathbf{u} \cdot \mathbf{x} & a\mathbf{w} + d\mathbf{u} - \mathbf{v} \times \mathbf{x} \\ c\mathbf{v} + b\mathbf{x} + \mathbf{u} \times \mathbf{w} & bd + \mathbf{v} \cdot \mathbf{w} \end{bmatrix}$$

where $\mathbf{u} \cdot \mathbf{v}$ and $\mathbf{u} \times \mathbf{v}$ represent the usual dot product and cross product of $\mathbf{u}$ and $\mathbf{v}$. This is the same formula that Paige uses in (16) and can also be found in this form in (8), (19), and (20).

Some basic properties of the cross product and dot product are used repeatedly throughout this section and later sections. Specifically,

1. $\mathbf{u} \cdot (\mathbf{u} \times \mathbf{v}) = 0$
2. $\mathbf{u} \times \mathbf{v} = -(\mathbf{v} \times \mathbf{u})$
3. $\mathbf{u} \times (\mathbf{v} \times \mathbf{w}) = (\mathbf{u} \cdot \mathbf{w})\mathbf{v} - (\mathbf{u} \cdot \mathbf{v})\mathbf{w}$

hold in R because R is a commutative ring. Verification of these three equations is a simple matter of writing out each side and noting that they are identical.

Proposition 2.1.1. Zorn(R) *is an alternative algebra.*

Proof. Since R is an abelian group under its addition, and addition is carried out in Zorn(R) componentwise, it is obvious that Zorn(R) forms an abelian group under addition. Now calculations verify that the multiplication indeed distributes over the addition:

$$\begin{aligned}
&\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \left(\begin{bmatrix} c & \mathbf{w} \\ \mathbf{x} & d \end{bmatrix} + \begin{bmatrix} e & \mathbf{y} \\ \mathbf{z} & f \end{bmatrix} \right) = \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} c+e & \mathbf{w}+\mathbf{y} \\ \mathbf{x}+\mathbf{z} & d+f \end{bmatrix} \\
&= \begin{bmatrix} ac + ae + \mathbf{u}\cdot\mathbf{x} + \mathbf{u}\cdot\mathbf{z} & a\mathbf{w} + a\mathbf{y} + \mathbf{u}d + \mathbf{u}f - \mathbf{v}\times\mathbf{x} - \mathbf{v}\times\mathbf{z} \\ c\mathbf{v} + e\mathbf{v} + b\mathbf{x} + b\mathbf{z} + \mathbf{u}\times\mathbf{w} + \mathbf{u}\times\mathbf{y} & bd + bf + \mathbf{v}\cdot\mathbf{w} + \mathbf{v}\cdot\mathbf{y} \end{bmatrix} \\
&= \begin{bmatrix} ac + \mathbf{u}\cdot\mathbf{x} & a\mathbf{w} + \mathbf{u}d - \mathbf{v}\times\mathbf{x} \\ \mathbf{v}c + b\mathbf{x} + \mathbf{u}\times\mathbf{w} & bd + \mathbf{u}\cdot\mathbf{w} \end{bmatrix} + \begin{bmatrix} ae + \mathbf{u}\cdot\mathbf{z} & a\mathbf{y} + \mathbf{u}f - \mathbf{v}\times\mathbf{z} \\ \mathbf{v}e + b\mathbf{z} + \mathbf{u}\times\mathbf{y} & bf + \mathbf{u}\cdot\mathbf{y} \end{bmatrix} \\
&= \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} c & \mathbf{w} \\ \mathbf{x} & d \end{bmatrix} + \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} e & \mathbf{y} \\ \mathbf{z} & f \end{bmatrix}.
\end{aligned}$$

This is actually fairly obvious, since matrix multiplication is distributive, multiplication in the ring is distributive, and both the dot product and cross product are distributive.

While the multiplication is not associative, it does satisfy the alternative law. That is, $x(xy) = (xx)y$ and $(xy)y = x(yy)$. The calculation is elementary and only one of the identities is included:

$$\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} . \begin{bmatrix} c & \mathbf{w} \\ \mathbf{x} & d \end{bmatrix} = \begin{bmatrix} a^2 + \mathbf{u}\cdot\mathbf{v} & (a+b)\mathbf{u} \\ (a+b)\mathbf{v} & b^2 + \mathbf{u}\cdot\mathbf{v} \end{bmatrix} \begin{bmatrix} c & \mathbf{w} \\ \mathbf{x} & d \end{bmatrix},$$

whereas

$$\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} . \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} c & \mathbf{w} \\ \mathbf{x} & d \end{bmatrix} = \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} ac + \mathbf{u}\cdot\mathbf{x} & a\mathbf{w} + d\mathbf{u} - \mathbf{v}\times\mathbf{x} \\ c\mathbf{v} + b\mathbf{x} + \mathbf{u}\times\mathbf{w} & bd + \mathbf{v}\cdot\mathbf{w} \end{bmatrix}$$

The upper left coordinate in the first multiplication is

$$a^2c + c\mathbf{u}\cdot\mathbf{v} + a\mathbf{u}\cdot\mathbf{x} + b\mathbf{u}\cdot\mathbf{x}\,.$$

In the second multiplication, the upper left coordinate is

$$a^2c + a\mathbf{u}\cdot\mathbf{x} + c\mathbf{u}\cdot\mathbf{v} + b\mathbf{u}\cdot\mathbf{x} + \mathbf{u}\cdot(\mathbf{u}\times\mathbf{w})\,.$$

These two clearly coincide since $\mathbf{u}\cdot(\mathbf{u}\times\mathbf{w})$ is zero.

The upper right coordinate in the first multiplication is

$$(a^2 + \mathbf{u}\cdot\mathbf{v})\mathbf{w} + d(a+b)\mathbf{u} - (a+b)\mathbf{v}\times\mathbf{x}\,,$$

and in the second multiplication it is

$$a^2\mathbf{w} + ad\mathbf{u} - a\mathbf{v}\times\mathbf{x} + bd\mathbf{u} + (\mathbf{v}\cdot\mathbf{w})\mathbf{u} - b\mathbf{v}\times\mathbf{x} - \mathbf{v}\times(\mathbf{u}\times\mathbf{w})\,.$$

The tow are equal to each other because $\mathbf{v}\times(\mathbf{u}\times\mathbf{w}) = (\mathbf{v}\cdot\mathbf{w})\mathbf{u} - (\mathbf{v}\cdot\mathbf{u})\mathbf{w}$.

Equality in the other coordinates follows similarly, and so the first alternative law is satisfied. The second can be proved in an analogous fashion. □

Since Zorn(R) is an alternative algebra, the multiplicative elements obey the Moufang laws:

$$a(x(ay)) = (axa)y,\ ((xa)y)a = x(aya),\ (ax)(ya) = a(xy)a$$

This is shown in (3), and Paige references this same work in (16). This reference contains a lot of information about the properties of alternative rings and Albert's paper (1) also has some classic results on these structures.

Following Paige, define a norm on Zorn(R).

Definition 2.1.2. The *norm* of an element, x, is denoted $N(x)$ and defined by

$$N\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} := ab - \mathbf{u}\cdot\mathbf{v}.$$

Note that this is an obvious analogue of the determinant.

Proposition 2.1.3. *The norm is multiplicative on elements of* Zorn(R).

Proof.

$$\begin{aligned}
N\left(\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix}\begin{bmatrix} c & \mathbf{w} \\ \mathbf{x} & d \end{bmatrix}\right) &= N\left(\begin{bmatrix} ac+\mathbf{u}\cdot\mathbf{x} & a\mathbf{w}+d\mathbf{u}-\mathbf{v}\times\mathbf{x} \\ c\mathbf{v}+b\mathbf{x}+\mathbf{u}\times\mathbf{w} & bd+\mathbf{v}\cdot\mathbf{w} \end{bmatrix}\right) \\
&= (ac+\mathbf{u}\cdot\mathbf{x})(bd+\mathbf{v}\cdot\mathbf{w}) - (a\mathbf{w}+\mathbf{u}d-\mathbf{v}\times\mathbf{x})\cdot(c\mathbf{v}+b\mathbf{x}+\mathbf{u}\times\mathbf{w}) \\
&= acbd + (\mathbf{u}\cdot\mathbf{x})(\mathbf{v}\cdot\mathbf{w}) - ab\mathbf{w}\cdot\mathbf{x} - dc\mathbf{u}\cdot\mathbf{v} + (\mathbf{v}\times\mathbf{x})\cdot(\mathbf{u}\times\mathbf{w}) \\
&= acbd + (\mathbf{u}\cdot\mathbf{x})(\mathbf{v}\cdot\mathbf{w}) - ab\mathbf{w}\cdot\mathbf{x} - dc\mathbf{u}\cdot\mathbf{v} + (\mathbf{u}\cdot\mathbf{v})(\mathbf{w}\cdot\mathbf{x}) - (\mathbf{u}\cdot\mathbf{x})(\mathbf{v}\cdot\mathbf{w}) \\
&= ab(cd-\mathbf{w}\cdot\mathbf{x}) - \mathbf{u}\cdot\mathbf{v}(cd-\mathbf{w}\cdot\mathbf{x}) \\
&= (ab-\mathbf{u}\cdot\mathbf{v})(cd-\mathbf{w}\cdot\mathbf{x}) \\
&= N\left(\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix}\right) N\left(\begin{bmatrix} c & \mathbf{w} \\ \mathbf{x} & d \end{bmatrix}\right).
\end{aligned}$$

□

Proposition 2.1.4. *A vector matrix is invertible if and only if its norm is a unit in R.*

Proof. Let M be an invertible vector matrix. Then:

$$\begin{aligned} MM^{-1} &= I \Rightarrow \\ N(MM^{-1}) &= N(I) \Rightarrow \\ N(M)N(M^{-1}) &= 1\,, \end{aligned}$$

so $N(M)$ must be a unit in R. If $N(M)$ is a unit, then

$$\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} N(M)^{-1}b & -N(M)^{-1}\mathbf{u} \\ -N(M)^{-1}\mathbf{v} & N(M)^{-1}a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

□

The results of this section are summarized in the following proposition.

Proposition 2.1.5. *Let $GLL(R)$ be the set of invertible elements of* $\mathrm{Zorn}(R)$*. Then $GLL(R)$ is a Moufang loop.*

2.2 Extensions over a kernel

Let R be a commutative ring with an ideal I. Let

$$\pi : GLL(R) \to GLL(R/I); [a_{ij}] \mapsto [a_{ij} + I]$$

be componentwise projection from R to R/I.

Definition 2.2.1. Define the set Γ to be the pre-image of the identity element of R/I under the projection π. That is, $\Gamma = \pi^{-1}\{1_{R/I}\}$.

Note that Γ is a subloop of $GLL(R)$, since π is a homomorphism.

Definition 2.2.2. If $f : S \to R$, call a section of f *normalized* if it maps the identity of S to the identity of R.

Proposition 2.2.3. *Let i be a normalized section of π. Then $\Gamma \times GLL(R/I)$ forms a loop with multiplication given by*

$$\langle n, q\rangle * \langle m, r\rangle = \langle (n(qi) \cdot m(ri))((qr)i)^{-1}, qr\rangle. \tag{2.2.1}$$

Proof. The second coordinate of this product is again an element of $GLL(R/I)$, but calculation must verify that the first coordinate of the product is an element of Γ. Since π is a loop homomorphism,

$$\begin{aligned}((n(qi) \cdot m(ri))((qr)i)^{-1})\pi &= ((n(qi) \cdot m(ri))\pi((qr)i\pi)^{-1} \\ &= ((n\pi(qi\pi) \cdot m\pi(ri\pi)) \cdot ((qr)i\pi)^{-1} \\ &= (qr)(qr)^{-1} \\ &= 1\,,\end{aligned}$$

so $(n(qi)\cdot m(ri))((qr)i)^{-1} \in \Gamma$. Thus the multiplication is indeed a map from $(\Gamma \times GLL(R/I))^2$ to $\Gamma \times GLL(R/I)$.

Obviously,

$$\langle n, q\rangle * \langle 1_{GLL(R)}, 1_{GLL(R/I)}\rangle = \langle n(qi)(qi)^{-1}, q\rangle = \langle n, q\rangle$$

and

$$\langle 1_{GLL(R)}, 1_{GLL(R/I)}\rangle * \langle n, q\rangle = \langle n(qi)(qi)^{-1}, q\rangle = \langle n, q\rangle\,,$$

so $\langle 1_{GLL(R)}, 1_{GLL(R/I)}\rangle$ acts as an identity on this binar.

Furthermore,

$$\begin{aligned}
&\langle n, q\rangle * \langle (qi)^{-1}n^{-1}\cdot(q^{-1}i)^{-1}), q^{-1}\rangle \\
&\qquad = \langle n(qi)\cdot((qi)^{-1}n^{-1}\cdot(q^{-1}i)^{-1})(q^{-1}i)\cdot(qq^{-1})i^{-1}, qq^{-1}\rangle \\
&\qquad = \langle n(qi)\cdot((qi)^{-1}n^{-1}\cdot(q^{-1}i)^{-1})(q^{-1}i), 1_{GLL(R/I)}\rangle \\
&\qquad = \langle n(qi)\cdot((qi)^{-1}n^{-1}\cdot(q^{-1}i)^{-1}(q^{-1}i)), 1_{GLL(R/I)}\rangle \\
&\qquad = \langle n(qi)\cdot(qi)^{-1}n^{-1}, 1_{GLL(R/I)}\rangle \\
&\qquad = \langle 1_{GLL(R)}, 1_{GLL(R/I)}\rangle.
\end{aligned}$$

So the inverse of any element is easily calculated.

This inverse element is actually in the set $\Gamma \times GLL(R/I)$, specifically $(qi)^{-1}n^{-1}\cdot(q^{-1}i)^{-1} \in \Gamma$:

$$\begin{aligned}
((qi)^{-1}n^{-1}\cdot(q^{-1}i)^{-1})\pi &= ((qi)^{-1}n^{-1})\pi\cdot(q^{-1}i\pi)^{-1} \\
&= (qi\pi)^{-1}(n\pi)^{-1}\cdot(q^{-1})^{-1} \\
&= q^{-1}q \\
&= 1_{GLL(R/I)}\,.
\end{aligned}$$

So indeed this multiplication forms a loop on the set $\Gamma \times GLL(R/I)$. □

Proposition 2.2.4. *The loops $GLL(R)$ and $\Gamma \times GLL(R/I)$ are isomorphic when the latter is equipped with the multiplication from* (2.2.1).

Proof. Define a map $\phi : GLL(R) \to \Gamma \times GLL(R/I); g \mapsto \langle g\cdot(g\pi i)^{-1}, g\pi\rangle$. First, $g\cdot(g\pi i)^{-1}$ must indeed be an element of Γ. Since π is a loop homomorphism,

$$(g\cdot(g\pi i)^{-1})\pi = g\pi\cdot(g\pi i\pi)^{-1} = g\pi\cdot(g\pi)^{-1} = 1_{GLL(R/I)}.$$

Therefore $g\cdot(g\pi i)^{-1}$ is in Γ.

The following shows that ϕ is a loop homomorphism. Let $g, h \in GLL(R)$. Then

$$\begin{aligned} g\phi h\phi &= \langle g(g\pi i)^{-1}, g\pi\rangle * \langle h(h\pi i)^{-1}, h\pi\rangle \\ &= \langle (g(g\pi i)^{-1} \cdot g\pi i)(h(h\pi i)^{-1} \cdot h\pi i) \cdot ((g\pi h\pi)i)^{-1}, g\pi h\pi\rangle \\ &= \langle (g \cdot (g\pi i)^{-1} g\pi i)(h \cdot (h\pi i)^{-1} h\pi i) \cdot ((gh)\pi i)^{-1}, gh\pi\rangle \\ &= \langle gh \cdot ((gh)\pi i)^{-1}, gh\pi\rangle \\ &= (gh)\phi\,. \end{aligned}$$

Note that this depends on the multiplication in $GLL(R)$ being diassociative. Since $GLL(R)$ is a Moufang loop, this is fine.

Define another map $\psi : \Gamma \times GLL(R/I) \to GLL(R); \langle n, q\rangle \mapsto n(qi)$. Next note that ψ is also a loop homomorphism. In order to ensure that ψ preserves the identity, it is necessary to force i to preserve the identity. This is the only restriction on the choice of the section i:

$$\begin{aligned} (\langle n, q\rangle * \langle m, r\rangle)\psi &= \langle (nqi \cdot mri)((qr)i)^{-1}, qr\rangle\psi \\ &= (nqi \cdot mri)((qr)i)^{-1} \cdot (qr)i \\ &= (nqi \cdot mri) \cdot ((qr)i)^{-1}(qr)i \\ &= nqi \cdot mri \\ &= \langle n, q\rangle\psi\langle m, r\rangle\psi\,. \end{aligned}$$

Now it is easy to simply verify that ϕ and ψ are inverses of each other:

$$\begin{aligned} g\phi\psi &= \langle g(g\pi i)^{-1}, g\pi\rangle\psi \\ &= g(g\pi i)^{-1} \cdot g\pi i \\ &= g \cdot (g\pi i)^{-1} g\pi i \\ &= g \end{aligned}$$

and

$$\begin{aligned}\langle n,q\rangle\psi\phi &= n(qi)\phi \\ &= \langle nqi\cdot((nqi)\pi i)^{-1}, nqi\pi\rangle \\ &= \langle nqi\cdot(n\pi qi\pi i)^{-1}, n\pi qi\pi\rangle \\ &= \langle nqi\cdot(qi)^{-1}, q\rangle \\ &= \langle n\cdot qi(qi)^{-1}, q\rangle \\ &= \langle n,q\rangle\,.\end{aligned}$$

Thus $GLL(R)$ is isomorphic to $(\Gamma\times GLL(R/I),*)$. In the language of loop extensions, $GLL(R)$ is an extension of Γ by $GLL(R/I)$. □

Now examine possibilities for the structure of Γ. Let $A=\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix}$ be an element of Γ. Then since $A\pi=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, it must be the case that a and b are both in $1+I$ and that the entries of $\mathbf{u}$ and $\mathbf{v}$ are in I.

Proposition 2.2.5. *If $I^2=0$, then Γ is isomorphic to the direct product I^8.*

Proof. Note that if all the entries of $\mathbf{u}$ and $\mathbf{v}$ are in I, then clearly $\mathbf{u}\cdot\mathbf{v}$ and the entries of $\mathbf{u}\times\mathbf{v}$ are all in I^2, and hence 0.

Consider the map

$$f: I^8\to\Gamma; (x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)\mapsto \begin{bmatrix} 1+x_1 & (x_2,x_3,x_4) \\ (x_5,x_6,x_7) & 1+x_8 \end{bmatrix}.$$

This map is actually a group isomorphism.

Let $\mathbf{x}=(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)$ and $\mathbf{y}=(y_1,y_2,y_3,y_4,y_5,y_6,y_7,y_8)$ be elements of I^8.

Then

$$\begin{aligned} f(\mathbf{x})f(\mathbf{y}) &= \begin{bmatrix} 1+x_1 & (x_2,x_3,x_4) \\ (x_5,x_6,x_7) & 1+x_8 \end{bmatrix} \begin{bmatrix} 1+y_1 & (y_2,y_3,y_4) \\ (y_5,y_6,y_7) & 1+y_8 \end{bmatrix} \\ &= \begin{bmatrix} 1+x_1+y_1 & (x_2+y_2,x_3+y_3,x_4+y_4) \\ (x_5+y_5,x_6+y_6,x_7+y_7) & 1+x_8+y_8 \end{bmatrix} \\ &= f(\mathbf{x}+\mathbf{y})\,, \end{aligned}$$

so f is a homomorphism. The kernel of f is clearly trivial, so f is injective. Furthermore, f is obviously onto and hence an isomorphism. □

From here on, when this paper refers to $\Gamma \times GLL(R/I)$, assume the multiplication $*$ defined in (2.2.1).

2.2.1 Subloop extension structure

Let L be a subloop of $GLL(R)$ for some commutative ring with identity, R. Then the same methods detailed above can decompose L into two pieces: a subgroup of the kernel, and a subloop of $GLL(R/I)$.

Proposition 2.2.6. *Let L be a subloop of $GLL(R)$. Choose $i : L\pi \to L$ to be a normalized section of π which maps an element $x\pi$ to an element of $L \cap (x\pi + I)$. Then the set $\Gamma(L) = \{x \cdot (x\pi i)^{-1} : x \in L\} = L \cap \Gamma$ is a subgroup of Γ and $L \cong \Gamma(L) \times L\pi$.*

Proof. By construction, $x\pi i \in L$ and so $\Gamma(L)$ is a contained in L. Applying π to the elements of $\Gamma(L)$ gives

$$(x(x\pi i)^{-1})\pi = x\pi \cdot (x\pi i\pi)^{-1} = x\pi \cdot (x\pi)^{-1} = 1_{\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*}\,,$$

so $\Gamma(L)$ is contained in $L \cap \Gamma$.

If $x \in L \cap \Gamma$, then $x\pi = 1_{GLL(R/I)}$ and so since i is normalized, $x\pi i = 1_{GLL(R)}$. Thus $x = x(x\pi i)^{-1} \in \Gamma(L)$ and so $\Gamma(L) = L \cap \Gamma$, which is obviously a subgroup of Γ.

The maps ϕ and ψ restricted to L and $\Gamma(L) \times L\pi$ respectively exhibit the necessary isomorphism. $\square$

2.3 Representing Chein's Construction

In (4), Chein details a method of constructing a non-associative Moufang loop of order $2n$ from a non-abelian group of order n. The goal of this section is to represent many of these constructed loops using vector matrices.

Let G be a non-abelian group with a faithful, two-dimensional representation over a commutative ring with identity, R. Then there exists a homomorphism $\phi : G \to GL_2(R)$ which is an embedding.

First we choose two orthogonal unit vectors in R^3 whose cross product is also of unit length. That is, we choose $\mathbf{u}$ and $\mathbf{v}$ such that $\mathbf{u} \cdot \mathbf{v} = 0$ and $(\mathbf{u} \times \mathbf{v}) \cdot (\mathbf{u} \times \mathbf{v}) = \mathbf{u} \cdot \mathbf{u} = \mathbf{v} \cdot \mathbf{v} = 1$.

Consider the map $\psi : GL_2(R) \to \mathrm{Z}(R)$; $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix}$.

Proposition 2.3.1. *The map ψ is an embedding.*

Proof. Note that the norm of $\begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} = ad - b\mathbf{u} \cdot c\mathbf{u} = ad - bc\mathbf{u} \cdot \mathbf{u} = ad - bc$ so ψ does indeed map elements of $GL_2(R)$ to invertible vector matrices.

The map is obviously injective, so we simply show that it is a homomorphism.

$$\begin{aligned}
\begin{bmatrix} a & b \\ c & d \end{bmatrix} \psi \begin{bmatrix} w & x \\ y & z \end{bmatrix} \psi &= \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} \begin{bmatrix} w & x\mathbf{u} \\ y\mathbf{u} & z \end{bmatrix} \\
&= \begin{bmatrix} aw + by & (ax + bz)\mathbf{u} \\ (cw + dy)\mathbf{u} & cx + dz \end{bmatrix} \\
&= \begin{bmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{bmatrix} \psi \\
&= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} w & x \\ y & z \end{bmatrix} \right) \psi
\end{aligned}$$

□

Now we have an embedding $\phi\psi : G \to \mathrm{Z}(R)$. In Chein's construction the underlying set of the loop is all elements of the form gh^a where $g \in G$ and h is an abstract element of order two. The multiplication is given by

$$g_1 h^\delta \cdot g_2 h^\epsilon = (g_1^\nu g_2^\mu)^\nu h^{\delta+\epsilon}$$

where $\nu = (-1)^\epsilon$ and $\mu = (-1)^{\delta+\epsilon}$ (4). This could also be summarized as

$$\begin{aligned} g_1 h \cdot g_2 h &= (g_1^{-1} g_2)^{-1} = g_2^{-1} g_1 \\ g_1 h \cdot g_2 &= g_1 g_2^{-1} h \\ g_1 \cdot g_2 h &= (g_1^{-1} g_2^{-1})^{-1} x = g_2 g_1 h \\ g_1 \cdot g_2 &= g_1 g_2. \end{aligned}$$

This construction can be done entirely within $\mathrm{Z}(R)$ by using the images $g\phi\psi$ for the elements of G and the vector matrix $\begin{bmatrix} 0 & \mathbf{v} \\ \mathbf{v} & 0 \end{bmatrix}$ for the element h.

Note that $\begin{bmatrix} 0 & \mathbf{v} \\ \mathbf{v} & 0 \end{bmatrix} \begin{bmatrix} 0 & \mathbf{v} \\ \mathbf{v} & 0 \end{bmatrix} = \begin{bmatrix} \mathbf{v}\cdot\mathbf{v} & 0 \\ 0 & \mathbf{v}\cdot\mathbf{v} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ so h is indeed order two.

Also, by direct computation, we see that

$$\begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} \begin{bmatrix} 0 & \mathbf{v} \\ \mathbf{v} & 0 \end{bmatrix} = \begin{bmatrix} b\mathbf{u}\cdot\mathbf{v} & a\mathbf{v} - c\mathbf{u}\times\mathbf{v} \\ d\mathbf{v} + b\mathbf{u}\times\mathbf{v} & c\mathbf{u}\cdot\mathbf{v} \end{bmatrix} = \begin{bmatrix} 0 & a\mathbf{v} - c\mathbf{u}\times\mathbf{v} \\ d\mathbf{v} + b\mathbf{u}\times\mathbf{v} & 0 \end{bmatrix}.$$

Now we simply check that each multiplication behaves appropriately.

$$
\begin{aligned}
g_1 h \cdot g_2 h &= \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} h \cdot \begin{bmatrix} w & x\mathbf{u} \\ y\mathbf{u} & z \end{bmatrix} h \\
&= \begin{bmatrix} 0 & a\mathbf{v} - c\mathbf{u} \times \mathbf{v} \\ d\mathbf{v} + b\mathbf{u} \times \mathbf{v} & 0 \end{bmatrix} \begin{bmatrix} 0 & w\mathbf{v} - y\mathbf{u} \times \mathbf{v} \\ z\mathbf{v} + x\mathbf{u} \times \mathbf{v} & 0 \end{bmatrix} \\
&= \begin{bmatrix} (a\mathbf{v} - c\mathbf{u} \times \mathbf{v}) \cdot (z\mathbf{v} + x\mathbf{u} \times \mathbf{v}) & -(d\mathbf{v} + b\mathbf{u} \times \mathbf{v}) \times (z\mathbf{v} + x\mathbf{u} \times \mathbf{v}) \\ (a\mathbf{v} - c\mathbf{u} \times \mathbf{v}) \times (w\mathbf{v} - y\mathbf{u} \times \mathbf{v}) & (d\mathbf{v} + b\mathbf{u} \times \mathbf{v}) \cdot (w\mathbf{v} - y\mathbf{u} \times \mathbf{v}) \end{bmatrix} \\
&= \begin{bmatrix} az|\mathbf{v}|^2 - cx|\mathbf{u} \times \mathbf{v}|^2 & -dx|\mathbf{v}|^2\mathbf{u} + bz|\mathbf{v}|^2\mathbf{u} \\ -ay|\mathbf{v}|^2\mathbf{u} + cw|\mathbf{v}|^2\mathbf{u} & dw|\mathbf{v}|^2 - by|\mathbf{u} \times \mathbf{v}|^2 \end{bmatrix} \\
&= \begin{bmatrix} az - cx & (bz - dx)\mathbf{u} \\ (cw - ay)\mathbf{u} & dw - by \end{bmatrix} \\
&= \begin{bmatrix} z & -x\mathbf{u} \\ -y\mathbf{u} & w \end{bmatrix} \cdot \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} \\
&= g_2^{-1} g_1.
\end{aligned}
$$

$$
\begin{aligned}
g_1 h \cdot g_2 &= \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} x \cdot \begin{bmatrix} w & x\mathbf{u} \\ y\mathbf{u} & z \end{bmatrix} \\
&= \begin{bmatrix} 0 & a\mathbf{v} - c\mathbf{u}\times\mathbf{v} \\ d\mathbf{v} + b\mathbf{u}\times\mathbf{v} & 0 \end{bmatrix} \begin{bmatrix} w & x\mathbf{u} \\ y\mathbf{u} & z \end{bmatrix} \\
&= \begin{bmatrix} 0 & (az-by)\mathbf{v} + (dy-cz)\mathbf{u}\times\mathbf{v} \\ (dw-cx)\mathbf{v} + (bw-ax)\mathbf{u}\times\mathbf{v} & 0 \end{bmatrix} \\
&= \begin{bmatrix} az-by & (bw-ax)\mathbf{u} \\ (cz-dy)\mathbf{u} & dw-cx \end{bmatrix} h \\
&= \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} \begin{bmatrix} z & -x\mathbf{u} \\ -y\mathbf{u} & w \end{bmatrix} h \\
&= g_1 g_2^{-1} \cdot h
\end{aligned}
$$

$$
\begin{aligned}
g_1 \cdot g_2 h &= \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} \cdot \begin{bmatrix} w & x\mathbf{u} \\ y\mathbf{u} & z \end{bmatrix} x \\
&= \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} \begin{bmatrix} 0 & w\mathbf{v} - y\mathbf{u}\times\mathbf{v} \\ z\mathbf{v} + x\mathbf{u}\times\mathbf{v} & 0 \end{bmatrix} \\
&= \begin{bmatrix} 0 & (aw+cx)\mathbf{v} - (ay+cz)\mathbf{u}\times\mathbf{v} \\ (dz+by)\mathbf{v} + (bw+dx)\mathbf{u}\times\mathbf{v} & 0 \end{bmatrix} \\
&= \begin{bmatrix} aw+cx & (bw+dx)\mathbf{u} \\ (ay+cz)\mathbf{u} & dz+by \end{bmatrix} h \\
&= \begin{bmatrix} w & x\mathbf{u} \\ y\mathbf{u} & z \end{bmatrix} \begin{bmatrix} a & b\mathbf{u} \\ c\mathbf{u} & d \end{bmatrix} \cdot h \\
&= g_2 g_1 \cdot h
\end{aligned}
$$

The fourth and final multiplication does not involve h and is obviously correct. Therefore there is an isomorphism between Chein's constructed loop, called $M_{2n}(G, 2)$ where $n = |G|$, and subloop of $\mathrm{Z}(R)$. The isomorphism is given by mapping g to $g\phi\psi$ and x to the element specified above.

CHAPTER 3. PREVIOUS RESULTS

This chapter will explain some previous work done in this area.

The information in this chapter is taken primarily from a paper by Guiliani and Milies (14) and Vojtěchovský's PhD thesis (21) portions of which have been published as well such as (23) and (22).

3.1 The smallest simple Moufang loop

The smallest simple Moufang loop is, in the notation of this work, $GLL(\mathbb{Z}/2\mathbb{Z})$. This was first constructed by Paige (16) and is done by taking the vector matrix construction over the finite field of order 2. Elements of $GLL(\mathbb{Z}/2\mathbb{Z})$ are either order 2 or 3 and each has a recognizable structure.

Proposition 3.1.1. *Elements of order* 2 *have the form* $\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & a \end{bmatrix}$ *and elements of order* 3 *have the form* $\begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & a+1 \end{bmatrix}$.

Proof. This is Lemma 2.2 in (14). □

It is also shown in (14) that there are 63 elements of order 2 and 56 elements of order 3 in $GLL(\mathbb{Z}/2\mathbb{Z})$. This fact is of use later when counting elements in $GLL(\mathbb{Z}/4\mathbb{Z})$.

As mentioned previously, the lack of elements of order 5 is one of the main obstacles to a complete analogue of the theorem for the existence of Sylow subloops. The authors continue to classify all the associative and nonassociative subloops.

Proposition 3.1.2. *The associative subloops of* $GLL(\mathbb{Z}/2\mathbb{Z})$ *are* C_2, C_3, C_2^2, C_2^3, S_3, *and* A_4.

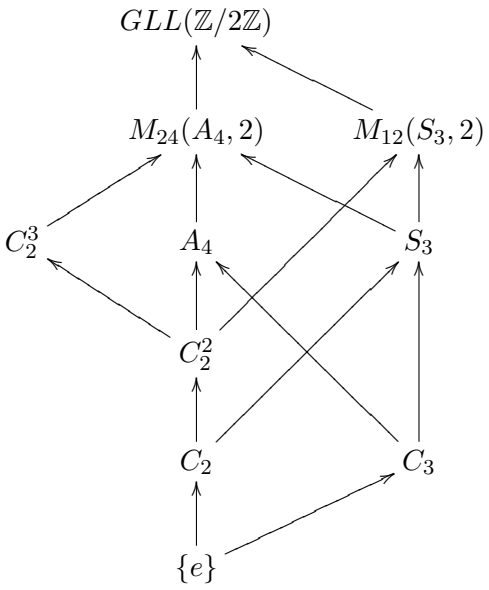

Figure 3.1 Subloop lattice of $GLL(\mathbb{Z}/2\mathbb{Z})$

Here C_n is used to describe the cyclic group of order n to avoid possible confusion with the underlying ring $\mathbb{Z}/2\mathbb{Z}$. The notation C_2^2 and C_2^3 are shorthand for $C_2 \times C_2$ and $C_2 \times C_2 \times C_2$ respectively. The groups S_3 and A_4 are the usual permutation and alternating groups.

Proposition 3.1.3. *The nonassociative subloops of* $GLL(\mathbb{Z}/2\mathbb{Z})$ *are* $M_{12}(S_3, 2)$ *and* $M_{24}(A_4, 2)$.

The proofs can all be found in (14). These two loops refer to the notation established in Section 1.4.

Since subloops of $GLL(\mathbb{Z}/4\mathbb{Z})$ project down to subloops of $GLL(\mathbb{Z}/2\mathbb{Z})$, this provides a natural way to organize the subloops that are examined in the next chapters.

A skeletal look at the subloop lattice of $GLL(\mathbb{Z}/2\mathbb{Z})$ is given in Figure 3.1. In reality, there are many copies of each subloop so this is just a basic view.

A much more detailed lattice complete with Hasse constants and other information is available in (23).

3.2 Chinese Remainder Theorem

The original goal of this project was to examine the structure for all loops of the form $GLL(\mathbb{Z}/n\mathbb{Z})$ for any natural number n. Obviously, if n was prime, $GLL(\mathbb{Z}/n\mathbb{Z})$ was isomorphic

to a Paige loop, or it modulo its center was isomorphic to a Paige loop. Indeed, these are precisely the loops constructed in (16). The first natural question was if $GLL(\mathbb{Z}/n\mathbb{Z}) \cong GLL(\mathbb{Z}/m_1\mathbb{Z}) \times GLL(\mathbb{Z}/m_2\mathbb{Z})$ where $(m_1, m_2) = 1$ and $m_1 m_2 = n$. This turns out to be true and the proof involves the Chinese Remainder Theorem.

Proposition 3.2.1. *If m_1, m_2, and n are natural numbers such that $(m_1, m_2) = 1$ and $m_1 m_2 = n$, then $GLL(\mathbb{Z}/n\mathbb{Z}) \cong GLL(\mathbb{Z}/m_1\mathbb{Z}) \times GLL(\mathbb{Z}/m_2\mathbb{Z})$.*

Proof. Since $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ as rings, we have an isomorphism between the two rings, ϕ. The map ϕ respects addition and multiplication and when applied componentwise to vectors it obviously respects the dot product, which is just a combination of these two operations. Likewise,

$$\begin{aligned}(u_1, u_2, u_3)\phi \times (v_1, v_2, v_3)\phi =& (u_2\phi v_3\phi - u_3\phi v_2\phi, u_3\phi v_1\phi - u_1\phi v_3\phi, u_1\phi v_2\phi - u_2\phi v_1\phi) \\ =& (u_2 v_3 - u_3 v_2, u_3 v_1 - u_1 v_3, u_1 v_2 - u_2 v_1)\phi\end{aligned}$$

and so it respects the cross product as well. Therefore, simply applying ϕ componentwise to $GLL(\mathbb{Z}/n\mathbb{Z})$ produces a loop homomorphism from $GLL(\mathbb{Z}/n\mathbb{Z})$ to $GLL(\mathbb{Z}/m_1\mathbb{Z}) \times GLL(\mathbb{Z}/m_2\mathbb{Z})$.

There is also a ring isomorphism ϕ^{-1} which also corresponds to a loop homomorphism in the same way. These two maps applied componentwise are inverses of each other and provide the required isomorphism. □

Thus, in order to understand the structure of loops of the form $GLL(\mathbb{Z}/n\mathbb{Z})$, all that truly remained was to examine $n = p^e$ for some prime p and some natural number e. Toward this end, the next two chapters take an in depth look at the structure of the first such loop, $GLL(\mathbb{Z}/4\mathbb{Z})$.

CHAPTER 4. THE LOOP GLL($\mathbb{Z}/4\mathbb{Z}$)

4.1 Basic Properties

By Proposition 2.2.4 and Proposition 2.2.5,

$$GLL(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^8 \times GLL(\mathbb{Z}/2\mathbb{Z})$$

with the appropriate multiplication (2.2.1). The total number of elements in $GLL(\mathbb{Z}/4\mathbb{Z})$ is $256 \cdot 120 = 30720$.

To begin, this section will examine the behavior of the images of elements of $GLL(\mathbb{Z}/2\mathbb{Z})$ under a normalized section, i.

Proposition 4.1.1. *Let $x \in GLL(\mathbb{Z}/2\mathbb{Z})$ be of order 2, and let i be a normalized section of the projection map π. Then xi is of order either 2 or 4 in $GLL(\mathbb{Z}/4\mathbb{Z})$.*

Proof. Since

$$(xi \cdot xi)\pi = xi\pi \cdot xi\pi = x^2 = 1$$

in $GLL(\mathbb{Z}/2\mathbb{Z})$, $(xi \cdot xi)$ is in the kernel of π, referred to above as Γ. Call $(xi \cdot xi) = g$. Then $(xi)^3 = g \cdot xi$ and

$$(xi)^4 = (g \cdot xi)xi = g(xi \cdot xi) = g^2 = 1$$

in $GLL(\mathbb{Z}/4\mathbb{Z})$. Thus the order of xi divides 4, and since x is not the identity in $GLL(\mathbb{Z}/2\mathbb{Z})$, it must be of order either two or four. □

Proposition 4.1.2. *Let $y \in GLL(\mathbb{Z}/2\mathbb{Z})$ be of order 3, and let i be a normalized section of the projection map π which maps y^2 to $(yi)^2$. Then yi is of order 3 or 6 in $GLL(\mathbb{Z}/4\mathbb{Z})$.*

Proof. This proof is much the same as the previous one. Since $y^2 \neq 1$ in $GLL(\mathbb{Z}/2\mathbb{Z})$, $(yi)^2 \notin \Gamma$. Then $(yi)^3\pi = 1$ in $GLL(\mathbb{Z}/2\mathbb{Z})$ so $(yi)^3 \in \Gamma$. Thus, $(yi)^6 = ((yi)^3)^2 = 1$ in $(\mathbb{Z}/4\mathbb{Z})^*$. The order of yi must divide 6, but the order is not 2, so it must be 3 or 6. □

There are 63 elements of order 2 in $\text{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ (14). So all $256 \cdot 63$ elements in $\text{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$ that project down to these elements are order 2 or 4. In addition, all the elements of Γ are of order 2 except for the identity. This leads to $256 \cdot 63 + 255 = 16383$ elements of order 2 or 4 in $\text{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$.

Lets look at elements of order two. They must satisfy the equations

1. $a^2 + be + cf + dg = 1$
2. $b(a + h) = 0$
3. $c(a + h) = 0$
4. $d(a + h) = 0$
5. $e(a + h) = 0$
6. $f(a + h) = 0$
7. $g(a + h) = 0$
8. $h^2 + be + cf + dg = 1$

Say $a = h = 0$. Then the diagonal dot product must equal one. There are 896 such vector pairs.

Now say that $a = 0$ and h is odd. Then b, c, d, e, f and g must all be zero, since two times an odd number is two and an odd number times another odd number is odd. Then the first entry must be zero so there is no element of this form.

Now say that $a = 0$ and $h = 2$. Then all of b, c, d, e, f and g must be even. This makes the diagonal dot product equal to zero so the first and last entries must also be zero. Again, no elements of this form exist.

Now say that $a = 2$ and $h = 2$. Then the diagonal dot product must be one. There are 896 such vector pairs.

Now say that $a = 1$ and $h = 1$. Then all of b, c, d, e, f and g must be even. This makes the diagonal dot product equal to zero and so the first and last entries are automatically satisfied. Thus there are $2^6 = 64$ possible elements of this form.

Now say that $a = 1$ and $h = 2$. Then b, c, d, e, f and g must all be zero, since two times an odd number is even and an odd number times another odd number is odd. This forces the last entry to be zero so there are no elements of this form.

Now say that $a = 1$ and $h = 3$. Then the off diagonal requirements are satisfied automatically and the diagonal dot product must be zero. There are 1184 such vector pairs.

Now say $a = 2$ and $h = 3$. Then b, c, d, e, f and g must all be zero, since two times an odd number is even and an odd number times another odd number is odd. Then the first entry must be zero so there is no element of this form.

Now say that $a = 3$ and $h = 3$. Then all of b, c, d, e, f and g must be even. This makes the diagonal dot product equal to zero and so the first and last entries are automatically satisfied. Thus there are $2^6 = 64$ possible elements of this form.

The total number of elements of order two is $896 + 896 + 64 + 2(1184) + 64 = 4288$. Of these, $2^8 = 256$ are lifted from the identity element and so are elements of Γ and $63 \cdot 2^6 = 4032$ are lifted from elements of order two in $GLL(\mathbb{Z}_2)$.

This means that there should be $63 \cdot 2^8 - 4032 = 12096$ elements of order 4.

The above results can be summarized into the following proposition.

Proposition 4.1.3. *If x is a kernel element, then it is of the form* $\begin{bmatrix} 2a+1 & 2\mathbf{u} \\ 2\mathbf{v} & 2b+1 \end{bmatrix}$. *Such an element either has trace 2 and norm 1 or trace 0 and norm 3.*

If x is a non kernel element of order 2, then it is of the form $\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a \end{bmatrix}$ *where $\mathbf{u} \cdot \mathbf{v} = 1$ or of the form* $\begin{bmatrix} 2a+1 & \mathbf{u} \\ \mathbf{v} & 2a+3 \end{bmatrix}$ *where $\mathbf{u} \cdot \mathbf{v} = 0$ but $\mathbf{u}$ and $\mathbf{v}$ have some odd entries. In either case, $Tr(x) = 0$ and $N(x) = 3$.*

If x is an element of order 4, then it is of the form $\begin{bmatrix} 2a+1 & \mathbf{u} \\ \mathbf{v} & 2a+1 \end{bmatrix}$ *with* $\mathbf{u} \cdot \mathbf{v}$ *even but either* $\mathbf{u}$ *or* $\mathbf{v}$ *having some odd entries or of the form* $\begin{bmatrix} 2a+1 & \mathbf{u} \\ \mathbf{v} & 2a+3 \end{bmatrix}$ *with* $\mathbf{u} \cdot \mathbf{v} = 2$ *or of the form* $\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a \end{bmatrix}$ *with* $\mathbf{u} \cdot \mathbf{v} = 3$ *or of the form* $\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a+2 \end{bmatrix}$ *with* $\mathbf{u} \cdot \mathbf{v}$ *odd. There are three relevant combinations of trace and norm:* $Tr(x) = 0$ *and* $N(x) = 1$ *or* $Tr(x) = 2$ *in which case* $N(x)$ *can be either* 1 *or* 3.

Proof. The above calculations prove the results for elements of order 2. Then, since it has been shown that elements of order 2 in $GLL(\mathbb{Z}/2\mathbb{Z})$ are of the form $\begin{bmatrix} n & \mathbf{u} \\ \mathbf{v} & n \end{bmatrix}$ and Proposition 4.1.1 and Proposition 4.1.2 together assure that elements of order 4 project down to elements of order 2, elements of order 4 must have even trace. Each such case is listed in the proposition. □

The remaining $2 \cdot 28 \cdot 256 = 14336$ elements are order 3 or 6.

Now consider elements of order three. They must satisfy the equations

1. $a^3 + (2a + h)(be + cf + dg) = 1$
2. $b(a^2 + ah + h^2 + be + cf + dg) = 0$
3. $c(a^2 + ah + h^2 + be + cf + dg) = 0$
4. $d(a^2 + ah + h^2 + be + cf + dg) = 0$
5. $e(a^2 + ah + h^2 + be + cf + dg) = 0$
6. $f(a^2 + ah + h^2 + be + cf + dg) = 0$
7. $g(a^2 + ah + h^2 + be + cf + dg) = 0$
8. $h^3 + (a + 2h)(be + cf + dg) = 1$

First assume $a = h = 0$. Then the first entry is zero so there are no elements of this form.

Now assume $a = 0$ and $h = 1$. Then the diagonal dot product must be one. Then $a^2 + ah + h^2 + be + cf + dg = 1 + 1 = 2$. That forces b to be even a long with all the other off diagonal entries which in turn forces the dot product to be zero. Therefore no such elements exist.

Assume $a = 0$ and $h = 2$. Then the first entry is even so there are no elements of this form.

Assume $a = 0$ and $h = 3$. Then the diagonal dot product must be three as well. But then $h^3 + (a + 2h)(be + cf + dg) = 3 + (2)(3) = 1$, and $a^2 + ah + h^2 + be + cf + dg = 1 + 3 = 0$ so all the other entries are satisfied. There are 896 such vector pairs.

Assume $a = 1$ and $h = 1$. Then the first entry is $1 + 3(be + cf + dg)$, so the diagonal dot product must be zero. Then $b(a^2 + ah + h^2 + be + cf + dg) = 3b$ and so b and all the vector entries must be zero. This is simply the identity element.

Assume $a = 1$ and $h = 2$. Then by the last entry, the diagonal dot product must be one. The first entry is automatically satisfied. But then $a^2 + ah + h^2 + be + cf + dg = 1 + 2 + 1$ so all the other entries are satisfied. There are 896 such vector pairs.

Assume $a = 1$ and $h = 3$. Then the first entry is $1 + 1(be + cf + dg)$, so the diagonal dot product must be zero. The final entry is automatically 3, so there is a contradiction and no elements of this form exist.

Assume $a = 2$ and $h = 2$. Then the first entry is even so there are no elements of this form.

Assume $a = 2$ and $h = 3$. Then the first entry is $0 + 3(be + cf + dg)$ so the diagonal dot product must be three. But then $h^3 + (a + 2h)(be + cf + dg) = 3 + (0)(3) = 3$, and so no elements of this form exist.

Assume $a = 3$ and $h = 3$. Then the first entry is $3 + 1(be + cf + dg)$ so the diagonal dot product must be 2. Then $(a^2 + ah + h^2 + be + cf + dg) = 1$ and so b and all the vector entries must be zero, but this forces the diagonal dot product to be 0. Therefore there are no elements of this form.

In total, there are $4(896) = 3584$ elements of order 3. Note that this is exactly $2^6 \cdot 56$, and so there are $2^8 \cdot 56 - 2^6 \cdot 56 = 10752$ elements of order 6.

Again, a proposition summarizes the most relevant information.

Proposition 4.1.4. *If x is an element of order 3, then x is of the form, $\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a+3 \end{bmatrix}$ or $\begin{bmatrix} 2a+3 & \mathbf{u} \\ \mathbf{v} & 2a \end{bmatrix}$ with $\mathbf{u}$ and $\mathbf{v}$ chosen so that $N(x) = 1$. All elements of order 3 have trace 3 and norm 1.*

If x is an element of order 6, then it is of the form of an element of order 3 except it has norm 3 or it is of the form $\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a+1 \end{bmatrix}$ or $\begin{bmatrix} 2a+1 & \mathbf{u} \\ \mathbf{v} & 2a \end{bmatrix}$ with $\mathbf{u} \cdot \mathbf{v}$ odd. Thus, either $Tr(x) = 3$ and $N(x) = 3$ or $Tr(x) = 1$ in which case $N(x)$ can be either 1 or 3.

Proposition 4.1.5. *If x and y are elements of $GLL(\mathbb{Z}/4\mathbb{Z})$ such that $x^2 = y^2 = 1$ and $xy = yx$, then one of x, y, or xy is an element of Γ.*

Proof. If x and y commute, then since $\langle x, y \rangle$ is associative, xy is an element of order 2. Assume that neither x nor y is in Γ. Then $N(x) = N(y) = 3$ and so $N(xy) = 1$ and so xy is an element of Γ. □

Proposition 4.1.6. *Let L be a loop in $GLL(\mathbb{Z}/4\mathbb{Z})$ such that $L\pi \cong C_2^2$. Then L is not isomorphic to C_2^2 in $GLL(\mathbb{Z}/4\mathbb{Z})$.*

Proof. If L is isomorphic to C_2^2, then it contains three elements of order two which commute with each other. By Proposition 4.1.5, one of these elements is in Γ. Thus, $|L\pi| < 4$ and this is a contradiction. □

Corollary 4.1.7. *Let L be a loop in $GLL(\mathbb{Z}/4\mathbb{Z})$ such that $L\pi$ is isomorphic to C_2^3, A_4, $M_{12}(S_3, 2)$, $M_{12}(A_4, 2)$ or $M^*(2)$. Then L is not isomorphic to $L\pi$.*

Proof. Note simply that these loops contain subloops isomorphic to C_2^2. By Proposition 4.1.6, $|L\pi| < |L|$. □

It can and will be shown through examples that there are loops in $GLL(\mathbb{Z}/4\mathbb{Z})$, which are isomorphic to S_3 and which project down to a copy of S_3 in $GLL(\mathbb{Z}/2\mathbb{Z})$. Also this is obviously possible for loops isomorphic to C_2 or C_3.

4.2 Commuting elements

It is of value for later work to take the time to consider under what conditions two elements of $GLL(\mathbb{Z}/4\mathbb{Z})$ commute.

Let $x = \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix}$ and $y = \begin{bmatrix} c & \mathbf{r} \\ \mathbf{s} & d \end{bmatrix}$. Then

$$xy = \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} c & \mathbf{r} \\ \mathbf{s} & d \end{bmatrix} = \begin{bmatrix} ab + \mathbf{u} \cdot \mathbf{s} & a\mathbf{r} + d\mathbf{u} - \mathbf{v} \times \mathbf{s} \\ c\mathbf{v} + b\mathbf{s} + \mathbf{u} \times \mathbf{r} & bd + \mathbf{v} \cdot \mathbf{r} \end{bmatrix}$$

and

$$yx = \begin{bmatrix} c & \mathbf{r} \\ \mathbf{s} & d \end{bmatrix} \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} = \begin{bmatrix} ab + \mathbf{v} \cdot \mathbf{r} & b\mathbf{r} + c\mathbf{u} - \mathbf{s} \times \mathbf{v} \\ a\mathbf{s} + d\mathbf{v} + \mathbf{r} \times \mathbf{u} & bd + \mathbf{u} \cdot \mathbf{s} \end{bmatrix}.$$

In order for x and y to commute, the following four equations must therefore hold:

$$\begin{aligned} ab + \mathbf{u} \cdot \mathbf{s} &= ab + \mathbf{v} \cdot \mathbf{r} \\ a\mathbf{r} + d\mathbf{u} - \mathbf{v} \times \mathbf{s} &= b\mathbf{r} + c\mathbf{u} - \mathbf{s} \times \mathbf{v} \\ c\mathbf{v} + b\mathbf{s} + \mathbf{u} \times \mathbf{r} &= a\mathbf{s} + d\mathbf{v} + \mathbf{r} \times \mathbf{u} \\ bd + \mathbf{v} \cdot \mathbf{r} &= bd + \mathbf{u} \cdot \mathbf{s} \end{aligned}$$

and these simplify to the following three:

$$\begin{aligned} \mathbf{u} \cdot \mathbf{s} &= \mathbf{v} \cdot \mathbf{r} \\ (a-b)\mathbf{r} + (d-c)\mathbf{u} + 2\mathbf{s} \times \mathbf{v} &= 0 \\ (a-b)\mathbf{s} + (d-c)\mathbf{v} + 2\mathbf{u} \times \mathbf{r} &= 0. \end{aligned}$$

Proposition 4.2.1. *If x and y are both non-kernel elements of order 2 and $xy = yx$, then*

$x\pi = y\pi$.

Proof. Let x and y both be non-kernel elements of order 2 such that $a = b$ and $c = d$ and so $\mathbf{u} \cdot \mathbf{v} = \mathbf{r} \cdot \mathbf{s} = 1$. Then the equations simplify to

$$\begin{aligned} \mathbf{u} \cdot \mathbf{s} &= \mathbf{v} \cdot \mathbf{r} \\ 2\mathbf{s} \times \mathbf{v} &= 0 \\ 2\mathbf{u} \times \mathbf{r} &= 0. \end{aligned}$$

If $\mathbf{s} \times \mathbf{v}$ is even, then $\mathbf{s} \times \mathbf{v} = \mathbf{0}$ modulo 2 so either $\mathbf{s}\pi = \mathbf{v}\pi$ or one of them consists only of even entries. Since $\mathbf{u} \cdot \mathbf{v} = \mathbf{r} \cdot \mathbf{s} = 1$ none of the vectors can be all even. Thus, $\mathbf{s}\pi = \mathbf{v}\pi$ and $\mathbf{r}\pi = \mathbf{u}\pi$ for similar reasons. So in fact, $x\pi = y\pi$.

Now let x be a non-kernel elements of order 2 such that $a = b$ and $\mathbf{u} \cdot \mathbf{v} = 1$ and y be a non-kernel element of order 2 such that $d - c = 2$ and $\mathbf{r} \cdot \mathbf{s} = 0$. Then the equations simplify to

$$\begin{aligned} \mathbf{u} \cdot \mathbf{s} &= \mathbf{v} \cdot \mathbf{r} \\ 2\mathbf{u} &= 2\mathbf{s} \times \mathbf{v} \\ 2\mathbf{v} + 2\mathbf{u} \times \mathbf{r} &= 0. \end{aligned}$$

This implies that

$$\begin{aligned} 2\mathbf{v} + (2\mathbf{s} \times \mathbf{v}) \times \mathbf{r} &= 0 \\ 2\mathbf{v} + 2((\mathbf{r} \cdot \mathbf{v})\mathbf{s} - (\mathbf{r} \cdot \mathbf{s})\mathbf{v}) &= 0 \\ 2\mathbf{v} &= 2(\mathbf{r} \cdot \mathbf{v})\mathbf{s} \end{aligned}$$

so either $\mathbf{v}\pi = \mathbf{s}\pi$ (if $\mathbf{r} \cdot \mathbf{v}$ is odd) or $\mathbf{v}$ is all even. Again, $\mathbf{v}$ can not be all even since $\mathbf{u} \cdot \mathbf{v} = 1$.

Thus, $\mathbf{s} = \mathbf{v} + 2\mathbf{w}$ for some vector $\mathbf{w}$. Then,

$$2\mathbf{u} = 2\mathbf{s} \times \mathbf{v} = 2(\mathbf{v} + 2\mathbf{w}) \times \mathbf{v} = 2\mathbf{v} \times \mathbf{v} = \mathbf{0}$$

so $\mathbf{u}$ must be all even, but this is a contradiction since $\mathbf{u} \cdot \mathbf{v} = 1$. No such elements x and y can ever commute.

Now let x and y both be non-kernel elements of order 2 such that $a - b = d - c = 2$ and $\mathbf{u} \cdot \mathbf{v} = \mathbf{r} \cdot \mathbf{s} = 0$. Then the equations simplify to

$$\begin{aligned} \mathbf{u} \cdot \mathbf{s} &= \mathbf{v} \cdot \mathbf{r} \\ 2\mathbf{r} + 2\mathbf{u} + 2\mathbf{s} \times \mathbf{v} &= 0 \\ 2\mathbf{s} + 2\mathbf{v} + 2\mathbf{u} \times \mathbf{r} &= 0. \end{aligned}$$

This implies

$$\begin{aligned} 2\mathbf{s} + 2\mathbf{v} + \mathbf{u} \times (2\mathbf{u} + 2\mathbf{s} \times \mathbf{v}) &= 0 \\ 2\mathbf{s} + 2\mathbf{v} + 2(\mathbf{u} \cdot \mathbf{v})\mathbf{s} + (\mathbf{u} \cdot \mathbf{s})\mathbf{v} &= 0 \\ 2\mathbf{s} + 2\mathbf{v} + 2(\mathbf{u} \cdot \mathbf{s})\mathbf{v} &= 0 \\ 2\mathbf{s} + 2\mathbf{v} + 2(\mathbf{u} \cdot \mathbf{s})\mathbf{v} &= 0 \\ 2\mathbf{s} &= 2(1 + \mathbf{u} \cdot \mathbf{s})\mathbf{v} \end{aligned}$$

and

$$\begin{aligned} 2\mathbf{r} + 2\mathbf{u} + (2\mathbf{v} + 2\mathbf{u} \times \mathbf{r}) \times \mathbf{v} &= 0 \\ 2\mathbf{r} + 2\mathbf{u} + 2(\mathbf{u} \times \mathbf{r}) \times \mathbf{v} &= 0 \\ 2\mathbf{r} + 2\mathbf{u} + 2(\mathbf{v} \cdot \mathbf{r})\mathbf{u} + 2(\mathbf{v} \cdot \mathbf{u})\mathbf{r} &= 0 \\ 2\mathbf{r} = 2(1 + \mathbf{u} \cdot \mathbf{s})\mathbf{u} &= 0 \end{aligned}$$

so that $\mathbf{r}$ is a multiple of $\mathbf{u}$ modulo 2 and $\mathbf{s}$ is a multiple of $\mathbf{v}$ modulo 2. If $\mathbf{s}\pi = \mathbf{v}\pi$ and $\mathbf{r}\pi = \mathbf{u}\pi$ then $x\pi = y\pi$ as before. If $\mathbf{r}\pi = \mathbf{0}$ and $\mathbf{u}\pi \neq \mathbf{0}$, then $\mathbf{u} \cdot \mathbf{s}$ is odd and so $\mathbf{s}\pi = 0$ Then, $y \in \Gamma$. □

Elements of order 4 interact in a similar way and a number of the following equations will be familiar.

Proposition 4.2.2. *If x is an element of order 4 and y is a non-kernel element of order 2, and $xy = yx$, then $x\pi = y\pi$.*

Proof. Let x be an element of order 4 and y be a non-kernel element of order 2. First consider x to be of the form where $a - b = 0$ and $\mathbf{u} \cdot \mathbf{v} = 3$. No matter which form y takes, this is identical to the first two cases in the previous work. Only the fact that $\mathbf{u} \cdot \mathbf{v}$ is odd is of any importance. Thus, in this case, again $x\pi = y\pi$.

Now consider x of the form where $a - b = 2$ and $\mathbf{u} \cdot \mathbf{v} = 2$. This case plays out identically to the last case in the previous work.

Now consider x of the form where $a - b = 0$ and $\mathbf{u} \cdot \mathbf{v}$ is even and y is of the form where

$d - c = 0$ and $\mathbf{r} \cdot \mathbf{s} = 1$. Then the equations simplify to

$$\begin{aligned} \mathbf{u} \cdot \mathbf{s} &= \mathbf{v} \cdot \mathbf{r} \\ 2\mathbf{s} \times \mathbf{v} &= 0 \\ 2\mathbf{u} \times \mathbf{r} &= 0. \end{aligned}$$

If $\mathbf{s}\pi = \mathbf{v}\pi$, then $\mathbf{u}\pi \neq \mathbf{r}\pi$ since $\mathbf{u} \cdot \mathbf{v}$ is even and $\mathbf{r} \cdot \mathbf{s}$ is odd. Thus every entry in $\mathbf{r}$ must be even but $\mathbf{r} \cdot \mathbf{s} = 1$ so this is impossible.

Now consider y of the form where $d - c = 2$ and $\mathbf{r} \cdot \mathbf{s} = 0$. Then the equations simplify to

$$\begin{aligned} \mathbf{u} \cdot \mathbf{s} &= \mathbf{v} \cdot \mathbf{r} \\ 2\mathbf{u} &= 2\mathbf{s} \times \mathbf{v} \\ 2\mathbf{v} + 2\mathbf{u} \times \mathbf{r} &= 0. \end{aligned}$$

This implies that

$$\begin{aligned} 2\mathbf{v} + (2\mathbf{s} \times \mathbf{v}) \times \mathbf{r} &= 0 \\ 2\mathbf{v} + 2((\mathbf{r} \cdot \mathbf{v})\mathbf{s} - (\mathbf{r} \cdot \mathbf{s})\mathbf{v}) &= 0 \\ 2\mathbf{v} &= 2(\mathbf{r} \cdot \mathbf{v})\mathbf{s} \end{aligned}$$

which implies that $\mathbf{v}\pi = \mathbf{s}\pi$ or one of $\mathbf{v}$ or $\mathbf{s}$ is all even. If $\mathbf{v}\pi = \mathbf{s}\pi$ then $2\mathbf{s} \times \mathbf{v} = \mathbf{0}$ and so $\mathbf{u}$ must be all even. But then $2\mathbf{u} \times \mathbf{r} = 0$ so $\mathbf{v}$ must be all even. This is impossible since x is not a kernel element.

Finally consider the case when x is of the form where $a - b = 2$ and $\mathbf{u} \cdot \mathbf{v}$ is odd and y is

of the form where $d - c = 0$ and $\mathbf{r} \cdot \mathbf{s} = 1$. Then the equations simplify to

$$\begin{aligned} \mathbf{u} \cdot \mathbf{s} &= \mathbf{v} \cdot \mathbf{r} \\ 2\mathbf{r} + 2\mathbf{s} \times \mathbf{v} &= 0 \\ 2\mathbf{s} + 2\mathbf{u} \times \mathbf{r} &= 0. \end{aligned}$$

This implies that

$$2\mathbf{r} \cdot \mathbf{s} = 2(\mathbf{s} \times \mathbf{v}) \cdot \mathbf{s} = 0$$

but this contradicts that $\mathbf{r} \cdot \mathbf{s} = 1$. So these elements will not commute.

Now consider the case where y is of the form where $d - c = 2$ and $\mathbf{r} \cdot \mathbf{s} = 0$. Then the equations simplify to

$$\begin{aligned} \mathbf{u} \cdot \mathbf{s} &= \mathbf{v} \cdot \mathbf{r} \\ 2\mathbf{r} + 2\mathbf{u} + 2\mathbf{s} \times \mathbf{v} &= 0 \\ 2\mathbf{s} + 2\mathbf{v} + 2\mathbf{u} \times \mathbf{r} &= 0. \end{aligned}$$

This implies that

$$2\mathbf{u} \cdot \mathbf{v} = \mathbf{u} \cdot (2\mathbf{s} + 2\mathbf{u} \times \mathbf{r}) = 2\mathbf{u} \cdot \mathbf{s}$$

and

$$2\mathbf{r} \cdot \mathbf{s} = \mathbf{r} \cdot (2\mathbf{v} + 2\mathbf{u} \times \mathbf{r}) = 2\mathbf{r} \cdot \mathbf{v}$$

which means that

$$2\mathbf{u} \cdot \mathbf{v} = 2\mathbf{r} \cdot \mathbf{s}$$

which is a contradiction. These elements will never commute. □

4.3 Associative subloops

Lemma 4.3.1. *Let* $\begin{bmatrix} e & \mathbf{y} \\ \mathbf{z} & f \end{bmatrix}$ *be an element of* $GLL(\mathbb{Z}/4\mathbb{Z})$*, and let* $\begin{bmatrix} 2a+1 & 2\mathbf{u} \\ 2\mathbf{v} & 2b+1 \end{bmatrix}$ *and* $\begin{bmatrix} 2c+1 & 2\mathbf{w} \\ 2\mathbf{x} & 2d+1 \end{bmatrix}$ *be elements of* Γ*. These three elements generate an associative subloop.*

Proof. Note that since the off-diagonal entries of elements in Γ must be even, and the diagonal elements must be odd, they may be written in the form appearing in the lemma. Consider

$$\begin{aligned} M &= \begin{bmatrix} e & \mathbf{y} \\ \mathbf{z} & f \end{bmatrix} \begin{bmatrix} 2a+1 & 2\mathbf{u} \\ 2\mathbf{v} & 2b+1 \end{bmatrix} \cdot \begin{bmatrix} 2c+1 & 2\mathbf{w} \\ 2\mathbf{x} & 2d+1 \end{bmatrix} \\ &= \begin{bmatrix} 2ea+e+2\mathbf{y}\cdot\mathbf{v} & 2e\mathbf{u}+2b\mathbf{y}+\mathbf{y}-2\mathbf{z}\times\mathbf{v} \\ 2a\mathbf{z}+\mathbf{z}+2f\mathbf{v}+2\mathbf{y}\times\mathbf{u} & 2bf+f+2\mathbf{z}\cdot\mathbf{v} \end{bmatrix} \begin{bmatrix} 2c+1 & 2\mathbf{w} \\ 2\mathbf{x} & 2d+1 \end{bmatrix}. \end{aligned}$$

Then the entries of M are as follows:

$$\begin{aligned} M_{11} &= 2ec + 2ea + e + 2\mathbf{y}\cdot\mathbf{v} + 2\mathbf{y}\cdot\mathbf{x}\,; \\ M_{12} &= 2e\mathbf{w} + 2e\mathbf{u} + 2d\mathbf{y} + 2b\mathbf{y} + \mathbf{y} - 2\mathbf{z}\times\mathbf{v} - 2\mathbf{z}\times\mathbf{x}\,; \\ M_{21} &= 2c\mathbf{z} + 2a\mathbf{z} + \mathbf{z} + 2(\mathbf{y}\times\mathbf{u}) + 2f\mathbf{x} + 2f\mathbf{v} + 2(\mathbf{y}\times\mathbf{w})\,; \\ M_{22} &= 2\mathbf{w}\cdot\mathbf{z} + 2df + 2bf + f + 2\mathbf{z}\cdot\mathbf{u}\,. \end{aligned}$$

On the other hand,

$$M' = \begin{bmatrix} e & \mathbf{y} \\ \mathbf{z} & f \end{bmatrix} \cdot \begin{bmatrix} 2a+1 & 2\mathbf{u} \\ 2\mathbf{v} & 2b+1 \end{bmatrix} \begin{bmatrix} 2c+1 & 2\mathbf{w} \\ 2\mathbf{x} & 2d+1 \end{bmatrix}$$
$$= \begin{bmatrix} e & \mathbf{y} \\ \mathbf{z} & f \end{bmatrix} \begin{bmatrix} 2a+2c+1 & 2\mathbf{w}+2\mathbf{u} \\ 2\mathbf{v}+2\mathbf{x} & 2b+2d+1 \end{bmatrix},$$

and so the entries of M' are:

$$M'_{11} = 2ea + 2ec + e + 2\mathbf{y}\cdot\mathbf{v} + 2\mathbf{y}\cdot\mathbf{x}\,;$$
$$M'_{12} = 2e\mathbf{w} + 2e\mathbf{u} + 2b\mathbf{y} + 2d\mathbf{y} + \mathbf{y} - 2\mathbf{z}\times\mathbf{v} - 2\mathbf{z}\times\mathbf{x}\,;$$
$$M'_{21} = 2a\mathbf{z} + 2c\mathbf{z} + \mathbf{z} + 2f\mathbf{v} + 2f\mathbf{x} + 2\mathbf{y}\times\mathbf{w} + 2\mathbf{y}\times\mathbf{u}\,;$$
$$M'_{22} = 2\mathbf{z}\cdot\mathbf{w} + 2\mathbf{z}\cdot\mathbf{u} + 2bf + 2df + f\,.$$

Note that these correspond exactly to the entries of M. By Moufang's Theorem, since these elements associate in one order, they form an associative subloop (15). □

This tells us a great deal about the structure of the subloops of the form $G \times L$, where G is a subloop of Γ and L is a cyclic subloop of $GLL(\mathbb{Z}/4\mathbb{Z})$. Let $L = \langle x \rangle$, then for any element $g \in \Gamma$, $\langle x, g \rangle$ is a group because Moufang loops are diassociative. Since Γ is itself a group, Lemma 4.3.1 shows that any loop of the form $G \times L$ must also be associative and hence a group.

4.4 Sylow subloops of $GLL(\mathbb{Z}/4\mathbb{Z})$

The order of $GLL(\mathbb{Z}/4\mathbb{Z})$ is $30720 = 2^{11} \cdot 3 \cdot 5$ so each of the primes 2, 3, and 5 need to be checked to see if they are Sylow primes as mentioned in Chapter 1. The only composition factor of $GLL(\mathbb{Z}/4\mathbb{Z})$ which is isomorphic to a Paige loop is $GLL(\mathbb{Z}/2\mathbb{Z})$ so in order to be a

Sylow prime, $p \nmid \frac{2^2+1}{(2,1)} = 5$. Clearly both 2 and 3 are Sylow primes, whereas 5 is not. Indeed, the primes 2 and 3 are always Sylow primes as has been noted in (12), and many other places. The absence of Sylow-5 loops is not surprising at all, since there are not any elements of order 5 in $GLL(\mathbb{Z}/4\mathbb{Z})$.

A Sylow-3 subloop would have order 3 and so is a cyclic group of order 3. There are 1792 such subgroups. A Sylow-2 subloop is order $2^{11} = 2048$. Since it contains only elements of order 2 or 4, it must project down to a 2-loop in $GLL(\mathbb{Z}/2\mathbb{Z})$. The largest such loop is C_2^3 so all Sylow-2 subloops are of the form $\Gamma \times C_2^3$. Every 2-loop is a subloop of one of these Sylow-2 loops.

CHAPTER 5. SUBLOOPS OF GLL$(\mathbb{Z}/4\mathbb{Z})$

It is now possible to begin describing the possible subloops of $GLL(\mathbb{Z}/4\mathbb{Z})$. Proposition 2.2.6 shows that every subloop $L \subseteq GLL(\mathbb{Z}/4\mathbb{Z})$ can be written as $\Gamma(L) \times L\pi$, where $\Gamma(L)$ is a subloop (subgroup in this case) of $\Gamma \cong (\mathbb{Z}/2\mathbb{Z})^8$ and $L\pi$ is a subloop of $GLL(\mathbb{Z}/2\mathbb{Z})$.

Note that elements of Γ have the form $\begin{bmatrix} 2a+1 & (2b, 2c, 2d) \\ (2e, 2f, 2g) & 2h+1 \end{bmatrix}$ since they must project down to the identity element in $GLL(\mathbb{Z}/2\mathbb{Z})$.

5.1 Loops projecting into GLL$(\mathbb{Z}/2\mathbb{Z})$

Consider all subloops of the form $\Gamma \times L$. If a non-kernel element of $GLL(\mathbb{Z}/4\mathbb{Z})$ is added to $\Gamma \times L$, the resulting subloop will be of the form $\Gamma \times \langle L, x\pi \rangle$. This indicates that the lattice structure of $GLL(\mathbb{Z}/2\mathbb{Z})$ is preserved in $GLL(\mathbb{Z}/4\mathbb{Z})$ at the top of the subloop lattice of $GLL(\mathbb{Z}/4\mathbb{Z})$. More generally,

Proposition 5.1.1. *Let L be a subloop of $GLL(\mathbb{Z}/4\mathbb{Z})$ so of the form $\Gamma(L) \times L\pi$ and M a subloop of the form $\Gamma(M) \times M\pi$. Then the subloop generated by all elements of L and M is of the form $G \times \langle L\pi, M\pi \rangle$ where G is some subloop of Γ.*

Proof. This is simply because π is a homomorphism. As a result, the subloops must project down to the subloop in $GLL(\mathbb{Z}/2\mathbb{Z})$ which their projected elements generate. □

Because of this, it makes sense to break the subloop lattice of $GLL(\mathbb{Z}/4\mathbb{Z})$ into pieces based on what the subloops project to in $GLL(\mathbb{Z}/2\mathbb{Z})$. In the following subsections, there will primarily be an effort to prove that subloops of certain orders exist in $GLL(\mathbb{Z}/4\mathbb{Z})$. For the smaller subloops, an explanatory proof is available, but for the larger loops, only the actual construction of examples is available. All examples are collected in the first Appendix.

5.1.1 Loops which project down to C_2

All of these subloops are associative by Proposition 4.3.1 since they must be generated by elements of Γ and one element of order 2 which is not in Γ. Such loops are of the form $\Gamma(L) \times C_2$. The goal of this section is to determine the possible orders of $\Gamma(L)$.

The interplay between the kernel elements and a generic non-kernel element of order two is vital to this problem. So the beginning of this section will establish some useful information in this direction.

Proposition 5.1.2. *Let x be an element of $GLL(\mathbb{Z}/4\mathbb{Z}) \setminus \Gamma$ such that $x^4 = 1$. Let $\gamma(x) = \{g \in \Gamma | xg = gx\}$. Then $|\gamma(x)| = 64$.*

Proof. Let $x = \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix}$ and let $g = \begin{bmatrix} 2c+1 & 2\mathbf{r} \\ 2\mathbf{s} & 2d+1 \end{bmatrix}$ be a generic element of Γ. Then

$$xg = \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} \begin{bmatrix} 2c+1 & 2\mathbf{r} \\ 2\mathbf{s} & 2d+1 \end{bmatrix} = \begin{bmatrix} 2ac + a + 2\mathbf{u} \cdot \mathbf{s} & 2a\mathbf{r} + 2d\mathbf{u} + \mathbf{u} - 2\mathbf{v} \times \mathbf{s} \\ 2c\mathbf{v} + \mathbf{v} + 2b\mathbf{s} + 2\mathbf{u} \times \mathbf{r} & 2bd + b + 2\mathbf{v} \cdot \mathbf{r} \end{bmatrix}$$

and

$$gx = \begin{bmatrix} 2c+1 & 2\mathbf{r} \\ 2\mathbf{s} & 2d+1 \end{bmatrix} \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix} = \begin{bmatrix} 2ac + a + 2\mathbf{r} \cdot \mathbf{v} & 2c\mathbf{u} + \mathbf{u} + 2b\mathbf{r} - 2\mathbf{s} \times \mathbf{v} \\ 2a\mathbf{s} + 2d\mathbf{v} + \mathbf{v} + 2\mathbf{r} \times \mathbf{u} & 2\mathbf{s} \cdot \mathbf{u} + 2db + b \end{bmatrix}$$

So for $gx = xg$ to be true, it must be the case that

$$*2ac + a + 2\mathbf{u} \cdot \mathbf{s} = 2ac + a + 2\mathbf{r} \cdot \mathbf{v} \tag{5.1.1}$$

$$2\mathbf{u} \cdot \mathbf{s} = 2\mathbf{r} \cdot \mathbf{v} \tag{5.1.2}$$

and

$$\begin{aligned}
2a\mathbf{r} + 2d\mathbf{u} + \mathbf{u} - 2\mathbf{v} \times \mathbf{s} =& 2c\mathbf{u} + \mathbf{u} + 2b\mathbf{r} - 2\mathbf{s} \times \mathbf{v} \\
2a\mathbf{r} + 2d\mathbf{u} + 2\mathbf{s} \times \mathbf{v} =& 2c\mathbf{u} + 2b\mathbf{r} - 2\mathbf{s} \times \mathbf{v} \\
2a\mathbf{r} + 2d\mathbf{u} + 4\mathbf{s} \times \mathbf{v} =& 2c\mathbf{u} + 2b\mathbf{r} \\
2a\mathbf{r} + 2d\mathbf{u} =& 2c\mathbf{u} + 2b\mathbf{r} \\
2d\mathbf{u} =& 2c\mathbf{u}
\end{aligned}$$

noting that for all elements of order 2 or 4, $2a = 2b$ since a and b are either both odd or both even. Thus $d = c$ is a necessary condition on g. The other entry comparisons simply duplicate these two. All that remains is to determine when $2\mathbf{u} \cdot \mathbf{s} = 2\mathbf{r} \cdot \mathbf{v}$. Let $\mathbf{u} = (u_1, u_2, u_3)$ and so on so that this equation becomes

$$2(u_1s_1 + u_2s_2 + u_3s_3) = 2(v_1r_1 + v_2r_2 + v_3r_3).$$

Since x is not a kernel element, at least one entry of $\mathbf{u}$ or $\mathbf{v}$ is odd. Without loss of generality, say u_1 is odd. Then

$$2s_1 = 2(v_1r_1 + v_2r_2 + v_3r_3 + u_2s_2 + u_3s_3)$$

and so if the other entries of $\mathbf{s}$ and $\mathbf{r}$ are specified, then there is exactly one value of s_1 that satisfies this equation. Thus there are 2^5 such possible vectors. Combining this with the fact that $c = d$, there must be exactly $2^6 = 64$ elements of Γ which commute with x. □

Proposition 5.1.3. *Let x be an element of $GLL(\mathbb{Z}/4\mathbb{Z})\backslash\Gamma$ such that $x^4 = 1$. Then the element* $g = \begin{bmatrix} 1 & (000) \\ (000) & 1 \end{bmatrix}$ *is not in $\gamma(x)$ and $xgx^{-1} = hg$ for some element $h \in \gamma(x)$.*

Proof. The fact that $g \notin \gamma(x)$ follows from the proof of Proposition 5.1.2.

Suppose x is of the form $\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a \end{bmatrix}$ where $\mathbf{u} \cdot \mathbf{v}$ is odd, then

$$\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix} \begin{bmatrix} 2aN(x) & 3N(x)\mathbf{u} \\ 3N(x)\mathbf{v} & 2aN(x) \end{bmatrix} = \begin{bmatrix} 2a & 3\mathbf{u} \\ \mathbf{v} & 2a \end{bmatrix} \begin{bmatrix} 2aN(x) & 3N(x)\mathbf{u} \\ 3N(x)\mathbf{v} & 2aN(x) \end{bmatrix}$$
$$= \begin{bmatrix} N(x)\mathbf{u}\cdot\mathbf{v} & \mathbf{0} \\ \mathbf{0} & 3N(x)\mathbf{u}\cdot\mathbf{v} \end{bmatrix}$$
$$= \begin{bmatrix} 3 & \mathbf{0} \\ \mathbf{0} & 1 \end{bmatrix}.$$

Note that in this case, $N(x) = 3\mathbf{u}\cdot\mathbf{v}$. The resulting matrix is obviously the product $\begin{bmatrix} 3 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix}$ so the proposition holds in this case.

Now let x be of the form $\begin{bmatrix} 2a+1 & \mathbf{u} \\ \mathbf{v} & 2a+31 \end{bmatrix}$ where $\mathbf{u} \cdot \mathbf{v}$ is even. Then

$$\begin{bmatrix} 2a+1 & \mathbf{u} \\ \mathbf{v} & 2a+3 \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix} \begin{bmatrix} 2aN(x)+3N(x) & 3N(x)\mathbf{u} \\ 3N(x)\mathbf{v} & 2aN(x)+N(x) \end{bmatrix}$$
$$= \begin{bmatrix} 2a+1 & 3\mathbf{u} \\ \mathbf{v} & 2a+1 \end{bmatrix} \begin{bmatrix} 2aN(x)+3N(x) & 3N(x)\mathbf{u} \\ 3N(x)\mathbf{v} & 2aN(x)+N(x) \end{bmatrix}$$
$$= \begin{bmatrix} (3+\mathbf{u}\cdot\mathbf{v})N(x) & 2\mathbf{u} \\ 2\mathbf{v} & (3+\mathbf{u}\cdot\mathbf{v})3N(x) \end{bmatrix}.$$

This is the product $\begin{bmatrix} 1 & 2\mathbf{u} \\ 2\mathbf{v} & 1 \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix}$, or $\begin{bmatrix} 3 & 2\mathbf{u} \\ 2\mathbf{v} & 3 \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix}$ and it is easy to verify that $\begin{bmatrix} 1 & 2\mathbf{u} \\ 2\mathbf{v} & 1 \end{bmatrix}$ commutes with x.

Now let x be of the form $\begin{bmatrix} 2a+1 & \mathbf{u} \\ \mathbf{v} & 2a+1 \end{bmatrix}$ where $\mathbf{u} \cdot \mathbf{v}$ is even. Then

$$\begin{bmatrix} 2a+1 & \mathbf{u} \\ \mathbf{v} & 2a+1 \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix} \begin{bmatrix} 2aN(x)+N(x) & 3N(x)\mathbf{u} \\ 3N(x)\mathbf{v} & 2aN(x)+N(x) \end{bmatrix}$$
$$= \begin{bmatrix} 2a+1 & 3\mathbf{u} \\ \mathbf{v} & 2a+3 \end{bmatrix} \begin{bmatrix} 2aN(x)+N(x) & 3N(x)\mathbf{u} \\ 3N(x)\mathbf{v} & 2aN(x)+N(x) \end{bmatrix}$$
$$= \begin{bmatrix} (1+\mathbf{u}\cdot\mathbf{v})N(x) & 2\mathbf{u} \\ 2\mathbf{v} & 3(1+\mathbf{u}\cdot\mathbf{v})N(x) \end{bmatrix}$$

This is again the product $\begin{bmatrix} 1 & 2\mathbf{u} \\ 2\mathbf{v} & 1 \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix}$, or $\begin{bmatrix} 3 & 2\mathbf{u} \\ 2\mathbf{v} & 3 \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix}$.

Finally, let x be of the form $\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a+2 \end{bmatrix}$ where $\mathbf{u} \cdot \mathbf{v}$ is odd, then

$$\begin{bmatrix} 2a & \mathbf{u} \\ \mathbf{v} & 2a+2 \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 3 \end{bmatrix} = \begin{bmatrix} 2aN(x)+2N(x) & 3N(x)\mathbf{u} \\ 3N(x)\mathbf{v} & 2aN(x) \end{bmatrix}$$
$$= \begin{bmatrix} 2a & 3\mathbf{u} \\ \mathbf{v} & 2a+2 \end{bmatrix} \begin{bmatrix} 2aN(x)+2N(x) & 3N(x)\mathbf{u} \\ 3N(x)\mathbf{v} & 2aN(x) \end{bmatrix}$$
$$= \begin{bmatrix} N(x)\mathbf{u}\cdot\mathbf{v} & \mathbf{0} \\ \mathbf{0} & 3N(x)\mathbf{u}\cdot\mathbf{v} \end{bmatrix}$$
$$= \begin{bmatrix} 3 & \mathbf{0} \\ \mathbf{0} & 1 \end{bmatrix}.$$

Thus, the proposition holds in every case. □

Proposition 5.1.4. *For $0 \leq n \leq 8$, there exist loops in $GLL(\mathbb{Z}/4\mathbb{Z})$ which are isomorphic to*

$(\mathbb{Z}/2\mathbb{Z})^n \times C_2$ *equipped with the multiplication from 2.2.1.*

Proof. It has been shown already in this chapter that elements of order 2 exist in $GLL(\mathbb{Z}/4\mathbb{Z})$. Any one of these elements, call it x, forms a loop isomorphic to $(\mathbb{Z}/2\mathbb{Z})^0 \times C_2$.

By adding elements of Γ to the generating set one at a time, other subloops of the form $(\mathbb{Z}/2\mathbb{Z})^n \times C_2$ can be constructed. Note that, if $g \in \Gamma$, then $xgx \in \Gamma$, so an arbitrary choice of kernel element may increase the order of $\Gamma(L)$ by more than a factor of 2. If x and g commute, however, then $xgx = g$ and no extra kernel elements appear in the subloop, so a convenient set of elements to consider is $\gamma(x)$.

By Proposition 5.1.2, $\gamma(x) \cong (\mathbb{Z}/2\mathbb{Z})^6$. Then choose $\{g_1, g_2, \dots g_6\}$ to be a generating set for $\gamma(x)$. Then the elements $g_1, \dots, g_6$ can be added to the generating set of the loop one at a time to obtain loops isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m \times C_2$ for $0 \leq m \leq 6$.

For a loop of the form $(\mathbb{Z}/2\mathbb{Z})^7 \times C_2$ an element of Γ which does not necessarily commute with x, but for which xgx is contained in $\langle g, \gamma(x)\rangle$ is necessary. Of course, by Proposition 5.1.3 precisely such an element is guaranteed to exist. Thus a subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z})^7 \times C_2$ exists. Then, of course, adding any remaining element of the kernel to this subloop gives a subloop isomorphic to $\Gamma \times C_2 \cong (\mathbb{Z}/2\mathbb{Z})^8 \times C_2$. □

Thus, above the loop C_2 in the subloop lattice is a chain of loops:

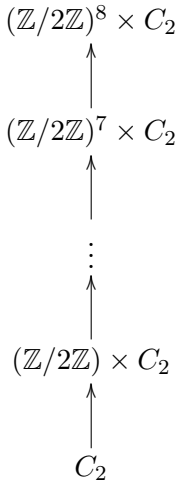

Figure 5.1 Subloop Lattice Over C_2

5.1.2 Loops that project down to C_3

Again, all of these subloops are associative by Proposition 4.3.1 since they must be generated by elements of Γ and one element of order 3. Such loops are of the form $\Gamma(L) \times C_3$. The goal of this section is to determine the possible orders of $\Gamma(L)$.

Proposition 5.1.5. *If x is an element of order 3, then $|\gamma(x)| = 4$.*

Proof. Let $x = \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix}$ and let $g = \begin{bmatrix} 2c+1 & 2\mathbf{r} \\ 2\mathbf{s} & 2d+1 \end{bmatrix}$ be a generic element of Γ. Then, just as in the proof of Proposition 5.1.2, the following equations must hold:

The comparing of the first entries of gx and xg gives a familiar equation, since it was the same in the order 2 case.

$$2ac + a + 2\mathbf{u} \cdot \mathbf{s} = 2ac + a + 2\mathbf{r} \cdot \mathbf{v}$$

$$2\mathbf{u} \cdot \mathbf{s} = 2\mathbf{r} \cdot \mathbf{v}$$

Note that comparing the final entries of gx and xg duplicates this equation.

The comparing of the second entries of gx and xg is slightly different than before since a and b must have different parity because $x^3 = 1$.

$$\begin{aligned} 2a\mathbf{r} + 2d\mathbf{u} + \mathbf{u} - 2\mathbf{v} \times \mathbf{s} =& 2c\mathbf{u} + \mathbf{u} + 2b\mathbf{r} - 2\mathbf{s} \times \mathbf{v} \\ 2a\mathbf{r} + 2d\mathbf{u} =& 2c\mathbf{u} + 2b\mathbf{r} \\ 2(a+b)\mathbf{r} =& 2(c+d)\mathbf{u} \\ 2\mathbf{r} =& 2(c+d)\mathbf{u} \end{aligned}$$

noting here that since x is order three, $a + b = 3$.

The comparing of the third entries of gx and xg gives a similar

$$\begin{aligned} 2c\mathbf{v} + \mathbf{v} + 2b\mathbf{s} + 2\mathbf{u} \times \mathbf{r} =& 2a\mathbf{s} + 2d\mathbf{v} + \mathbf{v} + 2\mathbf{r} \times \mathbf{u} \\ 2c\mathbf{v} + 2b\mathbf{s} =& 2a\mathbf{s} + 2d\mathbf{v} \\ 2(a+b)\mathbf{s} =& 2(c+d)\mathbf{v} \\ 2\mathbf{s} =& 2(c+d)\mathbf{v}. \end{aligned}$$

If c and d are chosen, then there exist unique choices of $\mathbf{s}$ and $\mathbf{r}$ that satisfy these equations. Note that if the last two are satisfied, then the first one becomes

$$\begin{aligned} 2\mathbf{u} \cdot \mathbf{s} &= 2\mathbf{r} \cdot \mathbf{v} \\ \mathbf{u} \cdot 2\mathbf{s} &= \mathbf{v} \cdot 2\mathbf{r} \\ \mathbf{u} \cdot 2(c+d)\mathbf{v} &= \mathbf{v} \cdot 2(c+d)\mathbf{u} \end{aligned}$$

and so is automatically satisfied. Therefore there are exactly $2^2 = 4$ choices for $g \in \gamma(x)$. □

Remark 5.1.6. Since the elements $\begin{bmatrix} 1 & (000) \\ (000) & 1 \end{bmatrix}$ and $\begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}$ obviously commute with any element, the non-central elements of $\gamma(x)$ must be of the form $\begin{bmatrix} 1 & \mathbf{u} \\ \mathbf{v} & 3 \end{bmatrix}$ and $\begin{bmatrix} 3 & \mathbf{r} \\ \mathbf{s} & 1 \end{bmatrix}$.

Proposition 5.1.7. *Let x be order 3. Then there exist 2^6 elements, $g \in \Gamma$ such that gx is order 3.*

Proof. From earlier calculations, recall that

$$gx = \begin{bmatrix} 2ac + a + 2\mathbf{r} \cdot \mathbf{v} & 2c\mathbf{u} + \mathbf{u} + 2b\mathbf{r} - 2\mathbf{s} \times \mathbf{v} \\ 2a\mathbf{s} + 2d\mathbf{v} + \mathbf{v} + 2\mathbf{r} \times \mathbf{u} & 2\mathbf{s} \cdot \mathbf{u} + 2db + b \end{bmatrix}.$$

Since x is order 3, either a or b is even. Without loss of generality, assume that b is even and a is odd. Furthermore, $\mathbf{u} \cdot \mathbf{v}$ must be odd. Since all elements of order 3 have norm 1, g must have norm 1 so $c = d$. Incorporating these facts yields

$$gx = \begin{bmatrix} 2c + a + 2\mathbf{r} \cdot \mathbf{v} & 2c\mathbf{u} + \mathbf{u} - 2\mathbf{s} \times \mathbf{v} \\ 2\mathbf{s} + 2c\mathbf{v} + \mathbf{v} + 2\mathbf{r} \times \mathbf{u} & 2\mathbf{s} \cdot \mathbf{u} + b \end{bmatrix}.$$

Then since the trace of elements of order three must be 3, $2c + a + 2\mathbf{r} \cdot \mathbf{v} + 2\mathbf{s} \cdot \mathbf{u} + b = 3$. Of course, $a + b = 3$ so the requirement on g can be summarized as

$$2c + 2\mathbf{r} \cdot \mathbf{v} + 2\mathbf{s} \cdot \mathbf{u} = 0$$

and since $\mathbf{u} \cdot \mathbf{v}$ is odd, at least one entry of those vectors must be odd, so if 6 of the variables in the above expression are fixed, then the last is determined uniquely. Recalling the $c = d$, there are thus 2^6 different elements of Γ such that gx is order 3. □

Proposition 5.1.8. *For $0 \leq n \leq 8$, there exist loops in $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$ which are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n \times C_3$ equipped with the multiplication from 2.2.1.*

Proof. Choose x to be an element of order 3. Then $\langle x \rangle \cong C_3$. By Proposition 5.1.5, there are 4 elements of Γ which commute with x. Let M_1 and M_2 generate this set. By Proposition 5.1.7, there are 2^6 elements in Γ such that gx is order 3 so let N_1, N_2 and N_3 be elements of this set. Note that $(gx)^3 = 1$ implies that $xgx^2 = gx^2gx$. For any element $g \in \Gamma$, the subloop $\langle g, x \rangle$ will include the kernel elements g, x^2gx and xgx^2. If $xg = gx$, then all these elements are just equal to g, and so $\Gamma(\langle g, x \rangle) = \{1, g\}$. If $(gx)^3 = 1$ then xgx^2 is the product of g and x^2gx so $\Gamma(\langle g, x \rangle) = \{1, g, xgx^2, x^2gx\}$. Thus the order of the subloop increases by a factor of 2 if g commutes with x and a factor of 4 if $(gx)^3 = 1$. Since all elements of Γ commute with each

other, this will remain true when adding kernel elements to $\langle g, x\rangle$ and so on. In summary,

$$\begin{aligned}
\langle x\rangle &\cong C_3\\
\langle x, M_1\rangle &\cong \mathbb{Z}/2\mathbb{Z}\times C_3\\
\langle x, M_1, M_2\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^2\times C_3\\
\langle x, M_1, N_1\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^3\times C_3\\
\langle x, M_1, M_2, N_1\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^4\times C_3\\
\langle x, M_1, N_1, N_2\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^5\times C_3\\
\langle x, M_1, M_2, N_1, N_2\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^6\times C_3\\
\langle x, M_1, N_1, N_2, N_3\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^7\times C_3\\
\langle x, \Gamma\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^8\times C_3
\end{aligned}$$

□

So above C_3 in the subloop lattice is a lattice of subloops that looks like:

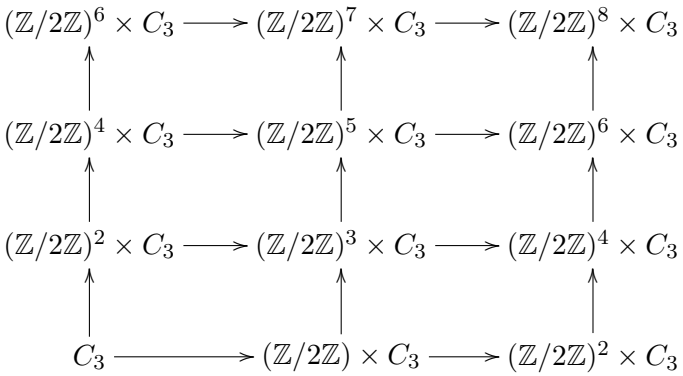

Figure 5.2 Subloop Lattice Over C_3

It is important to note that although all of these subloops exist, they are not always nested inside each other as the corresponding C_2 subloops are. For instance, the $(\mathbb{Z}/2\mathbb{Z})^6\times C_3$ above is not contained in the $(\mathbb{Z}/2\mathbb{Z})^7\times C_3$ above, though both are obviously contained in $(\mathbb{Z}/2\mathbb{Z})^8\times C_3$.

5.1.3 Loops that project down to C_2^2

It was already shown in Proposition 4.1.6 that if $L\pi \cong C_2^2$ then $|L| > 4$ for any subloop L of $GLL(\mathbb{Z}/4\mathbb{Z})$. The following proposition goes into somewhat more detail about when elements of order 2 commute with each other.

Proposition 5.1.9. *Let $x, y \in GLL(\mathbb{Z}/4\mathbb{Z}) \setminus \Gamma$ such that $x^2 = y^2 = 1$. Then $xy = yx$ if and only if $x\pi = y\pi$.*

Proof. By Proposition 4.1.5, $xy \in \Gamma$ so $(xy)\pi = 1$ in $GLL(\mathbb{Z}/2\mathbb{Z})$. Then $x\pi y\pi = 1$ and since x is order 2, $x\pi$ must be order 2 in $GLL(\mathbb{Z}/2\mathbb{Z})$. Thus $y\pi = x\pi$.

If $x\pi = y\pi$, then $(xy)\pi = 1$ and so $xy \in \Gamma$ which implies $(xy)(xy) = 1$ which further implies $xy = yx$. Note the use of diassociativity in this argument. □

If $L\pi \cong C_2^2$, then L contains an element of order 4. Now is a good time to examine some of the basic properties of elements of order 4.

Proposition 5.1.10. *If x is an element of $GLL(\mathbb{Z}/4\mathbb{Z})$ of order 4, then*

1. *$x\pi$ is order 2 in $GLL(\mathbb{Z}/4\mathbb{Z})$*
2. *$x^2 \in \Gamma$*
3. *$|\gamma(x)| = 64$*

Proof. 1. This is a combination of Proposition 4.1.1 and Proposition 4.1.2.

2. Simply $N(x^2) = N(x)^2 = 1$ and x^2 is obviously order 2, so it must lie in Γ.

3. This is from Proposition 5.1.2.

□

Let x and y be elements in $GLL(\mathbb{Z}/4\mathbb{Z})$ such that $\langle x\pi, y\pi\rangle \cong C_2^2$ in $GLL(\mathbb{Z}/2\mathbb{Z})$. Since Proposition 5.1.9 says that some element in $\langle x, y\rangle$ has order 4, assume simply that x has order 4 and y has order 2. Then by Proposition 5.1.10 $x^2 \in \Gamma$. Note that Proposition 4.2.2 shows that $xy \neq yx$. If $(xy)^2 = 1$, then $xyxy = 1$ which implies that $xy = yx^3$ in this case, $\langle x, y\rangle \cong D_8$ in

$GLL(\mathbb{Z}/4\mathbb{Z})$. This group is of the form $\mathbb{Z}/2\mathbb{Z} \times C_2^2$ and is the smallest possible subloop that projects to C_2^2.

Proposition 5.1.11. *Let x and y be non-kernel elements such that $x^4 = y^4 = 1$ then $|\gamma(x) \cap \gamma(y)| = 32$.*

Proof. Let $x = \begin{bmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{bmatrix}$ and $y = \begin{bmatrix} e & \mathbf{p} \\ \mathbf{q} & f \end{bmatrix}$. If $g \in \Gamma$ is $\begin{bmatrix} 2c+1 & 2\mathbf{r} \\ 2\mathbf{s} & 2d+1 \end{bmatrix}$ then in order for $g \in \gamma x \cap \gamma y$, the following three equations must be true:

$$2\mathbf{u} \cdot \mathbf{s} = 2\mathbf{r} \cdot \mathbf{v}$$

$$2\mathbf{p} \cdot \mathbf{s} = 2\mathbf{r} \cdot \mathbf{q}$$

$$c = d$$

Since neither x nor y are kernel elements, there must be some odd entries in at least 2 of the vectors $\mathbf{u}$, $\mathbf{v}$, $\mathbf{p}$, and $\mathbf{q}$. Furthermore, since $x\pi \neq y\pi$, at least one of the pairs $\mathbf{u}$ and $\mathbf{p}$ or $\mathbf{v}$ and $\mathbf{q}$ have a slot in which one vector has an odd entry and the other an even entry. Without loss of generality, assume that u_1 is odd, p_1 is even, and p_2 is odd. Then,

$$2(p_1s_1 + p_2s_2 + p_3s_3) = 2(q_1r_1 + q_2r_2 + q_3r_3)$$

$$2p_2s_2 = 2(q_1r_1 + q_2r_2 + q_3r_3 + p_3s_3)$$

and since p_1 is even, it disappears from the equation. So fixing $\mathbf{r}$ and s_3 uniquely determines s_2. Note that only whether s_2 is even or odd is of any consequence since the vector is originally $2\mathbf{s}$. Similarly,

$$2(u_1s_1 + u_2s_2 + u_3s_3) = 2(v_1r_1 + v_2r_2 + v_3r_3)$$
$$2u_1s_1 = 2(v_1r_1 + v_2r_2 + v_3r_3 + u_2s_2 + u_3s_3)$$

since u_1 is odd, and we need only choose whether s_1 is even or odd, there is a unique solution provided that $\mathbf{r}$, s_2, and s_3 are fixed. Thus, fixing four variables in these two equations uniquely determine the other two. Combining this with the simple fact that $c = d$ shows that there are $2^5 = 32$ elements in $\gamma(x) \cap \gamma(y)$. □

Proposition 5.1.12. *There exist subloops of the form* $(\mathbb{Z}/2\mathbb{Z})^n \times C_2^2$ *for* $0 < n \leq 8$.

Proof. From above analysis, start with a loop, $\langle x, y\rangle$, such that $xy = yx^3$ so it is of the form $\mathbb{Z}/2\mathbb{Z} \times C_2^2$. The kernel element in $\langle x, y\rangle$ is x^2 which commutes with x and y, so let M_1, M_2, M_3, M_4 be a generating set for $\gamma(x) \cap \gamma(y) \setminus \langle x, y\rangle$. For any $g \in \Gamma$, the elements ygy, x^3gx, and yx^3gxy will also be kernel elements. Note that since x^2 is in Γ, $x^2gx^2 = g$ and $xgx^3 = x^3gx$. Furthermore, $x^3ygyx = yxgx^3y = yx^3gxy$. If g commutes with y, then only the elements g and x^3gx and their products will be added $\Gamma(\langle g, x, y\rangle)$. So if $g \in \gamma(x) \cap \gamma(y)$ the order of the subloop increases by a factor of 2, if $g \in \gamma(x) \setminus \gamma(y)$ or $g \in \gamma(y) \setminus \gamma(x)$ then the order of the subloop increases by a factor of 4. Let N_1 be an element of $\gamma(x) \setminus \gamma(y)$. Note that the element $N_1(yN_1y)$ obviously commutes with x, but also commutes with y since

$$yN_1(yN_1y)y = yN_1yN_1 = (yN_1y)N_1 = N_1(yN_1y).$$

This means that adding N_1 also adds an element that is in $\gamma(x) \cap \gamma(y)$ so that adding N_1 will only increase the order by a factor of 2 if $\gamma(x) \cap \gamma(y)$ has already been added. Finally, let $Q = \begin{bmatrix} 1 & (000) \\ (000) & 3 \end{bmatrix}$ which will also only increase the order of the loop by a factor of 2 provided $\gamma(x) \cap \gamma(y)$ as shown in Proposition 5.1.3. Since all elements of Γ commute with each

other, this will remain true when adding kernel elements to $\langle g, x\rangle$ and so on. In summary,

$$\begin{aligned}
\langle x, y\rangle &\cong (\mathbb{Z}/2\mathbb{Z}) \times C_2^2 \\
\langle x, y, M_1\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^2 \times C_2^2 \\
\langle x, y, M_1, M_2\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^3 \times C_2^2 \\
\langle x, y, M_1, M_2, M_3\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^4 \times C_2^2 \\
\langle x, y, M_1, M_2, M_3, M_4\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^5 \times C_2^2 \\
\langle x, y, M_1, M_2, M_3, Q, N_1\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^6 \times C_2^2 \\
\langle x, y, M_1, M_2, M_3, M_4, N_1, Q\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^7 \times C_2^2 \\
\langle x, y, \Gamma\rangle &\cong (\mathbb{Z}/2\mathbb{Z})^8 \times C_2^2
\end{aligned}$$

□

An example of this subloop and the corresponding lattice appear in the appendix.

5.1.4 Loops that project down to C_2^3

Let x, y, z be elements in $GLL(\mathbb{Z}/4\mathbb{Z})$ such that $\langle x\pi, y\pi, z\pi\rangle \cong C_2^3$ in $GLL(\mathbb{Z}/2\mathbb{Z})$. Then the orders of x, y, and z are either 2 or 4. By Proposition 4.1.6 at least 2 of these elements must be order 4 so assume without loss of generality that x and y are order 4 and z is order 2. This means that at least x^2 and y^2 are elements of Γ so that $|\langle x, y, z\rangle| \geq 32$. Obviously, if x, y and z commute, then these (and x^2y^2) are the only kernel elements in $\langle x, y, z\rangle$. For now, assume this is the case.

Proposition 5.1.13. *Let x, y and z be non-kernel elements such that $x^4 = y^4 = z^4 = 1$ then $|\gamma(x) \cap \gamma(y) \cap \gamma(z)| = 16$.*

Proof. The proof is very similar to the proof of Proposition 5.1.11. Let $x = \begin{bmatrix} x_1 & \mathbf{u} \\ \mathbf{v} & x_2 \end{bmatrix}$, $y =$

$\begin{bmatrix} y_2 & \mathbf{p} \\ \mathbf{q} & y_2 \end{bmatrix}$, and $z = \begin{bmatrix} z_1 & \mathbf{m} \\ \mathbf{n} & z_2 \end{bmatrix}$ and let $g = \begin{bmatrix} 2c+1 & 2\mathbf{r} \\ 2\mathbf{s} & 2d+1 \end{bmatrix}$ be an element of $\gamma(x) \cap \gamma(y) \cap \gamma(z)$. Then the following 4 equations hold:

$$2\mathbf{u} \cdot \mathbf{s} = 2\mathbf{r} \cdot \mathbf{v}$$

$$2\mathbf{p} \cdot \mathbf{s} = 2\mathbf{r} \cdot \mathbf{q}$$

$$2\mathbf{m} \cdot \mathbf{s} = 2\mathbf{r} \cdot \mathbf{n}$$

$$c = d.$$

Just like in the proof of Proposition 5.1.11, each matrix x, y, and z have some odd entries in their vectors. Not all of those odd entries can be in the same spot, since x, y, and z all project down to different elements of $GLL(\mathbb{Z}/2\mathbb{Z})$. Thus, each of these equations fixes one entry of g, leaving a total of 4 free. Thus, there are $2^4 = 16$ elements in $\gamma(x) \cap \gamma(y) \cap \gamma(z)$. □

Proposition 5.1.14. *There exist subloops of the form* $(\mathbb{Z}/2\mathbb{Z})^n \times C_2^3$ *for* $1 < n \leq 8$.

Proof. At this point in the lattice, it is easier to simply construct an appropriate example and note its existence. This is done in the Appendix. □

5.1.5 Loops that project down to other subloops

Again, constructions are presented in the Appendix to verify the following proposition:

Proposition 5.1.15. *There exist subloops of the forms* $(\mathbb{Z}/2\mathbb{Z})^n \times S_3$ *for* $0 \leq n \leq 8$. *There exist subloops of the form* $(\mathbb{Z}/2\mathbb{Z})^n \times A_4$ *for* $0 < n \leq 8$.

5.2 The size of the subloop lattice

While the analysis of the previous section does provide a significant amount of information, there is still a lot remaining to be learned. One useful piece of information that can be obtained

from the results of this chapter without much more work is a general sense of the size of the subloop lattice of $GLL(\mathbb{Z}/4\mathbb{Z})$.

Proposition 5.2.1. *There is a chain of subloops in the subloop lattice of $GLL(\mathbb{Z}/4\mathbb{Z})$ of length 14, in which each subloop is maximal in the subloop that follows it. Furthermore, no chain of subloops with that property in the lattice is longer.*

Proof. The chain in question starts at the trivial subloop, which is maximal in a loop of order 2, call it $\langle x \rangle$. Proposition 5.1.4 guarantees a chain from C_2 to $\Gamma \times C_2$ of length 8 where each loop is index 2 in the next loop. From there, adding any element, y of order 2 such that $y\pi \neq x\pi$ gives a loop of the form $\Gamma \times C_2^2$ which contains the previous loop. Similarly, adding a third element of order 2 which projects to a different element in $GLL(\mathbb{Z}/2\mathbb{Z})$ creates a loop of the form $\Gamma \times C_2^3$ which contains the previous loop. Then there are subloops of the form $\Gamma \times A_4$ and $\Gamma \times M_{24}(A_4, 2)$ which contain the previous loops. Finally, $\Gamma \times M_{24}(A_4, 2)$ is maximal in $GLL(\mathbb{Z}/4\mathbb{Z})$. This is a total length of 14.

If $L_1 \subset L_2$ in the lattice of subloops of $GLL(\mathbb{Z}/4\mathbb{Z})$, then either $\Gamma(L_1) \subset \Gamma(L_2)$, $L_1\pi \subset L_2\pi$, or both. The longest chain in Γ is length 8 and the longest chain in $GLL(\mathbb{Z}/2\mathbb{Z})$, which is where $L_1\pi$ and $L_2\pi$ are, is 6. Thus, a chain of subloops can have length at most $8+6 = 14$. $\square$

CHAPTER 6. FURTHER QUESTIONS

This paper provides a simple method of constructing Moufang loops over commutative rings based on the construction of Paige loops. It shows that studying the loop constructed over a quotient ring provides a lot of insight into the structure of the loop constructed over the original ring. It also establishes a number of results about the structure of $GLL(\mathbb{Z}/4\mathbb{Z})$. Ideally, these results could be expanded or generalized to other powers of primes.

While this paper focused on subloops whose images in $GLL(\mathbb{Z}/2\mathbb{Z})$ were associative, the same techniques could be applied to the other subloops. Indeed this is one of the first things I intend to do. The analysis in these cases is more complicated due to the more inherent lack of associativity, however, with more work I believe that a complete knowledge of the subloop lattice of $GLL(\mathbb{Z}/4\mathbb{Z})$ is possible.

In the rest of this chapter I will highlight some possibilities for further research extending or relating to the ideas presented in this thesis.

6.1 Loops over other rings

The first and most obvious direction of research is to extend the results for $GLL(\mathbb{Z}/p^2\mathbb{Z})$ to higher powers of primes. Is there perhaps a similar decomposition in these cases, and if so, can it be used to completely classify the loops of this type? As higher powers of p are examined, it may be fruitful to consider whether the p-adic integers is a natural home for this construction and what kind of structure arises there.

Obviously, many rings are not integer rings and the study of loops constructed over polynomial rings or really any other commutative ring could provide an interesting direction. What can be said about the resulting loop if the underlying ring is a principal ideal domain or

unique factorization domain, for instance? Because of this work's focus on $GLL(\mathbb{Z}/4\mathbb{Z})$, the only ideals of the underlying ring that were really examined were nilpotent of class 2. The basic decomposition works for any ideal, and so connecting the properties of the ideal used, to the properties of any loop that results could prove very insightful.

A final potential direction is possibly using a map that is not a projection map to conduct the decomposition in Chapter 2. Looking at how maps on the underlying ring translate into maps on the resulting loops is an interesting project which is perhaps more of a categorical nature. Perhaps a different map allows for a more general result.

6.2 Representable loops

The Zorn vector matrix construction provides a way to represent abstract Moufang loops as combinatorial objects in a manner different from a latin square. An interesting question is what loops can be embedded into $GLL(R)$ for some commutative ring, R. Section 2.3 has found a class of such loops but there is no reason to think it is exhaustive. Representations and modules are intimately connected in group theory and it would be interesting to investigate whether there is some connection between loop modules and vector matrix representations. A good reference to start with would be Smith's book on quasigroup representations (18). In general, searching for loop analogues of group characters or other representation theory objects could be very profitable.

APPENDIX A. EXAMPLE SUBLOOPS

Example Projecting Down to C_2

For this development, we will choose the involution in $GLL(\mathbb{Z}/4\mathbb{Z})$ to be the element $x := \begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix}$. Note that $\begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix}$ has order two.

The subgroup $\gamma(x)$ is generated by the following 6 elements.

$$\begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & (200) \\ (200) & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & (020) \\ (020) & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & (002) \\ (002) & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & (200) \\ (020) & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & (200) \\ (002) & 1 \end{bmatrix}$$

Any set of n of these elements and x generates a loop of the form $(\mathbb{Z}/2\mathbb{Z})^n \times C_2$. The loop generated by x, all the above elements together with the element $\begin{bmatrix} 1 & (000) \\ (000) & 3 \end{bmatrix}$ is of the form $(\mathbb{Z}/2\mathbb{Z})^7 \times C_2$. Adding any other kernel element at this point gives a subloop $\Gamma \times C_2$.

Example Projecting Down to C_3

We choose an element, x, of order three in $GLL(\mathbb{Z}/4\mathbb{Z})$ to be the element $\begin{bmatrix} 3 & (0,3,3) \\ (1,1,0) & 0 \end{bmatrix}$.

Note that $x^2 = \begin{bmatrix} 0 & (0,1,1) \\ (3,3,0) & 3 \end{bmatrix}$.

The subgroup $\gamma(x)$ has only four elements

$$\begin{bmatrix} 1 & (0,0,0) \\ (0,0,0) & 1 \end{bmatrix}, \begin{bmatrix} 3 & (0,0,0) \\ (0,0,0) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (0,2,2) \\ (2,2,0) & 3 \end{bmatrix}, \begin{bmatrix} 3 & (0,2,2) \\ (2,2,0) & 1 \end{bmatrix}$$

Let $M_1 = \begin{bmatrix} 3 & (0,0,0) \\ (0,0,0) & 3 \end{bmatrix}$ and $M_2 = \begin{bmatrix} 1 & (0,2,2) \\ (2,2,0) & 3 \end{bmatrix}$ be generators for this set.

Define the matrices

$$N_1 = \begin{bmatrix} 3 & (200) \\ (000) & 3 \end{bmatrix}$$

$$N_2 = \begin{bmatrix} 1 & (002) \\ (000) & 1 \end{bmatrix}$$

$$N_3 = \begin{bmatrix} 1 & (202) \\ (220) & 1 \end{bmatrix}$$

noting that xN_i is order three for each i.

Example Projecting Down to C_2^2

Here we need an element of order 4 and an element of order 2 such that their product is also order 2. The x and y listed below satisfy this requirement.

$$x = \begin{bmatrix} 1 & (111) \\ (000) & 1 \end{bmatrix} \qquad y = \begin{bmatrix} 0 & (103) \\ (013) & 0 \end{bmatrix}$$

Now we list three elements in $\gamma(x) \cap \gamma(y)$.

$$M1 = \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix} \qquad M2 = \begin{bmatrix} 1 & (020) \\ (220) & 1 \end{bmatrix} \qquad M3 = \begin{bmatrix} 1 & (000) \\ (202) & 1 \end{bmatrix}$$

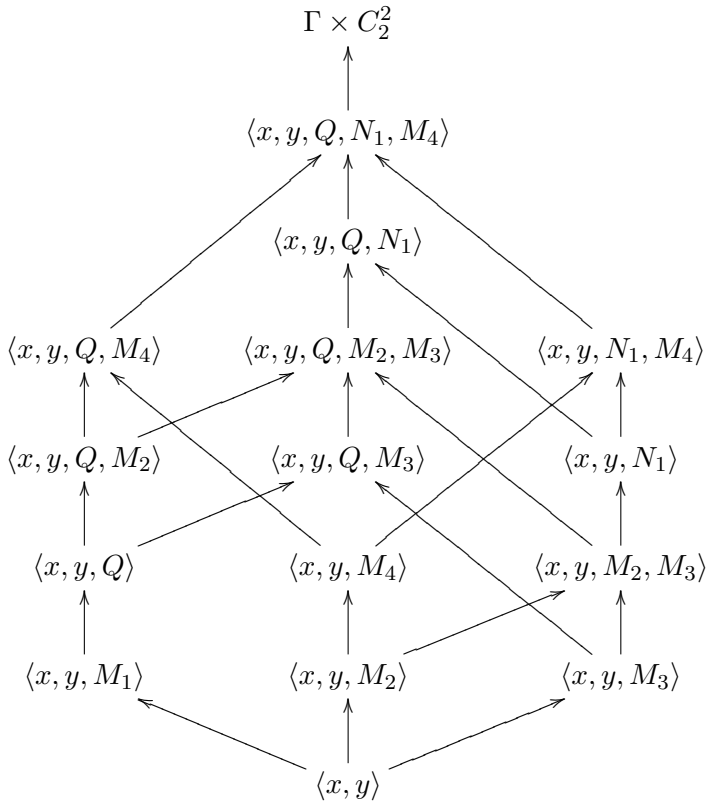

Figure A.1 Subloop Lattice over C_2^2

Finally, M_4 is an element of $\gamma(x) \cap \gamma(y)$ which does not commute with xy, N_1 is an element which commmutes with x but not y, and Q is the element from Proposition 5.1.3.

$$M4 = \begin{bmatrix} 1 & (200) \\ (000) & 1 \end{bmatrix} \qquad N1 = \begin{bmatrix} 1 & (000) \\ (220) & 1 \end{bmatrix} \qquad Q = \begin{bmatrix} 1 & (000) \\ (000) & 3 \end{bmatrix}$$

These elements form subloops of all the relevant orders. A partial drawing of this lattice is presented in Figure A.

Example Projecting Down to C_2^3

For this example we start with two elements of order 4 and one element of order 2 such that the product of either element of order 4 with the element of order 2 is also order 2. The

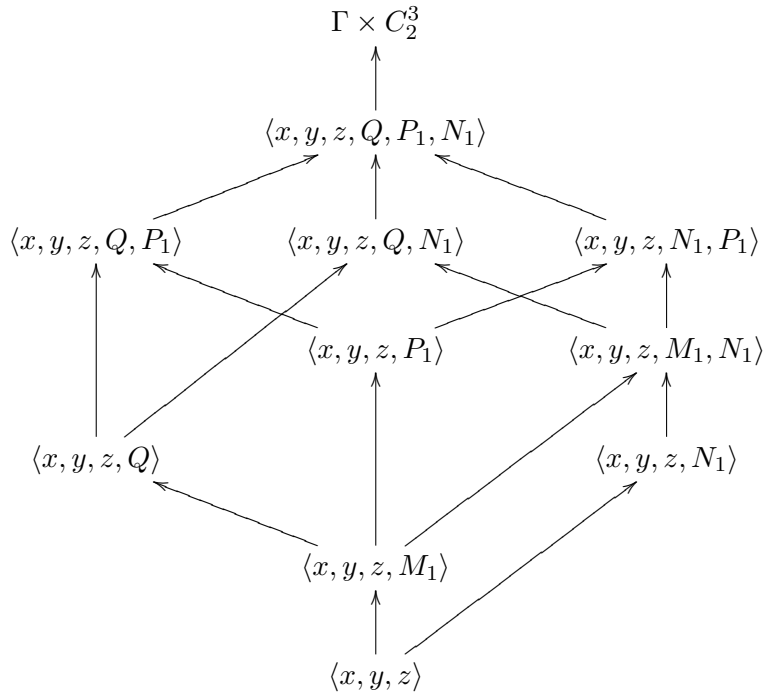

Figure A.2 Subloop Lattice over C_2^3

elements x, y and z satisfy this requirement.

$$x = \begin{bmatrix} 1 & (111) \\ (000) & 1 \end{bmatrix} \qquad y = \begin{bmatrix} 1 & (000) \\ (121) & 1 \end{bmatrix} \qquad z = \begin{bmatrix} 0 & (103) \\ (013) & 0 \end{bmatrix}$$

The elements M_1 is an element of $\gamma(x) \cap \gamma(y) \cap \gamma(z)$, N_1 is an element of $\gamma(x) \cap \gamma(y)$ but not $\gamma(z)$ and P_1 is an element of only $\gamma(x)$.

$$M1 = \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix} \qquad N1 = \begin{bmatrix} 1 & (020) \\ (000) & 1 \end{bmatrix} \qquad P1 = \begin{bmatrix} 1 & (200) \\ (000) & 1 \end{bmatrix}$$

Finally, Q is the element from Proposition 5.1.3. These elements form subloops of all the relevant orders. A partial drawing of this lattice is presented in Figure A.

Example Projecting Down to S_3

For convenience, use the elements $x = \begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix}$ and $y = \begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}$ from above as generators of S_3. This loop is a copy of S_3 in Zorn($\mathbb{Z}/4\mathbb{Z}$), since

$$xyx = \begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix} \begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix} \begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix} = \begin{bmatrix} 0 & (011) \\ (330) & 3 \end{bmatrix} = y^2.$$

Only one kernel element commutes with both x and y by Proposition 5.1.2 and Proposition 5.1.5, and that is $M_1 = \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}$. Clearly, there is a loop isomorphic to $\mathbb{Z}/2\mathbb{Z} \times S_3$ which is generated by x, y, and M_1.

First consider the elements in $\gamma(y)$. Note that

$$x \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix} x = \begin{bmatrix} 3 & (022) \\ (220) & 1 \end{bmatrix},$$

which is also in $\gamma(y)$. Thus, since there are four such elements, including these elements of $\gamma(y)$ constructs a subloop isomorphic to $\mathbb{Z}/2\mathbb{Z}^2 \times S_3$. Note that this subloop already contains the element M_1 so it cannot further be augmented by including it. Call $M_2 = \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}$.

Now consider kernel elements in $\gamma(x)$, but not in $\gamma(y)$. There are two possibilities for such a kernel element, M. First, it is possible that yMy^{-1} is another element of $\gamma(x)$. In this case, the dimension of the kernel will increase by three, since the kernel elements M, yMy^{-1}, $y^{-1}My$ and their products, but no others will be generated.

Analysis of this sort can continue, and by looking at elements which are fixed by some conjugation maps, but not others, a sublattice which includes examples of every possible order of subloop of the form $\Gamma(L) \times S_3$ results. This lattice is Figure A.

Define

$$M_3 = \begin{bmatrix} 1 & (022) \\ (000) & 1 \end{bmatrix}, \qquad N = \begin{bmatrix} 1 & (220) \\ (000) & 1 \end{bmatrix}.$$

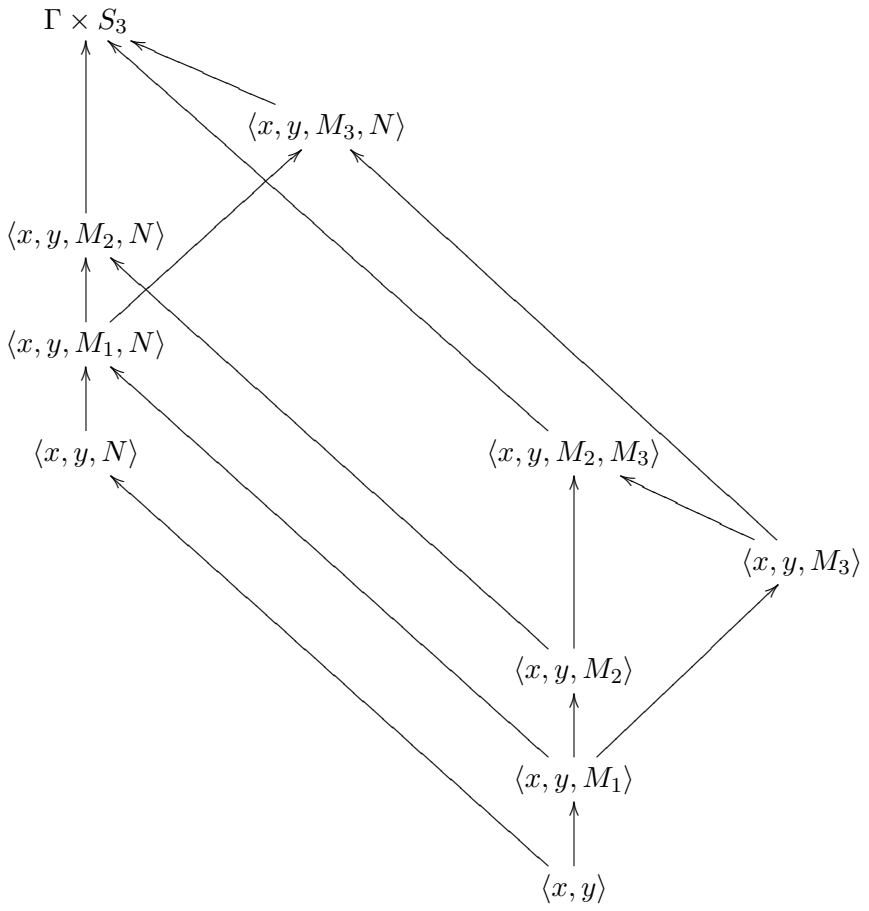

Figure A.3 Subloop Lattice over S_3

Example Projecting Down to A_4

Since A_4 contains a copy of C_2^2, the smallest possible loop projecting to A_4 would need to be order 24. Indeed, such a loop exists and is generated by

$$x = \begin{bmatrix} 0 & (331) \\ (111) & 0 \end{bmatrix} \qquad y = \begin{bmatrix} 0 & (110) \\ (300) & 3 \end{bmatrix}.$$

A table showing some possible subloops and their generators is provided in Table A.

Changing x and y slightly can result in subloops of order 48 or 96. For instance, if $x = \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}$, then $|\langle x, y \rangle| = 96$.

Table A.1 Generators for groups of the form $\Gamma L \times A_4$

Loop	*Generators*
$(\mathbb{Z}/2\mathbb{Z}) \times A_4$	$\begin{bmatrix} 0 & (331) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (110) \\ (300) & 3 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^4 \times A_4$	$\begin{bmatrix} 0 & (331) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (110) \\ (300) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (220) \\ (200) & 3 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^5 \times A_4$	$\begin{bmatrix} 0 & (331) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (110) \\ (300) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (200) \\ (200) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^6 \times A_4$	$\begin{bmatrix} 0 & (331) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (110) \\ (300) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (220) \\ (200) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (200) \\ (200) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^7 \times A_4$	$\begin{bmatrix} 0 & (331) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (110) \\ (300) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (200) \\ (000) & 1 \end{bmatrix}$

APPENDIX B. COMPUTER CODE

I encoded vector matrices as 2×4 matrices for the visual benefit. The vector matrix $\begin{bmatrix} 1 & (203) \\ (112) & 3 \end{bmatrix}$ would be entered as [1 2 0 3; 1 1 2 3].

zornproda

This is the basic function to multiply vector matrices together. It takes two vector matrices A and B, and a number n which tells the code to take everything modulo n.

```
function x = zornproda(A,B,n)


Temp1 = A(1,1)*[B(1,2:4)]+B(2,4)*[A(1,2:4)]-cross([A(2,1:3)],[B(2,1:3)]);


Temp2 = B(1,1)*[A(2,1:3)]+A(2,4)*[B(2,1:3)]+cross([A(1,2:4)],[B(1,2:4)]);


x = mod([A(1,1)*B(1,1)+dot(A(1,2:4),B(2,1:3)),Temp1(1,1),Temp1(1,2),
    Temp1(1,3);Temp2(1,1),Temp2(1,2),Temp2(1,3),dot([A(2,1:3)],[B(1,2:4)])
    +A(2,4)*B(2,4)],n);
```

zornorm

This function simply calculates the norm of a vector matrix, A, modulo n.

```
function n = zornorm(A)
n = A(1,1)*A(2,4)-dot(A(1,2:4),A(2,1:3));
```

zornorder

This function finds the order of a vector matrix. It takes as inputs a vector matrix, A and the modulus n. In order to keep it from looping eternally, if the order is greater than 150 or infinite, the code terminates and reports 150. Obviously, this could be adjusted up or down as required.

```
function x = zornorder(A,n)
m=1;
E=A;
while ~(all(all(E==[1 0 0 0; 0 0 0 1]))) & m < 150
    m = m+1;
    E = zornproda(E,A,n);
end
m
```

zorninv

This function calculates the inverse of a given vector matrix A in $GLL(\mathbb{Z}/n\mathbb{Z})$. It does not test this inverse, so will provide misleading (although obviously misleading) results if the input matrix is not invertible.

```
function x = zorninv(A,n)
temp1 = mod([A(2,4), -A(1,2:4);-A(2,1:3), A(1,1)],n);
x = zornproda(temp1,[mod(zornorm(A),n), 0 0 0; 0 0 0 mod(zornorm(A),n)],n);
```

zorngenerater

This is a complicated function that takes an array of vector matrices as an input and then outputs a list of vector matrices which are generated by the input list. These arrays are created using

```
loop = cat(3,M1,M2,...)
```

where $M1, M2, \ldots$ is a list of vector matrices. By running it multiple times with

```
loop = zorngenerater(loop,n)
```

it can be used to find the loop generated by a set of vector matrices. There is a cutoff built in at $2^7 \cdot 120$ elements to prevent it from running on very large loops. This can of course be changed or removed as needed. The loops I was concerned with were all smaller than this so I put in this line so I would know if the loop in question was too large without having to wait for the program to finish.

```
function x = zorngenerater(C,n)
for m = 1:size(C,3)
        for k = 1:size(C,3)
            temp = zornproda(C(:,:,m),C(:,:,k),n);
            bigtemp = repmat(temp, [1 1 size(C,3)]);
            if all(any(any(C-bigtemp)))
                C(:,:,size(C,3)+1) = temp;
                if size(C,3)==2^7*120
                    return
                end
                size(C,3)
            end
        end
end
x = C;
```

cayleytable

This function takes an array of vector matrices as an input and creates a Cayley table. The array of vector matrices should include every element of the loop in question. Ideally,

the identity element should be first to increase readability of the table. These tables can be exported to text documents and then read into GAP for use. This was used in conjunction with zorngenerater to classify some large groups and loops.

```
function x = cayleytable(C,n)
for j = 1:size(C,2)
for k = 1:size(C,2)
for i = 1:size(C,2)
    if zornproda(C{j},C{k},n) == C{i}
        D(j,k)=i;
        break
    end
end
end
end
x = D;
```

orderofzorn

This code calculates the order of the loop $GLL(\mathbb{Z}/n\mathbb{Z})$ for any composite number n. It does not mod out by the center, so it displays numbers twice what would be expected for the Paige loops over $\mathbb{Z}/p\mathbb{Z}$. It acheives the counting very combinatorially, by running each invertible norm and counting how many vector matrices have that norm. The helper functions numberoffactorpairs(m1,n) and numberoftriples(m2,n) count how many pairs of elements multiply together to get m1 in $\mathbb{Z}/n\mathbb{Z}$ and how many vector pairs have a dot product equal to $m2$ in $\mathbb{Z}/n\mathbb{Z}$ respectively.

```
function x = numberoffactorpairs(element,grouporder)
N=0;
for n = 0:(grouporder-1)
```

```
    for m = 0:(grouporder-1)
        if (mod(n.*m,grouporder) == element)
            N=N+1;
        else
        end
    end
end
x=N;

function x = numberoftriples(element,grouporder)
N=0;
for n1=0:(grouporder-1)
    for n2=0:(grouporder-1)
        for n3=0:(grouporder-1)
            if (mod(n1+n2+n3,grouporder)==element)
                N=N+numberoffactorpairs(n1,grouporder)
                .*numberoffactorpairs(n2,grouporder)
                .*numberoffactorpairs(n3,grouporder);
            else
            end
        end
    end
end
x=N;

function x = orderofzorn(n)
M=0;
for m = 0:(n-1)
```

```
    if (gcd(m,n)==1)
        for m1 = 0:(n-1)
            for m2 = 0:(n-1)
                if (mod(m1-m2,n)==m)
                    M=M+numberoffactorpairs(m1,n).*numberoftriples(m2,n);
                else
                end
            end
        end
    else
    end
end
M
```

BIBLIOGRAPHY

[1] A. A. Albert, *On simple alternative rings*, Canadian J. Math. **4** (1952), 129–135. MR 0048420 (14,11d)

[2] R. H. Bruck, *A Survey of Binary Systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie, Springer Verlag, Berlin, 1958. MR 0093552 (20 #76)

[3] R. H. Bruck and E. Kleinfeld, *The structure of alternative division rings*, Proc. Nat. Acad. Sci. U. S. A. **37** (1951), 88–90. MR 0041834 (13,8c)

[4] O. Chein, *Moufang loops of small order. I*, Trans. Amer. Math. Soc. **188** (1974), 31–51. MR 0330336 (48 #8673)

[5] O. Chein and H. O. Pflugfelder, *The smallest Moufang loop*, Arch. Math. (Basel) **22** (1971), 573–576. MR 0297914 (45 #6966)

[6] O. Chein, H. O. Pflugfelder, and J. D. H. Smith (eds.), *Quasigroups and Loops: Theory and Applications*, Sigma Series in Pure Mathematics, vol. 8, Heldermann Verlag, Berlin, 1990. MR 1125806 (93g:20133)

[7] S. Doro, *Simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **83** (1978), no. 3, 377–392. MR 0492031 (58 #11195)

[8] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, and R. Remmert, *Numbers*, Graduate Texts in Mathematics, vol. 123, Springer-Verlag, New York, 1990, With an introduction by K. Lamotke, Translated from the second

German edition by H. L. S. Orde, Translation edited and with a preface by J. H. Ewing, Readings in Mathematics. MR 1066206 (91h:00005)

[9] S. M. Gagola, III, *The development of Sylow p-subloops in finite Moufang loops*, J. Algebra **322** (2009), no. 5, 1565–1574. MR 2543623

[10] S. M. Gagola, III and J. I. Hall, *Lagrange's theorem for Moufang loops*, Acta Sci. Math. (Szeged) **71** (2005), no. 1-2, 45–64. MR 2160355 (2006f:20079)

[11] A. N. Grishkov and A. V. Zavarnitsine, *Lagrange's theorem for Moufang loops*, Math. Proc. Cambridge Philos. Soc. **139** (2005), no. 1, 41–57. MR 2155504 (2006d:20122)

[12] ———, *Sylow's theorem for Moufang loops*, J. Algebra **321** (2009), no. 7, 1813–1825. MR 2494749

[13] M. W. Liebeck, *The classification of finite simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **102** (1987), no. 1, 33–47. MR 886433 (88g:20146)

[14] M. L. Merlini Giuliani and C. Polcino Milies, *The smallest simple Moufang loop*, J. Algebra **320** (2008), no. 3, 961–979. MR 2427625 (2009e:20145)

[15] R. Moufang, *Zur Struktur von Alternativkörpern*, Math. Ann. **110** (1935), no. 1, 416–430. MR 1512948

[16] L. J. Paige, *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7** (1956), 471–482. MR 0079596 (18,110f)

[17] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics, vol. 7, Heldermann Verlag, Berlin, 1990. MR 1125767 (93g:20132)

[18] J. D. H. Smith, *An Introduction to Quasigroups and Their Representations*, Studies in Advanced Mathematics, Chapman & Hall/CRC, Boca Raton, FL, 2007. MR 2268350 (2008a:20104)

[19] J. D. H. Smith and A. B. Romanowska, *Post-Modern Algebra*, Pure and Applied Mathematics (New York), John Wiley & Sons Inc., New York, 1999, A Wiley-Interscience Publication. MR 1673047 (2000d:00001)

[20] T. A. Springer and F. D. Veldkamp, *Octonions, Jordan Algebras and Exceptional Groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000. MR 1763974 (2001f:17006)

[21] P. Vojtěchovský, *Finite simple Moufang loops*, Ph.D. thesis, Iowa State University, 2001.

[22] ———, *Generators of nonassociative simple Moufang loops over finite prime fields*, J. Algebra **241** (2001), no. 1, 186–192. MR 1838849 (2002e:20145)

[23] ———, *Investigation of subalgebra lattices by means of Hasse constants*, Algebra Universalis **50** (2003), no. 1, 7–26. MR 2026823 (2004j:20128)