Andrew Wells

Moufang loops arising from Zorn vector matrix algebras

Commentationes Mathematicae Universitatis Carolinae, Vol. 51 (2010), No. 2, 371--388

Persistent URL: `http://dml.cz/dmlcz/140113`

Moufang loops arising from Zorn vector matrix algebras

Andrew Wells

Abstract. In *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7** (1956), 471–482, Paige used the vector matrix construction over fields to produce simple Moufang loops. The purpose of this paper is to generalize the construction to the class of commutative rings, and examine the Moufang loops arising in this fashion. Specific attention is paid to the construction over the ring of integers modulo four.

Keywords: Zorn vector matrix, Moufang loop, Paige loop

Classification: 20N05

1. Introduction

The goal of this paper is to take the Zorn vector matrix construction over fields, which Paige used to create a class of simple Moufang loops [6], and extend it to commutative rings. This done, it examines the structure of the resulting loops in general, and then in more detail in one specific case.

Paige defines a Zorn vector matrix algebra over a field, and shows that under a certain multiplication, it forms an alternative algebra. For a field, $\mathbb{F}$, refer to this algebra as Zorn($\mathbb{F}$). Paige then takes the invertible elements of this algebra, and shows that they form a Moufang loop, which in this paper will be denoted as Zorn$(\mathbb{F})^*$. After some preliminaries in Section 2, Section 3 mirrors the construction over commutative rings, and shows that all of the main properties still hold. These loops are not simple, since Liebeck showed that all finite nonassociative simple Moufang loops are Paige loops in [3]. The rest of this paper examines the structure of these non-simple Moufang loops.

Section 4 examines the projection of Zorn$(R)^*$ down to Zorn$(R/I)^*$, for any ideal I of a ring R. This leads to a convenient decomposition of the original loop into the kernel of the projection and the image of the projection. The decomposition also applies to subloops of the original loop, and can be used to investigate the subloop lattice of such loops.

It is well known that the loop of units of the Zorn vector matrix algebra over the field $\mathbb{Z}/p\mathbb{Z}$, for p a prime, is either a Paige loop itself or a Paige loop when taken modulo its center [6]. The main motivation for this paper is to examine the structure of Zorn$(\mathbb{Z}/n\mathbb{Z})^*$ for any integer n, and to see how it relates to the Paige loops. It is a simple exercise using the Chinese Remainder Theorem to show that Zorn$(\mathbb{Z}/pq\mathbb{Z})^* \cong$ Zorn$(\mathbb{Z}/p\mathbb{Z})^* \times$ Zorn$(\mathbb{Z}/q\mathbb{Z})^*$ when p and q are relatively prime. In this way, the loops can be broken down into a product of loops based on prime powers. To see the structure of a loop of the form $\mathrm{Zorn}(\mathbb{Z}/p^e\mathbb{Z})^*$ is difficult in general, so Section 5 investigates the first example, $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$, in some depth. Toward this end, the paper analyzes key pieces of the subloop lattice of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$, including maximal and minimal subloops.

2. Preliminaries

Definition 2.1. A *quasigroup* is a set with a binary operation which satisfies the property that $xy = z$ has a unique solution if any two of the three variables are fixed.

Definition 2.2. A *loop* is a quasigroup with an identity element. That is, there exists an element 1 such that $1x = x1 = x$ for all x.

Definition 2.3. A *Moufang loop* further satisfies the 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

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

The main result on Moufang loops that is used in this paper is Moufang's Theorem [5] which is stated below:

Theorem 2.4. *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. Thus any two elements generate an associative subloop. This fact is used repeatedly throughout this paper without specific mention.

3. 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 $\left[\begin{smallmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{smallmatrix}\right]$ 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 $\mathbf{v}$.

Proposition 3.1. $\mathrm{Zorn}(R)$ *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:

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

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:

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

whereas

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

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 [1], and Paige references this same work in [6].

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

Definition 3.2. The *norm* of an element, x, is denoted $N(x)$ and defined by $N\left[\begin{smallmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{smallmatrix}\right] := ab - \mathbf{u}\cdot\mathbf{v}$.

Note that this is an obvious analogue of the determinant.

Proposition 3.3. *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 3.4. *A vector matrix is invertible if and only if its norm is a unit in R.*

Proof: Let $M = \left[\begin{smallmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{smallmatrix}\right]$ 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 3.5. *Let* $\operatorname{Zorn}(R)^*$ *be the set of invertible elements of* $\operatorname{Zorn}(R)$*. Then* $\operatorname{Zorn}(R)^*$ *is a Moufang loop.*

4. Extensions over a kernel

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

$$\pi : \operatorname{Zorn}(R)^* \to \operatorname{Zorn}(R/I)^*; [a_{ij}] \mapsto [a_{ij} + I]$$

be componentwise projection from R to R/I.

Definition 4.1. 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 $\operatorname{Zorn}(R)^*$, since π is a homomorphism.

Definition 4.2. If $f : S \to R$, call a section of f *normalized* if it maps the identity of R to the identity of S.

Proposition 4.3. *Let* i *be a normalized section of* π*. Then* $\Gamma \times \operatorname{Zorn}(R/I)^*$ *forms a loop with multiplication given by*

$$\langle n, q\rangle * \langle m, r\rangle = \langle (n(qi) \cdot m(ri))((qr)i)^{-1}, qr\rangle. \tag{4.1}$$

Proof: The second coordinate of this product is again an element of $\operatorname{Zorn}(R/I)^*$, 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 $(\Gamma \times \operatorname{Zorn}(R/I)^*)^2$ to $\Gamma \times \operatorname{Zorn}(R/I)^*$.

Obviously,

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

and

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

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

Furthermore,

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

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

So the inverse of any element is easily calculated.

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

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

So indeed this multiplication forms a loop on the set $\Gamma \times \mathrm{Zorn}(R/I)^*$. □

Proposition 4.4. *The loops* $\mathrm{Zorn}(R)^*$ *and* $\Gamma \times \mathrm{Zorn}(R/I)^*$ *are isomorphic when the latter is equipped with the multiplication from* (4.1).

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

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

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

The following shows that ϕ is a loop homomorphism. Let $g, h \in \mathrm{Zorn}(R)^*$. 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 $\mathrm{Zorn}(R)^*$ being diassociative. Since $\mathrm{Zorn}(R)^*$ is a Moufang loop, this is fine.

Define another map $\psi : \Gamma \times \mathrm{Zorn}(R/I)^* \to \mathrm{Zorn}(R)^*; \langle n, q\rangle \mapsto n(qi)$. 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:

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

$$\begin{aligned} &= nqi \cdot mri \\ &= \langle n, q\rangle\psi\langle m, r\rangle\psi\,. \end{aligned}$$

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 $\mathrm{Zorn}(R)^*$ is isomorphic to $(\Gamma \times \mathrm{Zorn}(R/I)^*, *)$. In the language of loop extensions, $\mathrm{Zorn}(R)^*$ is an extension of Γ by $\mathrm{Zorn}(R/I)^*$. □

Now examine possibilities for the structure of Γ. Let $A = \left[\begin{smallmatrix} a & \mathbf{u} \\ \mathbf{v} & b \end{smallmatrix}\right]$ be an element of Γ. Then since $A\pi = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, 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 4.5. *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 $\Gamma \times \mathrm{Zorn}(R/I)^*$, assume the multiplication $*$ defined in (4.1).

Let L be a subloop of $\mathrm{Zorn}(R)^*$ 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 $\mathrm{Zorn}(R/I)^*$.

Proposition 4.6. *Let L be a subloop of $\mathrm{Zorn}(R)^*$. 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 $x\pi = 1_{\mathrm{Zorn}(R/I)^*}$ and so since i is normalized, $x\pi i = 1_{\mathrm{Zorn}(R)^*}$. 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. □

5. The structure of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$

By Proposition 4.4 and Proposition 4.5,

$$\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^8 \times \mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$$

with the appropriate multiplication (4.1).

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

Proposition 5.1. *Let $x \in \mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ 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 $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$.*

Proof: Since

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

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

Proposition 5.2. *Let $y \in \mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ 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 $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$.*

Proof: This proof is much the same as the previous one. Since $y^2 \neq 1$ in $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$, $(yi)^2 \notin \Gamma$. Then $(yi)^3\pi = 1$ in $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ 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. □

5.1 Maximal subloops.

Let G be a noncommutative group of order n. Then let $M_{2n}(G)$ denote the nonassociative Moufang loop constructed from G via the loop extension process that Chein describes in [2].

Note that $M_{24}(A_4)$ and $M_{12}(S_3)$ are the maximal subloops of $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$, as shown in [4].

Proposition 5.3. *If L is a maximal subloop of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$, then it is of the form*

$$\mathbb{Z}/2\mathbb{Z}^7 \times \mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*, \ \mathbb{Z}/2\mathbb{Z}^8 \times M_{12}(S_3), \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z}^8 \times M_{24}(A_4).$$

Proof: Let L be a subloop of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$. Then L is isomorphic to $\Gamma(L) \times L\pi$ by Proposition 4.6. Note that in the multiplication

$$\langle n, 1\rangle * \langle m, r\rangle = \langle (n \cdot m(ri))(ri)^{-1}, r\rangle ,$$

the kernel element $\langle n, 1\rangle$ does not affect the second coordinate at all. This means that every subloop of the form $\Gamma(L) \times L\pi$ is a subloop of $\Gamma \times L\pi$. Thus, if L is maximal, then either $\Gamma(L) = \Gamma$ or $L\pi = \mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$. If $\Gamma(L) = \Gamma$ then $L\pi$ must be a maximal subloop of $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$, and if $L\pi = \mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$, then $\Gamma(L)$ must be a maximal subloop of Γ. These possibilities are exactly those listed in the proposition. □

An example of a maximal subloop of the form $\mathbb{Z}/2\mathbb{Z}^7 \times \mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ is the loop of all elements of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$ that have norm 1 as opposed to norm 3.

Note that a copy of the lattice of subloops of $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ exists at the top of the lattice of subloops of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$. That is, if $L\pi$ is a subloop of $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$, then the subloops $\mathbb{Z}/2\mathbb{Z}^8 \times L\pi$ form a lattice isomorphic to the subloop lattice of $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ as described in [7].

5.2 Minimal subloops.

Lemma 5.4. *Let $\left[\begin{smallmatrix} e & \mathbf{y} \\ \mathbf{z} & f \end{smallmatrix}\right]$ be an element of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$, and let $\left[\begin{smallmatrix} 2a+1 & 2\mathbf{u} \\ 2\mathbf{v} & 2b+1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 2c+1 & 2\mathbf{w} \\ 2\mathbf{x} & 2d+1 \end{smallmatrix}\right]$ 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,

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

and so the entries of M' are:

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

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 [5]. □

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 $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$. 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 5.4 shows that any loop of the form $G \times L$ must also be associative and hence a group.

It is now possible to begin describing the possible subloops of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$. Proposition 4.6 shows that every subloop $L \subseteq \mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$ 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 $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$.

Note that elements of Γ have the form $\left[\begin{smallmatrix} 2a+1 & (2b,2c,2d) \\ (2e,2f,2g) & 2h+1 \end{smallmatrix}\right]$ since they must project down to the identity element in $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$.

5.3 Subloops of the form $\Gamma(L) \times C_2$. For this development, choose the involution in $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ to be the element $x_0 := \left[\begin{smallmatrix} 0 & (111) \\ (111) & 0 \end{smallmatrix}\right]$, and for the sake of simplicity, choose $x_0 i = \left[\begin{smallmatrix} 0 & (111) \\ (111) & 0 \end{smallmatrix}\right] i = \left[\begin{smallmatrix} 0 & (111) \\ (333) & 0 \end{smallmatrix}\right]$. Note that $\left[\begin{smallmatrix} 0 & (111) \\ (333) & 0 \end{smallmatrix}\right]$ has order two in $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$.

Proposition 5.5. *For $0 \le n \le 8$, there exist loops in $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$ which are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n \times C_2$.*

Proof: Obviously, the loop generated by $x_0 i$ is isomorphic to C_2, which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^0 \times C_2$.

By adding elements of Γ to the generating set one at a time, the other subloops of the form $(\mathbb{Z}/2\mathbb{Z})^n \times C_2$ can be constructed. Ideally, the dimension of $\Gamma(L)$ would increase by one for each added kernel element, however, if $g \in \Gamma$, then $(x_0 i)g(x_0 i) \in \Gamma$, so an arbitrary choice of kernel element may increase the dimension of $\Gamma(L)$ more than this. To build the subloops one dimension at a time, it is necessary that $(x_0 i)g(x_0 i)$ is not a new kernel element for each $g \in \Gamma$ added. A convenient set of such elements is the set of elements which commute with $x_0 i$.

Let $M = \left[\begin{smallmatrix} 2a+1 & (2b,2c,2d) \\ (2e,2f,2g) & 2h+1 \end{smallmatrix}\right] \in \Gamma$. Then

$$\begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix} \begin{bmatrix} 2a+1 & (2b,2c,2d) \\ (2e,2f,2g) & 2h+1 \end{bmatrix} \begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix} = \begin{bmatrix} 2h+1 & 2\mathbf{u} \\ 2\mathbf{v} & 2a+1 \end{bmatrix},$$

where $\mathbf{u} = (c+d+e+f+g, b+d+e+f+g, b+c+e+f+g)$ and $\mathbf{v} = (b+c+d+f+g, b+c+d+e+g, b+c+d+e+f)$. This leads to the equations

$$\begin{aligned} 2b &= 2(c+d+e+f+g)\,, \\ 4b &= 2(b+c+d+e+f+g)\,, \\ 0 &= 2(b+c+d+e+f+g)\,, \end{aligned}$$

so $(b+c+d+e+f+g)$ must be even, or equivalently, there must be an even number of twos and an even number of zeros between the two off diagonal vectors. Obviously, $a = h$ as well. Since this restricts two of the eight dimensions of Γ, there are 2^6 vector matrices that commute with $x_0 i$.

Choose $\{M_1, M_2, \dots M_6\}$ to be a generating set for the subgroup of Γ which commutes with $x_0 i$. Then the elements $M_1, \dots, M_6$ can be added to L one at a time to obtain loops isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m \times C_2$ for $0 \le m \le 6$.

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 $x_0 i$, but for which $(x_0 i)M(x_0 i)$ is generated by the kernel elements already added is needed. Note that

$$\begin{aligned}\begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix} \begin{bmatrix} 1 & (000) \\ (000) & 3 \end{bmatrix} \begin{bmatrix} 0 & (111) \\ (333) & 0 \end{bmatrix} &= \begin{bmatrix} 3 & (000) \\ (000) & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & (000) \\ (000) & 3 \end{bmatrix} \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}.\end{aligned}$$

Since $\left[\begin{smallmatrix} 3 & (000) \\ (000) & 3 \end{smallmatrix}\right]$ is a matrix that commutes with $x_0 i$, it must be generated by $\{M_1, M_2, \ldots, M_6\}$, and so is an element of the subloop generated by $\{M\} \cup \{M_1, M_2, \ldots, M_6\}$. Therefore, adding M to the subloop $(\mathbb{Z}/2\mathbb{Z})^6 \times C_2$ constructs a subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z})^7 \times C_2$. 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:

$$\begin{tikzcd}
(\mathbb{Z}/2\mathbb{Z})^8 \times C_2 \\
(\mathbb{Z}/2\mathbb{Z})^7 \times C_2 \arrow[u] \\
\vdots \arrow[u] \\
(\mathbb{Z}/2\mathbb{Z}) \times C_2 \arrow[u] \\
C_2 \arrow[u]
\end{tikzcd}$$

5.4 Subloops of the form $\Gamma(L) \times C_3$. To construct subloops of this form, an element of order three in Zorn$(\mathbb{Z}/2\mathbb{Z})^*$ must be chosen. Choose $y_0 = \left[\begin{smallmatrix} 1 & (011) \\ (110) & 0 \end{smallmatrix}\right]$. For convenience choose a section that maps y_0 to an element of order three in Zorn$(\mathbb{Z}/4\mathbb{Z})^*$. Let i be such that

$$\begin{bmatrix} 1 & (011) \\ (110) & 0 \end{bmatrix} i = \begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & (011) \\ (110) & 1 \end{bmatrix} i = \begin{bmatrix} 0 & (011) \\ (330) & 3 \end{bmatrix}.$$

Note then that $(y_0^2)i = (y_0 i)^2$, and that $y_0 i$ has order three. Obviously, the loop generated by $y_0 i$ is isomorphic to C_3, which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^0 \times C_3$.

First, in the same way as done above, look for elements of Γ to add to the starting subloop to increase its size. Again, the elements which commute with $y_0 i$ are a convenient starting place:

$$\begin{aligned}
&\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix} \begin{bmatrix} 2a+1 & (2b,2c,2d) \\ (2e,2f,2g) & 2h+1 \end{bmatrix} \begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}^{-1} \\
&= \begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix} \begin{bmatrix} 2a+1 & (2b,2c,2d) \\ (2e,2f,2g) & 2h+1 \end{bmatrix} \begin{bmatrix} 0 & (011) \\ (330) & 3 \end{bmatrix} \\
&= \begin{bmatrix} 2b+2c+2h+1 & 2(g, a{+}f{+}c{+}h{+}b, a{+}g{+}h{+}e{+}c{+}b) \\ 2(b{+}g{+}d{+}f{+}e, c+g, b+g) & 2a+1+2b+2c \end{bmatrix}.
\end{aligned}$$

If this kernel element commutes, it must be the case that

$$\begin{aligned}
&\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix} \begin{bmatrix} 2a+1 & (2b,2c,2d) \\ (2e,2f,2g) & 2h+1 \end{bmatrix} \begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}^{-1} \begin{bmatrix} 2a+1 & (2b,2c,2d) \\ (2e,2f,2g) & 2h+1 \end{bmatrix} \\
&\qquad\qquad = \begin{bmatrix} 1 & (000) \\ (000) & 1 \end{bmatrix},
\end{aligned}$$

Solving the resulting system of equations shows that there are four elements which commute with $y_0 i$. Those four elements in particular are:

$$\begin{bmatrix} 1 & (000) \\ (000) & 1 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}, \begin{bmatrix} 3 & (022) \\ (220) & 1 \end{bmatrix}.$$

So it is possible to add any one of the non-identity elements to the starting subloop and obtain a subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times C_3$, and add another element to obtain a subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times C_3$. Now, just as before, elements which do not commute with $y_0 i$ but for which $(y_0 i)M(y_0 i)^{-1}M$ is a kernel element which is already contained in $\Gamma(L)$ can be added to increase the dimension of the subloop.

The element $(y_0 i)M(y_0 i)^{-1}M$ was calculated in general above. Unfortunately, it is not possible for $(y_0 i)M(y_0 i)^{-1}M$ to be one of the four elements already added to $\Gamma(L)$. Suppose that $(y_0 i)M(y_0 i)^{-1}M$ is $\left[\begin{smallmatrix} 3 & (000) \\ (000) & 3 \end{smallmatrix}\right]$. Solving the resulting system of equations shows that there is no matrix with this property. The same analysis on the other remaining kernel matrices gives the same conclusion.

If $(y_0 i)M(y_0 i)^{-1}$ is an element of the set generated by M and the above matrices, then $(y_0 i)M(y_0 i)^{-1} = MN$, where N is one of those four matrices. This implies that $(y_0 i)M(y_0 i)^{-1}M = N$, which was just shown to be impossible. Therefore $(y_0 i)M(y_0 i)^{-1}$ is linearly independent from the generating set. Thus, no matter what kernel element is added to the kernel, the dimension of the kernel will increase by at least two. This means that it is impossible to obtain a subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3 \times C_3$ by adding kernel elements to the previously constructed subloop $(\mathbb{Z}/2\mathbb{Z})^2 \times C_3$.

Thus, adding any other element of the kernel, M, to the subloop $(\mathbb{Z}/2\mathbb{Z})^2 \times C_3$ creates a subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4 \times C_3$. Note that when M is added, then $(y_0 i)M(y_0 i)^{-1}$ is also generated as demonstrated above. Conjugating this new element simply provides $(y_0 i)^{-1}M(y_0 i)$, since $y_0 i$ has order three. But $(y_0 i)^{-1}M(y_0 i)$ is just the inverse of $(y_0 i)M(y_0 i)^{-1}$, and therefore the dimension increases by two and no more.

It is possible to construct a subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3 \times C_3$. Simply add a kernel elements which is not fixed by conjugation with $y_0 i$ to the subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times C_3$ generated by $y_0 i$ and $\left[\begin{smallmatrix} 3 & (000) \\ (000) & 3 \end{smallmatrix}\right]$ to obtain a subloop isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3 \times C_3$. Further combinations of kernel elements construct subloops of each possible order. Sample generating sets for all the possible types of subloops are listed in Table 1.

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

$$\begin{tikzcd}
(\mathbb{Z}/2\mathbb{Z})^6 \times C_3 \arrow[r] & (\mathbb{Z}/2\mathbb{Z})^7 \times C_3 \arrow[r] & (\mathbb{Z}/2\mathbb{Z})^8 \times C_3 \\
(\mathbb{Z}/2\mathbb{Z})^4 \times C_3 \arrow[r] \arrow[u] & (\mathbb{Z}/2\mathbb{Z})^5 \times C_3 \arrow[r] \arrow[u] & (\mathbb{Z}/2\mathbb{Z})^6 \times C_3 \arrow[u] \\
(\mathbb{Z}/2\mathbb{Z})^2 \times C_3 \arrow[r] \arrow[u] & (\mathbb{Z}/2\mathbb{Z})^3 \times C_3 \arrow[r] \arrow[u] & (\mathbb{Z}/2\mathbb{Z})^4 \times C_3 \arrow[u] \\
C_3 \arrow[r] \arrow[u] & (\mathbb{Z}/2\mathbb{Z}) \times C_3 \arrow[r] \arrow[u] & (\mathbb{Z}/2\mathbb{Z})^2 \times C_3 \arrow[u]
\end{tikzcd}$$

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 $(\mathbb{Z}/2\mathbb{Z})^8 \times C_3$.

5.5 Subloops of the form $\Gamma(L) \times S_3$. For convenience, use the elements x_0 and y_0 from above as generators of S_3. Extending the section i from the first two examples to the whole loop, causes the image of this loop to be a copy of S_3 in $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})$. Only one kernel element commutes with both $x_0 i$ and $y_0 i$, and that is $\left[\begin{smallmatrix} 3 & (0,0,0) \\ (0,0,0) & 3 \end{smallmatrix}\right]$. The calculations showing this are contained in the previous subsections. Clearly, there is a loop isomorphic to $\mathbb{Z}/2\mathbb{Z} \times S_3$ which is generated by

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

As before elements $M \in \Gamma$ such that $x_0 i M x_0 i$ and $y_0 i M (y_0 i)^{-1}$ are in $M\Gamma(L)$ could be added to increase the size of the subloop in a controlled manner.

First consider the elements which are fixed under conjugation by $y_0 i$. Note that

$$x_0 i \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix} x_0 i = \begin{bmatrix} 3 & (022) \\ (220) & 1 \end{bmatrix},$$

which is also fixed under conjugation by $y_0 i$. Thus, since there are four such elements, including these kernel elements fixed by $y_0 i$ constructs a subloop isomorphic to $\mathbb{Z}/2\mathbb{Z}^2 \times S_3$. Note that this subloop already contains the element $\left[\begin{smallmatrix} 3 & (000) \\ (000) & 3 \end{smallmatrix}\right]$ so it cannot further be augmented by including it.

Now consider kernel elements which are fixed under conjugation by $x_0 i$, but not under conjugation by $y_0 i$. There are two possibilities for such a kernel element, M. First, it is possible that $y_0 i M (y_0 i)^{-1}$ is another element fixed under conjugation by $x_0 i$. In this case, the dimension of the kernel will increase by three, since the kernel elements M, $y_0 i M (y_0 i)^{-1}$, $(y_0)^{-1} i M y_0 i$ 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.

$$\begin{tikzcd}
 & & (\mathbb{Z}/2\mathbb{Z})^7 \times S_3 \arrow[r] & (\mathbb{Z}/2\mathbb{Z})^8 \times S_3 \\
 & \widetilde{(\mathbb{Z}/2\mathbb{Z})}^4 \times S_3 \arrow[r] & (\mathbb{Z}/2\mathbb{Z})^5 \times S_3 \arrow[r] \arrow[u] & (\mathbb{Z}/2\mathbb{Z})^6 \times S_3 \arrow[u] \\
 & (\mathbb{Z}/2\mathbb{Z})^3 \times S_3 \arrow[r] \arrow[uur] & (\mathbb{Z}/2\mathbb{Z})^4 \times S_3 \arrow[uur] & \\
S_3 \arrow[r] \arrow[uur] & \mathbb{Z}/2\mathbb{Z} \times S_3 \arrow[r] \arrow[u] \arrow[uur] & (\mathbb{Z}/2\mathbb{Z})^2 \times S_3 \arrow[u] \arrow[uur] &
\end{tikzcd}$$

The loops in the lattice are listed by generators in Table 2. The loop denoted $\widetilde{(\mathbb{Z}/2\mathbb{Z})}^4 \times S_3$ is just a different copy of $(\mathbb{Z}/2\mathbb{Z})^4 \times S_3$ with different generators.

6. Further inquiry

The investigations performed in this paper for the lattices over C_2, C_3 and S_3 could be carried out for every subloop of $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$, and that would give a very complete description of the subloop lattice. From there, it may be possible to generalize some statements about the structure of $\mathrm{Zorn}(\mathbb{Z}/p^2\mathbb{Z})^*$ or even $\mathrm{Zorn}(\mathbb{Z}/p^e\mathbb{Z})^*$.

Each of the three intervals looked at above gives a distributive subloop lattice but the subloop lattice of the smallest Paige loop from [7] is not distributive. Perhaps any non distributive lattice features of $\mathrm{Zorn}(\mathbb{Z}/4\mathbb{Z})^*$ is tied directly to the lattice of $\mathrm{Zorn}(\mathbb{Z}/2\mathbb{Z})^*$ and not the kernel structure at all.

Another fruitful direction in general is to look at the effect of various properties of the ideal I. For instance, if I is maximal or prime, what can be said about the structure of $\mathbb{Z}\mathrm{orn}(R/I)^*$?

TABLE 1. Generators for groups of the form $\Gamma L \times C_3$

Loop	Generators
C_3	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z}) \times C_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^2 \times C_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^3 \times C_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (020) \\ (002) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^4 \times C_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (020) \\ (002) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^5 \times C_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (020) \\ (002) & 1 \end{bmatrix}, \begin{bmatrix} 1 & (200) \\ (020) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^6 \times C_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (020) \\ (002) & 1 \end{bmatrix}, \begin{bmatrix} 1 & (200) \\ (020) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^7 \times C_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (020) \\ (002) & 1 \end{bmatrix}, \begin{bmatrix} 1 & (200) \\ (020) & 1 \end{bmatrix}, \begin{bmatrix} 1 & (222) \\ (000) & 1 \end{bmatrix}$

TABLE 2. Generators for groups of the form $\Gamma L \times S_3$

Loop	*Generators*
S_3	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z}) \times S_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^2 \times S_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^3 \times S_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (000) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^4 \times S_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (000) & 1 \end{bmatrix}$
$\widetilde{(\mathbb{Z}/2\mathbb{Z})}^4 \times S_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 1 & (220) \\ (000) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^5 \times S_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 3 & (000) \\ (000) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (220) \\ (000) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^6 \times S_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (220) & 3 \end{bmatrix}, \begin{bmatrix} 1 & (220) \\ (000) & 1 \end{bmatrix}$
$(\mathbb{Z}/2\mathbb{Z})^7 \times S_3$	$\begin{bmatrix} 3 & (033) \\ (110) & 0 \end{bmatrix}, \begin{bmatrix} 0 & (333) \\ (111) & 0 \end{bmatrix}, \begin{bmatrix} 1 & (022) \\ (000) & 1 \end{bmatrix}, \begin{bmatrix} 1 & (220) \\ (000) & 1 \end{bmatrix}$

References

[1] Bruck R.H., Kleinfeld E., *The structure of alternative division rings*, Proc. Nat. Acad. Sci. U.S.A. **37** (1951), 88–90; MR0041834 (13,8c).

[2] Chein O., *Moufang loops of small order. I*, Trans. Amer. Math. Soc. **188** (1974), 31–51; MR0330336 (48 #8673).

[3] Liebeck M.W., *The classification of finite simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **102** (1987), no. 1, 33–47; MR886433 (88g:20146).

[4] Merlini Giuliani M.L., Polcino Milies C., *The smallest simple Moufang loop*, J. Algebra **320** (2008), no. 3, 961–979; MR2427625 (2009e:20145).

[5] Moufang R., *Zur Struktur von Alternativkörpern*, Math. Ann. **110** (1935), no. 1, 416–430; MR1512948.

[6] Paige L.J., *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7** (1956), 471–482; MR0079596 (18,110f).

[7] Vojtěchovský P., *Investigation of subalgebra lattices by means of Hasse constants*, Algebra Universalis **50** (2003), no. 1, 7–26; MR2026823 (2004j:20128).

Mathematics Department, Iowa State University, Ames, IA 50011, USA

E-mail: wellsat@iastate.edu

(*Received* October 20, 2009, *revised* February 12, 2010)