A NOTE ON MOUFANG LOOPS ARISING FROM OCTONION ALGEBRAS OVER RINGS

S. PUMPLÜN

Abstract. We construct Moufang loops and generalized Paige loops out of octonion algebras over a ring.

Introduction

Examples of nonassociative Moufang loops canonically arise out of the invertible elements of an octonion algebra over a field. In particular, Paige [Pa] used Zorn's algebra of vector matrices to construct an important class of simple Moufang loops. This construction was extended for instance by Wells [W] and Vergara, Rosa, Martinez and Enrique [VRME] using Zorn's algebra of vector matrices $\mathrm{Zor}(R)$ over a commutative unital ring R. The resulting Moufang loops $M(R)$ of elements of determinant one in $\mathrm{Zor}(R)$ display some nice properties. For instance, each finite index subloop L, such that $M(R)$ has the weak Lagrange property relative to L, is a congruence subloop, if R is a Dedekind domain that contains a unit of infinite order [VRME].

In this paper we go one step further: Let R be an arbitrary commutative unital base ring. Given any projective R-module T of constant rank three, we consider the split octonion algebra $\mathrm{Zor}(T,\alpha)$ over an arbitrary base ring R as constructed by Petersson [P], and its invertible elements. The structure of the resulting Moufang loops is briefly investigated along the lines developed in [W] in Section 3, after introducing split octonion algebras over rings in Section 2. Section 4 presents a possible generalization of Paige loops. It can be expected that octonion algebras over rings with underlying non-free R-module structure will yield interesting examples of nonassociative Moufang loops: octonion algebras over rings do not need to contain any composition subalgebra, contrary to octonion algebras over fields. Some examples of nonassociative Moufang loops of infinite order constructed from octonions over rings are given in the last section.

1. Preliminaries

Let R be a unital commutative associative ring. The *rank* of a finitely generated projective R-module M is defined as $\sup\{\mathrm{rank}_{R_P} M_P \mid P \in \mathrm{Spec}\, R\}$. An R-module M has *full support* if $\mathrm{Supp}\,(M) = \{P \in \mathrm{Spec}\, R | M_P \neq 0\} = \mathrm{Spec}\, R$.

Date: 2.4.2013.

2000 *Mathematics Subject Classification.* Primary: 20N05, Secondary: 17D05.

Key words and phrases. Alternative algebras, Moufang loop, Paige loop, Zorn's vector matrix, split octonion algebra.

In the following, the term "R-algebra" refers to unital nonassociative algebras which are finitely generated projective with full support as R-modules. This implies that every such algebra is *faithful*, i.e., $rA = 0$ for $r \in R$ implies $r = 0$. Since A is finitely generated projective and faithful as R-module, $R1_A$ is a direct summand of A.

The *nucleus* of an R-algebra A is the set $\mathrm{Nuc}(A) = \{x \in A \,|\, [x, A, A] = [A, x, A] = [A, A, x] = 0\}$. The nucleus is an associative subalgebra of A and by definition, we have $x(yz) = (xy)z$ for x, y or $z \in \mathrm{Nuc}(A)$.

The *center* $Z(A)$ of an algebra A over R is the set of all elements which commute and associate with all elements of A, that is $Z(A) = \{x \in \mathrm{Nuc}(A) \,|\, xy = yx \text{ for all } y \in A\}$ [S4, p. 14].

Let M be a finitely generated projective R-module. A map $N : M \to R$ is called a *quadratic form* on M if $N(rx) = r^2N(x)$ for all $r \in R$, $x \in M$ and if $N_b : M \times M \to R$,

$$N_b(x, y) = N(x + y) - N(x) - N(y)$$

is a (necessarily symmetric) bilinear form. N_b is then called the *bilinear form associated with* N. A quadratic form $N : M \to R$ is called *nondegenerate*, if N_b determines an R-module isomorphism $M \xrightarrow{\sim} M^\vee = \mathrm{Hom}_R(M, R)$, $x \to N_b(x, \cdot)$.

An R-algebra A is called *quadratic* if there exists a quadratic form $N \colon A \to R$ such that $N(1_A) = 1$ and $x^2 - N_b(1_A, x)x + N(x)1_A = 0$ for all $x \in A$. N is uniquely determined and called the *norm* of A. An R-algebra C is called a *composition algebra* if it carries a nondegenerate quadratic form $N \colon C \to R$ such that $N(xy) = N(x)N(y)$ for all $x, y \in C$.

An algebra is called *alternative* if its associator $[x, y, z] = (xy)z - x(yz)$ is alternating. Composition algebras are quadratic alternative algebras. A quadratic form N on the composition algebra satisfying the conditions mentioned above agrees with its norm as a quadratic algebra and thus is unique. It is called the *norm* of C and is also denoted by N_C. A quadratic alternative algebra is a composition algebra if and only if its norm is nondegenerate [M, 4.6]. Composition algebras only exist in ranks 1, 2, 4 or 8. Those of constant rank 2 are exactly the quadratic étale R-algebras, those of constant rank 4 are called *quaternion algebras*, those of constant rank 8 *octonion algebras.* A composition algebra is called *split* if it contains an isomorphic copy of $R \times R$ as a subalgebra.

A composition algebra C has a *canonical involution* $\sigma = \bar{\ }$ given by $\overline{x} = T(x)1_C - x$, where $T \colon C \to R$ is the *trace* given by $T(x) = N_b(1_C, x)$. This involution satisfies $\bar{x}x = N(x)1 \in R1$. Moreover, $T(x, y) := T(xy)$ is a nondegenerate symmetric bilinear form on C, called the *trace form* of C (cf. [P, Section 1]).

An element $x \in C$ is invertible if and only if its norm is: If $x \in C$ is invertible then there is $y \in C$ such that $xy = 1 = yx$, hence $N(xy) = N(x)N(y) = 1$ and $N(x)$ is a unit in R. Conversely, if $N(x)$ is invertible in R then $x^{-1} = N(x)^{-1}\bar{x}$. Any composition algebra of constant rank greater than 2 over R has R as its center.

2. Zorn algebras

2.1. It is well-known that the free R-module

$$\mathrm{Zor}(R) = \begin{bmatrix} R & R^3 \\ R^3 & R \end{bmatrix}$$

is an octonion algebra over R under the multiplication

$$\begin{bmatrix} a & u \\ u' & a' \end{bmatrix}\begin{bmatrix} b & v \\ v' & b' \end{bmatrix} = \begin{bmatrix} ab +^t uv' & av + b'u - u' \times v' \\ bu' + a'v' + u \times v & {}^t u'v + a'b' \end{bmatrix},$$

with norm

$$\det \begin{bmatrix} a & u \\ u' & a' \end{bmatrix} = aa' -^t uu'$$

given by the determinant (see for instance [VRME], [W]). Here, ${}^t uv$ represents the usual dot product between the vectors u and v. If R is a field, this is the only split octonion algebra over R. However, if there exist projective R-modules of constant rank 3 with trivial determinant which are not free, this need not be the only one (cf. [P, 3.3, 3.4, 3.5]):

Let T be a projective R-module of constant rank 3 such that $\det T = \bigwedge^3(T) \cong R$. Let $\langle\, , \,\rangle : T \times T^\vee \to R$, $\langle u, \check{v}\rangle = \check{v}(u)$ be the canonical pairing. An isomorphism $\alpha : \bigwedge^3(T) \to R$ induces a bilinear map $\times : T \times T \longrightarrow T^\vee$ via

$$(u, v) \to u \times v = \alpha(u \wedge v \wedge -).$$

We call this map the *vector product* on T, since locally it is the ordinary vector product. Moreover, α also determines an isomorphism $\beta : \det T^\vee \longrightarrow R$ via

$$\alpha(u_1 \wedge u_2 \wedge u_3)\beta(u_1^\vee \wedge u_2^\vee \wedge u_3^\vee) = \det(\langle u_i, u_j^\vee\rangle)$$

for all $u_i \in T$, $u_j^\vee \in T^\vee$, $1 \leq i, j \leq 3$. Thus we analogously obtain a vector product $T^\vee \times T^\vee \longrightarrow T$ using β instead of α. The R-module

$$\mathrm{Zor}(T, \alpha) = \begin{bmatrix} R & T \\ T^\vee & R \end{bmatrix}$$

becomes an octonion algebra over R under the multiplication

$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix}\begin{bmatrix} b & v \\ v^\vee & b' \end{bmatrix} = \begin{bmatrix} ab + \langle u, v^\vee\rangle & av + b'u - u^\vee \times v^\vee \\ bu^\vee + a'v^\vee + u \times v & \langle v, u^\vee\rangle + a'b' \end{bmatrix}$$

with norm

$$\det \begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} = aa' - \langle u, u^\vee\rangle$$

given by the determinant. $\mathrm{Zor}(T, \alpha)$ is called a *Zorn algebra.* The construction is functorial in the parameters involved. Obviously, $\mathrm{Zor}(T, \alpha)$ is a split octonion algebra. Conversely, every split octonion algebra over R is isomorphic to such a Zorn algebra. Locally, $\mathrm{Zor}(T, \alpha)$ looks like $\mathrm{Zor}(R)$. Thus $\mathrm{Zor}(T, \alpha)$ can be viewed as the canonical generalization of Zorn's algebra of vector matrices $\mathrm{Zor}(R)$. Note that if R is a principal ideal domain or a Dedekind domain then $\mathrm{Zor}(R)$ is, up to isomorphism, the only split octonion algebra.

2.2. Some explicit automorphisms. As observed in [P, 3.4], given two projective R-modules T and T' of constant rank 3 such that $\det T \cong R$ and $\det T' \cong R$, we obtain $\mathrm{Zor}(T,\alpha) \cong \mathrm{Zor}(T',\alpha')$ for two isomorphisms $\alpha : \bigwedge^3(T) \to R$ and $\alpha' : \bigwedge^3(T') \to R$, if there is an R-linear map $\varphi : T \to T'$ such that $\alpha' \circ (\det(\varphi)) = \alpha$. Then φ is bijective and the algebra isomorphism induced by φ is

$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} \to \begin{bmatrix} a & \varphi(u) \\ \varphi^{\vee -1}(u^\vee) & a' \end{bmatrix}.$$

Similarly, $\mathrm{Zor}(T,\alpha) \cong \mathrm{Zor}(T^\vee,\beta)$ with the above notation, where the isomorphism is given by

$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} \to \begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix}^{*t} = \begin{bmatrix} a' & -u^\vee \\ -u & a \end{bmatrix}.$$

Corollary 1. *(i) If there is an R-linear map $\varphi : T \to T$ such that $\det(\varphi) = id$ then*

$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} \to \begin{bmatrix} a & \varphi(u) \\ \varphi^{\vee -1}(u^\vee) & a' \end{bmatrix}$$

lies in $\mathrm{Aut}(\mathrm{Zor}(T,\alpha))$.
(ii) If there is $\mu \in R^\times$ such that $\mu^3 = 1$ then

$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} \to \begin{bmatrix} a & \mu u \\ \mu^{-1}(u^\vee) & a' \end{bmatrix}.$$

lies in $\mathrm{Aut}(\mathrm{Zor}(T,\alpha))$*, i.e. there exist two nontrivial automorphisms induced by a primitive third root of unity μ in* $\mathrm{Aut}(\mathrm{Zor}(T,\alpha))$*.*

This result generalizes the diagonal isomorphisms described in [V, 3.14].

3. Moufang loops out of Zorn algebras

A *quasigroup* is a set with a binary operation usually denoted by juxtaposition such that the equation $xy = z$ has a unique solution if any of the two of the three variables x, y, z are fixed. A *loop* is a quasigroup with a unit element and a *Moufang loop* is a loop which satisfies one of the following equivalent the Moufang identities:

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

The elements in a Moufang loop satisfy the alternativity and flexibility laws. From the results listed in the previous section we conclude immediately:

Proposition 1. *(i) The set of invertible elements $C^\times$ in a composition algebra C over R is a Moufang loop under algebra multiplication.*
(ii) The set of elements of norm one in a composition algebra C over R is a normal Moufang subloop of $C^\times$.

We denote the Moufang subloop of elements of norm one in $\mathrm{Zor}(T,\alpha)$ by $M(T,\alpha)$.

Let I be an ideal in R, then T/IT is a projective R/I module of constant rank 3 such that $\det(T/IT) = \bigwedge^3(T/IT) \cong R/I$. Reducing the isomorphism $\alpha : \bigwedge^3(T) \to R$ modulo I

yields an isomorphism $\alpha_I : \bigwedge^3(T/IT) \to R/I$. Using that $T^\vee/IT^\vee \cong (T/IT)^\vee$ we define the canonical projection

$$\pi : \mathrm{Zor}(T,\alpha)^\times \to \mathrm{Zor}(T/IT,\alpha_I)^\times$$

via

$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} \to \begin{bmatrix} a+I & u+IT \\ u^\vee + IT^\vee & b'+I \end{bmatrix}.$$

A tedious but straightforward calculation shows that π is a loop homomorphism. Let $\Gamma = \pi^{-1}(\{1_{R/I}\}) = \pi^{-1}(\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\})$. Since π is a homomorphism, Γ is a subloop of $\mathrm{Zor}(T,\alpha)^\times$. As in [W], we call a section of a homomorphism $f : S \to R$ *normalized* if it maps the identity of R to the identity of S. From here the proof of [W, 4.3] carries over verbatim to our setting and yields:

Proposition 2. *Let i be a normalized section of π. Then $\Gamma \times \mathrm{Zor}(T/IT,\alpha_I)^\times$ together with the multiplication given by*

$$(n,q) \star (m,r) = (n(qi)(m(ri))^{-1}, qr).$$

forms a loop.

Proposition 3. *The loops $\mathrm{Zor}(T,\alpha)^\times$ and $(\Gamma \times \mathrm{Zor}(T/IT,\alpha_I)^\times, \star)$ are isomorphic.*

Proof. Define $\Phi : \mathrm{Zor}(T,\alpha)^\times \longrightarrow \Gamma \times \mathrm{Zor}(T/IT,\alpha_I)^\times$ via $g \to (g(\pi i)^{-1}, g\pi)$. Since $\mathrm{Zor}(T,\alpha)^\times$ is a Moufang loop, it is diassociative and the proof of [W, Proposition 4.4] can be again applied verbatim to show that Φ is a loop homomorphism with inverse $\Gamma \times \mathrm{Zor}(T/IT,\alpha_I)^\times \longrightarrow \mathrm{Zor}(T,\alpha)^\times$, $(n,q) \to n(qi)$. □

Looking at the set Γ now, let

$$A = \begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} \in \Gamma.$$

Since

$$A\pi = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

we have $a, a' \in 1 + I$ and $u \in IT$, $u^\vee \in IT^\vee$. Note that if $u, v \in IT$, $u^\vee, v^\vee \in IT^\vee$ then $\langle u, v^\vee\rangle$ and $\langle v, u^\vee\rangle$ lie in I^2T, $u \times v$ lies in $I^2T^\vee$ and $u^\vee \times v^\vee$ lies in I^2T. This observation leads to the following result, which extends [W, 4.5]:

Proposition 4. *If $I^2 = 0$ then Γ is isomorphic to the direct product $I^2 \times T \times T^\vee$.*

Proof. Consider the map $f : I \times T \times I \times T^\vee \longrightarrow \Gamma$,

$$(a, u, a', u^\vee) \to \begin{bmatrix} 1+a & u \\ u^\vee & 1+a' \end{bmatrix}$$

Then $f(x)f(y) =$

$$\begin{bmatrix} 1+a & u \\ u^\vee & 1+a' \end{bmatrix} \begin{bmatrix} 1+b & v \\ v^\vee & 1+b' \end{bmatrix} = \begin{bmatrix} 1+a+b+\langle u, v^\vee\rangle & u+v+av+b'u-u^\vee \times v^\vee \\ u^\vee + v^\vee + bu^\vee + a'v^\vee + u \times v & \langle v, u^\vee\rangle + 1 + a' + b' \end{bmatrix}$$

$$= \begin{bmatrix} 1+a+b & av+b'u-u^\vee\times v^\vee \\ bu^\vee+a'v^\vee+u\times v & 1+a'+b' \end{bmatrix} = \begin{bmatrix} 1+a+b & u+v \\ u^\vee+v^\vee & 1+a'+b' \end{bmatrix} = f(x+y).$$

Thus f is a group homomorphism which is clearly surjective. It is injective since obviously $f(a,u,a',u^\vee)=0$ implies $u=u^\vee=0$ and $a=a'=0$. □

We remark that this observation again also holds for subloops of $\mathrm{Zor}(T,\alpha)^\times$, cf. [W, 4.6]:

Proposition 5. *Let L be a subloop of $\mathrm{Zor}(T,\alpha)^\times$. Choose a normalized section $i: L\pi\to L$ which maps an element $x\pi$ to an element of $L\cap(x\pi+I)$. Then the set $\Gamma(L)=\{x(x\pi i)^{-1}\,|\,x\in L\}=L\cap\Gamma$ is a subgroup of Γ and $L\cong\Gamma(L)\times L\pi$.*

Thus also subloops are decomposable.

To our knowledge there are no known examples yet of split octonion algebras $\mathrm{Zor}(T,\alpha)$ over a ring with an underlying module structure which is not free. It would be interesting to find suitable projective R-modules T of constant rank 3 with trivial determinant. Non-trivial examples do exist when studying the more general setting of locally free modules (and split octonion algebras) over locally ringed spaces, e. g. elliptic curves.

4. Generalizations of Paige loops

4.1. Suppose that T is a torsion-free module over R. A straightforward calculation yields:

Lemma 1.
$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} \in Z(\mathrm{Zor}(T,\alpha)^\times)$$
if and only if $u=0$, $u^\vee=0$ and $a=a'\in R^\times$.

Proof. If
$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix} \in Z(\mathrm{Zor}(T,\alpha)^\times)$$
then
$$\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & b' \end{bmatrix} = \begin{bmatrix} b & 0 \\ 0 & b' \end{bmatrix}\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix}$$
for all $b,b'\in R^\times$. This implies $(b-b')u^\vee=0$ and $(b'-b)u=0$ for all $b,b'\in R^\times$. Since T is torsion-free we obtain $u=0$ and $u^\vee=0$. Moreover,
$$\begin{bmatrix} a & 0 \\ 0 & a' \end{bmatrix}\begin{bmatrix} 1 & 0 \\ v^\vee & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ v^\vee & 1 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a' \end{bmatrix}$$
for all $v^\vee\in T^\vee$ implies that $a=a'\in R^\times$. Conversely, every such element clearly lies in the center. □

Consider the Moufang loop $M(T,\alpha)=\{x\in\mathrm{Zor}(T,\alpha)\,|\,\det(x)=1\}$ of elements of norm one. The two-sided inverse of an element $x\in M(T,\alpha)$ is given by $x^{-1}=\bar{x}$, i.e.
$$x^{-1}=\begin{bmatrix} a & u \\ u^\vee & a' \end{bmatrix}^{-1} = \begin{bmatrix} a' & -u \\ -u^\vee & a \end{bmatrix}.$$

The center Z of $M(T,\alpha)$ is $\{1\}$ if $2 \notin R^\times$ and $\{1,-1\}$ if $2 \in R^\times$. Denote the noncommutative and nonassociative Moufang loop $M(T,\alpha)/Z$ by $M^* = M^*(T,\alpha)$, with the multiplication given by the algebra multiplication of $\mathrm{Zor}(T,\alpha)$. If R is a field, $M^*(T,\alpha) = M^*(R)$ is called a *Paige loop* and is simple [Pa, 4.1].

We do not need to use a special notation for the two-element cosets of $M^*(T,\alpha)$ if $2 \in R^\times$. We simply write x for $xZ(M^*(T,\alpha))$ and tacitly identify x with $-x$.

Note that if $f \in \mathrm{Aut}(\mathrm{Zor}(T,\alpha))$ then $f|_{M(T,\alpha)} \in \mathrm{Aut}((T,\alpha))$. It is not clear, however, if for $f,g \in \mathrm{Aut}(\mathrm{Zor}(T,\alpha))$ with $f \neq g$ we obtain that $f|_{M(T,\alpha)} \neq g|_{M(T,\alpha)}$. In order for this to be true, we would have to be able to prove that $\mathrm{Zor}(T,\alpha)$ is additively and multiplicatively generated by elements of norm one.

4.2. Conjugations. A *(right) pseudo-automorphism* of a quasi-group Q is a bijection $f : Q \to Q$ such that $x^f(y^f c) = (xy)^f c$ for all $x,y \in Q$ and some fixed $c \in Q$. c is called a *companion* of f. The set of all companions of a pseudo-automorphism f of a Moufang loop is the coset $cN(Q)$ with c a companion of Q and $N(Q)$ the nucleus of Q. With the nucleus of a Moufang loop being a normal subloop, every pseudo-automorphism of a (classical) Paige loop thus has a unique companion.

For every $x \in M^* = M^*(T,\alpha)$, define the conjugation $T : Q \to Q$ via $yT(x) = x^{-1}yx$. By [B, VII.2, p.122 ff] (or, alternatively, by adjusting the proof of [V, 3.18] accordingly), we can now conclude: if x has order 3 then $T(x) \in \mathrm{Aut}(M^*)$. If $T(x) \in \mathrm{Aut}(M^*)$ then it is a pseudo-automorphism and $x^{-3} \in 1N(M^*)$, that is

$$x^{-3} = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$$

with $a \in R^\times$.

Remark 1. This raises the question if and when $M^*(T,\alpha)$ contains non-trivial elements of order 3. For instance, suppose there are $u \in T$, $u^\vee \in T^\vee$ such that $u^\vee(u) = -1$ and $2 \in R^\times$. Then $M^*(T,\alpha)$ contains non-trivial elements of order 2: We have

$$x = \begin{bmatrix} 0 & u \\ u^\vee & 0 \end{bmatrix} \in M(T,\alpha)$$

and $x^2 = \begin{bmatrix} \langle u,u^\vee\rangle & 0 \\ 0 & \langle u,u^\vee\rangle \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$.

5. Infinite Moufang loops obtained from a non-orthogonal Cayley-Dickson doubling

For $K = \mathbb{Q}$, $C = \mathrm{Cay}(K,-1,-1,-1)$ is up to isomorphism the only octonion division algebra. The Coxeter lattice, let us denote it by $\Lambda(-1,-1,-1)$, is up to isomorphism the only maximal $\mathbb{Z}$-order in C [C] and is an octonion algebra over $\mathbb{Z}$ which does not contain any proper composition subalgebras. Let $M(\Lambda(-1,-1,-1)) = \{x \in \Lambda(-1,-1,-1) \,|\, N_C(x) = 1\}$. Then $|M(\Lambda(-1,-1,-1))| = 240$ and it is well-known that the Moufang loop

$$M^*(\Lambda(-1,-1,-1)) = M(\Lambda(-1,-1,-1))/\{1,-1\}$$

is isomorphic to $M^*(2)$. We can find other octonion algebras which do not contain a proper composition subalgebra over suitable rings as follows:

Let R be an integral domain with quotient field $K = \mathrm{Quot}(R)$ of characteristic not 2. Assume that 2 is not an invertible element in R. Let $C = \mathrm{Cay}(K, a, b, c)$ be an octonion algebra over K such that $a, b, c \in R^\times$ are invertible elements in R, with standard generating set $1, i, j, k, e$ as a K-algebra, that is

$$i^2 = a, \quad j^2 = b, \quad k^2 = -ab, \quad e^2 = c, \quad ij = k, \quad ji = -ij,$$

$$ej = -je, \quad ek = -ke, \quad ei = -ie, \quad jk = -bi = -kj, \quad ik = aj = -ki.$$

Define $h = \frac{1}{2}(i + j + k + e)$. If $a, b, c \in R^\times$ satisfy

$$a + b - ab + c \equiv 0 \bmod 4,$$

the R-submodule $\Lambda(a, b, c)$ in C generated by $1, i, j, k, h, ih, jh, kh$ is an octonion algebra over R [Pu, 2.1, 2.4]. Let $M(\Lambda(a, b, c)) = \{x \in \Lambda(a, b, c) \mid N_C(x) = 1\}$ then $M^*(\Lambda(a, b, c)) = \{x \in \Lambda(a, b, c) \mid N_C(x) = 1\}/\{1, -1\}$. In certain cases, $\Lambda(a, b, c)$ is an octonion algebra over R without any proper composition subalgebras. We propose in the following that this might be a good set-up to look for examples of an infinite simple nonassociative Moufang loop:

Example 1. Consider the ring

$$S = \mathbb{Z}[x, 1/x, y, 1/y, z, 1/z, t]/(x + y - xy + z - 4t),$$

and the octonion algebra $B = \Lambda(x, y, z)$ over S.
If $A = \Lambda(a, b, c)$ is an octonion algebra over a ring R, then there is a $\mathbb{Z}$-algebra homomorphism $G : B \to A$ obtained by specializing $x \to a$, $y \to b$, $z \to c$, and if $a + b - ab + c = 4r$, then $t \to r$. The map G described this way canonically extends to all of B. In particular, if B has a composition subalgebra B_0, then $G(B_0)R$ is an R-subalgebra, thus a composition subalgebra of A, by seeing that G sends the discriminant of the trace on B_0 to the discriminant of the trace on $G(B_0)$.

Let $R = \mathbb{Z}$ and $A = \Lambda(-1, -1, -1)$ be Coxeter's algebra from now on. A does not have any proper composition subalgebras. Thus B also is an octonion algebra over S which does not contain any proper composition subalgebras, so in particular it is not split [Pu, 2.6]. Let us now construct Moufang loops in this set-up:

Let $u = r + qh \in \Lambda(x, y, z)$ where $r, q \in (x, y)_K$ with $r = a_0 1 + a_1 i + a_2 j + a_3 k$ and $q = a_4 1 + a_5 i + a_6 j + a_7 k$, $a_0, \ldots, a_7 \in S$. The canonical involution σ on $\Lambda(x, y, z)$ is given by

$$\sigma(u) = \sigma(r + qh) = \sigma(r) - qh + (a_5 x + a_6 y - a_7 xy)1$$

[Pu, 2.3] and it is straightforward to check that $G(\sigma(u)) = \sigma(G(u))$ for all $u \in \Lambda(x, y, z)$. Therefore $G(N(u)) = G(u\sigma(u)) = G(u)\sigma(G(u)) = N(G(u))$ and if $N(u) = 1$ also $N(G(u)) = 1$.

The map $G : M(\Lambda(x, y, z)) \to M(\Lambda(-1, -1, -1))$ obtained by restricting G to the elements in C of norm one is thus a well-defined loop homomorphism and canonically induces a homomorphism $G : M^*(\Lambda(x, y, z)) \to M^*(\Lambda(-1, -1, -1))$. Now we know that $M^*(\Lambda(-1, -1, -1))$ is isomorphic to the Paige loop $M^*(2)$ and as such is simple. On the other hand, $M^*(\Lambda(x,y,z))$ is a nonassociative Moufang loop of infinite order. Because of the close relation between composition algebras and Moufang loops we suspect that $M^*(\Lambda(x,y,z))$ is simple, but are not able to prove it: If N is a normal subloop of $M^*(\Lambda(x,y,z))$ then $G(N)$ is a normal subloop of $M^*(\Lambda(-1,-1,-1))$. Therefore $G(N) = M^*(\Lambda(-1,-1,-1))$ or $G(N)$ is trivial. If $G(N)$ is trivial, then so is N. Thus we have $G(N) = M^*(\Lambda(-1,-1,-1))$. In order to show that $M^*(\Lambda(x,y,z))$ is an infinite nonassociative simple Moufang loop this must imply that N must be all of $M(\Lambda(x,y,z))$, but we do not see if this is the case.

References

[B] Bruck, R., "A Survey of Binary Systems", Springer Verlag Berlin-Göttingen-Heidelberg (1958).

[C] Coxeter, H.S.M., *Integral Cayley Numbers*, Duke Math. J. 13 (1946), 561-578.

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

[P] Petersson, H., *Composition algebras over algebraic curves of genus 0*, Trans. Amer. Math. Soc. 337 (1993), 473-491.

[Pu] Pumplün, S., *A non-orthogonal Cayley-Dickson doubling.* Journal of Algebra and Its Applications 5 (2) (2006), 193-199.

[VRME] Vergara, G., Rosa, C., Martinez, B., Enrique, F., *Zorn's matrices and finite index subloops.* Comm. Alg. 33 (10) (2005), 3691 - 3698.

[V] Vojtěchovský, P., *Finite simple Moufang loops.* Dissertation, Iowa State University, Ames, Iowa, 2001.

[W] Wells, A., *Moufang loops arising from Zorn vector matrix algebras.* Comment. Math. Univ. Carolin. 51 (2) (2010), 371-388.

E-mail address: susanne.pumpluen@nottingham.ac.uk

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom