with powers of p_{m+3}, $\cdots$, and finally to $N_x(s)/\prod_{i=1}^{n-m-1} p_{m+i}^{n_i-1}$ with powers of p_n. The number we seek is $N_x(s)/\prod_{i=1}^{n-m} p_{m+i}^{n_i-1}$.

For the case of a k of the form (2) with $n=m$, an infinite set of primitive k-nondeficients is easy to find—for example, the set of all numbers $N_x=q_x\cdot\prod_{i=1}^{n} p_i^{\alpha_i}$ where the q_x are sufficiently large to insure primitiveness and the p_i, α_i stem from k.

Reference

1. Harold N. Shapiro, *Note on a theorem of Dickson*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 450–452.

University of Michigan

A CLASS OF SIMPLE MOUFANG LOOPS

LOWELL J. PAIGE

1. Introduction. A Moufang loop is a loop that satisfies the associative identities

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

The only known examples of simple Moufang loops are the simple groups. In the present paper we will prove the following theorem.

THEOREM. *Let R be a simple alternative, not-associative, ring possessing an idempotent not its unit element. Let L be the loop of all regular elements of R and let Z be the center of L. Then either L/Z is a simple, not-associative, Moufang loop or L/Z contains a simple, not-associative, Moufang subloop M which is a normal subloop of index 2.*

As we shall see in the course of our proof, the present theorem is a nonassociative analogue of the well known results on the special projective group $PSL(n, K)$ (see [4, p. 44]).

In §5, we shall prove that the Cayley-Dickson numbers of norm 1 over the real field R^* (modulo their center) are simple and indicate how this is the best possible result.

Our results will yield finite, not-associative, simple Moufang loops whose possible orders are $(2^{7n}-2^{3n})$ and $2^{-1}(p^{7n}-p^{3n})$ if p is an odd prime. Thus we obtain a simple, not-associative, Moufang loop of order 120.

Although we have tried to make this paper reasonably self contained, some of the results by Bruck (2) on Moufang loops will be used without reference.

Presented to the Society, September 2, 1955; received by the editors May 30, 1955.

2. **Simple alternative rings.** Let F be a field and consider the set R of all matrices

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

where $a, b \in F$ and α and β are 3-dimensional coordinate vectors (x_1, x_2, x_3) over F.

We may construct an alternative ring R (i.e., $x(xy)=(xx)y$, $(yx)x=y(xx)$) from these matrices by first defining equality and addition to be ordinary matrix equality and addition with vector equality and addition for the vector elements of the matrices.

For $\alpha=(a_1, a_2, a_3)$ and $\beta=(b_1, b_2, b_3)$ denote by $\alpha \circ \beta$ and $\alpha \times \beta$ the scalar and vector products $a_1b_1+a_2b_2+a_3b_3$ and $[a_2b_3-a_3b_2, a_3b_1-a_1b_3, a_1b_2-a_2b_1]$.

Following Max Zorn, we now define multiplication in R by

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \circ \delta & a\gamma + \alpha d - \beta \times \delta \\ \beta c + b\delta + \alpha \times \gamma & \beta \circ \gamma + bd \end{pmatrix}. \tag{2.1}$$

Although not explicitly in this form, Albert (1) has shown that every simple alternative ring containing an idempotent not its unit element is either associative or a ring R as defined above. It should be noted that these rings are the Cayley algebras that are not division algebras.

3. **Moufang loops in simple alternative rings.** The only rings R that we will consider in §§3 and 4 will be the simple alternative rings constructed in §2.

A regular element of a ring R is an element x for which elements y and z exist such that $xy=zx=1$.

LEMMA 3.1. *An element*

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$$

of the ring R is a regular element if and only if $ab-\alpha \circ \beta \neq 0$.

PROOF. We note

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = \begin{pmatrix} ab - \alpha \circ \beta & 0 \\ 0 & ab - \alpha \circ \beta \end{pmatrix}$$

and the proof is immediate.

LEMMA 3.2. *The mapping T, defined by*

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} T = ab - \alpha \circ \beta,$$

is a homomorphism of the multiplicative groupoid of R upon F.

PROOF. From the definition of multiplication (2.1), we compute

$$\begin{aligned} &(ac + \alpha \circ \delta)(\beta \circ \gamma + bd) - (\beta c + b\delta + \alpha \times \gamma) \circ (a\gamma + \alpha d - \beta \times \delta) \\ &= abcd + (\alpha \circ \delta)(\beta \circ \gamma) - ab\gamma \circ \delta - cd\alpha \circ \beta + (\alpha \times \gamma) \circ (\beta \times \delta); \end{aligned} \tag{3.1}$$

and recalling that $(\alpha \times \gamma) \circ (\beta \times \delta) = (\alpha \circ \beta)(\gamma \circ \delta) - (\alpha \circ \delta)(\beta \circ \gamma)$, the right member of (3.1) reduces to $(ab - \alpha \circ \beta)(cd - \gamma \circ \delta)$. This completes the proof.

R is an alternative ring and it follows from the work of Bruck and Kleinfeld [3, Lemma 2.2] that the elements of R satisfy the Moufang identities (M). Moreover, every two elements of a Moufang loop generate a subgroup and we can combine these observations with Lemmas 3.1 and 3.2 to obtain the following theorem.

THEOREM 3.3. *The set of all regular elements of the ring R is a Moufang loop L. The set of all regular elements of R such that $ab - \alpha \circ \beta = 1$ is a normal Moufang subloop M of L.*

An element c of a loop L is in the center Z_L of L if and only if $cx = xc$, $c(xy) = (cx)y$, $(xc)y = x(cy)$, $(xy)c = x(yc)$ for all $x, y \in L$.

LEMMA 3.4. *The element*

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$$

is in the center Z of the loop L of regular elements of the ring R if and only if $a = b \neq 0$, $\alpha = \beta = 0$.

PROOF. If

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$$

is in the center Z of L, the equality

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

with $st \neq 0$, $s \neq t$, implies that

$$\alpha(t - s) = \beta(s - t) = 0. \tag{3.3}$$

Except when F is a field of 2 elements, (3.3) implies that $\alpha=\beta=0$. The exception may be removed by a more detailed analysis.

The equality

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

implies that $(a-b)\beta=0$ or $a=b$. The proof of the sufficiency is a straight-forward verification.

COROLLARY. *The center Z_M of the subloop M (Theorem 3.3) is a group of order 2 if the characteristic of F is not 2; otherwise $Z_M=1$.*

The proof of the corollary, except for the fields of 2 or 3 elements, merely requires that we take $s=t^{-1}$ in the first argument and $a=b^{-1}$ in the second. We then observe that $x^2=1$ has two solutions except when F has characteristic 2. Again the exceptional fields of 2 or 3 elements yield to special analysis.

LEMMA 3.5. *The Moufang loop M is not a group.*

PROOF. We compute,

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

$$\begin{pmatrix} 1 & (0,0,1) \\ 0 & 1 \end{pmatrix}\left[\begin{pmatrix} 1 & (1,0,0) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & (0,1,0) \\ (0,-1,0) & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & (1,1,1) \\ (-1,0,1) & 1 \end{pmatrix}.$$

In the case that the field F is the Galois field $GF(p^n)$, we see that the order of R is p^{8n}. We may compute the order of the subloop M by observing that the first row of the element

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$$

may be chosen in $(p^{4n}-1)$ ways and then choosing b in p^n ways with the subsequent restriction of the choices of β to p^{2n}. Thus the order of M is $(p^{4n}-1)p^{3n}$ and the order of M/Z_M (by the corollary to Lemma 3.4) is $2^{-1}(p^{4n}-1)p^{3n}$ if p is an odd prime; in the case of $GF(2^n)$ the order of M/Z_M is $(2^{7n}-2^{3n})$. We see at the same time that the order of L is $(p^{4n}-1)p^{3n}(p^n-1)$ and the order of L/Z is

$(p^{4n}-1)p^{3n}$; thus M/Z_M is isomorphic to a subloop of index 2 in the loop L/Z for p an odd prime.

4. **Simple Moufang loops.** In this section M will be the Moufang loop of the ring R consisting of all elements

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$$

such that $ab-\alpha\circ\beta=1$. We wish to prove the following theorem.

THEOREM 4.1. *If Z_M is the center of the loop M, the loop M/Z_M is a simple, not-associative, Moufang loop.*

The theorem in the introduction follows from Theorem 4.1 and §2, since $L/Z\supseteq M/M\wedge Z$ (to within an isomorphism) and $M\wedge Z=Z_M$ from Lemma 3.4 and corollary. $L/Z\cong M/M\wedge Z$ if and only if $L=MZ$ and this will be true if the field F is closed under the "square root operation."

For the sake of simplicity we shall formulate the proof of Theorem 4.1 as a sequence of lemmas. Rather than operate modulo the center of M we shall consider all normal subloops N of M in these lemmas to contain Z_M properly.

We define permutations $R(x)$ and $L(x)$ for any loop L by the equations

$$aR(x) = ax, \qquad aL(x) = xa, \qquad \text{for all } a \in L$$

and associate with the loop L the group G generated by all the permutations $R(x)$ and $L(x)$. The *inner mapping group* I^* of a loop L is defined to be the set of all elements $U\in G$, such that $1U=1$. It is well known that I^* is generated by the permutations

$$T(x) = R(x)L(x)^{-1}; \qquad R(x, y) = R(x)R(y)R(xy)^{-1};$$
$$L(x, y) = L(x)L(y)L(yx)^{-1}.$$

Moreover, N is a normal subloop of a loop L if and only if $N\cdot I^*\subseteq N$.

Two elements $x, y\in L$ are said to be conjugate elements if there exists a $V\in I^*$ such that $xV=y$. It is clear that if an element x is contained in a normal subloop N, all conjugates of x are in N.

In any Moufang loop, $xx^{-1}=x^{-1}x=1$ and $R(x)^{-1}=R(x^{-1})$, $L(x)^{-1}=L(x^{-1})$. Since any two elements of a Moufang loop generate a subgroup, the associative law will apply in most of our computations. With this word of caution and the observation that

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}^{-1} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}$$

for elements of M we begin our proof of Theorem 4.1.

LEMMA 4.2. *The elements*

$$\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix},$$

for all nonzero α *and* β, *are conjugate elements in* M *and generate all elements of the form*

$$\begin{pmatrix} 1 & \alpha \\ \beta & 1 \end{pmatrix}.$$

PROOF. We have the following equations, arising from the consideration of conjugate elements of the form $zT(x)$:

$$\begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix}\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -\alpha \\ -\beta & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}; \tag{4.1}$$

$$\begin{pmatrix} 0 & \alpha_1 \\ \beta & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}\begin{pmatrix} 0 & -\alpha_1 \\ -\beta & 0 \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 \\ 0 & 1 \end{pmatrix}. \tag{4.2}$$

For any two linearly independent vectors α and α_1, there always exists a vector β such that $\beta \circ \alpha = -1$, $\beta \circ \alpha_1 = -1$. We conclude from (4.1) and (4.2) that

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & \alpha_1 \\ 0 & 1 \end{pmatrix}$$

are conjugate. If α and α_1 are linearly dependent we choose α_2 linearly independent of α and α_1 and prove that the elements involving α and α_1 are conjugate in two steps.

If we consider the equations similar to (4.1) and (4.2) that are obtained by interchanging the roles played by α and β we see that all elements

$$\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$$

are conjugate and using (4.2) are conjugate to elements of the form

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

Next, we have

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ \beta & 1 \end{pmatrix}$$

if $\alpha \circ \beta = 0$ and our proof is complete.

LEMMA 4.3. *The elements*

$$\begin{pmatrix} 1 & \alpha \\ \beta & 1 \end{pmatrix}$$

of M *generate* M/Z_M.

PROOF. For any (noncenter) element

$$\begin{pmatrix} A & \alpha^* \\ \beta^* & B \end{pmatrix}$$

of M we will show that it is always possible to find two elements such that

$$\begin{pmatrix} 1 & \alpha \\ \beta & 1 \end{pmatrix}\begin{pmatrix} 1 & \gamma \\ \delta & 1 \end{pmatrix} = \begin{pmatrix} 1+\alpha\circ\delta & \alpha+\gamma-\beta\times\delta \\ \beta+\delta+\alpha\times\gamma & \beta\circ\gamma+1 \end{pmatrix} = \begin{pmatrix} A & \alpha^* \\ \beta^* & B \end{pmatrix}. \tag{4.3}$$

If (4.3) is to be satisfied, we are led to the equations

$$1+\alpha\circ\delta = A; \tag{4.4}$$

$$1+\beta\circ\gamma = B; \tag{4.5}$$

$$\beta+\delta+\alpha\times\gamma = \beta^*; \tag{4.6}$$

$$\alpha+\gamma-\beta\times\delta = \alpha^*. \tag{4.7}$$

Solving (4.6) for δ and substituting in (4.7) we have $\alpha^*=\alpha+\gamma-\beta\times(\beta^*-\beta-\alpha\times\gamma)=\alpha+\gamma-\beta\times\beta^*+\beta\times(\alpha\times\gamma)=\alpha+\gamma-\beta\times\beta^*+\alpha(\beta\circ\gamma)-\gamma(\alpha\circ\beta)=\alpha+\gamma-\beta\times\beta^*+\alpha(B-1)=\gamma-\beta\times\beta^*+B\alpha$. Thus, $\gamma=\alpha^*+\beta\times\beta^*-B\alpha$ and similarly $\delta=\beta^*-\alpha\times\alpha^*-A\beta$.

Using (4.6), we see that $\alpha\circ\beta^*=\alpha\circ(\beta+\delta+\alpha\times\gamma)=\alpha\circ\delta$ and similarly $\beta\circ\alpha^*=\beta\circ\gamma$. Substituting these results in (4.4) and (4.5), we arrive at the three equations

$$\alpha\circ\beta^* = A-1, \qquad \beta\circ\alpha^* = B-1 \quad \text{and} \quad \alpha\circ\beta = 0.$$

These equations always have a solution. Clearly, either α^* or β^* is not zero for otherwise $A=B=\pm 1$ and we have nothing to prove. Assume $\alpha^*\neq 0$; we pick a β such that $\beta\cdot\alpha^*=B-1$ and linearly independent of β^*. The remaining equations are then solved for α. It is a simple verification that (4.4), (4.5), (4.6) and (4.7) are now satisfied and our proof is complete.

In view of Lemmas 4.2 and 4.3, we continue our proof of Theorem 4.1 by showing that every normal subloop N of M properly containing Z_M contains an element of the form

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix},$$

with α not zero.

LEMMA 4.4. *Let N be a normal subloop of M containing an element*

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

with $\alpha \circ \beta \neq 0, -1$. Then N contains a nonunit element of the form

$$\begin{pmatrix} 1 & \alpha_1 \\ \beta_1 & 1 \end{pmatrix}.$$

PROOF. Assume $a \neq \pm 1$. If we let

$$x = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & \alpha \\ \beta_1 & 0 \end{pmatrix}; \qquad xy = \begin{pmatrix} 0 & a^{-1}\alpha \\ a\beta_1 & 0 \end{pmatrix}$$

and a straight-forward calculation reveals

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} R(x, y) = \begin{pmatrix} a & \alpha \\ (\alpha \circ \beta)(a^{-2} - 1)\beta_1 - a^{-2}\beta & b \end{pmatrix}.$$

Hence, N contains an element

$$\begin{pmatrix} a & \alpha \\ \beta_2 & b \end{pmatrix},$$

with $\beta_2 \neq \beta$. The inverse of this element is in N and consequently the element

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} b & -\alpha \\ -\beta_2 & a \end{pmatrix} = \begin{pmatrix} 1 & \beta \times \beta_2 \\ b(\beta - \beta_2) & 1 \end{pmatrix}$$

is in N.

If $a = \pm 1$ and $b \neq \pm 1$, an interchange of the roles played by a and b, α and β, verifies the lemma.

If $a = b = 1$ we are through. If $a = b = -1$, merely square the element (except when F has characteristic 2, in which case we are already through).

If $a = -b = 1$, we note that when $\alpha \circ \beta_1 = 0$,

$$\begin{pmatrix} 1 & 0 \\ \beta_1 & 1 \end{pmatrix}\begin{pmatrix} 1 & \alpha \\ \beta & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -\beta_1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha - 2\beta_1 \times \beta \\ 2\beta_1 + \beta & -1 \end{pmatrix}.$$

The inverse of this element is in N and consequently

$$\begin{pmatrix} 1 & \alpha \\ \beta & -1 \end{pmatrix}\begin{pmatrix} -1 & -\alpha + 2\beta_1 \times \beta \\ -2\beta_1 - \beta & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2\beta_1 & 1 \end{pmatrix}$$

is in N. A similar argument holds for $a = -b = -1$, and neither argument is necessary for fields of characteristic 2.

LEMMA 4.5. *Let N be a normal subloop of M containing an element*

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

with $\alpha \circ \beta = -1$. Then N contains a nonunit element of the form

$$\begin{pmatrix} 1 & \alpha_1 \\ \beta_1 & 1 \end{pmatrix}.$$

PROOF. Since $ab=0$, we assume $a=0$ and choose $\beta_1 \neq \beta$ to compute

$$\begin{pmatrix} 0 & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} 0 & \alpha \\ \beta_1 & 0 \end{pmatrix}\begin{pmatrix} 0 & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} 0 & -\alpha \\ -\beta_1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & -2\beta \times \beta_1 \\ 2b\beta_1 & -1 \end{pmatrix}$$

as an element of N. The square of this element completes the proof of the lemma for fields of characteristic different from 2.

For fields of characteristic 2, let $\beta_1 \neq \beta$, and the element

$$\begin{pmatrix} b & \alpha \\ \beta & 0 \end{pmatrix}\begin{pmatrix} b & \alpha \\ \beta_1 & 0 \end{pmatrix}\begin{pmatrix} 0 & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} 0 & \alpha \\ \beta_1 & b \end{pmatrix} = \begin{pmatrix} 1 & b^2(\beta_1 \times \beta) \\ \beta_1 + \beta & 1 \end{pmatrix}$$

is in N.

LEMMA 4.6. *Let N be a normal subloop of M containing the noncenter element*

$$\begin{pmatrix} a & \alpha \\ \beta & a^{-1} \end{pmatrix}.$$

Then N contains a nonunit element of the form

$$\begin{pmatrix} 1 & \alpha_1 \\ \beta_1 & 1 \end{pmatrix}.$$

PROOF. For $\alpha \neq 0$ and $\beta_i \neq 0$ with $\beta_1 \neq \beta_2$, the elements

$$\begin{pmatrix} 0 & \alpha \\ \beta_i & 0 \end{pmatrix}\begin{pmatrix} a & \alpha \\ \beta & a^{-1} \end{pmatrix}\begin{pmatrix} 0 & -\alpha \\ -\beta_i & 0 \end{pmatrix} = \begin{pmatrix} a^{-1} & 0 \\ \beta_i - \beta & a \end{pmatrix}$$

($i=1, 2$) are in N. Thus the element

$$\begin{pmatrix} a^{-1} & 0 \\ \beta_1 - \beta & a \end{pmatrix}\begin{pmatrix} a & 0 \\ -(\beta_2 - \beta) & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & (\beta_1 - \beta) \times (\beta_2 - \beta) \\ a(\beta_1 - \beta_2) & 1 \end{pmatrix}$$

is in N.

If $\beta \neq 0$, a dual argument completes this case.

For $\alpha = \beta = 0$, the element

$$\begin{pmatrix} 1 & \alpha_1 \\ \beta_1 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & -\alpha_1 \\ -\beta\delta & \end{pmatrix} = \begin{pmatrix} a & (a - a^{-1})\alpha_1 \\ (a - a^{-1})\beta_1 & a^{-1} \end{pmatrix}$$

is in N and the proof proceeds as above.

LEMMA 4.7. *Every normal subloop N of M containing Z_M properly contains a nonunit element of the form*

$$\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

PROOF. From the three previous lemmas we know that N contains an element

$$\begin{pmatrix} 1 & \alpha \\ \beta & 1 \end{pmatrix}$$

with α or $\beta \neq 0$. We assume $\alpha \neq 0$ and choose $\beta_1 \circ \alpha = 1$, computing as elements of N;

$$\begin{pmatrix} 1 & 0 \\ \beta_1 & 1 \end{pmatrix}\begin{pmatrix} 1 & \alpha \\ \beta & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -\beta_1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \alpha + 2\beta \times \beta_1 \\ \beta - \beta_1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & \alpha + 2\beta \times \beta_1 \\ \beta - \beta_1 & 2 \end{pmatrix}\begin{pmatrix} 1 & \alpha \\ \beta & 1 \end{pmatrix} = \begin{pmatrix} 0 & \alpha + \beta \times \beta_1 \\ 3\beta - \beta_1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & \alpha + \beta \times \beta_1 \\ 3\beta - \beta_1 & 0 \end{pmatrix}\begin{pmatrix} 0 & \alpha + \beta \times \beta_1 \\ 3\beta - \beta_1 & 1 \end{pmatrix}$$

$$\cdot \begin{pmatrix} 0 & -\alpha - \beta \times \beta_1 \\ -3\beta + \beta_1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 2(\alpha + \beta \times \beta_1) \\ 0 & -1 \end{pmatrix}.$$

The square of this last element completes the proof in the case that the field F is not of characteristic 2. For fields of characteristic 2, we have

$$\begin{pmatrix} 1 & 0 \\ \beta - \beta_1 & 1 \end{pmatrix}\begin{pmatrix} 0 & \alpha \\ \beta - \beta_1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \beta - \beta_1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$$

contained in N.

The dual argument for $\beta \neq 0$ completes the proof of the lemma.

The only concluding remarks necessary in the proof of Theorem 4.1 are to observe that the elements used in the proof of Lemma 3.4 lie in different cosets modulo Z_M so that M/Z_M is not a group.

5. Simple Moufang loops of Cayley-Dickson division algebras. In the previous sections we have considered the simple alternative rings that are not division algebras of order 8 over their center (so-called Cayley-Dickson algebras). In the case of division algebras our results cannot be as complete since we shall show that there do exist examples in which the elements of "norm 1" modulo their center are not simple Moufang loops.

We consider the Cayley-Dickson division algebras A over the real field R^* and let a basis for A be given by $1, e_1, \cdots, e_7$. We recall that $1, e_i, e_j, e_k$, for $(i, j, k) = (1, 2, 4), (2, 3, 5), (3, 4, 6), (4, 5, 7), (5, 6, 1), (6, 7, 2), (7, 1, 3)$ form a basis for ordinary quaternion subalgebras; i.e., $e_i^2 = e_j^2 = e_k^2 = -1$ and $e_ie_j = -e_je_i = e_k$, $e_je_k = -e_ke_j = e_i$, $e_ke_i = -e_ie_k = e_j$. If $a = a_0 + a_1e_1 + \cdots + a_7e_7$, we define the conjugate of a by $\bar{a} = a_0 - a_1e_1 - \cdots - a_7e_7$ and the norm of a by $N(a) = a\bar{a} = \bar{a}a = a_0^2 + a_1^2 + \cdots + a_7^2$. Every element $a \in A$ satisfies an equation $x^2 - 2a_0x + N(a) = 0$ and consequently is contained in a quaternion subalgebra of A.

We now prove the following theorem.

THEOREM 5.1. *Let A be the Cayley-Dickson division algebra over the real field R^*. Let M be the loop of all elements of norm 1 with center Z_M. Then the loop M/Z_M is a simple Moufang loop.*

PROOF. The center Z_M consists of the elements ± 1 and again we will consider only those subloops of M properly containing Z_M. Thus, if N is any normal subloop of M under consideration, N contains an element x not in the center of A and x will lie in a quaternion subalgebra $Q(x)$.

It is well known [6, p. 215] that the quaternions of norm 1 mod Z are a simple group and consequently N must contain all the elements of $Q(x)$ of norm 1. We choose a basis for $Q(x)$, $1, x_1, x_2, x_3$, where each element is of norm 1 and hence in N. For any $y \in M$ and not in $Q(x)$ there is a basis element x_i that does not commute with y for otherwise we would have a commutative division algebra of order 4 over R^*. Thus x_i and y lie in another quaternion subalgebra and again applying our result on quaternions we see that $y \in N$. Our proof is now complete since N contains all elements of norm 1.

The following example will show that Theorem 5.1 is perhaps the only result of interest in the case of division algebras.

Analogous to an example of Dieudonné's for quaternions [5, p. 34], we define a Cayley-Dickson division algebra over the field K of all formal power series $\sum_{k=n}^{\infty} a_kt^k$ with real coefficients and n either positive, negative or zero. The coefficients of the basis elements of the algebra for elements of norm 1 are power series of the form $\sum_{k=0}^{\infty} a_kt^k$.

We take as a subgroup N of the loop M of all elements of norm 1 those elements of the form $1 + tx$, where the coefficients of the basis elements in the element x of A are again of the form $\sum_{k=0}^{\infty} a_kt^k$. Since the inner mapping group I^* leaves the element 1 fixed, it is quite clear that $(1 + tx)T(a) = 1 + txT(a)$, $(1 + tx)R(a, b) = 1 + txR(a, b)$, $(1 + tx)L(a, b) = 1 + txL(a, b)$; moreover, the elements $xT(a)$, $xR(a, b)$,

$xL(a, b)$ have no negative powers of t in their coefficients. Thus N is a normal subloop of M. Hence M/Z_M is not a simple Moufang loop.

Although Theorem 5.1 can be extended to fields other than the real field R^*, the example given above indicates that such an extension is probably without interest.

BIBLIOGRAPHY

1. A. A. Albert, *On simple alternative rings*, Canadian Journal of Mathematics vol. 4 (1952) pp. 129–135.

2. R. H. Bruck, *Pseudo-automorphisms and Moufang loops*, Proc. Amer. Math. Soc. vol. 3 (1952) pp. 66–72.

3. R. H. Bruck and Erwin Kleinfeld, *The structure of alternative division rings*, Proc. Amer. Math. Soc. vol. 2 (1951) pp. 878–890.

4. J. Dieudonné, *Les déterminants sur un corps non commutatif*, Bull. Soc. Math. France vol. 71 (1943) pp. 27–45.

5. ———, *Sur les groupes classiques*, Actualités Scientifique et Industrielles, no. 1040, 1948.

6. W. I. Smirnow, *Lehrgang der Höheren Mathematik*, Berlin, Deutscher Verlag der Wissenschaften, 1954.

UNIVERSITY OF CALIFORNIA, LOS ANGELES