PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 132, Number 2, Pages 313–316
S 0002-9939(03)07260-5
Article electronically published on August 28, 2003

MOUFANG LOOPS AND ALTERNATIVE ALGEBRAS

IVAN P. SHESTAKOV

(Communicated by Lance W. Small)

ABSTRACT. Let $\mathbf{O}$ be the algebra $\mathbf{O}$ of classical real octonions or the (split) algebra of octonions over the finite field $GF(p^2)$, $p > 2$. Then the quotient loop $\mathbf{O}^*/Z^*$ of the Moufang loop $\mathbf{O}^*$ of all invertible elements of the algebra $\mathbf{O}$ modulo its center Z^* is not embedded into a loop of invertible elements of any alternative algebra.

It is well known that for an alternative algebra A with the unit 1 the set $U(A)$ of all invertible elements of A forms a Moufang loop with respect to multiplication [3]. But, as far as the author knows, the following question remains open (see, for example, [1]).

Question 1. Is it true that any Moufang loop can be imbedded into a loop of type $U(A)$ for a suitable unital alternative algebra A?

A positive answer to this question was announced in [5]. Here we show that, in fact, the answer to this question is negative: the Moufang loop $U(\mathbf{O})/\mathbf{R}^*$ for the algebra $\mathbf{O}$ of classical octonions over the real field $\mathbf{R}$ and the similar loop for the algebra of octonions over the finite field $GF(p^2)$, $p > 2$, are not imbeddable into the loops of type $U(A)$.

Below $\mathbf{O}$ denotes an algebra of octonions (or Cayley–Dickson algebra) over a field F of characteristic $\neq 2$, $\mathbf{O}^* = U(\mathbf{O})$ is the Moufang loop of all the invertible elements of $\mathbf{O}$, $L = \mathbf{O}^*/F^*$.

For an element $a \in \mathbf{O}^*$ we will denote by $\overline{a}$ its image in the quotient loop $L = \mathbf{O}^*/F^*$.

Assume that L is imbedded into a loop $U(A)$ for a certain alternative ring A. We will identify the elements from L with their images in A. The operations of addition and difference in A we will denote by $\oplus$ and $\ominus$, in order not to confuse them with those of $\mathbf{O}$. By $t(x)$ and $n(x)$ we denote the trace and the norm of an element $x \in \mathbf{O}$ (see [6]). Recall that $\mathbf{O}$ is quadratic over $\mathbf{R}$, that is,

$$x^2 = t(x) \cdot x - n(x) \cdot 1$$

for every $x \in \mathbf{O}$.

Let us prove first the following.

Received by the editors January 2, 2002.
2000 *Mathematics Subject Classification.* Primary 17D05, 20N05.
Key words and phrases. Moufang loop, alternative algebra.
Partially supported by CNPq grant 300528/99-0.

Lemma 1. *Let $\mathbf{O}_0 = \{x \in \mathbf{O} \,|\, t(x) = 0\}$, and let $a, b, c \in \mathbf{O}_0$ be such that $ab = -ba = c$, $n(a) = n(b) = 1$. Let, furthermore, $v \in \mathbf{O}_0$ be such that v anticommutes with a, b, c. Then*

$$\overline{b+v} \ominus \overline{b-v} = \overline{a+v} \ominus \overline{a-v}. \tag{1}$$

Proof. Observe first that $n(b \pm v) = n(a \pm v) = 2$; hence $a \pm v, b \pm v \in U(\mathbf{O})$. Consider the associators

$$\begin{aligned}
(\overline{a+b}, \overline{a+v}, \overline{c}) &= (\overline{a+b} \cdot \overline{a+v})\,\overline{c} \ominus \overline{a+b} \cdot (\overline{a+v} \cdot \overline{c}) \\
&= \overline{(-1-c+av+bv)c} \ominus \overline{(a+b)(-b+vc)} \\
&= \overline{-c+1+(av)c+(bv)c} \ominus \overline{-c+1+a(vc)+b(vc)}, \\
(\overline{a+v}, \overline{a+b}, \overline{c}) &= \overline{(-1+c+va+vb)c} \ominus \overline{(a+v)(-b+a)} \\
&= \overline{-c-1+(va)c+(vb)c} \ominus \overline{-c-1+va-vb}.
\end{aligned}$$

We have

$$\begin{aligned}
&(bv)c = b(vc+cv) - (bc)v = -(bc)v = -av,\ (av)c = -(ac)v = bv, \\
&a(vc) = -v(ac) = vb,\ b(vc) = -v(bc) = -va, \\
&(va)c = -(av)c = (ac)v = -bv,\ (vb)c = -(bv)c = (bc)v = av.
\end{aligned}$$

Therefore, by the alternativity of A,

$$\begin{aligned}
0 &= (\overline{a+b}, \overline{a+v}, \overline{c}) \oplus (\overline{a+v}, \overline{a+b}, \overline{c}) \\
&= \overline{-c+1+bv-av} \ominus \overline{-c+1+vb-va} \oplus \overline{-c-1-bv+av} \ominus \overline{-c-1+va-vb}.
\end{aligned}$$

Let us multiply this equality by $\overline{1-c}$ from the left. We have

$$\begin{aligned}
(1-c)^2 &= -2c, \\
(1-c)(1+c) &= 2, \\
(1-c)(bv-av) &= (1-c)(va-vb) = 2va;
\end{aligned}$$

hence

$$\overline{-2c+2va} \ominus \overline{-2c-2va} \oplus \overline{-2-2va} \ominus \overline{-2+2va} = 0,$$

or

$$\overline{-c+va} \ominus \overline{c+va} \oplus \overline{1+va} \ominus \overline{-1+va} = 0.$$

Multiplying this equality by $\overline{a}$ from the right, we finally get

$$\overline{b+v} \ominus \overline{b-v} \oplus \overline{a-v} \ominus \overline{a+v} = 0,$$

which implies (1). $\square$

Theorem 1. *Let $\mathbf{O}$ be the real octonion division algebra or the octonion algebra over the finite field $GF(p^2)$, $p > 2$. Then the corresponding Moufang loop $L = \mathbf{O}^*/F^*$ is not imbedded into a loop of type $U(A)$ for any unital alternative algebra A.*

Proof. Observe first that in both cases the algebra $\mathbf{O}$ has a basis $1, e_1, \ldots, e_7$ with the multiplication defined by the conditions:

$$\begin{aligned}
&e_i e_{i+1} = e_{i+3} \text{ (indices mod 7)}, \\
&e_i e_j = -e_j e_i,\ e_i^2 = -1, \\
&\text{ if } e_i e_j = e_k,\ i, j, k \neq,\ \text{then } e_{\sigma(i)} e_{\sigma(j)} = (-1)^{sgn\,\sigma} e_{\sigma(k)}
\end{aligned}$$

for any permutation σ of i, j, k. If $\mathbf{O}$ is the real octonion division algebra, it is just the canonical basis of $\mathbf{O}$ (see, for example, [2]). In the case of the field $GF(p^2)$, the algebra $\mathbf{O}$ is split and is isomorphic to $\mathbf{O}(-1,-1,-1)$, in the notation of [2]. The equation $x^2+1=0$ is solvable in $GF(p^2)$ (since any quadratic equation with coefficients from $GF(p)$ is solvable in $GF(p^2)$). Now, it is easy to see (for example, see [2]), that a split octonion algebra over a field F that contains $\sqrt{-1}$ has a basis with the needed properties.

Observe also that the equation $x^2-2=0$ is solvable in $GF(p^2)$, and so we may consider an element $\sqrt{2}\in F$.

Applying the lemma consequently to the triples

$$\begin{aligned}
&a=e_1,\ b=e_3,\ v=e_2,\\
&a=e_2,\ b=e_4,\ v=e_3,\\
&a=e_3,\ b=(e_1+e_2+\sqrt{2}e_5)/2,\ v=e_4,\\
&a=e_4,\ b=(e_1+e_2-\sqrt{2}e_5)/2,\ v=(e_1+e_2+\sqrt{2}e_5)/2,
\end{aligned}$$

we get the equalities

$$\begin{aligned}
&\overline{e_1+e_2}\ominus\overline{e_1-e_2}=\overline{e_3+e_2}\ominus\overline{e_3-e_2}=\overline{e_4+e_3}\ominus\overline{e_4-e_3}\\
=\ &\overline{e_4+(e_1+e_2+\sqrt{2}e_5)/2}\ominus\overline{e_4-(e_1+e_2+\sqrt{2}e_5)/2}\\
=\ &\overline{(e_1+e_2+\sqrt{2}e_5)/2+(e_1+e_2-\sqrt{2}e_5)/2}\\
&\qquad\ominus\overline{(e_1+e_2+\sqrt{2}e_5)/2-(e_1+e_2-\sqrt{2}e_5)/2}\\
=\ &\overline{e_1+e_2}\ominus\overline{e_5}.
\end{aligned}$$

Therefore, $\overline{e_1-e_2}=\overline{e_5}$ or $e_1-e_2=\alpha e_5$ for some $0\neq\alpha\in F$, a contradiction. □

Since the algebra of octonions over $GF(p^2)$ is finite, we get

Corollary 1. *There exist finite Moufang loops that are not imbeddable into the loops of invertible elements of alternative algebras.*

Our example suggests that "the right version" of question 1 should be as follows.

Question 1′. Is it true that any Moufang loop can be imbedded into a homomorphic image of a loop of type $U(A)$ for a suitable unital alternative algebra A?

The equivalent versions of this question are: whether the variety generated by the loops of type $U(A)$ is a proper subvariety of the variety of all Moufang loops, or whether a free Moufang loop is embedded into a loop of type $U(A)$?

If the answer to this question is negative, then there should exist a nontrivial element in a free Moufang loop that is identically equal to 1 in all the Moufang loops of type $U(A)$; it would be an analogue of the so-called *s-identities* from the theory of Jordan algebras (see [6]).

Observe finally that question 1 is still open for commutative Moufang loops. It was pointed out to us by the referee that some partial positive results in this direction were obtained in [4].

I would like to thank the referee for valuable suggestions and comments. In particular, the case of finite loops was not considered in the original version of the manuscript and was included due to a suggestion of the referee.

References

[1] E. Goodaire, A brief history of loop rings. 15th Brasilian School of Algebra (Canela, 1998). Mat. Contemp. 16 (1999), 93–109. MR **2001i:**17044

[2] E. N. Kuzmin and I. P. Shestakov, *Nonassociative structures*, VINITI, Itogi nauki i tekhniki, seria "Fundamental Branches", vol. 57, 179–266, Moscow, 1990; English transl. in "Encyclopaedia of Math. Sciences, vol. 57, Algebra VI, 199–280", edited by A. I. Kostrikin and I. R. Shafarevich, Springer-Verlag, 1995. MR **91i:**17001

[3] R. Moufang, Zur Structur von Alternativekörpern, Math. Ann. 110 (1935), 416–430.

[4] G. B. Nagy, *Applications of Bol reflections*, Ph.D. Dissertation, Szeged (Hungary), 1999.

[5] N. Sandu, About the embedding of Moufang loops in alternative algebras, Loops '99 Conference, July 27, 1999–Aug. 1, 1999, Prague, Abstracts, 33-34.

[6] K. A. Zhevlakov, A. M. Slin′ko, I. P. Shestakov, and A. I. Shirshov, *Rings that are nearly associative*, Nauka, Moscow, 1978; English transl., Pure and Applied Mathematics, vol. 104, Academic Press, 1982. MR **80h:**17002, MR **83i:**17001

Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66281 - CEP 05315-970, São Paulo, Brazil and Sobolev Institute of Mathematics, Novosibirsk, 630090, Russia

E-mail address: `shestak@ime.usp.br`