

HALF-ISOMORPHISMS OF MOUFANG LOOPS

MICHAEL KINYON, IZABELLA STUHL, AND PETR VOJTĚCHOVSKÝ

ABSTRACT. We prove that if the squaring map in the factor loop of a Moufang loop Q over its nucleus is surjective, then every half-isomorphism of Q onto a Moufang loop is either an isomorphism or an anti-isomorphism. This generalizes all earlier results in this vein.

1. INTRODUCTION

A *loop* (Q, \cdot) is a set Q with a binary operation \cdot such that for each $a, b \in Q$, the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions $x, y \in Q$, and there exists a neutral element $1 \in Q$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$. We will often write xy instead of $x \cdot y$ and use \cdot to indicate priority of multiplications. For instance, $xy \cdot z$ stands for $(x \cdot y) \cdot z$.

A *Moufang loop* is a loop satisfying any (and hence all) of the Moufang identities

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

In this paper we will only need the first Moufang identity, namely

$$xy \cdot zx = x(yz \cdot x). \tag{1.1}$$

Basic references to loop theory in general and Moufang loops in particular are [2, 16].

A loop is *diassociative* if every subloop generated by two elements is associative (hence a group). By Moufang's theorem [15], if three elements of a Moufang loop associate in some order, then they generate a subgroup. In particular, every Moufang loop is diassociative. We will drop further unnecessary parentheses while working with diassociative loops, for instance in the expression xyx .

If Q, Q' are loops, a mapping $\varphi : Q \rightarrow Q'$ is a *half-homomorphism* if, for every $x, y \in Q$, either $\varphi(xy) = \varphi x \cdot \varphi y$ or $\varphi(xy) = \varphi y \cdot \varphi x$. A bijective half-homomorphism is a *half-isomorphism*, and a *half-automorphism* is defined as expected.

The starting point for the investigation of half-isomorphisms of loops is the following result of Scott.

Proposition 1.1 ([17], Theorem 1). *Let G, G' be groups. Every half-isomorphism of G onto G' is either an isomorphism or an anti-isomorphism.*

Scott actually stated and proved Proposition 1.1 in the more general situation where both G and G' are cancellative semigroups. Kuznecov [12] showed that the same conclusion holds if G' is an arbitrary semigroup and G is a semigroup containing a densely imbedded completely simple ideal. Proposition 1.1 eventually became an exercise in Bourbaki's *Algebra I* [1, §4, Exercise 26, p. 139] with the steps in the exercise essentially following Scott's proof.

Date: November 13, 2015.

2000 Mathematics Subject Classification. 20N05.

Key words and phrases. Moufang loop, half-isomorphism.

Scott gave an example of a loop of order 8 which shows that Proposition 1.1 does not directly generalize to loops. It is nevertheless natural to ask if the result generalizes to Moufang loops, since these are highly structured loops that are, in some sense, very close to groups. This question was first addressed by Gagola and Giuliani [5] who proved the following.

Proposition 1.2 ([5]). *Let Q, Q' be Moufang loops of odd order. Every half-isomorphism of Q onto Q' is either an isomorphism or an anti-isomorphism.*

We will call a half-isomorphism which is neither an isomorphism nor an anti-isomorphism a *proper* half-isomorphism. (In [5, 6], the word “nontrivial” is used instead.)

Gagola and Giuliani also showed that there exist Moufang loops of even order with proper half-automorphisms [6].

The next result in the same vein was by Grishkov *et al.* A loop is *automorphic* if all of its inner mappings are automorphisms [3, 11].

Proposition 1.3 ([7]). *Every half-automorphism of a finite automorphic Moufang loop is either an automorphism or an anti-automorphism.*

Grishkov *et al* conjectured that the finiteness assumption can be dropped, and that the corresponding result holds for all half-isomorphisms.

Our main result simultaneously generalizes Propositions 1.1, 1.2 and 1.3, and as a by-product answers the conjecture of [7] in the affirmative.

To state the main result, we first recall that the *nucleus* of a loop Q is defined by

$$N(Q) = \{a \in Q \mid ax \cdot y = a \cdot xy, xa \cdot y = x \cdot ay, xy \cdot a = x \cdot ya, \forall x, y \in Q\}.$$

The nucleus is a subloop of any loop, and if Q is a Moufang loop, then $N(Q)$ is a normal subloop [2, Theorem 2.1].

Theorem 1.4. *Let Q, Q' be Moufang loops, and let $N = N(Q)$ be the nucleus of Q . Suppose that in Q/N the squaring map $xN \mapsto x^2N$ is surjective. Then every half-isomorphism of Q onto Q' is either an isomorphism or an anti-isomorphism.*

To see why Theorem 1.4 generalizes Proposition 1.1, we note that if Q is a group, then $N(Q) = Q$, and hence the squaring map in $Q/N(Q) = 1$ is trivially surjective. Since the order of any element of a finite Moufang loop divides the order of the loop, a finite Moufang loop Q of odd order certainly has a surjective (in fact, bijective) squaring map, and hence so does $Q/N(Q)$. Thus Theorem 1.4 generalizes Proposition 1.2. Finally, if Q is an automorphic Moufang loop, then $Q/N(Q)$ has exponent 3 by [10, Corollary 2], and so Theorem 1.4 generalizes Proposition 1.3 as well.

We conclude this introduction with some motivational remarks. Scott’s original result might seem at first to be a curiosity, but there is interest in it centered around the result of Formanek and Sibley [4] that the group determinant determines a group. A shorter and more constructive proof of [4] was later given by Mansfield [13]. Hoehnke and Johnson generalized this to show that the 1-, 2-, and 3-characters of a group determine the group [8]. A more explicit use of the fact that group half-isomorphisms are either isomorphisms or anti-isomorphisms can be found in [8], which cites the aforementioned exercise in (the 1970 French edition of) [1].

Loops have determinants as well [9], and all the results on half-isomorphisms of Moufang loops are motivated by the following open question: *Let \mathcal{M} be a class of Moufang loops in which every half-isomorphism is an isomorphism or an anti-isomorphism. Does the loop determinant of a loop in \mathcal{M} determine the loop?*

2. PROPER HALF-ISOMORPHISMS

Our goal in this section is Theorem 2.6, which describes necessary conditions for the existence of a proper half-isomorphism between Moufang loops. We start by expanding upon a lemma of Scott.

Lemma 2.1. *Let $\varphi : Q \rightarrow Q'$ be a half-isomorphism of diassociative loops and let $x, y \in Q$.*

- (i) *If $xy = yx$, then $\varphi x \cdot \varphi y = \varphi y \cdot \varphi x$.*
- (ii) *If $\varphi(xy) = \varphi x \cdot \varphi y$, then $\varphi(yx) = \varphi y \cdot \varphi x$.*
- (iii) *$\varphi(1) = 1$ and $(\varphi x)^{-1} = \varphi(x^{-1})$.*
- (iv) *If $\emptyset \neq X \subseteq Q$, then $\varphi(\langle X \rangle) = \langle \varphi x \mid x \in X \rangle$.*

Proof. For (i) and (ii), the proofs of steps (1) and (2) in [17, Theorem 1] go through word for word in the setting of diassociative loops. For (iii), note that $\varphi 1 = \varphi(1 \cdot 1) = \varphi 1 \cdot \varphi 1$, so $\varphi 1 = 1$. Then $1 = \varphi 1 = \varphi(xx^{-1}) = \varphi x \cdot \varphi(x^{-1})$ by (i), so $\varphi(x^{-1}) = (\varphi x)^{-1}$.

Since left and right divisions can be expressed in terms of multiplication and inverses in diassociative loops, every element of $\langle X \rangle$ is a word w involving only multiplications and inverses of elements from X , parenthesized in some way. Since $(\varphi x)^{-1} = \varphi(x^{-1})$ by (iii), we can assume that $X = X^{-1}$ and that no inverses occur in w . Suppose that w has leaves $x_1, \dots, x_n \in X$, possibly with repetitions. Applying φ to w yields a term with leaves $\varphi(x_1), \dots, \varphi(x_n)$ in some order. Therefore $\varphi(\langle X \rangle) \subseteq \langle \varphi x \mid x \in X \rangle$.

For the converse, consider a word w in $\langle \varphi(x_1), \dots, \varphi(x_n) \rangle$. We prove by induction on the height of w that $w \in \varphi(\langle X \rangle)$. If $w = \varphi x$, there is nothing to prove. Suppose that $w = \varphi u \cdot \varphi v$ for some $u, v \in \langle X \rangle$. If $w = \varphi(vu)$, we are done. Otherwise $\varphi(vu) = \varphi v \cdot \varphi u$, and (ii) implies $w = \varphi(uv)$. \square

We can now generalize [5, Lemma 3].

Lemma 2.2. *Let $\varphi : Q \rightarrow Q'$ be a half-isomorphism of diassociative loops. For all $a, b \in Q$:*

- (i) *If $\varphi(ab) = \varphi a \cdot \varphi b$, then $\varphi \upharpoonright \langle a, b \rangle$ is an isomorphism of groups.*
- (ii) *If $\varphi(ab) = \varphi b \cdot \varphi a$, then $\varphi \upharpoonright \langle a, b \rangle$ is an anti-isomorphism of groups.*

Proof. By Lemma 2.1, $\varphi(\langle a, b \rangle) = \langle \varphi a, \varphi b \rangle$, so $\psi = \varphi \upharpoonright \langle a, b \rangle$ is a half-isomorphism of groups. By Proposition 1.1, ψ is either an isomorphism or an anti-isomorphism. Suppose that $\varphi(ab) = \varphi a \cdot \varphi b$. If ψ is an isomorphism, we are done. If ψ is an anti-isomorphism then $\varphi b \cdot \varphi a = \varphi(ab) = \varphi a \cdot \varphi b$, thus $\langle \varphi a, \varphi b \rangle$ is commutative, and ψ is also an isomorphism. Part (ii) follows similarly. \square

A *semi-homomorphism* $\varphi : Q \rightarrow Q'$ of diassociative loops is a mapping satisfying $\varphi(1) = 1$ and

$$\varphi(xyx) = \varphi x \cdot \varphi y \cdot \varphi x$$

for all $x, y \in Q$. From Lemma 2.2, we immediately obtain a generalization of [5, Corollary 4]:

Corollary 2.3. *Every half-isomorphism of diassociative loops is a semi-isomorphism.*

From now on, we will use diassociativity, the Moufang identity (1.1) and Corollary 2.3 without explicit reference.

Lemma 2.4. *Let $\varphi : Q \rightarrow Q'$ be a half-isomorphism of Moufang loops Q, Q' , and let*

$$\begin{aligned} A &= \{a \in Q \mid \varphi(ax) = \varphi a \cdot \varphi x \ \forall x \in Q\}, \\ B &= \{a \in Q \mid \varphi(ax) = \varphi x \cdot \varphi a \ \forall x \in Q\}. \end{aligned}$$

Then A and B are subloops of Q .

Proof. By Lemma 2.2, it is clear that both A and B are closed under taking inverses $a \mapsto a^{-1}$. Thus it remains to show that both A and B are closed under multiplication. Fix $a, b \in Q$. Then for all $x \in Q$,

$$\varphi(ab \cdot x) = \varphi(ab \cdot (xa^{-1} \cdot a)) = \varphi(a(b \cdot xa^{-1})a) = \varphi a \cdot \varphi(b \cdot xa^{-1}) \cdot \varphi a. \quad (2.1)$$

If $a, b \in A$, then (2.1) yields

$$\varphi(ab \cdot x) = \varphi a \cdot (\varphi b \cdot \varphi(xa^{-1})) \cdot \varphi a = (\varphi a \cdot \varphi b)(\varphi(xa^{-1}) \cdot \varphi a) = \varphi(ab) \cdot \varphi(xa^{-1} \cdot a) = \varphi(ab) \cdot \varphi x.$$

On the other hand, if $a, b \in B$, then (2.1) gives

$$\varphi(ab \cdot x) = \varphi a \cdot (\varphi(xa^{-1}) \cdot \varphi b) \cdot \varphi a = (\varphi a \cdot \varphi(xa^{-1})) \cdot (\varphi b \cdot \varphi a) = \varphi(xa^{-1} \cdot a) \cdot \varphi(ab) = \varphi x \cdot \varphi(ab).$$

□

Lemma 2.5. *No loop is the union of two proper subloops.*

Proof. This is a standard exercise in group theory and the same proof holds here. For a contradiction, suppose that A, B are proper subloops of a loop Q with $Q = A \cup B$. Fix $a \in A \setminus B$ and $b \in B \setminus A$. We have $ab \in A$ or $ab \in B$ since $Q = A \cup B$. However, $ab \in A$ implies $b \in A$ since A is closed under left division, and similarly $ab \in B$ implies $a \in B$. □

A version of the following result (without the third part of the conclusion) was proved in [5, Proposition 5]. Their proof used the general finiteness assumption of Proposition 1.2 in an essential way. Our statement and proof make no reference to cardinality.

Theorem 2.6. *Suppose that there is a proper half-isomorphism between Moufang loops Q, Q' . Then there is a proper half-isomorphism $\varphi : Q \rightarrow Q'$ and elements $a, b, c \in Q$ such that the following properties hold:*

- (i) $\varphi \upharpoonright \langle a, b \rangle$ is an isomorphism and $\langle a, b \rangle$ is nonabelian,
- (ii) $\varphi \upharpoonright \langle a, c \rangle$ is an anti-isomorphism and $\langle a, c \rangle$ is nonabelian,
- (iii) $\varphi \upharpoonright \langle b, c \rangle$ is an isomorphism and $\langle b, c \rangle$ is nonabelian.

Proof. Assume $\varphi : Q \rightarrow Q'$ is a proper half-isomorphism, and let A, B be defined as in Lemma 2.4. Since φ is proper, both A and B are proper subloops by Lemma 2.4. By Lemma 2.5, $Q \neq A \cup B$, so there is an element $a \in Q$ which is in neither subloop.

Since $a \notin B$, there exists $b \in Q$ such that $\varphi(ab) = \varphi a \cdot \varphi b \neq \varphi b \cdot \varphi a$. By Lemma 2.2, $\varphi \upharpoonright \langle a, b \rangle$ is an isomorphism and $\langle a, b \rangle$ is nonabelian, proving (i).

Since $a \notin A$, there exists $c \in Q$ such that $\varphi(ac) = \varphi c \cdot \varphi a \neq \varphi a \cdot \varphi c$. By Lemma 2.2, $\varphi \upharpoonright \langle a, c \rangle$ is an anti-isomorphism and $\langle a, c \rangle$ is nonabelian, proving (ii).

Let $J : x \mapsto x^{-1}$ denote the inversion permutation on Q . Now, $\varphi \upharpoonright \langle b, c \rangle$ is either an isomorphism or an anti-isomorphism by Lemma 2.2. If the latter case holds, then $\varphi \circ J$ is still a proper half-isomorphism, $(\varphi \circ J) \upharpoonright \langle b, c \rangle$ is an isomorphism, $(\varphi \circ J) \upharpoonright \langle a, b \rangle$ is an

anti-isomorphism and $(\varphi \circ J) \upharpoonright \langle a, c \rangle$ is an isomorphism. In particular, conditions (i) and (ii) hold for $\varphi \circ J$ with the roles of b and c reversed. Thus there is no loss of generality in assuming that $\varphi \upharpoonright \langle b, c \rangle$ is an isomorphism.

Next we compute

$$\varphi(cb \cdot ac) = \varphi(c \cdot ba \cdot c) = \varphi c \cdot \varphi(ba) \cdot \varphi c = \varphi c \cdot (\varphi b \cdot \varphi a) \cdot \varphi c = (\varphi c \cdot \varphi b)(\varphi a \cdot \varphi c) = \varphi(cb) \cdot \varphi(ca).$$

If also $\varphi(cb) \cdot \varphi(ca) = \varphi(cb \cdot ca)$, then $cb \cdot ac = cb \cdot ca$, and so $ac = ca$, a contradiction. Therefore $\varphi(cb \cdot ac) = \varphi(cb) \cdot \varphi(ca) = \varphi(ca \cdot cb)$, and this establishes $cb \cdot ac = ca \cdot cb$. If $\langle b, c \rangle$ were an abelian group, then we would have $c \cdot ba \cdot c = cb \cdot ac = ca \cdot cb = ca \cdot bc = c \cdot ab \cdot c$, which implies $ba = ab$, a contradiction. This establishes the remaining claim in (iii) and completes the proof of the theorem. \square

Given a proper half-isomorphism $\varphi : Q \rightarrow Q'$ of Moufang loops, we will refer to a triple (a, b, c) of elements $a, b, c \in Q$ satisfying the conditions of Theorem 2.6 as a *Scott triple*, since the idea of considering triples satisfying conditions (i) and (ii) of the theorem goes back to Scott's original paper [17].

Theorem 2.7. *Let $\varphi : Q \rightarrow Q'$ be a proper half-isomorphism of Moufang loops, and let (a, b, c) be a Scott triple. Then $\langle a^2, c \rangle$ and $\langle a, c^2 \rangle$ are abelian groups.*

Proof. Note that if (a, b, c) is a Scott triple then (c, b, a) is also a Scott triple. It therefore suffices to verify that $\langle a^2, c \rangle$ is an abelian group. For $k \geq 1$, we calculate

$$\varphi(b \cdot a^k c \cdot b) = \varphi b \cdot \varphi(a^k c) \cdot \varphi b = \varphi b \cdot (\varphi c \cdot \varphi(a^k)) \cdot \varphi b = (\varphi b \cdot \varphi c)(\varphi(a^k) \cdot \varphi b) = \varphi(bc) \cdot \varphi(a^k b),$$

and so

$$\varphi(b \cdot a^k c \cdot b) = \varphi(bc) \cdot \varphi(a^k b). \quad (2.2)$$

Suppose for a while that $\varphi(bc) \cdot \varphi(ab) = \varphi(bc \cdot ab) = \varphi(b \cdot ca \cdot b)$. Comparing this with (2.2) for $k = 1$ yields $ac = ca$, a contradiction. Thus $\varphi(bc) \cdot \varphi(ab) = \varphi(ab \cdot bc)$, and so $b \cdot ac \cdot b = ab \cdot bc$. Rearranging this gives $ac = b^{-1}(ab \cdot bc)b^{-1} = b^{-1}ab \cdot bcb^{-1}$, and thus

$$a^2 c = a(b^{-1}ab \cdot bcb^{-1}). \quad (2.3)$$

Now suppose for a while that $\varphi(bc) \cdot \varphi(a^2 b) = \varphi(a^2 b \cdot bc)$. Comparing this with (2.2) for $k = 2$ yields $b \cdot a^2 c \cdot b = a^2 b \cdot bc$, and so

$$a^2 c = b^{-1}(a^2 b \cdot bc)b^{-1} = b^{-1}a^2 b \cdot bcb^{-1} = (b^{-1}ab)^2 \cdot bcb^{-1} = b^{-1}ab \cdot (b^{-1}ab \cdot bcb^{-1}). \quad (2.4)$$

Comparing (2.3) and (2.4), we conclude that $b^{-1}ab = a$, that is, $ab = ba$, a contradiction. Therefore $\varphi(bc) \cdot \varphi(a^2 b) = \varphi(bc \cdot a^2 b)$ and

$$\varphi(b \cdot a^2 c \cdot b) = \varphi(bc) \cdot \varphi(a^2 b) = \varphi(bc \cdot a^2 b) = \varphi(b \cdot ca^2 \cdot b),$$

which implies $a^2 c = ca^2$. \square

3. PROOF OF THE MAIN THEOREM

In this section we prove Theorem 1.4. For a contradiction, suppose that Q, Q' are Moufang loops, $N = N(Q)$ is the nucleus of Q , the squaring map in Q/N is surjective, and let $\varphi : Q \rightarrow Q'$ be a proper half-isomorphism. By Theorem 2.6, Q contains a Scott triple (a, b, c) . By the assumption on Q/N , there is $d \in Q$ such that $d^2 N = (dN)^2 = aN$, and so there is also $n \in N$ such that $d^2 = an$.

Throughout the proof we will use the observation that $\langle n, x, y \rangle$ is a subgroup of Q for any $x, y \in Q$, thanks to Moufang's theorem.

Lemma 3.1. *In the above situation, (d, b, c) is a Scott triple, and $\langle n, d \rangle$ and $\langle n, c \rangle$ are abelian groups.*

Proof. Since $\langle n, d, b \rangle$ is a group, $\langle a, b \rangle$ is nonabelian, $\langle a, b \rangle \leq \langle n, d, b \rangle$ and $\varphi \upharpoonright \langle a, b \rangle$ is an isomorphism, we have that $\varphi \upharpoonright \langle n, d, b \rangle$ is an isomorphism, and therefore $\varphi \upharpoonright \langle d, b \rangle$ is an isomorphism.

Since $\langle n, d, c \rangle$ is a group, $\langle a, c \rangle$ is nonabelian, $\langle a, c \rangle \leq \langle n, d, c \rangle$ and $\varphi \upharpoonright \langle a, c \rangle$ is an anti-isomorphism, we have that $\varphi \upharpoonright \langle n, d, c \rangle$ is an anti-isomorphism, and therefore $\varphi \upharpoonright \langle d, c \rangle$ is an anti-isomorphism.

Since $\langle n, b, c \rangle$ is a group, $\langle b, c \rangle$ is nonabelian, $\langle b, c \rangle \leq \langle n, b, c \rangle$ and $\varphi \upharpoonright \langle b, c \rangle$ is an isomorphism, we have that $\varphi \upharpoonright \langle n, b, c \rangle$ is an isomorphism.

Now $\varphi \upharpoonright \langle n, d \rangle$ is both an isomorphism and an anti-isomorphism, and so $\langle n, d \rangle$ is an abelian group. Also, $\varphi \upharpoonright \langle n, c \rangle$ is both an isomorphism and an anti-isomorphism, and so $\langle n, c \rangle$ is an abelian group.

If $\langle c, d \rangle$ were abelian, then from the above it would follow that $\langle n, c, d \rangle$ is abelian, contradicting the fact that $\langle a, c \rangle$ is nonabelian. Thus $\langle c, d \rangle$ is nonabelian.

Suppose $\langle d, b \rangle$ is abelian. We calculate

$$\varphi(db \cdot cd) = \varphi(d \cdot bc \cdot d) = \varphi d \cdot \varphi(bc) \cdot \varphi d = \varphi d \cdot (\varphi b \cdot \varphi c) \cdot \varphi d = (\varphi d \cdot \varphi b)(\varphi c \cdot \varphi d) = \varphi(db) \cdot \varphi(dc).$$

If $\varphi(db) \cdot \varphi(dc) = \varphi(db \cdot dc)$, then $\varphi(db \cdot cd) = \varphi(db \cdot dc)$, and so $db \cdot cd = db \cdot dc$. This gives $cd = dc$, a contradiction. On the other hand, if $\varphi(db \cdot cd) = \varphi(dc \cdot db)$, then $d \cdot bc \cdot d = dc \cdot db = dc \cdot bd = d \cdot cb \cdot b$, so that $bc = cb$, another contradiction. Therefore $\langle d, b \rangle$ is nonabelian. \square

Let us now finish the proof of Theorem 1.4. By Lemma 3.1, $\langle n, c \rangle$ is abelian, $\langle n, d \rangle$ is abelian, and (d, b, c) is a Scott triple. By Theorem 2.7, $\langle d^2, c \rangle = \langle an, c \rangle$ is abelian. Finally, $na = nd^2n^{-1} = d^2 = an$ because $\langle n, d \rangle$ is abelian, so $\langle n, a \rangle = \langle n, an \rangle$ is abelian. Altogether, $\langle n, an, c \rangle$ is an abelian group. But then $\langle a, c \rangle \leq \langle n, an, c \rangle$ is abelian, a contradiction with (a, b, c) being a Scott triple.

4. REMARKS AND OPEN PROBLEMS

In this section we examine hypotheses and generalizations of Theorem 1.4.

The somewhat technical assumption of Theorem 1.4 that squaring in $Q/N(Q)$ is surjective can be replaced by the assumption that squaring in $Q/N(Q)$ is bijective. We do not know if these two assumptions are equivalent in Moufang loops.

Problem 4.1. *Is there a Moufang loop Q with nucleus $N(Q)$ such that the squaring map in $Q/N(Q)$ is surjective but not injective?*

Scott extended Proposition 1.1 to half-homomorphisms of groups by showing that the kernel of a half-homomorphism is a normal subloop and that the given half-homomorphism factors through the quotient via the natural homomorphism [17, Theorem 2].

It is easy to show that the kernel of a half-homomorphism of loops is a subloop:

Lemma 4.2. *Let $\varphi : Q \rightarrow Q'$ be a half-homomorphism of loops. Then $\text{Ker}(\varphi) = \{a \in Q \mid \varphi a = 1\}$ is a subloop of Q .*

Proof. Let $K = \text{Ker}(\varphi)$ and $a, b \in K$. Then $\varphi(ab) \in \{\varphi a \cdot \varphi b, \varphi b \cdot \varphi a\} = \{1\}$, so $ab \in K$. Denote by a/b the unique element of Q such that $(a/b)b = a$. Then $1 = \varphi a = \varphi((a/b)b)$ is equal to $\varphi(a/b) \cdot \varphi b = \varphi(a/b)$ or to $\varphi b \cdot \varphi(a/b) = \varphi(a/b)$. In either case, $a/b \in K$ follows. Similarly for the left division. \square

However, we do not know the answer to the following problem and hence whether Scott's result on kernels can be generalized:

Problem 4.3. *Let $\varphi : Q \rightarrow Q'$ be a half-homomorphism of a Moufang loop Q into a loop Q' . Is the kernel of φ necessarily normal in Q ?*

The present paper and all proofs in this context rely rather heavily on the assumption that one is working with Moufang loops. The following problem therefore suggests itself.

Problem 4.4. *Investigate half-isomorphisms in other classes of loops, such as Bol loops or automorphic loops.*

For automorphic loops, Grishkov *et al* gave an example with a proper half-automorphism [7, Example 2], so any reasonable theorem will have to restrict the hypotheses further, similarly to the case of Moufang loops. The authors are not aware of any work on half-isomorphisms of Bol loops that are not Moufang.

Finally, the following example shows that the target Q' of a half-isomorphism $Q \rightarrow Q'$ need not be a diassociative loop even if Q is a group.

Example 4.5. The identity mapping on the set $Q = \{0, \dots, 5\}$ is a half-isomorphism $(Q, \cdot) \rightarrow (Q, *)$ of the respective loops

\cdot	0	1	2	3	4	5		$*$	0	1	2	3	4	5
0	0	1	2	3	4	5		0	0	1	2	3	4	5
1	1	2	0	5	3	4		1	1	2	0	4	5	3
2	2	0	1	4	5	3		2	2	0	1	5	3	4
3	3	4	5	0	1	2		3	3	5	4	0	1	2
4	4	5	3	2	0	1		4	4	3	5	2	0	1
5	5	3	4	1	2	0		5	5	4	3	1	2	0

Here, (Q, \cdot) is the symmetric group S_3 , and $(Q, *)$ is an automorphic loop that is not diassociative, as witnessed by $3 * (3 * 1) = 3 * 5 = 2 \neq 1 = 0 * 1 = (3 * 3) * 1$.

Acknowledgment. Our investigations were aided by the automated deduction tool PROVER9 developed by McCune [14].

REFERENCES

- [1] N. Bourbaki, *Algebra. I. Chapters 13.*, Translation from the French. *Elements of Mathematics*, Springer-Verlag, Berlin, 1989.
- [2] R. H. Bruck, *A Survey of Binary Systems*, Springer, 1971.
- [3] R. H. Bruck and L. J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math. (2)* **63** (1956) 308–323.
- [4] E. Formanek and D. Sibley, The group determinant determines the group, *Proc. Amer. Math. Soc.* **112** (1991), 649–656.
- [5] S. Gagola III and M. L. Merlini Giuliani, Half-isomorphisms of Moufang loops of odd order, *J. Algebra Appl.* **11** (2012), 194–199.

- [6] S. Gagola III and M. L. Merlini Giuliani, On half-automorphisms of certain Moufang loops with even order, *J. Algebra* **386** (2013), 131–141.
- [7] A. Grishkov, M. L. Merlini Giuliani, M. Rasskazova and L. Sabinina, Half-automorphisms of finite automorphic Moufang loops, [arXiv:1412.5113](https://arxiv.org/abs/1412.5113).
- [8] H.-J. Hoehnke and K. W. Johnson, The 1-, 2-, and 3-characters determine a group. *Bull. Amer. Math. Soc. (N.S.)* **27** (1992), 243–245.
- [9] K. W. Johnson, Some recent results on quasigroup determinants. Universal algebra, quasigroups and related systems (Jadwisin, 1989). *Demonstratio Math.* **24** (1991), 83–93.
- [10] M. K. Kinyon, K. Kunen and J. D. Phillips, Every diassociative A -loop is Moufang, *Proc. Amer. Math. Soc.* **130** (2002), 619–624.
- [11] M. K. Kinyon, K. Kunen, J. D. Phillips and P. Vojtěchovský, The structure of automorphic loops, to appear in *Trans. Amer. Math. Soc.*
- [12] V. I. Kuznecov, On h -isomorphisms of semigroups with a densely imbedded completely simple ideal. (Ukrainian) *Dopovidi Akad. Nauk Ukraï. RSR* **1962** (1962), 1429–1431.
- [13] R. Mansfield, A group determinant determines its group, *Proc. Amer. Math. Soc.* **116** (1992), 939–941.
- [14] W. W. McCune, *Prover9 and Mace4*, version 2009-11A. <http://www.cs.unm.edu/~mccune/prover9/>
- [15] R. Moufang, Zur Struktur von Alternativkoerpern, *Math. Ann.* **110** (1935), 416–430.
- [16] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **7**, Heldermann, 1990.
- [17] W. R. Scott, Half-homomorphisms of groups, *Proc. Amer. Math. Soc.* **8** (1957), 1141–1144.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF DENVER, DENVER, CO 80208 USA

E-mail address, Kinyon: mkinyon@du.edu

E-mail address, Stuhl: izabella.stuhl@du.edu

E-mail address, Vojtěchovský: petr@math.du.edu